Exhibit D14

Contract N62742-14-D-1884, Delivery Order 0028

# Quantitative Risk and Vulnerability Assessment Phase 1 (Internal Events without Fire and Flooding)

November 12, 2018

# Red Hill Bulk Fuel Storage Facility NAVSUP FLC Pearl Harbor, HI (PRL)

Joint Base Pearl Harbor-Hickam

Administrative Order on Consent
In the matter of Red Hill Bulk Fuel Storage Facility
EPA Docket No. RCRA 7003-R9-2015-01
DOH Docket No. 15-UST-EA-01

Contract Agency:

NAVFAC Pacific
258 Makalapa Drive, Suite 100
JBPHH Hawaii 96860-3134

Prime Contract:

element environmental llc
environmental · engineering · water resources

First-Tier Subcontract:

Engineering, Inc.
1132 Bishop Street, Suite 1200
Honolulu, Hawaii 96813-2822

Prepared By:

ABS Consulting

300 Commerce Drive, Suite 200, Irvine, California 92602

ABS Consulting Report No. R-3751812-2043

**Note: Large Portions of Future Versions of Section 8 Documents will have removed portions with the statement: "FOR OFFICIAL USE ONLY: PRIVILEGED, subject to claim under 5 USC 552(b)(3); 10 U.S.C. 130(e). Contains information subject to a claim of privilege under 10 U.S.C 130e, such information and the pages containing such claims remain the property of the United States Navy and cannot be released without the review and written permission of the United States Navy."**

**RED HILL AOC SECTION 8 QRVA PHASE 1 REDACTED REPORT – FOR PUBLIC RELEASE**

ABS Consulting

# APPROVAL COVER SHEET

| | |
|---|---|
| **Title:** | Quantitative Risk and Vulnerability Assessment Phase 1 |
| | (Internal Events without Fire and Flooding) |
| | |
| | |
| **Report Number:** | R-3751812-2043 |
| **Client:** | NAVFAC Pacific |
| **Project:** | Red Hill Bulk Fuel Storage Facility QRVA Phase 1 |

| Revision Number | Approval Date | Prepared | Reviewed | Approved |
|---|---|---|---|---|
| 0 | November 12, 2018 | D. J. Wakefield | J. K. Liming | J. C. Lin |

# Executive Summary

ABSG Consulting Inc. (ABS Consulting) is pleased to present this report to HDR Engineering, Inc. (HDR). This report is designed to comply with and be fully responsive to the Naval Facilities Engineering Command (NAVFAC) Hawaii "Section 8.2: Risk/Vulnerability Assessment Scope of Work" dated April 13, 2017 (Reference ES-1). The associated work has been performed under United States Navy Contract N62742-14-D-1884, Delivery Order 0028, Amendment 64 Statement of Work dated June 1, 2017 (Reference ES-2). The Quantitative Risk and Vulnerability Assessment (QRVA) is designed to assess the level of risk the Red Hill Bulk Fuel Storage Facility (RHBFSF) may pose to the surrounding groundwater to inform the Government in subsequent development of best available practicable technology decisions.

During the scoping discussions for Section 8 of the Administrative Order on Consent (AOC) Statement of Work (SOW) (Reference ES-2), all Parties agreed that a qualitative risk vulnerability assessment had limited value to support prudent decision-making. A Quantitative Risk and Vulnerability Assessment was selected for providing a more rigorous and repeatable approach to evaluating risk. A normal baseline QRVA for a large, complex facility often requires 5 to 7 years to complete and is normally broken into phases. This specific baseline QRVA is broken into four distinct phases, as follows: (1) internal events (excluding internal fire and flooding), (2) internal/external fire and flooding, (3) seismic events, and (4) other external events.

The first phase of the baseline QRVA, which is the topic of this report, is designed to focus on internal events (not including the risk from internal fires or internal floods). This includes, but is not limited to equipment or structural failures in both frontline and support systems, human errors, etc. The report from the first phase (this report) is to be submitted by November 16, 2018, in compliance with the RHBFSF AOC SOW Section 8.3. The remaining three phases will be performed sequentially and overlapped where technically feasible to better support scheduling for the AOC.

As other sections of the AOC are completed and new information becomes available, future revised assessments can be performed in comparison to the baseline risk assessment presented in this report.

In this baseline QRVA, the term "risk" is defined as the set of triplet information characterized as (scenario, likelihood, consequence) where the consequence of interest is volume of fuel released per unit time (gallons per calendar year in this assessment) due to acute or chronic fuel release scenarios from the RHBFSF. Acute release scenarios involve sudden, scenario-specific, one-time fuel releases outside the containment control of the RHBFSF systems and operations staff, which could potentially impact public water table safety. Chronic release scenarios are combined into the class of generally undetected, potentially continuous fuel releases from the RHBFSF, again outside the containment control of RHBFSF systems and operations staff, which could potentially impact public water table safety.

In the baseline QRVA model developed for this Phase 1 project, 3,691,380 event sequences (or scenarios) were quantified. Of these, the top 32,889 event sequences were found to comprise 99% of the total calculated risk for the RHBFSF. The total combined acute scenario risk results are summarized in Table ES-1.

The final column of Table ES-1 presents the consolidated facility risk profile in the format assessed in this Phase 1 QRVA; i.e., the potential gallons of fuel released per calendar year by volume range category and the total potential gallons of fuel released from the facility per calendar year as a whole. It is important to note that these total "roll-up" values represent the risk from all the scenarios that fit into the associated category. It is also important to note that no specific individual scenario had a predicted frequency greater than 0.00136 events per year (about once each 735 years). These results are developed under the mathematical assumption that the facility will effectively be operated in the current configuration with the same operating profile (fuel movement profile, processes, operating procedures and policies, maintenance, testing, and design) hypothetically for hundreds of years with no intervening risk-mitigating improvements. Please see Section 4 of this report for an overview of key bases and assumptions applied in this assessment. The results of this Phase 1 QRVA are presented in greater detail in Section 12 of this report. The event sequence (scenario) specific results are presented in the RISKMAN model for this QRVA and are summarized in the spreadsheet file named RHBFSF QRVA Phase 1 Results (Revision 0).xlsx, which accompanies this report.

## Table ES-1. Acute Scenario Risk Results Summary

| Fuel Release Volume Range Category (gallons) | Sequence Group Frequency (events/year) | Exceedance Frequency (events/year) | Sequence Group Recurrence Interval (years) | Sequence Group Probability (1 year) | Sequence Group Probability (100 years) | Potential Volume Released – Point Estimate (gal./year) |
|---|---|---|---|---|---|---|
| 1000 to 30000 | 0.3230500 | 0.3424131 | 3.10 | 0.2760623 | 1.0000000 | 1,960 |
| 30000 to 60000 | 0.0129880 | 0.0193631 | 77.00 | 0.0129040 | 0.7271410 | 515 |
| 60000 to 120000 | 0.0022056 | 0.0063751 | 453.40 | 0.0022032 | 0.1979305 | 191 |
| 120000 to 250000 | 0.0011526 | 0.0041695 | 867.58 | 0.0011519 | 0.1088656 | 219 |
| 250000 to 500000 | 0.0024041 | 0.0030169 | 415.96 | 0.0024012 | 0.2136946 | 1,097 |
| 500000 to 1000000 | 0.0000622 | 0.0006128 | 16067.35 | 0.0000622 | 0.0062045 | 42 |
| 1000000 to 2000000 | 0.0003678 | 0.0005505 | 2718.94 | 0.0003677 | 0.0361109 | 604 |
| 2000000 to 10000000 | 0.0000335 | 0.0001828 | 29821.72 | 0.0000335 | 0.0033477 | 253 |
| > 10000000 | 0.0001492 | 0.0001492 | 6701.52 | 0.0001492 | 0.0148112 | 1,703 |
| **Total** | **0.342** | **0.342** | **2.920** | **0.290** | **1.000** | **6,584** |

The uncertainty analysis for this QRVA is presented in Section 11 of this report. The characteristic values of the estimated probability distribution for the RHBFSF total acute (sudden, scenario-specific, rare or one-time) fuel release risk is summarized as follows:

| 5th Percentile Value (gallons per year) | Median or 50th Percentile Value (gallons per year) | Mean Value (gallons per year) | 95th Percentile Value (gallons per year) |
|---|---|---|---|
| 1,831 | 4,685 | 6,584 | 17,139 |

It is important to note that one should not interpret acute risk results in the context of continuous or even near-continuous release (i.e., one should not think of this risk as equating to a hose dumping fuel to the hillsides at the RHBFSF at or near the mean value rate, 6,584 gallons/year), because this is a broad average composite risk result comprised of contributions from millions of potential unique event sequences, each having a relatively low frequency of occurrence and low annual probability, but each also having a relatively significant consequence ( fuel release volume per event sequence).

The combined chronic (undetected, near-continuous) scenario risk results, for all 18 RHBFSF tanks in operation, are summarized via the following probability distribution characteristic values:

| 5th Percentile Value (gallons per year) | Median or 50th Percentile Value (gallons per year) | Mean Value (gallons per year) | 95th Percentile Value (gallons per year) |
|---|---|---|---|
| 234 | 475 | 5,803 | 52,596 |

Based on Reference ES-4, the current risk thresholds of concern for the safety of the water table potentially affected by RHBFSF fuel release to the environment are:

- Acute (sudden, scenario-specific, one-time) fuel release incidents of 120,000 gallons or greater for the facility as a whole.

- Chronic (generally undetected, potentially continuous) releases of 2,300 gallons or greater per tank per year. For 18 active tanks at the facility (the configuration of the facility at the time of this assessment) this equates to 41,400 gallons or greater per year for the entire facility.

Given these risk thresholds of interest, the Phase 1 QRVA shows that the best point estimate cumulative frequency of event sequences leading to 120,000 gallons or greater of fuel release to the environment (outside the control and physical boundaries of the RHBFSF) that could potentially impact water table safety is 0.00417 events per year (or about one event every 240 years). This yields an annual probability of occurrence of 0.00416 and a probability of occurrence over 100 years of 0.342 (or about a 34% chance of occurrence sometime during the next 100 years). Another way to think of this risk is that there is about a 66% likelihood that such an event will not occur over the next 100 years of facility operation.

For chronic releases, the Phase 1 QRVA shows that the expected fuel release is 5,803 gallons per year for the entire facility (please see Section 5.3.6 of this report for details), well below the threshold of concern. These results are based on the as-built, as-operated, and as-maintained RHBFSF at the design freeze date for this risk assessment, July 27, 2017. The full spectrum of results for this Phase 1 QRVA is presented in detail in Section 12 of this report. The uncertainty analysis performed for this QRVA is presented in Section 11 of this report.

The important quantitative results of this Phase 1 QRVA are summarized, then, as follows:

- **For acute risk, 0.00417 events per year**, or about **one event every 240 years**, for event sequences leading to 120,000 gallons or greater of fuel release potentially threatening water table safety.

- **For chronic risk, 5,803 gallons per year** average expected fuel release for the entire facility, well below the risk threshold of interest.

It is important to note that these results are for events and conditions leading only to fuel release from the facility but not necessarily directly into the water table. The propagation of potential fuel releases from the facility to the water table is not within the scope of this risk assessment but is a focus of the activity associated with AOC Sections 6 and 7.

Ranked lists of contributors to risk, based on calculated risk model element importance measures, such as fractional importance, Fussell-Vesely importance, Birnbaum importance, risk achievement worth (RAW), and risk reduction worth (RRW), are presented in Section 13 of this report. A general summary of contributions to acute risk by initiating event category based on fractional importance is presented in Figure ES-1.

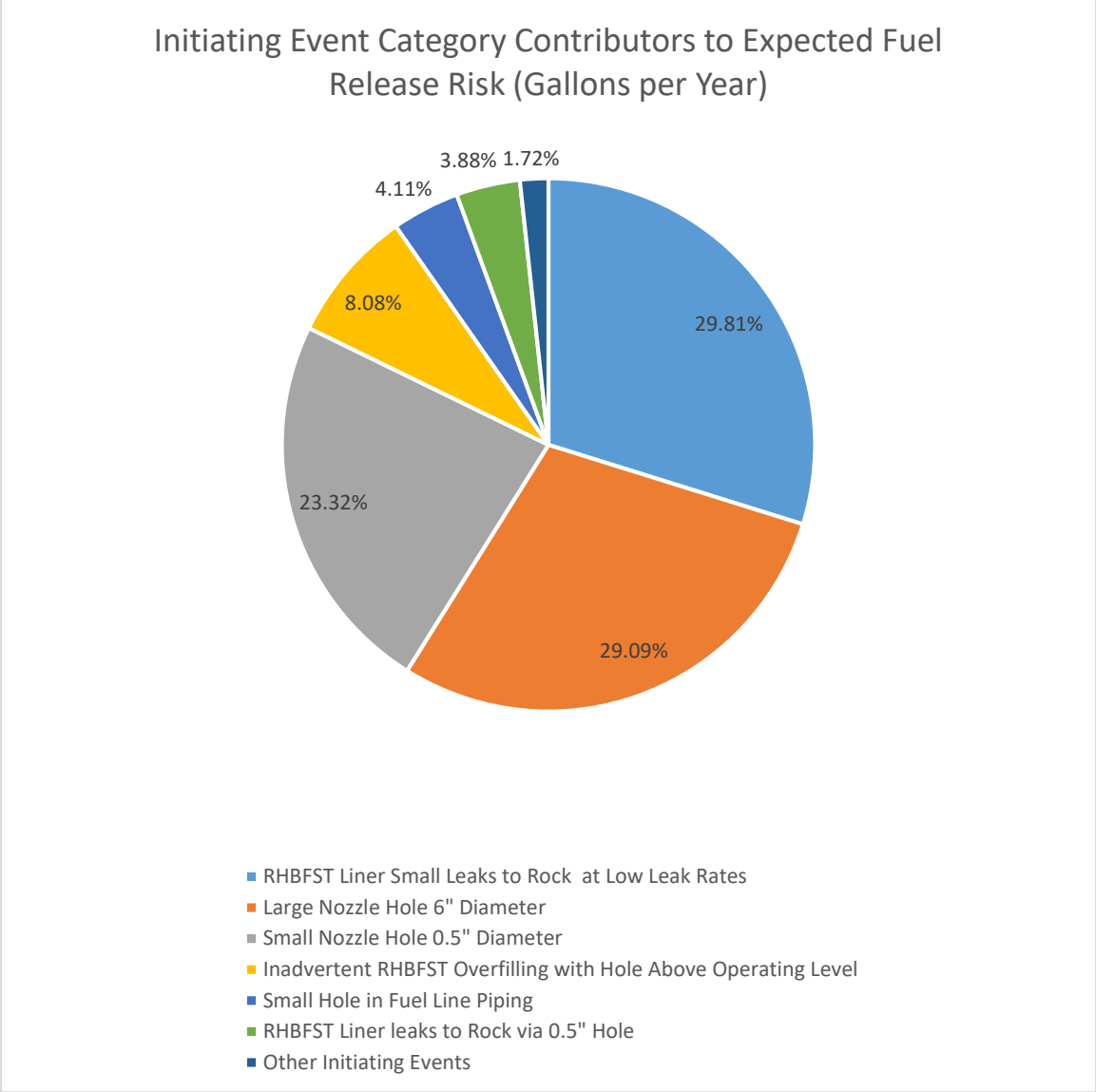



**Figure ES-1. Initiating Event Category Contributions to Acute Risk**

While the quantitative results of the QRVA are important to help facilitate prudent decision-making for the facility, the risk insights gained as a result of performing the QRVA may be even more valuable to RHBFSF decision-makers. While the charter of this risk assessment does not include development of detailed recommendations for specific risk management actions or alternatives for the RHBFSF, some of the general high-level risk insights resulting from the Phase 1 QRVA are summarized as follows:

1. The availability of tank ullage to accommodate emergency movement of fuel from a leaking tank to a safe storage tank or other safe container is important to risk.

2. The availability and quality of potential fuel release emergency response procedures and associated operator training are important to risk.

3. The capability and reliability of tank fuel inventory (fuel level) instrumentation and control systems are important to risk.

4. In response to potential fuel release scenarios, operator actions are generally more important than equipment failures to overall risk. Specific examples are identified in Sections 8 and 13 of this report.

5. Following tank inspections and maintenance, quality control during the tank return−to−service process is important to risk.

6. Strategies for responding to fuel releases inside the RHBFSF Lower Access Tunnel (e.g., strategies for removing and controlling fuel released into the Lower Access Tunnel) are important to risk.

7. Potential fuel releases from the tank nozzles (the main fuel flow piping leading into and out of the main storage tanks up to the upstream flange connections for the tank skin valves) are important to risk.

8. The capability and reliability of fuel piping isolation in response to fuel release incidents in the RHBFSF Lower Access Tunnel are important to risk.

9. Safety management and control of specific maintenance actions at the facility (e.g., tank nozzle and skin valve maintenance) is important to risk.

10. The design and proximity of the RHBFSF Lower Access Tunnel and the Red Hill Water Pump Area is important to risk. This is because potential fuel releases into the RHBFSF Lower Access Tunnel could potentially propagate to this area and flow (in a near-direct path) to the water table.

These insights are roughly ordered by predicted importance to potential risk mitigation based on a review of the vulnerability assessment reported in this Phase 1 QRVA (please see Section 13 of this report). Alternative-specific risk case studies are required to provide an accurate prioritization of these risk insights and to appropriately account for risk-benefit-to-cost considerations. Risk alternative-specific case studies are not within the scope of this Phase 1 baseline risk assessment project; however, this baseline risk assessment is the first fundamental building block of the tool enabling risk case studies to be performed to support prudent decision-making for the RHBFSF regarding risk and safety. While many of these insights may be apparent without a QRVA, the QRVA provides a critically valuable tool to help focus and prioritize these insights for effective and efficient decision support regarding facility risk management actions; e.g., improvements to facility design, operation, maintenance, inspection, and testing. More details on specific predicted vulnerabilities of the RHBFSF relative to potential fuel release incidents are presented in Section 13 of this report.

The general structure of this report, by section and topic, is:

Section 1 – Introduction
Section 2 – QRVA Methodology – General Overview
Section 3 – Facility Information Collection and Review
Section 4 – QRVA Bases and Assumptions – Overview
Section 5 – Data Analysis
Section 6 – Event Sequence Analysis
Section 7 – Systems Analysis
Section 8 – Human Reliability Analysis
Section 9 – Event Sequence Quantification
Section 10 – Fuel Release Accident Sequence Analysis
Section 11 – Risk Uncertainty Analysis
Section 12 – Facility Risk Quantitative Results (Phase 1)
Section 13 – Facility Risk Vulnerability Assessment
Section 14 – Phase 1 QRVA Conclusions
Section 15 – Considerations for Future Facility Risk Case Studies
Appendices

**Executive Summary References**

ES-1 Naval Facilities Engineering Command, Hawaii, "Section 8.2: Risk/Vulnerability Assessment Scope of Work," April 13, 2017.

ES-2 United States Navy Contract N62742-14-D-1884, Task Order 0028, Amendment 64 Statement of Work, June 1, 2017.

ES-3 Administrative Order on Consent for the Red Hill Bulk Fuel Storage Facility, U.S. Environmental Protection Agency, 2015 (https://www.epa.gov/red-hill/red-hill-administrative-order-consent).

ES-4 E-mail message from Steven L. Chow, NAVFAC Hawaii, to James K. Liming, ABSG Consulting Inc., dated July 27, 2018, 11:27 AM Pacific Time.

# Table of Contents


**Page**

**List of Acronyms ..... xxxi**
**1. Introduction ..... 1-1**
1.1 Background ..... 1-1
1.2 Project Scope ..... 1-2
1.2.1 Risk Assessment Levels ..... 1-2
1.2.2 Scope of Hazards ..... 1-2
1.2.3 Boundaries of Assessment ..... 1-4
1.3 Section 1 References ..... 1-4
**2. QRVA Methodology – General Overview ..... 2-1**
2.1 Definitions of Key Terms ..... 2-2
2.2 Description of QRVA Methodology ..... 2-3
2.3 Assumptions and Level of Uncertainty ..... 2-4
2.4 Evaluating and Prioritizing Events ..... 2-5
2.5 Section 2 References ..... 2-5
**3. Facility Information Collection and Review ..... 3-1**
**4. QRVA Bases and Assumptions – Overview ..... 4-1**
**5. Data Analysis ..... 5-1**
5.1 Introduction ..... 5-1
5.2 Bases and Assumptions ..... 5-1
5.3 QRVA Data Analysis General Methodology ..... 5-4
5.3.1 Generic Data Analysis ..... 5-8
5.3.1.1 Initiating Event Frequency Determination ..... 5-8
5.3.1.2 Component Failure Mode Failure Rate Determination ..... 5-9
5.3.1.3 Facility-Specific Data Collection, Review, and Interpretation ..... 5-20
5.3.1.4 Bayesian Updating of Generic Data with Facility-Specific Evidence ..... 5-24
5.3.2 Common Cause Failure Analysis ..... 5-35
5.3.2.1 Definition of Dependent Failures ..... 5-36
5.3.3 Data Uncertainty Analysis ..... 5-69
5.3.3.1 Sources of Uncertainty ..... 5-70
5.3.3.2 Procedures for Treating Modeling Uncertainties ..... 5-70
5.3.3.3 Procedures for Treating Parameter Uncertainties ..... 5-70
5.3.4 QRVA Database Development ..... 5-70
5.3.4.1 Documentation of the General Database ..... 5-71
5.3.4.2 Documentation of Data Applied to Each Model ..... 5-71

5.3.4.3 Assurance of Technical Quality ..... 5-74
5.4 Initiating Events Data ..... 5-74
5.4.1 Introduction ..... 5-74
5.4.2 Initiating Events Analysis Bayesian Update Process ..... 5-74
5.4.2.1 Synthesis of Generic Distributions ..... 5-75
5.4.2.2 Generic Distributions Using Estimates of Available Sources of Generic Data (Type 2) ..... 5-83
5.4.2.3 Incorporation of Site-Specific Evidence ..... 5-94
5.4.2.4 Advantage of Using a Bayesian Approach ..... 5-94
5.4.3 RHBFSF Tank Acute Initiating Events Analysis ..... 5-98
5.4.3.1 A Disposition of the Historically Observed Fuel Leakage Incidents, as Applicable to Operation of the Red Hill Facility in Future Years ..... 5-101
5.4.3.2 Information on the Number of RHBFST Outages and the Years Out of Service for Each RHBFST ..... 5-103
5.4.3.3 During RHBFST Operation, the Frequencies per RHBFST Year of Detected Leakage Incidents within the Range of Fuel Leakage Rates Historically Experienced (i.e., small leakage rate incidents) ..... 5-104
5.4.3.4 During RHBFST Operation, the Frequencies per RHBFST Year of Fuel Leakage Incidents with Fuel Leakage Flow Rates Larger than Those Historically Experienced (i.e., "large" leakage rate incidents) ..... 5-113
5.4.3.5 The Probability of a Leak Incident Occurring while Filling the RHBFST during a Return to Service Event Following an Extended Maintenance Period ..... 5-120
5.4.3.6 Probability of an Above Fuel Level Hole for Use with Overfill Events during Operation ..... 5-122
5.4.3.7 Probability of a Below Maximum Operating Level Hole for Use in Undetected Leakage Estimates ..... 5-125
5.4.3.8 Distribution of Hole Locations ..... 5-128
5.4.3.9 RHBFST Operating Years ..... 5-128
5.4.4 Tank Overfill Initiating Events ..... 5-131
5.4.5 Piping, Valve, and Connection Leakage Fuel Release Initiating Events ..... 5-132
5.4.5.1 Lower Dome Leak to Rock Initiators ..... 5-134
5.4.5.2 Nozzle Leak to Lower Access Tunnel (LAT) Initiators ..... 5-137
5.4.5.3 Pipeline Leak to Lower Access Tunnel Initiators ..... 5-146
5.4.6 Chronic Fuel Release Initiating Events – Undetected Through Holes in the RHBFST Liners ..... 5-150
5.4.6.1 Review of the Data ..... 5-151
5.4.6.2 Assembly of Undetected Through-Hole Growth and No-Growth Leakage Models ..... 5-157

5.4.6.3 Conclusions ..... 5-165
5.4.7 Maintenance Induced Leakage Fuel Release Initiating Events ..... 5-167
5.4.8 Fuel Movement Data ..... 5-171
5.4.9 Accounting for Potential of Corrosion Rates Increasing with Time ..... 5-175
5.4.10 Monitoring Well Data Review ..... 5-176
5.5 Response Events Data ..... 5-177
5.5.1 Response Equipment Failure Mode Failure Rate Data ..... 5-177
5.5.1.1 Elevator Reliability Data ..... 5-182
5.5.2 Equipment Common Cause Failure Data ..... 5-182
5.6 Section 5 References ..... 5-186
**6. Event Sequence Analysis ..... 6-1**
6.1 Introduction ..... 6-1
6.2 Bases and Assumptions ..... 6-1
6.3 QRVA Event Sequence Analysis General Methodology ..... 6-4
6.3.1 Event Sequence Diagram Development ..... 6-4
6.3.2 Event Tree Development ..... 6-7
6.3.3 Functional Event Tree Development ..... 6-9
6.3.3.1 System and Train Level Event Tree Development (including event tree top event definition, ordering, split fraction definition, end state definition, binning, etc.) ..... 6-10
6.3.3.2 Definition of System Success and Failure Criteria ..... 6-11
6.3.3.3 Dynamic Human Action Addition to Event Trees ..... 6-12
6.3.3.4 Event Sequence Recovery Action Addition to Event Trees ..... 6-12
6.3.3.5 Event Tree Split Fraction Logic Rule Development ..... 6-13
6.3.3.6 Event Tree Binning Rule Development ..... 6-16
6.4 Initiating Events ..... 6-17
6.5 System Dependencies ..... 6-31
6.6 Event Sequence Diagrams ..... 6-55
6.6.1 Event Sequence Diagrams for RHBFST Tank Leaks ..... 6-56
6.6.2 Event Sequence Diagrams for Leaks Resulting from Overfilling a RHBFST ..... 6-61
6.6.3 Event Sequence Diagrams for Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST ..... 6-65
6.6.4 Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel ..... 6-69
6.7 Event Tree Models ..... 6-75
6.7.1 Configuration Event Tree ..... 6-77
6.7.2 ELECTRICAL Event Tree ..... 6-82
6.7.3 OTHERSUP Event Tree ..... 6-84
6.7.4 VALVES Event Tree ..... 6-86
6.7.5 Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock ..... 6-88

6.7.6 Frontline Event Tree 2 – OVERFILL Event Tree ..... 6-92
6.7.7 Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT ..... 6-98
6.7.8 Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel ..... 6-103
6.8 Assessment of Acute Sequence End States – Gallons of Fuel Released ..... 6-109
6.8.1 Approaches for Evaluating Gallons Released ..... 6-109
6.8.1.1 Model of RHBFST Fuel Inventory Release ..... 6-110
6.8.1.2 Model for Fuel Line Leaks ..... 6-113
6.8.1.3 Gravity Flow of Released Fuel Downgrade in Tunnels (Manning flow) ..... 6-115
6.8.2 Gallons Released for Frontline Events Trees ..... 6-117
6.8.2.1 Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock ..... 6-117
6.8.2.2 Frontline Event Tree 2 – OVERFILL; Leaks to Rock above Maximum Operating Level ..... 6-126
6.8.2.3 Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT ..... 6-134
6.8.2.4 Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel ..... 6-143
6.9 Section 6 References ..... 6-161
**7. Systems Analysis ..... 7-1**
7.1 Introduction ..... 7-1
7.2 QRVA System Analysis General Methodology ..... 7-1
7.2.1 Systems Analysis ..... 7-1
7.2.1.1 Specification of Analysis Ground Rules and Model Resolution ..... 7-1
7.2.1.2 System Dependency Matrix Development ..... 7-4
7.2.1.3 Boolean Logic Model (e.g., fault tree) Top Event Definition ..... 7-4
7.2.1.4 System Failure Modes and Effects Analysis ..... 7-5
7.2.1.5 Boolean Logic Model (e.g., fault tree) Development ..... 7-5
7.3 QRVA Systems Analysis Assumptions ..... 7-12
7.4 QRVA Systems Analysis Details ..... 7-13
7.4.1 The Top Events for the Configuration Event Tree ..... 7-14
7.4.1.1 Top Event LKLOC — Location of Leak within Facility ..... 7-14
7.4.1.2 Top Event MOVE — Type of Fuel Movement Initially in Progress ..... 7-15
7.4.1.3 Top Event TKID — RHBFST Associated with Leak ..... 7-16
7.4.1.4 Top Event FUEL — Type of Leaking Fuel ..... 7-17
7.4.1.5 Top Event TKXF — Source RHBFST Associated with Inter-Tank Transfer ..... 7-18

7.4.1.6 Top Event TKLOC — LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT ..... 7-19
7.4.1.7 Top Event HEIGHT — Height of Hole in RHBFST that is Leaking to Rock ..... 7-19
7.4.1.8 Top Event SIZE – Size of Leak from RHBFST or Fuel Line Piping ..... 7-20
7.4.1.9 Top Event DIREC — Side of RHBFST that Leak Is On ..... 7-20
7.4.1.10 Top Event INVEN — Initial RHBFST Inventory Configuration ..... 7-21
7.4.2 The Top Events for the ELECTRICAL Event Tree ..... 7-22
7.4.2.1 Top Event GRID — Offsite Grid ..... 7-22
7.4.2.2 Top Event GRIDR – Recovery from Losses of Offsite Grid ..... 7-22
7.4.2.3 Top Event BUN24 — UGPH 2.4 kV Normal Bus ..... 7-23
7.4.2.4 Top Event BUN48 — UGPH 480V Normal Bus ..... 7-23
7.4.2.5 Top Event BUE48 — UGPH 480V Emergency Bus ..... 7-23
7.4.2.6 GEN1 – Backup Generator at ADIT 1 for UGPH 480V Emergency Bus ..... 7-24
7.4.2.7 Top Event UFAN — ADIT 1 Supply and Exhaust Fans for UGPH ..... 7-24
7.4.2.8 Top Event B3EA — ADIT 3 208V Panel A ..... 7-29
7.4.2.9 GEN3 – Backup Generator at ADIT 3 for 480V Panels B and A ..... 7-29
7.4.2.10 Top Event BRN48 — Red Hill 480V Normal Bus ..... 7-30
7.4.2.11 Top Event BRE48 — Red Hill 480V Emergency Bus ..... 7-30
7.4.2.12 GEN5 – Standby Generator at ADIT 5 for Red Hill 480V Emergency Bus ..... 7-31
7.4.2.13 Top Event LPRH – Red Hill Panels Supplying Lighting, Radios, and Cameras ..... 7-31
7.4.2.14 Top Event AFHE — Automatic Fuel Handling Equipment ..... 7-31
7.4.2.15 Top Event AFHR — AFHE Condensing and Fans for Heat Removal ..... 7-31
7.4.2.16 Top Event EFAN — Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply electrical room in LAT) ..... 7-32
7.4.2.17 Top Event TFAN — Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead) ..... 7-36
7.4.3 The Top Events for the OTHERSUP Event Tree ..... 7-39
7.4.3.1 Top Event CRM — Control Room Electrical Power, Lighting, and Air Conditioning ..... 7-39
7.4.3.2 Top Event ACRM — Alternate Control Room Electrical Power, Lighting, and Air Conditioning ..... 7-39

7.4.3.3 Top Event UHMOV – Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs ..... 7-40
7.4.3.4 Top Event CARGO – Two or More Cargo Pumps Available to Move Leaking Fuel Type ..... 7-40
7.4.3.5 Top Event ULIT – Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting ..... 7-44
7.4.3.6 Top Event EL72 – Personnel Elevator 72 and Controller ..... 7-45
7.4.3.7 Top Event EL73 – Cargo Elevator 73 ..... 7-45
7.4.3.8 Top Event RMOV – Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and All LAT MOVs ..... 7-45
7.4.3.9 Top Event RHIN – Support for Red Hill Instruments, Indications, Level Alarms, and Signals ..... 7-46
7.4.4 The Top Events for the VALVES Event Tree ..... 7-46
7.4.4.1 Top Event SKIN – Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree ..... 7-46
7.4.4.2 Top Event BALL – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree ..... 7-47
7.4.4.3 Top Event SKINX – Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree ..... 7-47
7.4.4.4 Top Even BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree ..... 7-47
7.4.4.5 Top Event FLISO – Successful Closure of the Upstream Sectional Valve ..... 7-47
7.4.4.6 Top Event FLTKC – Successful Isolation of the Fuel Line Leak from All ALIGNED RHBFSTs ..... 7-47
7.4.4.7 Top Event FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied ..... 7-48
7.4.4.8 Top Event EVAC – Sequence Conditions Necessitate Initial Evacuation from Red Hill ..... 7-48
7.4.5 The Top Events for the Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock ..... 7-48
7.4.5.1 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak ..... 7-49
7.4.5.2 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm ..... 7-49
7.4.5.3 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST ..... 7-49

7.4.5.4 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST ..... 7-49
7.4.5.5 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST ..... 7-49
7.4.5.6 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor ..... 7-49
7.4.5.7 Top Event XFR3 – Two-step Fuel Movement to Pump Fuel to Other RHBFSTs ..... 7-49
7.4.5.8 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor ..... 7-50
7.4.5.9 Top Event XFR5 – Fuel Movement to Empty Bottom 7.5' of Lower Dome Using RHBFST Lower Drain Line ..... 7-50
7.4.5.10 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures ..... 7-50
7.4.5.11 Top Event REL – Type of Fuel Release Scenario ..... 7-51
7.4.6 The Top Events for the Frontline Event Tree 2 – OVERFILL Event Tree ..... 7-52
7.4.6.1 Top Event OEV – Operators Correctly Specify Fill Evolution and Stop Evolution when Planned at Maximum Operating Level ..... 7-52
7.4.6.2 Top Event HOLE – Conditional Probability of Hole above Maximum Operating Level ..... 7-52
7.4.6.3 Top Event OTRIP – After AFHE High Level Alarm, Operators Actuate an Emergency Stop of the Cargo Pumps or Press the Panic Button, then Direct the Rover to Locally Ensure the Skin Valve Closed and to Manually Gauge the Same Tank ..... 7-53
7.4.6.4 Top Event SWITCH – High Level Mechanical FLOAT Switch Actuates Sending Signals to Deactivate All Facility Pumps, Actuate Timer for Valve Closures, and Signals Skin Valve on Affected Tank to Close ..... 7-53
7.4.6.5 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak ..... 7-53
7.4.6.6 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm ..... 7-53
7.4.6.7 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST ..... 7-53
7.4.6.8 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST ..... 7-53
7.4.6.9 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST ..... 7-54

7.4.6.10 Top Event XFR2 – Issue Fuel by gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor ..... 7-54
7.4.6.11 Top Event XFR3 – Two-step Fuel Movement to Pump Fuel to Other RHBFSTs ..... 7-54
7.4.6.12 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor ..... 7-54
7.4.6.13 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line ..... 7-54
7.4.6.14 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures ..... 7-54
7.4.6.15 Top Event REL – Type of Fuel Release Scenario ..... 7-54
7.4.7 The Top Events for the Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT ..... 7-55
7.4.7.1 Top Event MSUMP – 1 of 2 Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 ..... 7-55
7.4.7.2 Top Event DOOR – Oil-Tight Door below LAT Gallery Closes on High Float Level ..... 7-57
7.4.7.3 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak ..... 7-57
7.4.7.4 Top Event OSUM – CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak ..... 7-57
7.4.7.5 Top Event OPAN – CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button ..... 7-58
7.4.7.6 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFSTs that Have a Low Level Alarm ..... 7-58
7.4.7.7 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to empty RHBFST ..... 7-58
7.4.7.8 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST ..... 7-58
7.4.7.9 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST ..... 7-58
7.4.7.10 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor ..... 7-58
7.4.7.11 Top Event XFR3 – Two-Step Fuel Movement to Pump Fuel to other RHBFSTs ..... 7-58
7.4.7.12 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor ..... 7-58
7.4.7.13 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line ..... 7-58

7.4.7.14 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures ..... 7-59
7.4.7.15 Top Event REL - Type of Fuel Release Scenario ..... 7-59
7.4.8 The Top Events for the Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel ..... 7-59
7.4.8.1 Top Event USUMP – 1 of 2 Harbor Tunnel Sump Pumps at UGPH Entry Start and Transfer Leaked Fuel ..... 7-60
7.4.8.2 Top Event MSUMP – 1 of 2 Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 ..... 7-61
7.4.8.3 Top Event DOOR – Oil-Tight Door below LAT Gallery Closes on High Float Level Top Event ..... 7-62
7.4.8.4 Top Event PFL – Fuel Line Pressure Drops due to Leak and Is Detected ..... 7-62
7.4.8.5 Top Event OSUM – CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak ..... 7-62
7.4.8.6 Top Event OPAN – CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button ..... 7-62
7.4.8.7 Top Event OSEC – CR Operators REMOTE MANUALLY Close Sectional Valve(s) and Ball Valves as Applicable; Execution Only ..... 7-62
7.4.8.8 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak ..... 7-62
7.4.8.9 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm ..... 7-62
7.4.8.10 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST ..... 7-62
7.4.8.11 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST ..... 7-62
7.4.8.12 Top Event ISOL – FL Leak Isolated from All RHBFSTs; by Upgrade Sectional, RHBFST Idle or Isolated – No Need to Empty ..... 7-63
7.4.8.13 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST ..... 7-63
7.4.8.14 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor ..... 7-63
7.4.8.15 Top Event XFR3 – Two-Step Fuel Movement to Pump Fuel to other RHBFSTs ..... 7-63
7.4.8.16 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor ..... 7-63

7.4.8.17 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line ..... 7-63
7.4.8.18 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures ..... 7-63
7.4.8.19 Top Event REL – Type of Fuel Release Scenario ..... 7-64
7.5 Section 7 References ..... 7-64
**8. Human Reliability Analysis ..... 8-1**
8.1 Introduction ..... 8-1
8.2 QRVA Human Reliability Analysis General Methodology ..... 8-1
8.2.1 Human Failure Event Definition and Evaluation ..... 8-1
8.2.1.1 Operations, Maintenance, Testing, and Emergency Procedures Review ..... 8-2
8.2.1.2 Operator Interviews and Scenario Walk-Throughs ..... 8-3
8.2.2 Human Error Probability Evaluation and Analysis ..... 8-11
8.2.3 Human Action Dependency Analysis ..... 8-11
8.3 QRVA HRA Detailed Methodology ..... 8-18
8.3.1 General HRA Scope ..... 8-18
8.3.2 RHBFSF QRVA HRA Scope ..... 8-19
8.3.3 Methodology ..... 8-19
8.3.3.1 Analysis of Pre-Initiator (Type A) Human Failure Events ..... 8-19
8.3.3.2 Analysis of Post-Initiator (Type C) Human Failure Events ..... 8-25
8.3.4 Pre-Initiators ..... 8-54
8.3.4.1 HEP Summary ..... 8-54
8.3.4.2 Miscalibration Identification and Screening ..... 8-58
8.3.4.3 Historical Pre-Initiator Events ..... 8-58
8.3.4.4 Misalignment Identification and Screening ..... 8-58
8.3.5 Post-Initiators ..... 8-58
8.3.5.1 HEP Summary ..... 8-58
8.3.5.2 Post-Initiator HFE HEP Reasonableness Checks ..... 8-64
8.3.5.3 Identification ..... 8-69
8.3.5.4 Definition and Quantification ..... 8-69
8.4 Section 8 References ..... 8-69
**9. Event Sequence Quantification ..... 9-1**
9.1 Introduction ..... 9-1
9.2 Bases and Assumptions ..... 9-1
9.3 QRVA Event Sequence Quantification General Methodology ..... 9-1
9.3.1 Event Tree Split Fraction Quantification ..... 9-3
9.3.1.1 Computation of PDB Frequencies ..... 9-6
9.3.2 Event Tree Quantification ..... 9-7
9.4 Event Sequence Quantification Details ..... 9-8

9.4.1 Initiating Events ..... 9-8
9.4.2 Event Tree Linking ..... 9-10
9.4.3 Assignment Logic ..... 9-13
9.4.4 Quantification Parameters ..... 9-14
9.4.5 Saved Sequence Details ..... 9-15
9.4.6 List of Saved Sequences ..... 9-23
**10. Fuel Release Accident Sequence Analysis ..... 10-1**
10.1 Introduction ..... 10-1
10.2 Bases and Assumptions ..... 10-1
10.3 General Methodology ..... 10-2
10.3.1 RHBFSF Unscheduled Fuel Movement Data Analysis ..... 10-2
10.3.2 Acute Releases from Accident/Incident Event Sequences ..... 10-3
10.3.2.1 Probable Release Path Evaluation ..... 10-3
10.3.2.2 Event-Caused Structural Failure Evaluation ..... 10-3
10.3.2.3 Integration with Level 1 Risk Results ..... 10-3
10.4 Fuel Release Accident Sequence Analysis Details ..... 10-3
10.4.1 Direct Leaks from RHBFSTs ..... 10-4
10.4.2 Leaks from Fuel Lines and RHBFSTs within Zone 7 ..... 10-11
10.4.3 Leaks from Fuel Lines and RHBFSTs within the Tank Gallery ..... 10-13
10.4.4 Leaks from Fuel Lines and RHBFSTs below the Oil Door ..... 10-16
10.4.5 Leaks from Fuel Lines and RHBFSTs if the New Oil Door Does Not Close ..... 10-22
10.4.6 Summary ..... 10-25
10.4 Section 10 Reference ..... 10-25
**11. Risk Uncertainty Analysis ..... 11-1**
11.1 Introduction ..... 11-1
11.2 Bases and Assumptions ..... 11-1
11.3 QRVA Uncertainty Analysis General Methodology ..... 11-1
11.3.1 Sources of Uncertainty ..... 11-2
11.3.2 Some Procedures for Uncertainty and Sensitivity Analysis ..... 11-3
11.4 Monte Carlo Uncertainty Analysis ..... 11-6
11.5 Section 11 References ..... 11-9
**12. Facility Risk Quantitative Results (Phase 1) ..... 12-1**
12.1 Bases and Assumptions ..... 12-1
12.2 Sequence Group Frequency Results ..... 12-1
12.3 Initiating Event Frequency Contribution Results ..... 12-8
12.4 End State Frequency Contribution Results ..... 12-33
12.5 Importance of Human Failure Events and Equipment Failures to Risk ..... 12-39
**13. Facility Risk Vulnerability Assessment ..... 13-1**
13.1 Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences) ..... 13-1

13.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events ..... 13-1
13.2.1 Fractional Importance ..... 13-2
13.2.2 Risk Achievement Worth ..... 13-2
13.2.3 Risk Reduction Worth ..... 13-3
13.2.4 Fussell-Vesely Importance (risk participation index) ..... 13-4
13.2.5 Birnbaum Importance (risk derivative) ..... 13-4
13.3 Risk Contribution Sensitivity Analysis ..... 13-5
13.4 Vulnerability Assessment Results Presentation and Interpretation ..... 13-5
13.4.1 Insights from Sequence Group, Initiating Event, and End State Frequency Results ..... 13-5
13.4.2 Insights from Importance Measures ..... 13-7
13.4.3 Insights from Release Category Importance Measures ..... 13-9
13.5 Section 13 References ..... 13-12
**14. Phase 1 QRVA Conclusions ..... 14-1**
**15. Considerations for Future Facility Risk Case Studies ..... 15-1**

## List of Tables

Table 5-1. Sources of Facility Data ..... 5-21
Table 5-2. Effect of Two Types of Common Causes on Fault-Tree Quantification[a] ..... 5-40
Table 5-3. Generic Causes of Dependent Failures ..... 5-43
Table 5-4. Special Conditions ..... 5-44
Table 5-5. Dependent Failures Involving Subtle Dependences ..... 5-44
Table 5-6. Key Characteristics of Some Popular Parametric Models ..... 5-48
Table 5-7. MGL to Alpha Factor Conversion Formulae for Staggered Testing ..... 5-55
Table 5-8. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing ..... 5-57
Table 5-9. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing ..... 5-59
Table 5-10. Surface Area Covered by Inspections ..... 5-100
Table 5-11. Empirical Evidence of Small Leaks from Six Navy Underground Storage Tank Locations ..... 5-105
Table 5-12. RISKMAN Two-Stage Prior Distribution for Small Leaks from Six Navy Underground Storage Tank Locations ..... 5-105
Table 5-13. Bayesian Update of Navy UST Small Leaks with All RHBFST Evidence ..... 5-106
Table 5-14. Bayesian Update of Navy UST Small Leaks with Individual RHBFST Evidence ..... 5-106
Table 5-15. OGP Atmospheric Storage Tanks Small Leak Data ..... 5-108
Table 5-16. RISKMAN Two-Stage Prior Distribution from OGP Atmospheric Storage Tanks Small Leak Data ..... 5-109

Table 5-17. Bayesian Update of OGP Tank Small Leak Data with All RHBFST Evidence ..... 5-109
Table 5-18. RISKMAN Non-Informative Prior for Small Leaks Data from Six Navy Underground Storage Tank Locations Pooled ..... 5-111
Table 5-19. Bayesian Update of Pooled Navy UST Small Leak Data with All RHBFST Evidence ..... 5-111
Table 5-20. Empirical Evidence of Large External Leaks from Six Navy Underground Storage Tank Locations ..... 5-114
Table 5-21. RISKMAN Two-Stage Prior Distribution for Large External Leaks from Six Navy UST Locations ..... 5-115
Table 5-22. Bayesian Update of Navy UST Large Leaks with All RHBFST Evidence ..... 5-115
Table 5-23. OGP Atmospheric Storage Tanks Large Leak Data ..... 5-116
Table 5-24. RISKMAN Two-Stage Prior Distribution from OGP Atmospheric Storage Tanks Large Leak Data ..... 5-117
Table 5-25. Bayesian Update of OGP Tank Large Leak Data with All RHBFST Evidence ..... 5-117
Table 5-26. RISKMAN Non-Informative Prior for Large Leaks Data from Six Navy Underground Storage Tank Locations Pooled ..... 5-119
Table 5-27. Bayesian Update of Pooled Navy UST Large Leak Data with All RHBFST Evidence ..... 5-119
Table 5-28. Summary of RHBFST Maintenance Outages and Return to Service ..... 5-121
Table 5-29. Above-Maximum-Fuel-Level Holes Detected during Inspections ..... 5-123
Table 5-30. Probability of an Undetected Hole above the Fuel Level ..... 5-124
Table 5-31. Below-Maximum-Fuel-Level Holes Detected during Inspections ..... 5-126
Table 5-32. Probability of an Undetected Hole below Maximum Fuel Level ..... 5-126
Table 5-33. Distribution of Hole Locations ..... 5-128
Table 5-34. RHBFST Operating Years ..... 5-129
Table 5-35. Challenge for Overfill Leak to Rock ..... 5-131
Table 5-36. RHBFSF Pipeline Length by Section ..... 5-133
Table 5-37. Lower Dome Leak to Rock Initiators Frequencies ..... 5-135
Table 5-38. Nozzle Leak to LAT Initiators Frequencies ..... 5-138
Table 5-39. Small External Leak for MOV and XVM from Industry Data ..... 5-144
Table 5-40. Small External Leak Evidence for MOV and XVM from RHBFSF ..... 5-144
Table 5-41. Bayesian Update of Small External Leak for MOV and XVM Using RHBFSF Evidence ..... 5-145
Table 5-42. Bayesian Update of Large External Leak for MOV and XVM ..... 5-145
Table 5-43. Pipeline Leak to Lower Access Tunnel Initiators Frequencies ..... 5-147
Table 5-44. Average Hole Growth, Cumulated Gallons of Fuel Released, and Leak Rate at Time of Detection for Annual Leak Tightness Tests ..... 5-154
Table 5-45. Probability of Through-Hole Origination per Year ..... 5-156
Table 5-46. Modeling Assumption Set Probabilities and Total Fuel Releases for 18 RHBFSTs per Year ..... 5-158

Table 5-47. Fuel Released Each Year Following Though-Hole Origination in One RHBFST for Different Linear Growth Assumption Sets ..... 5-164
Table 5-48. Contribution to Mean Gallons of Fuel Release per Year ..... 5-165
Table 5-49. Summary of Sensitivity Results with Hole Probability Included in No-Growth Model ..... 5-167
Table 5-50. Maintenance Induced Leakage Fuel Release Initiating Events ..... 5-170
Table 5-51. Summary of Fuel Movement by Fuel Type and RHBFST ..... 5-171
Table 5-52. Number of Inter-Tank Fuel Transfers ..... 5-172
Table 5-53. Distributions of Fuel Movement Frequencies ..... 5-173
Table 5-54. Distributions of Fuel Movement Durations ..... 5-174
Table 5-55. RHBFSF Equipment Failure Mode Failure Rate Data for Response Event Data Analysis ..... 5-179
Table 5-56. Common Cause Parameters ..... 5-183
Table 6-1. Example of Format for a Cause Table for Double Failures (buses available) ..... 6-14
Table 6-2. List of Initiating Events Included in Model by Major Category ..... 6-18
Table 6-3. Hole Sizes and Flow Rates for Types of Initiating Events ..... 6-29
Table 6-4. Time to Drain a RHBFST from 212' to 50' versus Hole Size ..... 6-31
Table 6-5. Support to Support Dependencies among Electric Power Systems at the Underground Pump House and ADIT 1 ..... 6-34
Table 6-6. Support to Support Dependencies among the NAVFAC Water Pump House and ADIT 2 and ADIT 3 Systems ..... 6-36
Table 6-7. Support to Support Dependencies among the Supporting Electric Power Systems and Other Electric Power Systems at Red Hill ..... 6-37
Table 6-8. Support to Frontline Dependencies among the Underground Pump House and ADIT 1 Electric Power and AFHE Systems Including the Control Rooms ..... 6-39
Table 6-9. Support to Frontline Dependencies among the Underground Pump House, ADIT 1 Electric Power Systems and the AFHE Systems with the Frontline Systems at the Underground Pump House and Lower Harbor Tunnel ..... 6-41
Table 6-10. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Frontline Mechanical Systems at Red Hill ..... 6-44
Table 6-11. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Systems Requiring Electrical Support at Red Hill ..... 6-47
Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees ..... 6-49
Table 6-13. Output Quantity ..... 6-112
Table 6-14. Sectional Valve IDs at bottom of each Fuel Line Section ..... 6-113
Table 6-15. Fuel Inventories in Gallons by Fuel Line Section ..... 6-113
Table 6-16. Sequence Conditions Evaluated for Fuel Releases Leaks Directly to Rock ..... 6-118

Table 6-17. Time Delay Impacts of Top Event Failures ..... 6-121
Table 6-18. Logic for Sequence Dependent Time Delays ..... 6-125
Table 6-19. Summary of Gallons Leaked from 0.5" Hole at 212' Assuming 6-Hour Delay after Low Level Warning Alarm Detected ..... 6-128
Table 6-20. Time Delay Impacts for Top Event Failures ..... 6-130
Table 6-21. Overfill Logic for Sequence Dependent Time Delays ..... 6-134
Table 6-22. Summary of Gallons Released for Nozzle Leaks ..... 6-136
Table 6-23. Time Delay Impacts of Top Event Failures ..... 6-138
Table 6-24. NOZZLE Logic for Sequence Dependent Time Delays ..... 6-142
Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree ..... 6-145
Table 6-26. Time Delay Impacts of TUNLEAK Top Event Failures ..... 6-156
Table 6-27. TUNLEAK Logic for Sequence Dependent Time Delays ..... 6-160
Table 7-1. Event Tree Titles ..... 7-13
Table 7-2. Top Events Referenced by the Configuration Event Tree ..... 7-14
Table 7-3. LKLOC States Representing a Leak Location ..... 7-14
Table 7-4. MOVE States Representing Type of Fuel Movement ..... 7-15
Table 7-5. TKID States Representing Each RHBFST ..... 7-16
Table 7-6. FUEL States Representing Type of Fuel ..... 7-17
Table 7-7. TKXF States Representing Each RHBFST ..... 7-18
Table 7-8. TKLOC States Representing Each RHBFST Location Relative to the Fuel Line ..... 7-19
Table 7-9. HEIGHT States Representing Height of a Hole ..... 7-19
Table 7-10. SIZE States Representing Size of a Hole ..... 7-20
Table 7-11. DIRC States Representing Direction of the Leak ..... 7-20
Table 7-12. INVEN States Representing Initial Fuel Inventory ..... 7-21
Table 7-13. Top Events Referenced by ELECTRICAL Event Tree ..... 7-22
Table 7-14. Fans Fail to Start House Events ..... 7-25
Table 7-15. Top Events Referenced by OTHERSUP Event Tree ..... 7-39
Table 7-16. Top Events Referenced by VALVES Event Tree ..... 7-46
Table 7-17. FLTKC Switch Value ..... 7-47
Table 7-18. EVAC Switch Value ..... 7-48
Table 7-19. DELAY Switch Value ..... 7-50
Table 7-20. REL Switch Value ..... 7-51
Table 7-21. Top Events Referenced by Frontline Event Tree 2 – OVERFIL Event Tree ..... 7-52
Table 7-22. SWITCH Switch Value ..... 7-53
Table 7-23. Top Events Referenced by Frontline Event Tree 3 – NOZZLE Event Tree ..... 7-55
Table 7-24. Top Events Referenced by Frontline Event Tree 4 – TUNLEAK Event Tree ..... 7-59
Table 7-25. FLTKC Switch Value ..... 7-63
Table 8-1. Conditional Probability Equations ..... 8-12
Table 8-2. Pre-Initiator Screening Criteria ..... 8-22

Table 8-3. THERP Annunciator Response Model ..... 8-29
Table 8-4. Guidance on SIGMA Tree Decision Nodes ..... 8-32
Table 8-5. Estimates of σ from EPRI Report ..... 8-33
Table 8-6. CBDTM Failure Mechanisms ..... 8-34
Table 8-7. Guidance on Decision Nodes for $p_c$a, Data Not Available ..... 8-35
Table 8-8. Guidance on Decision Nodes for $p_c$b, Data Not Attended To ..... 8-37
Table 8-9. Guidance on Decision Nodes for $p_c$c, Data Misread or Miscommunicated ..... 8-39
Table 8-10. Guidance on Decision Nodes for $p_c$d, Information Misleading ..... 8-40
Table 8-11. Guidance on Decision Nodes for $p_c$e, Relevant Step in Procedure Missed ..... 8-42
Table 8-12. Guidance on Decision Nodes for $p_c$f, Misinterpret Instruction ..... 8-43
Table 8-13. Guidance on Decision Nodes for $p_c$g, Error in Interpreting Logic ..... 8-44
Table 8-14. Guidance on Decision Nodes for $p_c$h, Deliberate Violation ..... 8-45
Table 8-15. When Recovery Factors Could Be Credited ..... 8-46
Table 8-16. Recovery Factors in CBDTM ..... 8-47
Table 8-17. Conditional Probability Equations ..... 8-48
Table 8-18. Error Factors ..... 8-53
Table 8-19. Pre-Initiator HEP Summary ..... 8-55
Table 8-20. Post-Initiator HFE HEP Summary ..... 8-60
Table 8-21. HEP Stress Check ..... 8-65
Table 8-22. RHBFSF Post-Initiator HFE Timing ..... 8-67
Table 9-1. List of Sequence Groups Evaluated in the QRVA ..... 9-8
Table 9-2. Example Detailed Sequence Report ..... 9-17
Table 10-1. Fuel Release Final Locations ..... 10-5
Table 11-1. Contributors to Uncertainty in Estimates of Accident-Sequence Frequency ..... 11-3
Table 11-2. Uncertainty Distribution Characteristics for Selected Sequence Group Frequencies ..... 11-7
Table 12-1. Acute Sequence Group Frequencies per Year ..... 12-2
Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1) ..... 12-9
Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) ..... 12-14
Table 12-4. Frequency of Initiating Events Contributing to Acute Sequences Releasing Greater than 1 Million Gallons (Sequence Group ID = GGT1M) ..... 12-21
Table 12-5. Initiating Event Category % Contributions to Potential Volume Release by Release Range (gallons) and to Total Potential Volume Release (gallons per year) ..... 12-29
Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released ..... 12-34

Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures ..... 12-42
Table 13-1. Fuel Release Category Frequencies (events per year) for Selected Fuel Release Ranges in Gallons (1), (2) ..... 13-11

## List of Figures

Figure 5-1. Inputs, Outputs, and Steps in Database Development ..... 5-7
Figure 5-2. Test Intervals for Sample System ..... 5-10
Figure 5-3. Interface Schematic ..... 5-11
Figure 5-4. Modeling of Mutually Exclusive Events ..... 5-14
Figure 5-5. Fault Tree for a Three-Component System with Independent and Common Causes ..... 5-39
Figure 5-6. Example of Data Table for Hardware ..... 5-72
Figure 5-7. Example of Data Table for Test or Maintenance Acts ..... 5-73
Figure 5-8. Population Variability of the Failure Rate ..... 5-76
Figure 5-9. State-of-Knowledge Distribution over the Set of Frequency Distributions 5-77
Figure 5-10. Posterior Distribution for the Parameters of the Distribution of Pumps' Failure to Start on Demand Rates ..... 5-81
Figure 5-11. The Relation between the Population Variability Curve and Uncertainty about Individual Estimates ..... 5-89
Figure 5-12. Application of RISKMAN to Develop Generic Distribution for MOV Failure Rates ..... 5-93
Figure 5-13. Updating Generic Distributions with Site-Specific Evidence ..... 5-95
Figure 5-14. Treatment of Zero Failures Using Binomial Likelihood Function ..... 5-96
Figure 5-15. Plot of Probability of an Undetected Hole above the Fuel Level Distribution ..... 5-124
Figure 5-16. Plot of Probability of an Undetected Hole below Maximum Fuel Level Distribution ..... 5-127
Figure 5-17. Probability of Facility-Wide Chronic Releases Being Greater than Gallons per Year Shown on X-Axis ..... 5-166
Figure 6-1. Excerpt from an Event-Sequence Diagram ..... 6-6
Figure 6-2. Simplified Facility Event Tree ..... 6-8
Figure 6-3. Definition of QRVA Model Fuel Piping Sections ..... 6-28
Figure 6-4. Event Sequence Diagram for RHBFST Tank Leaks Directly to Rock (1 of 2) ..... 6-57
Figure 6-5. Event Sequence Diagram for Leaks Resulting from Overfilling a RHBFST (1 of 2) ..... 6-62
Figure 6-6. Event Sequence Diagram for Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST (1 of 2) ..... 6-66
Figure 6-7. Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel (1 of 3) ..... 6-70
Figure 6-8. Linking of Event Trees to Form an Entire Acute Sequence ..... 6-76
Figure 6-9. CONFIG Event Tree Structure ..... 6-80

Figure 6-10. ELECTRICAL Event Tree Structure ..... 6-83
Figure 6-11. OTHERSUP Event Tree Structure ..... 6-85
Figure 6-12. VALVES Event Tree Structure ..... 6-87
Figure 6-13. TKLEAK Event Tree Structure; for Direct Leaks to Rock ..... 6-91
Figure 6-14. OVERFILL Event Tree Structure; Overfills Resulting in Leaks to Rock ... 6-97
Figure 6-15. NOZZLE Event Tree Structure; Unisolable Leaks from a RHBFST to the LAT ..... 6-102
Figure 6-16. TUNLEAK Event Tree Structure; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel ..... 6-108
Figure 6-17. Example Output from Online Manning Flow Calculator ..... 6-116
Figure 7-1. Example of Format for a System-Interaction FMEA ..... 7-3
Figure 7-2. Fault Tree for Overrun of Motor 2 (relay logic only) ..... 7-6
Figure 7-3. Fault-Tree Symbols ..... 7-7
Figure 7-4. UFAN Common Cause Groups ..... 7-25
Figure 7-5. UFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-26
Figure 7-6. UFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-26
Figure 7-7. UFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-26
Figure 7-8. UFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-27
Figure 7-9. UFAN 4th Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-27
Figure 7-10. UFAN 4th Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-28
Figure 7-11. UFAN Maintenance Alignments ..... 7-28
Figure 7-12. UFAN Maintenance Alignment Equation ..... 7-29
Figure 7-13. UFAN Normal Alignment Equation ..... 7-29
Figure 7-14. EFAN Common Cause Groups ..... 7-33
Figure 7-15. EFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-33
Figure 7-16. EFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-34
Figure 7-17. EFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-34
Figure 7-18. EFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-34
Figure 7-19. EFAN Maintenance Alignments ..... 7-35
Figure 7-20. EFAN Maintenance Alignment Equation ..... 7-35
Figure 7-21. EFAN Normal Alignment Equation ..... 7-35
Figure 7-22. TFAN Common Cause Groups ..... 7-36
Figure 7-23. TFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-37
Figure 7-24. TFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-37

Figure 7-25. TFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-37
Figure 7-26. TFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-38
Figure 7-27. TFAN Maintenance Alignments ..... 7-38
Figure 7-28. TFAN Maintenance Alignment Equation ..... 7-38
Figure 7-29. TFAN Normal Alignment Equation ..... 7-39
Figure 7-30. CARGO Pumps Common Cause Groups ..... 7-41
Figure 7-31. CARGO Pumps Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-41
Figure 7-32. CARGO Pumps 2nd Order Alpha Factor Common Cause Parameters for Pumps Fail to Run Failure Mode ..... 7-42
Figure 7-33. CARGO Pumps Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-42
Figure 7-34. CARGO Pumps 2nd Order Alpha Factor Common Cause Parameters for Pumps Fail to Start Failure Mode ..... 7-42
Figure 7-35. CARGO Pumps Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-43
Figure 7-36. CARGO Pumps 4th Order Alpha Factor Common Cause Parameters for Pumps Fail to Run Failure Mode ..... 7-43
Figure 7-37. CARGO Pumps Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-44
Figure 7-38. CARGO Pumps 4th Order Alpha Factor Common Cause Parameters for Pumps Fail to Start Failure Mode ..... 7-44
Figure 7-39. MSUMP Common Cause Groups ..... 7-56
Figure 7-40. MSUMP Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-56
Figure 7-41. MSUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-56
Figure 7-42. MSUMP Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-57
Figure 7-43. MSUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-57
Figure 7-44. USUMP Common Cause Groups ..... 7-60
Figure 7-45. USUMP Common Cause Fail to Run Failure Mode and Failure Rate Equation ..... 7-60
Figure 7-46. USUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode ..... 7-61
Figure 7-47. USUMP Common Cause Fail to Start Failure Mode and Failure Rate Equation ..... 7-61
Figure 7-48. USUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode ..... 7-61
Figure 8-1. Type A Pre-Initiator HFE Questionnaire ..... 8-4
Figure 8-2. Type C Post-Initiator HFE Questionnaire ..... 8-6
Figure 8-3. Level of Dependence as a Function of Time ..... 8-11
Figure 8-4. HRA Dependency Rules for Post-Initiator HFEs ..... 8-17

Figure 8-5. Assessment of Post-Initiator HFE Probabilities ..... 8-26
Figure 8-6. Cue-Response Timeline ..... 8-29
Figure 8-7. SIGMA Decision Tree for HCR/ORE ..... 8-31
Figure 8-8. Decision Tree for $p_c$a, Data Not Available ..... 8-34
Figure 8-9. Decision Tree for $p_c$b, Data Not Attended To ..... 8-36
Figure 8-10. Decision Tree for $p_c$c, Data Misread or Miscommunicated ..... 8-38
Figure 8-11. Decision Tree for $p_c$d, Information Misleading ..... 8-39
Figure 8-12. Decision Tree for $p_c$e, Relevant Step in Procedure Missed ..... 8-41
Figure 8-13. Decision Tree for $p_c$f, Misinterpret Instruction ..... 8-43
Figure 8-14. Decision Tree for $p_c$g, Error in Interpreting Logic ..... 8-44
Figure 8-15. Decision Tree for $p_c$h, Deliberate Violation ..... 8-45
Figure 8-16. Level of Dependence as a Function of Time ..... 8-47
Figure 8-17. THERP (Reference 8-1) Table Selection Flowchart ..... 8-50
Figure 9-1. Sample Event Tree ..... 9-2
Figure 9-2. Example of Format for a Cause Table for Double Failures (buses available) ..... 9-5
Figure 9-3. Linking of Event Trees to Form an Entire Acute Sequence ..... 9-12
Figure 12-1. Frequency per Year of Exceeding a Given Number of Gallons in Any Single Acute Sequence ..... 12-6
Figure 12-2. The Frequencies Acute Sequences whose Potential Release, in Gallons, Lies within a Specified Range of Release ..... 12-7
Figure 12-3. Initiating Event Category Frequency Contribution to the Frequency of All Acute Sequences ..... 12-26
Figure 12-4. Initiating Event Category Frequency Contribution to the Frequency of Acute Sequences Each Potentially with a Release of Greater than 120,000 Gallons ..... 12-27
Figure 12-5. Initiating Event Category Frequency Contributions to the Frequency of Acute Sequences Each Potentially with a Release of Greater than 1 Million Gallons ..... 12-28
Figure 12-6. Initiating Event Category Contributions to Acute Expected Risk ..... 12-32

## List of Appendices

A. RISKMAN Software User Manual
B. Information Applied for the QRVA
C. Supporting Engineering Analyses
D. Bibliography
E. Glossary
F. In-Progress Review Feedback Summary

# List of Acronyms

| Acronym | Term |
|---|---|
| ABS Consulting | ABSG Consulting Inc. |
| AFHE | automated fuel handling equipment |
| AFRF | acute fuel release frequency |
| ANS | American Nuclear Society |
| AOC | administrative order on consent |
| AOO | anticipated operational occurrences |
| AOP | abnormal operating procedure |
| APET | accident progression event tree |
| API | American Petroleum Institute |
| ASME | American Society of Mechanical Engineers |
| ASTM | American Society of Testing and Materials |
| BDBA | beyond-design-basis accidents |
| BDBE | beyond-design-basis events |
| BDD | Binary Decision Diagram |
| BFR | binomial failure rate |
| BWS | Board of Water Supply |
| CAFRP | conditional acute fuel release probability |
| CBDTM | Cause-Based Decision Tree Method |
| CCF | common cause failure |
| CD | complete dependence |
| CET | containment event tree |
| CLOFICP | conditional loss of fuel inventory control probability |
| CMF | common-mode failure |
| CR | control room |
| CRS | cable and raceway database system |
| DBA | design-basis accident |
| DBD | design basis documentation |
| DBE | design-basis event |

| Acronym | Term |
|---|---|
| DI | dependence importance |
| DLA | Defense Logistics Agency |
| DoD | Department of Defense |
| DOH | Department of Health |
| DPD | discrete probability distribution |
| EDG | emergency diesel generator |
| EOC | error of commission |
| EOM | error of omission |
| EOP | emergency operating procedure |
| EP | emergency preparedness |
| EPA | Environmental Protection Agency |
| EPRI | Electric Power Research Institute |
| ERF | emergency response force |
| ESD | event sequence diagram |
| ET | event tree |
| F-76 | marine diesel |
| FDB | facility damage bin |
| FL | fuel line |
| FLC | Fleet Logistics Center |
| FMEA | failure modes and effects analysis |
| FORFAC | Fuel Oil Reclamation Facility |
| FR | fuel release |
| FRF | fuel release frequency |
| FTA | fault tree analysis |
| FTR | fail to run |
| FTS | fail to start |
| gpm | gallons per minute |
| GPH | gallons per hour |
| HDR | HDR Engineering, Inc. |
| HCLPF | high confidence in low probability of failure |
| HCR | human cognitive reliability |

| Acronym | Term |
|---|---|
| HD | high dependence |
| HECO | Hawaii Electric Company |
| HEP | human error probability |
| HFE | human failure event |
| HOL | high operating limit |
| HRA | human reliability analysis |
| HRR | heat release rate |
| HVAC | heating, ventilation, and air conditioning |
| IAEA | International Atomic Energy Agency |
| IE | initiating event |
| IPR | in-progress review |
| JBPHH | Joint Base Pearl Harbor-Hickam |
| JHEP | joint human error probability |
| JP-5 | Jet Propulsion Fuel No. 5 |
| JP-8 | Jet Propulsion Fuel No. 8 |
| LAT | Lower Access Tunnel |
| LD | low dependence |
| LOFIC | loss of fuel inventory control |
| LOFICF | loss of fuel inventory control frequency |
| LOOP | loss of offsite power |
| LRDP | low-range differential pressure |
| MD | medium dependence |
| MFF | master frequency file |
| MGL | Multiple Greek Letter |
| MLD | master logic diagram |
| MLE | maximum-likelihood estimate |
| MOV | motor-operated valve |
| MS | Microsoft |
| MTC | Mass Technology Corporation |
| MTTR | mean time to recovery |
| NAVFAC | Naval Facilities Engineering Command |

| Acronym | Term |
|---|---|
| NRC | U.S. Nuclear Regulatory Commission |
| OGP | Oil & Gas Producers |
| ORE | operator reliability experiments |
| P&ID | piping and instrument diagram |
| PRA | probabilistic risk assessment |
| QHO | quantitative health objectives |
| QRVA | quantitative risk and vulnerability assessment |
| RA | risk achievement |
| RAW | risk achievement worth |
| RH | Red Hill |
| RHBFSF | Red Hill Bulk Fuel Storage Facility |
| RHBFST | Red Hill Bulk Fuel Storage Tank |
| RTS | return to service |
| SDM | system dependency matrix |
| SHARP1 | Systematic Human Action Reliability Procedure, Revision 1 |
| SOKC | state-of-knowledge correlation |
| SOP | standard operating procedure |
| SOW | Statement of Work |
| SR | supporting requirement |
| SSC | structures, systems, and components |
| STA | shift technical advisor |
| THERP | Technique for Human Error Rate Prediction |
| TIRM | test inspection repair maintenance |
| TUA | tank upgrade alternative |
| UAT | Upper Access Tunnel |
| UFM | unplanned fuel movement |
| UGPH | underground pump house |
| UPS | uninterruptable power supply |
| UST | underground storage tanks |
| UTF | Upper Tank Farm |

| Acronym | Term |
|---|---|
| XVM | manual-operated valve |
| ZD | zero dependence |

# 1. Introduction

ABSG Consulting Inc. (ABS Consulting) is pleased to present this report to HDR Engineering, Inc. This report is designed to comply with and be fully responsive to the Naval Facilities Engineering Command (NAVFAC) Hawaii "Section 8.2: Risk/Vulnerability Assessment Scope of Work" dated April 13, 2017 (Reference 1-1). The associated work is proposed to be performed under United States Navy Contract N62742-14-D-1884, Delivery Order 0028, Amendment 64 Statement of Work dated June 1, 2017 (Reference 1-2).

The purpose of this report is to describe the processes, methodology, and results of phase one of the baseline Quantitative Risk and Vulnerability Assessment (QRVA) for the Red Hill Bulk Fuel Storage Facility (RHBFSF) performed in compliance with the RHBFSF Administrative Order on Consent – Statement of Work (AOC-SOW) Section 8.2. The complete QRVA is designed to serve as a tool to help facilitate decision making that will mitigate risk and improve safety for the RHBFSF throughout the remainder of its life cycle.

## 1.1 Background

The RHBFSF site is located approximately 2.5 miles northeast of Pearl Harbor on the island of Oahu in Hawaii. The facility lies along the western edge of the Koolau Range and is situated on a topographic ridge that divides the Halawa Valley and the Moanalua Valley. The site is bordered to the south by the Salt Lake volcanic crater and occupies approximately 144 acres of land. The surface topography varies from approximately 200 feet to 500 feet above mean sea level.

The facility consists of twenty 12.5-million-gallon, field-constructed underground storage tanks (UST) constructed in the early 1940s. The tanks are 250 feet tall and 100 feet in diameter, with a domed top and base. The facility currently stores Jet Propulsion Fuel No. 5 (JP-5), Jet Propulsion Fuel No. 8 (JP-8), and marine diesel (F-76). Historic fuel storage has included diesel oil, Navy Special Fuel Oil, Navy distillate, F-76, aviation gas, motor gas, JP-5, and JP-8.

In January 2014, up to 27,000 gallons of JP-8 was released from Tank 5, which was being returned to service after having undergone inspections, repair, and maintenance. As a result of the fuel release from Tank 5, the U.S. Environmental Protection Agency (EPA) and the Hawaii Department of Health (DOH) brought an enforcement action against the Navy and the Defense Logistics Agency (DLA) to address the fuel release and minimize the likelihood and impact of future releases. Regulatory experience has shown that a negotiated agreement, such as an administrative order on consent, is the appropriate enforcement tool to address such a unique facility and solve complex environmental problems since it allows for flexible, collaborative, and innovative solutions. The AOC-SOW is a proactive approach that goes beyond the normal scope of merely complying with current regulations.

## 1.2 Project Scope

The scope of this project QRVA, defined in this section, includes establishment of the appropriate QRVA level to be applied, the scope of hazards to be addressed, and the boundaries, both defined. Prior to initiating technical work on a facility QRVA, it is necessary to clearly establish the desired risk level, scope phase, and boundary assessments.

### 1.2.1 Risk Assessment Levels

"Levels" of risk assessment are frequently defined to focus the evaluations such that the associated results can efficiently and effectively support risk management. These levels of risk assessment can be defined, as desired, by the risk analyst, but the objective of defining these levels is to support an understanding of risk, which ultimately can facilitate the development and implementation of effective risk management actions or options. The "level" of a QRVA is often best described by characterizing the key figure(s) of merit desired to be developed and quantified via the QRVA. For example, any or all of the following levels of QRVA could be pursued for a RHBFSF QRVA:

- Level 1 – Frequency (and annual probability) of Loss of Fuel Inventory Control (by volume range) within the RHBFSF Property Boundaries

- Level 2 – Frequency (and annual probability) of Uncontrolled Release of Fuel Inventory (by volume range) outside the RHBFSF Property Boundaries that Could Impact Red Hill Groundwater Shaft Water Quality

- Level 3 – Frequency (and annual probability) of Exceeding Public Water Supply Quality Levels or Limits (e.g., within the Red Hill groundwater shaft) Directly Associated with Uncontrolled Release of Fuel Inventory outside the RHBFSF Property Boundaries

- Level 4 – Frequency (and annual probability) of Public Deaths (or injuries or illnesses) Directly Associated with Uncontrolled Release of Fuel Inventory outside the RHBFSF Property Boundaries

Experience has shown that Levels 1 and/or 2 above are often adequate to facilitate effective risk management decision-making for the facility owner/operator. The QRVA described in this report focuses on a Level 2 risk assessment, as defined above. The result of this risk assessment can provide evaluation information and metrics to support work being executed under the AOC-SOW Sections 6 and 7, which can support expansion of the risk assessment to a Level 3 assessment for the Red Hill groundwater shaft, as desired and directed by the Navy.

### 1.2.2 Scope of Hazards

Next, the scope of hazards to be addressed within the QRVA must be specified. Industry experience, supplemented by industry standards for risk assessment, has established that a comprehensive QRVA should generally consider risks from the hazard

sources below. They are grouped into phases, which are recommended to efficiently characterize the scope of hazards to be addressed in the RHBFSF QRVA:

- Phase 1 – Internal Events (not including fire or flood)
  - Equipment or Structural Failures in Both Frontline and Support Systems, Human Errors, Etc.
- Phase 2 – Internal and External Fire and Flood Events
  - Internal Flooding
  - Internal Fires
  - Internal Sabotage (not included within the scope of this analysis for security reasons)
  - External Flooding, Tsunami, and Heavy Precipitation
  - External Fires
- Phase 3 – Seismic Events
  - Earthquakes
- Phase 4 – Additional External Events
  - High Winds
  - Storms (tornados, hurricanes, etc.)
  - Landslides (or mud slides)
  - Proximity Transportation Accidents
  - Aircraft Crashes
  - External Hazardous Material or Chemical Spills or Releases
  - Extreme Weather (e.g., high temperature, etc.)
  - Terrorist Acts (not included within the scope of this analysis for security reasons)
  - Other Facility-Specific Hazards (often location-dependent hazards that can be special cases of other general hazard sources)

This QRVA report addresses only the Phase 1 scope of hazards presented above. The remaining phases will be addressed in future scopes of work, as directed and authorized by the Navy.

### 1.2.3 Boundaries of Assessment

The scope of a QRVA is defined via clear and comprehensive characterization of assessment boundaries. First, the functional and physical boundaries of the facility to be assessed must be clearly defined. The functional boundaries are facility-specific, depending upon the processes performed by or at the facility. The physical boundaries are generally defined by specifying the target property lines, structures, systems, and components (SSC) considered to be within the facility functional boundaries. Functional and physical boundaries are generally those supported by existing as-built, as-operated design basis documentation (DBD). DBD includes currently-effective documentation and schematic drawing information associated with the as-built, as-operated facility. DBD includes all effective documentation associated with facility design, operation, maintenance, and testing.

Closely related to analysis boundaries is the issue of the physical and functional basis or starting point for the QRVA. The boundaries for this assessment are the fuel handling and containment equipment within the fenced area of the RHBFSF, the piping tunnel that runs from the facility down to the Red Hill underground pump house (UGPH) on the base, Joint Base Pearl Harbor-Hickam (JBPHH), the Red Hill underground pump house itself, and sumps and surge tanks directly associated with RHBFSF operation in the area of the underground pump house. An effective design freeze date has been established to ensure a stable design basis for the QRVA. For this QRVA, the following design basis has been selected by the Navy:

> Freeze the facility design as of the date of approval of the Phase 1 QRVA commencement of work, July 27, 2017. The design basis is the as-built, as-operated facility as of the this approval date, to include design, operation, maintenance, and testing changes that have been approved and funded as of this date, but with no additional modification options.

## 1.3 Section 1 References

1-1 Naval Facilities Engineering Command, Hawaii, “Section 8.2: Risk/Vulnerability Assessment Scope of Work,” April 13, 2017.

1-2 United States Navy Contract N62742-14-D-1884, Task Order 0028, Amendment 64 Statement of Work, June 1, 2017.

# 2. QRVA Methodology – General Overview

QRVA is a scenario-based approach to assessing risk, defined as follows:

Risk is the combined answer to three questions that consider: (1) what can go wrong?, (2) how likely is it?, and (3) what are the potential consequences? More sophisticated definitions of risk include a fourth question: (4) what is our level of uncertainty (or confidence) associated with the answers to the first three questions?

In this assessment, we model scenarios that could lead to loss of fuel inventory control within the RHBFSF (the Level 1 QRVA) and continuations of those logical scenarios that could then result in release of fuel outside the RHBFSF, which could potentially result in fuel chemical (generally hydrocarbon) contamination of groundwater. The metric for each scenario in the risk assessment is a frequency measured in events per year. For Level 1 risk in this assessment, this would be the frequency of loss-of-fuel-inventory-control events per calendar year. For Level 2 risk in this assessment, this is the frequency of fuel release events per calendar year. However, as we are also assessing consequences for each of the Level 2 scenarios, in this QRVA, we are including fuel release location and fuel volume released (in ranges of volume release). Therefore, we are reporting results in tabular format with three primary characteristics, as follows:

- The Frequency of Event Sequences Resulting in Fuel Release (events/calendar-year)
- The Quantity of Fuel that May Be Released (ranges of gallons)
- The General Location of the Fuel Release Point

Thus, the results are presented in terms of gallons per year of fuel released per release location. The completed table of results can be viewed as a detailed risk matrix for the RHBFSF.

Technical work on the RHBFSF QRVA has been conducted applying the methodology, guidelines, and procedures outlined in the QRVA Methodology presented in each

technical section of this report. Primary guidance information sources include the following:

- American Nuclear Society (ANS) and Institute of Electrical and Electronic Engineers, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," sponsored by the U.S. Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute, NUREG/CR-2300, April 1983 (Reference 2-1).

- U.S. Nuclear Regulatory Commission, "PSA Procedures Guide," NUREG/CR-2815, 1985 (Reference 2-2).

- American Institute of Chemical Engineers Center for Chemical Process Safety, "Guidelines for Chemical Process Quantitative Risk Analysis," 2nd Edition, October 1999 (Reference 2-3).

Additional information on special QRVA topics and tasks is provided via the references cited in this report and via the information sources included in the bibliography of this report.

## 2.1 Definitions of Key Terms

The definitions of some key terms applied in QRVA are presented in this section. A comprehensive list of QRVA terms and definitions is presented in Appendix E. Some definitions of fundamental QRVA terms are presented as follows:

**Risk:** The combined answer to three questions that consider (1) what can go wrong?, (2) how likely is it?, and (3) what are the potential consequences? More sophisticated definitions of risk include a fourth question: (4) what is our level of uncertainty (or confidence) associated with the answers to the first three questions?

**Hazard:** Anything that has the potential to initiate or cause an undesired sequence of events and/or conditions to occur that leads to an undesired consequence. Examples of QRVA hazards are facility equipment failures, human errors, fires, floods, earthquakes, adverse weather, etc.

**Vulnerability:** Weakness in the design or operation of a system, component, or structure that could increase the probability of disabling its function and, thus, contribute, in a potentially significant way, to overall facility risk.

**Initiating Event (IE):** An event that perturbs the steady state operation of the facility and could lead to an undesired facility condition. This is an event that can start or precipitate a sequence of additional events or conditions that ultimately result in an undesired consequence.

**Basic Event:** An element of the QRVA model for which no further decomposition is performed because it is at the limit of resolution consistent with available data.

**Probability:** The likelihood that an event will occur as expressed by the ratio of the number of actual occurrences to the total number of possible occurrences.

**Frequency:** The actual (historical) or expected (future) number of occurrences of an event or accident condition expressed per unit of time.

**Boolean Logic:** A branch of algebra in which all operations are either true or false; i.e., yes or no, and all relationships between the operations can be expressed with logical operators such as AND, OR, or NOT. Invented by English mathematician George Boole.

## 2.2 Description of QRVA Methodology

The details of the QRVA methodology applied on this project are presented in the technical sections of this report. A conceptual overview of general QRVA activities is presented as follows:

- Facility Familiarization and QRVA Scope Determination
- Initiating Event Analysis
- Event Sequence (event tree) Analysis
- System (failure modes and effects analysis [FMEA] and fault tree) Analysis
- Data Analysis (including dependent events analysis)
- Human Reliability Analysis (HRA)
- Event Sequence Quantification (including uncertainty analysis)
- Risk Results Compilation (e.g., detailed risk matrix)
- Risk Decomposition and Vulnerability Assessment
- QRVA Documentation and Communication (presentation)

The QRVA Team must first review and evaluate facility information to become thoroughly familiar with facility SSCs and the operational profile of the facility. This includes review of facility operating, maintenance, and testing procedures for both normal and emergency operating conditions.

The team then conducts an analysis of potential event sequence initiating events, specifically initiating event frequencies, which may be precipitated via the hazards considered within the scope of the QRVA. For this QRVA, these hazards are those identified in Section 1.2.2 of this report.

The team then develops qualitative event sequences that could lead to undesired consequences contributing to risk. For this QRVA, the primary undesired consequence is the uncontrolled release of fuel from the RHBFSF.

The event sequence analysis is conducted via event tree analysis. The team conducts facility system FMEA and fault tree analysis to characterize event tree top events and split fractions. To support quantification of QRVA event sequences, data analysis must be performed to support quantification of event tree split fractions. Quantification of event tree split fractions is supported primarily via fault tree quantification. The data analysis is performed to quantify initiating event frequencies and conditional probability of individual event tree split fractions for event sequence quantification. The event tree split fraction conditional probability values are derived primarily via fault tree quantification. The data analysis includes derivation of fault tree basic event probability values. In developing event sequences and fault trees for a facility QRVA, it is

necessary to identify human actions (e.g., facility operator actions) that may contribute to facility event sequences. HRA is performed to identify and characterize these actions in terms of human failure events (HFE) for the fault trees and event trees. HRA also includes evaluation of HFE human error probability (HEP) values for application within the event sequence quantification.

When the fault tree models are completed and quantified, and the split fraction data is entered into the event trees, the event sequences can then be quantified, and baseline risk can be determined. Fault tree analysis and quantification and event tree analysis and quantification are accomplished via state-of-the-art QRVA software packages, such as RISKMAN™, to be applied on this project. The data for fault tree and event tree quantification are entered as probability distributions in the QRVA software. Uncertainty analysis is performed by propagating the input data probability distributions through the fault tree and event tree quantifications processes applying either a Monte Carlo or a Latin-Hypercube process in RISKMAN, resulting in a probability distribution for the baseline risk. Baseline risk results are compiled and expressed via a table of results sometimes called a risk matrix.

After the baseline risk results have been determined, the vulnerability assessment is performed by decomposing the risk into its component parts in a number of ways. We apply what are known as risk importance measures to decompose the total baseline risk into fractional risk contributors by event sequence, initiating event group, etc. We also calculate risk importance measures down to the basic component failure mode and human failure event levels of risk contributors to develop ranked lists of these risk model elements. These ranked lists of contributors by initiating event group, event sequence, and individual basic events or fundamental elements of risk contribution provide valuable insight into the vulnerability of the facility to risk. Finally, the baseline risk results and the vulnerability assessment are documented in a report in terms that can support prudent decision-making for the facility.

The QRVA team will analyze and quantify logic models (event trees and fault trees) for the QRVA applying ABS Consulting's RISKMAN Version 14.4 software. This software was developed and is maintained and audited under ABS Consulting's Nuclear Quality Assurance Program. The software is fully compliant with 10 CFR 50, Appendix B, nuclear quality requirements. Additionally, this software has been checked and audited via multiple nuclear power utility company software quality assurance programs, and it has passed multiple audits by the Nuclear Procurement Issues Corporation. [redacted]

## 2.3 Assumptions and Level of Uncertainty

The bases and assumptions associated with the QRVA are clearly documented in this QRVA report. In QRVA, every effort is made to develop and apply realistic "best estimate" models and data. In some cases, simplifying assumptions may be applied to simplify overall risk modeling and quantification. In cases, where simplifying assumptions are made in the QRVA, these assumptions are documented in the QRVA report.

Uncertainty is considered in rigorous high-quality QRVA. The RHBFSF QRVA Team applies probability distributions for applicable input data in the risk quantification

performed via the selected QRVA software, RISKMAN, for this QRVA. The source of input data probability distributions is documented in the QRVA report. The uncertainty represented by these input data probability distributions is propagated through the risk model quantifications of the QRVA via the RISKMAN software using either Monte Carlo simulation techniques or Latin-Hypercube simulation techniques. The more common of these two methods of uncertainty propagation is the Monte Carlo simulation technique. Propagation of input data uncertainty through the risk model enables the analysts to express overall baseline risk results in terms of probability distributions, which express our uncertainty in the baseline risk results.

By expressing our level of uncertainty in the QRVA, we greatly improve the ability of decision-makers to apply QRVA results in support of making prudent decisions. Guidelines for addressing uncertainty in QRVA are provided in this report and in NUREG-1855, which is applied as a guide supporting the uncertainty analysis performed for this QRVA.

## 2.4 Evaluating and Prioritizing Events

In this QRVA, event sequences and individual events are evaluated and prioritized based on their contribution to overall facility baseline risk, primarily via the vulnerability assessment portion of the QRVA. In some areas of the QRVA, simplifying assumptions are applied, which may be slightly conservative "locally" at the individual event or event sequence level of indenture in the risk model, but which "globally" have no significant effect on the overall quantification of facility baseline risk. In cases where simplifying assumptions are applied, they are documented in this QRVA report.

Screening analyses are applied in this QRVA to effectively simplify the risk quantification by eliminating insignificant contributors to risk. Any such screening analyses or evaluations applied in this QRVA are based on criteria for acceptable threshold of risk provided by the regulator; e.g., the EPA in this case, or by the Navy. For this assessment, the Navy has provided risk threshold information.

Based on Reference 2-4, the current risk thresholds of concern for the safety of the water table potentially affected by RHBFSF fuel release to the environment are:

1. Acute (sudden, scenario-specific, one-time) fuel release incidents of 120,000 gallons or greater.

2. Chronic (generally undetected, near-continuous) releases of 2,300 gallons or greater per tank per year. For 18 active tanks at the facility (the configuration of the facility at the time of this assessment) this equates to 41,400 gallons or greater per year for the entire facility.

The risk model elements (e.g., event sequences and model basic events) are evaluated and prioritized via risk importance measures, as described in Section 13 of this report.

## 2.5 Section 2 References

2-1 American Nuclear Society and Institute of Electrical and Electronic Engineers, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk

Assessments for Nuclear Power Plants," sponsored by the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute, NUREG/CR-2300, April 1983.

2-2 U.S. Nuclear Regulatory Commission, "PSA Procedures Guide," NUREG/CR-2815, 1985.

2-3 American Institute of Chemical Engineers Center for Chemical Process Safety, "Guidelines for Chemical Process Quantitative Risk Analysis," 2nd Edition, October 1999.

2-4 E-mail message from Steven L. Chow, NAVFAC Hawaii, to James K. Liming, ABSG Consulting Inc., dated July 27, 2018, 11:27 AM Pacific Time.

# 3. Facility Information Collection and Review

The QRVA team has, to date, submitted two formal information requests to the Navy to support this project. These two information requests are presented, as follows:

**Information Request #1 Submitted to the Navy on July 28, 2017**

1. RHBFSF general site and facility layout and arrangement drawings.

2. A comprehensive set of RHBFSF Piping and Instrument Diagrams (P&ID) or equivalent flow and/or logic diagrams.

3. Tank and piping isometric drawings or similar layout diagrams.

4. System description documentation.

5. A comprehensive electronic list of all SSCs included within the scope of the QRVA, including alpha-numeric component ID numbers, system designators, specific component service descriptions, component types, component locations, and reference(s) to SSC design documentation. This list should include all tanks, piping, pumps, valves, electric power, and associated instrumentation and controls equipment required to operate the facility.

6. SSC design documentation, preferably in electronic format, including design or building code information; e.g., American Petroleum Institute (API) and/or American Society of Mechanical Engineers (ASME) code information for tanks.

7. Structure and component seismic design criteria.

8. RHBFSF site location scheme; e.g., areas, zones, rooms, or compartments with associated location (e.g., 3D coordinate system) information. If fire zones have been designated for this facility based on fire area and barrier criteria, this information is preferred.

9. All facility operating and maintenance procedures, including normal and emergency (incident response) operating procedures and policies.

10. Facility operating logs, preferably for the entire history of the facility, but for at least the last 5 years (e.g., 2012 to present) of facility operation.

11. A list of all historical incidents involving hydrocarbon or other fuel or material release from RHBFSF and all other Navy fuel storage facility tanks and systems worldwide, to include not only tank or piping rupture events, but also releases associated with human errors; e.g., during fuel or other fluid tank fill, tank emptying, or other transfer, maintenance, or testing operations. This includes all unscheduled fuel movement (UFM) reports and associated corrective action taken.

12. Loss of fuel inventory incident reports over the entire history of the facility.

13. Either the record of all fuel movements over the past 5 years or an expected realistic facility operating profile to be used in the QRVA; i.e., average demand loading for all RHBFSF equipment over the long term. This includes estimates for run time and demand cycle numbers for all RHBFSF equipment per year over the long term; e.g., pump on/off cycles and run time, valve open/closure cycles, tank fill/offload cycles and timing, piping segment active flow time and standby/rest time, equipment sensor cycles and monitoring time, instrumentation and control equipment actuation cycles and monitoring time, and power source energize/de-energize cycles and power provision time over the long term.

14. The full text of any previous facility risk and vulnerability assessments and other risk assessment reports performed for the RHBFSF, along with all associated appendices, models, and databases.

15. Other documentation deemed pertinent to RHBFSF QRVA, as determined by the Department of Defense (DoD).

**Information Request #2 Submitted to the Navy on October 23, 2017**

1. RHBFSF equipment status and associated corrective maintenance information over the site history (or at least the last 10 years) identifying all component failures, associated component failure modes, associated component downtime, and associated corrective actions implemented. This is information provided in a typical DoD facility Failure Reporting and Corrective Action System.

2. RHBFSF preventive maintenance and inspection plan and records, including any failures or incidents that may have resulted related to the performance of preventive maintenance or inspection activities (e.g., the incident that precipitated the AOC). This also includes any revisions to inspection and/or preventive maintenance activities that were previously implemented or are planned to be implemented in response to such failures or incidents.

3. RHBFSF operator training and qualification materials.

4. List of incidents involving human error at the facility, including any associated follow-up training and corrective actions implemented.

5. RHBFSF incident report records over the site history (or at least the last 10 years).

6. Specific incident or component failure event root cause analysis reports or related causal factor analyses or assessments.

7. In the file named P-1551- Red Hill Fire Suppr and Ventilation System Oct-2015.pdf, from HDR\Govt_DataSet07, we note that there are some emergency power upgrade schematics. We request **all** the electrical schematics for the RHBFSF supplies and loads, including those for the underground pump house, and for the main and alternate control rooms (CR).

8. In the file named Entire Ventilation study_Final-2005.pdf from HDR\Govt_Dataset-05, we note that we have RHBFSF ventilation system schematics, showing fan locations and flow paths for the two systems; i.e., Tanks 1

to 16 and Tanks 17 to 20, but we understand that significant modifications have been implemented since 2005. Please provide the current associated RHBFSF ventilation system schematics.



The QRVA team has also conducted two question-answer-discussion sessions among the QRVA team, NAVFAC, and the FLC Fuels Department.

Additionally, the QRVA team has conducted site visits to the RHBFSF to tour the facility and collect and review information about the facility. The ABS Consulting project manager for the QRVA, Mr. James K. Liming, toured the facility in May 2016. Mr. Donald J. Wakefield, the QRVA Event Sequence Analysis lead for the project, and Mr. James C. Lin, the QRVA Systems Analysis lead for the project, conducted a RHBFSF site visit during the October 2 through 6, 2017, time period. Two additional site visits were conducted by Mr. James K. Liming, the HRA lead for the project, in December 2017 and March 2018. During these HRA visits, Mr. Liming conducted talk-throughs and walk-throughs of normal and emergency procedure actions at the facility.

# 4. QRVA Bases and Assumptions – Overview

The bases and assumptions applied in this QRVA are described in the technical sections of this report. As comprehensive operational history data on RHBFSF fuel receipt, distribution, and internal transfer were not provided to the QRVA team by the Navy, the QRVA team established the following assumed long-term average operational profile and has applied the following key bases and assumptions for the facility baseline QRVA:

- Modeled operation of the RHBFSF up to 100 years into the future of the design freeze date for the baseline QRVA, 100 years from July 27, 2017. While it is unlikely that this facility will operate for another 100 years, this exposure for facility life was agreed by the Navy and stakeholders to be appropriate for purposes of this QRVA.

- The facility will effectively be operated in the current configuration with the same operating profile (fuel movement profile, processes, operating procedures and policies, maintenance, testing, and design) hypothetically for thousands of years with no intervening risk-mitigating improvements.

- Each operational main fuel storage tank of the RHBFSF experiences an average of 10 fill operations and 50 distribution operations per calendar year.

- The RHBFSF conducts an average of 30 internal fuel transfers each calendar year.

- The RHBFSF supply pumps have the following capacities:

  - For F76, 7,000 Gallons per Minute (gpm)
  - For JP5, 5,000 gpm
  - For F24, 4,500 gpm

- All distribution operations are conducted using the gravity feed mode of operation.

- The RHBFSF main sump pump inlet and discharge isolation valves are in a normally open condition.

- Each main storage tank undergoes a major API 653 inspection once every 20 years on a rotating basis, with one tank inspection being performed each year, on average.

- RHBFSF fuel piping transferring fuel approximately 50% of all calendar time, with the time split equally among gravity feed time and main storage tank fill time (piping pressurized by operating fuel pumps).

- The QRVA Model assumes that going forward, 18 RHBFSTs will be in service throughout much of each calendar year. This is conservative compared to a realistic account assuming that each RHBFST must be inspected once every 20 years.

- There is insufficient ullage available at RHBFSF and the Upper Tank Farm (UTF) to fully empty a RHBFST holding F76 fuel. There is sufficient ullage available to fully empty a RHBFST containing either F24 or JP5 fuel.

- In the event of a leak through the RHBFST liner during a return to service, there is adequate ullage initially available, including for F76, to fully empty the leaking RHBFST.

- The QRVA model assumes that even under conditions requiring that a RHBFST be emptied, fuel levels in RHBFSTs of the same fuel type would not be filled above 212' and that offloaded fuel would not be added to RHBFSTs holding different fuel types.

- If there is initially insufficient ullage to empty a RHBFST that is leaking fuel, it is assumed sufficient ullage would be found within 2 weeks of the scenario initiating event.

- It is assumed that in the event of a RHBFST nozzle leak (i.e., nozzle is a term used to describe the section of pipe which exits the RHBFST lower dome and connects to the line's skin valve. It also includes the first isolation valve along that line which may be a MOV or a manual valve.), that for smaller size leaks (modeled as 0.5" holes), that the action to remotely move fuel from the associated RHBFST would be carried out. It is assumed that this action would be delayed for at least 24 hours from the time the control room receives a low level alarm in the associated RHBFST due to a requirement to evacuate the LAT and the confusion that would result.

- For the larger size nozzle leak (i.e., 6" equivalent diameter is assumed in the model), no credit is assumed for moving fuel from the associated RHBFST. This is because by the time a fuel movement strategy could be formulated and initiated, much of the fuel release would have already occurred, by then remote operation of the MOVs in the tunnels may be precluded.

- The NAVFAC pump house is fully sealed so that even if there is an accumulation of several feet of fuel within the pump house, there is little or no release path via the water tunnel to the aquifer.

- The old doorway from the LAT to the abandoned diesel power station is fully sealed so that even if there is an accumulation of released fuel upgrade of the normally closed fan door, there is no release path to the aquifer via the power plant riser shaft and the diesel station itself.

- The structural integrity of the tank inner shell is assumed robust for purposes of the Phase 1 QRVA, as this shell is subject to periodic inspection and continuous monitoring for leak integrity.

- The structural integrity of the concrete tanks and grouting is assumed robust for purposes of supporting the tank inner shell for this Phase 1 QRVA. However, as there has effectively been no inspection, testing, or maintenance performed on the concrete tanks and grouting since construction, no credit is given in this assessment for fuel containment (i.e., containment of fuel that may leak through the tank inner

shell). All fuel that passes through the tank inner shell is assumed to ultimately pass into the rock and soil surrounding the tank and, thus, have a capability of potentially propagating, over time, to the water table.

- Tank inner shell corrosion is primarily effectively initiating at the outside surface of the shell and propagating to the inner surface of the shell. While some could postulate tank shell failure rate acceleration over time due to corrosion, this potential corrosion rate acceleration factor is considered insignificant in this assessment. This assumption is supported by the fact that regular periodic thorough inspections of the tank inner shell integrity are performed with a focus on the impacts of corrosion, and any corrosion found to have caused near through-wall holes are appropriately monitored and repaired before the complete through-wall hole occurs; i.e., creating an effective continuous renewal process for the tank shell. Supporting this assumption is the fact that, over time, we can reasonably anticipate that methods for detecting and monitoring the impacts of tank shell corrosion will likely improve. Additional discussion on this issue is presented in Section 5 of this report.

# 5. Data Analysis

## 5.1 Introduction

Data required for a detailed rigorous QRVA consists of three major elements, as follows:

1. Analysis of events that can initiate an event sequence potentially leading to loss of fuel inventory control (LOFIC), and ultimately result in fuel release (FR) from the facility, which could impact groundwater contamination levels and pose a risk to the general public health. In the QRVA, these events are called initiating events.

2. Analysis of facility conditions and SSC failures that could affect the ability of the facility operators and systems to control or mitigate the impact of LOFIC and/or FR event sequences. In this QRVA, we call these conditions and failures hardware response events.

3. Analysis of human reliability associated with human (generally operator) actions taken in response to LOFIC and/or FR event sequences. Specifically, QRVA HRA focuses on HFEs that could impact the progression and severity of LOFIC and/or FR event sequences.

Conventionally, QRVA data analysis includes the first two of these three elements, as reported in this section of the QRVA report. The HRA is described in Section 8 of this report. This report section includes a description of general QRVA data analysis methodology, a description of the method and results for the initiating events data analysis, and a description of the method and results for the response events data analysis.

## 5.2 Bases and Assumptions

The bases and assumptions for the development of the data analysis are summarized below.

1. For the next 100 years of Red Hill facility operation, the initiating events and component failures are assumed to occur randomly and are modeled as a constant failure rate process. Demand based failure models are also assumed to have constant failure parameters over the 100-year period.

2. Common cause failure models are used only for models of identical redundant equipment.

3. Prior leakage events recorded only in the RHBFST unverified histories of Whitacre emails are counted as a leakage event unless it is documented in NAVFAC comments as the event being a release of water only.

4. Leakage events associated with the tell-tale systems in the first half of the facility operating history are not counted as leakage events going forward.

5. Past leakage incidents that occurred following extended maintenance, during RHBFST returns to service, are separated from leak incidents used to estimate the frequency of leaks during normal RHBFST operation and instead are modeled separately.

6. RHBFST liner through holes detected only during API 653 inspections and located below the maximum fuel levels are counted in the leakage rates for normal facility operation. Only RHBFST API 653 inspection findings of seven RHBFSTs with 100% liner inspection are used; i.e., those RHBFST inspections conducted since 2005.

7. RHBFST outages not explicitly identified in the available historical references were added to the total number outage if they were implicitly referred to; e.g., where a batch of RHBFSTs were upgraded for a specific purpose on a particular time frame. Simple RHBFST cleaning outages were, however, not counted as extensive maintenance outages.

8. RHBFST outage durations not explicitly recorded were estimated from outage event data from other RHBFSTs in the same time frame.

9. For the leakage rate from RHBFSTs, the prior distribution was developed from Navy underground storage tank data collected from six different sites. The posterior distribution for the RHBFST leakage rate during normal operation was then obtained by performing a Bayesian update of this prior to using the collected Red Hill facility leakage incidents.

10. None of the recorded leak incidents at the other Navy six sites exceeded the maximum leak rate recorded at Red Hill; i.e., 1.8 gpm, which was only for a short period of time during the RHBFST 5 event in 2014.

11. The frequency of “large” RHBFST liner leakage events (i.e., larger than what have been observed in the history of Red Hill) can be estimated by updating a prior distribution obtained from Navy underground storage tank data from six sites with zero events in the total duration of RHBFST operation.

12. The occurrence of issues, receipts, or transfers between RHBFSTs is assumed to have no effect on the frequency of either small or large leakage events from RHBFSTs during normal operation.

13. The frequency of any RHBFST return to service in future years is assumed once per calendar year consistent with the RHBFST planned inspection intervals.

14. For the large leak frequency during a return to service, it is assumed that the small leak rate for returns to service, reduced by the ratio of frequencies for large to small leaks for liner leaks during normal operation, is a reasonable assumption; i.e., a factor of 5.5E-3 reduction.

15. For the estimation of undetected holes above the fuel level during normal operation, the origination of the through-liner holes detected is assumed to occur at half the time interval between RHBFST inspections, not to exclude more than 25 years.

16. For the size of undetected through holes above the fuel level it, is conservatively estimated by averaging the four largest flow areas found at the final RHBFST inspection; i.e., at the end of the inspection interval.

17. The maximum operating fuel level is assumed at 212' for purposes of evaluating the probability of undetected through holes; i.e., including holes found in the lower dome, barrel, expansion areas, or the lower row of the upper dome. Through holes located further up in upper dome are excluded.

18. For RHBFST 15, a 1/8" hole was also found in the RHBFST's expansion area; i.e., just below the 212' level. It is assumed that the hole was not detected before shutting down for inspection because the actual fuel level did not cover it after the hole formed, or that the actual leakage rate did not exceed the minimum detectable leakage rate. Nevertheless, the detection of this through hole by an API 653 inspection is counted as being a hole below the fuel level and included in the count of incidents for evaluating the small leakage rate during normal operation.

19. The representative, undetected hole size is assumed to be a distribution of hole sizes with flow rates in a range below the minimum detectable rate in the annual leak tightness tests as these would not be detected during RHBFST operation. See Section 5.4.6 regarding chronic releases.

20. For the location of though holes in a RHBFST liner, the historical probabilities of through holes by RHBFST heights is used, except for through-hole events discovered during RHBFST returns to service, for which a liner area weighted location probabilities are used.

21. For pipe leakage or pipe break events, generic pipe leakage data from the Pipeline Risk Management Manual (Reference 5-1) along with the length of each pipe segment is applied in the QRVA.

22. Valve external leakage data from NUREG/CR-6928, Bayesian updated with Red Hill facility experience of no such events in the history of the facility is applied in the QRVA.

23. For the lower dome leak to rock initiators, the total pipe length is assumed approximately the same for all active RHBFSTs, 65 feet of 8-inch pipe, 65 feet of 18-inch pipe, and 54 feet of 32-inch pipe totaling 184 feet.

24. The nozzle leak frequency for each RHBFST considers the different number of fuel lines connected to the RHBFST and the corresponding number and type of valves involved; i.e., motor-operated or manual skin valves.

25. For chronic leakage rate estimates, two different hole growth models are postulated. Undetectable through holes are assumed to be present for the no-growth model, but have a probability of occurring per year in the hole-growth model. See Section 5.4.6 for a full description of the modeling assumptions.

26. For maintenance errors resulting in significant leakage events, they could occur when one of the fuel lines in the LAT is opened for valve maintenance, assumed to occur once on each fuel line every 10 years of operation. Selection of the wrong

component or piping segment could result in fuel being released from a fuel line that has not yet been drained.

27. Representative fuel evolution data was evaluated from a 90-day period of Red Hill specific fuel evolutions beginning January 1, 2017.

28. NUREG/CR-6928 (Reference 5-2) is assumed as the source of generic data for equipment failure mode failure rates.

29. The frequency and duration of offsite power events was determined solely from Red Hill specific historical evidence.

30. Elevator reliability data was evaluated from experiences in Australia; i.e., Reference 5-3.

31. Common cause parameter data developed by the NRC, documented in Reference 5-4, is applied in the QRVA for identical equipment in redundant systems.

## 5.3 QRVA Data Analysis General Methodology

The quantification of accident sequences requires a component database, which is developed by compiling data, selecting appropriate reliability models, establishing the parameters for those models, and then estimating the probabilities of component failures and the frequencies of initiating events. The data used in this subtask may be generic industry data or facility-specific data, or a combination of both. Guidance from the data analyst will assist in determining the level of detail to which to develop the facility-system models.

Two types of events identified during accident-sequence definition and system modeling must be quantified for the event and fault trees in order to estimate frequencies of occurrence for accident sequences: (1) initiating events (see Section 3.4.2 of NUREG/CR-2300) and (2) component failures, or primary events (see Section 3.5.3.1 of NUREG/CR-2300). This chapter describes how this quantification is performed.*

The quantification of initiating and primary events involves two separate activities. First the reliability model for each event must be established, and then the parameters of the model must be estimated. The quantification also involves various types of data analysis (e.g., a statistical analysis of event information), the use of generic and specific data, and in some cases, the collection and use of subjective data. The necessary data include component-failure rates, repair times, test frequencies and test downtimes, common-cause probabilities, and uncertainty characterizations. Also involved is the quantification of human errors, a subject not covered in this section because it is discussed in Chapter 4 of NUREG/CR-2300.

The objective of the task described in this chapter is to estimate the frequencies of the initiating events and the probability of the primary events identified in accident-sequence

* The numerical quantities obtained by the procedures of this chapter are in a very strict sense estimates; that is, these quantities should be considered judgments of the values for the numerical quantities of interest.

definition and system modeling (Chapter 3 of NUREG/CR-2300) and thus to develop a database for accident-sequence quantification (Chapter 6 of NUREG/CR-2300). It is important to note that the output of this task must be consistent with the general approach chosen and the tools to be used in accident-sequence quantification. Before this task is performed, a decision will have been made as to whether the QRVA will use a classical or a Bayesian framework for treating uncertainties. This decision will affect the way data are evaluated. In addition, the tools used in sequence quantification will also affect the data analysis, in that the data must be in a form compatible with the tools. For example, the data analysis may yield probability distributions for reliability models that cannot be exactly represented by any defined distribution (e.g., a gamma or a lognormal distribution), and yet the quantification tools require that all inputs be described by one of a set of predefined distributions. It will be the data analyst's job to make the data output fit this quantification requirement, by finding the "best" distribution to fit the actual result, and then to record any uncertainty (Chapter 12 of NUREG/CR-2300) that is thus introduced in the analysis. Hence, the task described in this chapter is closely linked with the tasks of Chapters 3, 6, and 12 of NUREG/CR-2300.

The development of a database for accident-sequence quantification is a multistep process involving the collection of data, the analysis of data, and the evaluation of appropriate reliability models. It produces tables that specify the quantity to be used for each event in the fault and event trees.

While the task of database development may seem to lie between the tasks of accident-sequence development and quantification (Chapters 3 and 6 of NUREG/CR-2300), it is most likely to be accomplished largely in parallel with accident sequence development.

The steps that need to be addressed in developing a database are outlined below, in the order the tasks would be accomplished. As in many engineering analyses, the order may be modified as the work progresses, or iteration may be required. It is also possible that time constraints, budget constraints, or study goals may allow, or even require, some steps to be shortened or bypassed. For example, instead of collecting and analyzing original event data, it may be sufficient to use data from a previous QRVA study. This could save considerable time and cost, but it may diminish confidence in the results. Figure 5-1 indicates the flow of the steps outlined below.

**Selection and Use of Event Models.** The data analyst must select several types of models for event quantification: failure models, maintenance models, test models, and initiating-event models. The factors to be considered in these decisions are discussed in Section 5.3 of NUREG/CR-2300.

**Data Gathering.** Early in the QRVA project, the gathering of all information that may be pertinent to events usually included in QRVA studies should begin. At this point the development of accident sequences will not have been completed, and hence this early information gathering must rely on previous experience. The information should include published data reports, data from other QRVA studies, and available information about the specific facility that is being analyzed. This task is described in Section 5.4 of NUREG/CR-2300.

**Estimation of Model Parameters.** After the models have been selected, their parameters must be evaluated. Two approaches to parameter estimation, the Bayesian approach and the classical approach, are described in Section 5.5 of NUREG/CR-2300.

**Evaluation of Dependent Failures.** It is generally recognized that dependent failures may make significant contributions to system unreliability. Section 5.6 of NUREG/CR-2300 addresses various methods available for estimating these contributions.

**Uncertainties in Data.** A major concern in a QRVA is the issue of uncertainty in the various evaluations. Section 5.7 of NUREG/CR-2300 discusses the factors in database development that contribute to uncertainty.

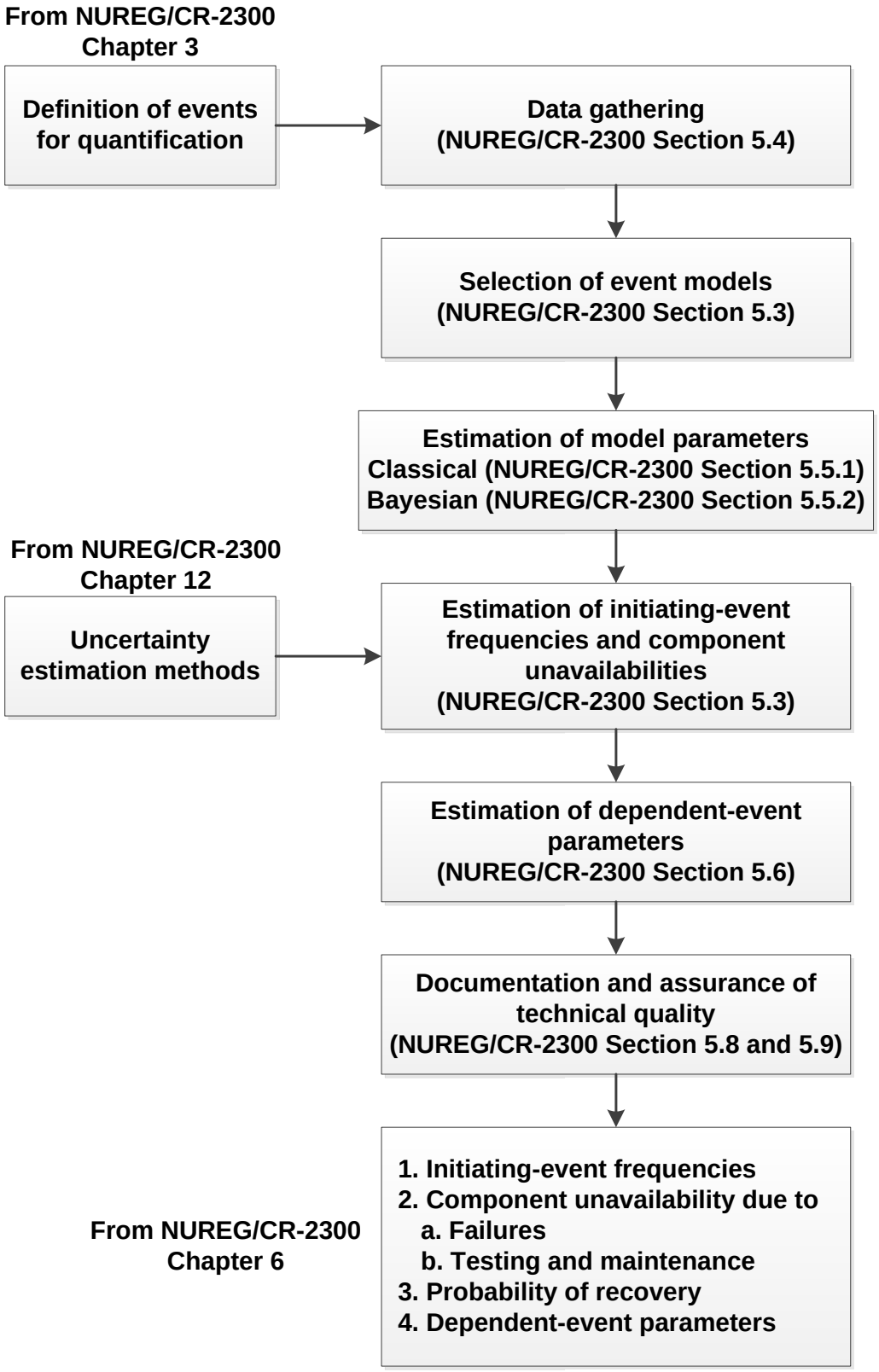



**Figure 5-1. Inputs, Outputs, and Steps in Database Development**

### 5.3.1 Generic Data Analysis

Before collecting and analyzing data, it is important to know what kind of data are needed. In a QRVA the events of interest are modeled as events that occur randomly. In general, they occur either randomly in time or randomly at each challenge. Thus, for each classification of events, data will be either x events in time T or x events in n trials (or demands). In addition, if it is necessary to test the component-reliability models, the actual time history of the failures is needed. More specifically, if the failure of motor-operated valves (MOV) to open when needed is a class of events to be evaluated, it will be necessary to search data sources to determine the number of occurrences for this event, either the number of demands or the time over which these events occurred, and when each failure to open occurred. It will also be useful to examine other databases for information about the event of interest.

In general, for events involving components in safety systems, the quantity of interest is the probability that the component cannot perform its intended function when the initiating event occurs.

Thus, the objective of the data-gathering task is to obtain the information needed for estimating the event-model parameters identified in the preceding section: (1) the number of failures in time or the number of demands for reliability models; (2) the frequency and duration of tests for systems or components; (3) the frequency and duration of maintenance on components; and (4) the frequency of initiating events. The data may also be used to test the applicability of the event model; in this case, it is necessary to have the time of each failure. The sources of data may include facility records, existing data reports, and previous QRVAs. This section describes various sources of available data and their attributes, it then discusses the process of data collection. It is strongly recommended that representative existing data sources be closely examined to establish clearly the type of data needed before beginning the collection of facility data.

Generic data may be available in many forms. The analyst may have original (unreduced) failure data or reduced failure-rate data in the form of point or interval estimates, percentiles, and so forth.

Two sources of generic failure-rate data that can be applied for analyses of fuel storage facilities are the OREDA Handbook (Reference 5-5) and NUREG/CR-6928 (Reference 5-2).

Another method of using original generic data for determining a prior distribution is described by Kaplan (Reference 5-6); it uses Bayes' theorem to determine the prior distribution.

#### *5.3.1.1 Initiating Event Frequency Determination*

Initiating events are the occurrences that initiate an accident sequence. The desired measure for such events is frequency. A facility may experience tens of these events per year or only one in 10,000 years.

Initiating events are assumed to occur randomly in time, and they are usually assumed to occur at a constant rate. However, data on events that occur more frequently indicate that the rate of occurrence may be higher during the facility's first years than during subsequent years. There are insufficient data to predict whether or not the frequency of these initiators might increase in later life.

For purposes of this chapter it is assumed that the model for initiating events will be based on a constant rate of occurrence (the Poisson model). In current state-of-the-art QRVA generic data references, such as NUREG/CR-6928, most initiating event frequency probability distributions apply the Gamma distribution, a practice that will generally be followed on this QRVA.

It should be noted that in most QRVAs initiating events are treated as single events. However, the initiating event can be quantified by combining several events. This combination can be accomplished through a fault tree, an event tree, or a similar tool. While this may not affect the underlying event modeling and data analysis, it may require quantification tools that differ from those used to evaluate system/sequence frequency-weighted unavailability via fault trees, event trees, etc. That is, it may be necessary to quantify the synthesized initiating event as a frequency, rather than a probability.

### *5.3.1.2 Component Failure Mode Failure Rate Determination*

Component-failure models can be divided into two general types: time-related models and demand models. This section defines both types of models and explains their application.

#### *5.3.1.2.1 Time-Related Models*

##### 5.3.1.2.1.1 Definition

Reliability as a function of time can be modeled by a number of probability distributions, the more common models being the exponential, the Weibull, the gamma, and the lognormal. Each represents a different type of failure process.

The exponential gives the distribution of time between independent events occurring at a constant rate. The Weibull gives the distribution of time between independent events occurring at a rate that varies in time. The gamma gives the distribution of time required for exactly k independent events to occur, assuming a constant rate of occurrence. An exponential distribution is a gamma with k = 1. The lognormal implies that the logarithms of lifetimes are normally distributed. There are also other models that provide for time-dependent failure rates, an example being the inverse Gaussian (Reference 5-7).

In most QRVA studies, the exponential is the most commonly used time-to-failure distribution. It is used basically for two reasons: (1) many reliability studies have found the exponential justifiable on empirical grounds and (2) both the theory and the required calculations are simple. It is important to note that, even though the time to failure is not exponential over the entire life of the component, the in-use portion may be exponential.

This assumes replacement by a component that is also in its exponential-behavior time period.

The validity of the assumptions underlying the choice of the exponential distribution can be examined by several methods. These methods are not discussed here because most QRVAs have not found it necessary to justify their choices of reliability models. Should there be a need to examine the time-to-occurrence distribution, the graphical methods described by Hahn and Shapiro (Reference 5-8) and the analytical methods described by Mann et al. (Reference 5-9) can be used.

In this section, the exponential distribution will be used to model the time to component failure. The equation for the exponential distribution is

$$U(t) = 1 - e^{-\lambda t} \tag{5.1}$$

which represents the cumulative probability that the event has occurred by time t. The parameter λ is the failure rate and is expressed in units of failures per unit time.

#### 5.3.1.2.1.2 Use of Time-Related Models

*Failure in Time: Standby*

Many components in a complex facility are in a standby mode. That is, they are not used until needed or tested. Often such components are assumed to fail in time while in this standby mode.

Standby components are usually subjected to periodic testing, which occurs, for example, once a month or perhaps once a year. The time between tests is the length of time the component is exposed to failure without detection, and hence the term "fault-exposure time". This time is often designated by τ. The fault-exposure time τ is usually determined from facility procedures, but some caution should be used when examining a system for test intervals. As an example, consider the system in Figure 5-2. This system is tested in various pieces, that is, the logic is tested once a month, as are the spray pumps.

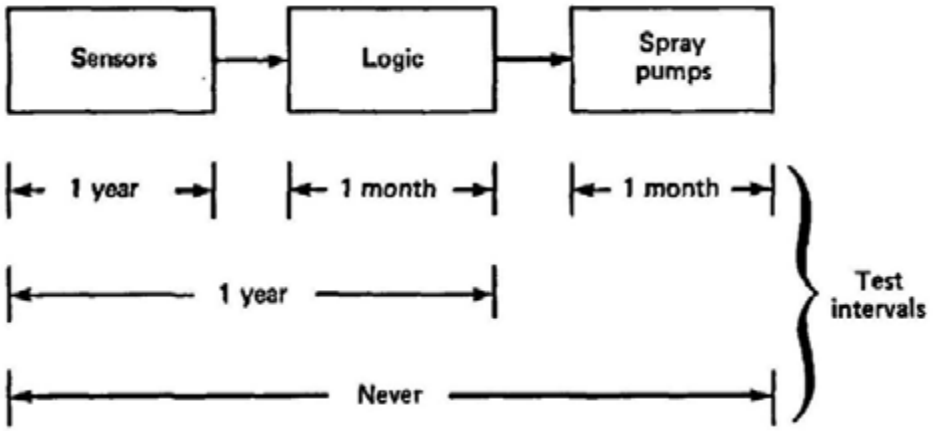



**Figure 5-2. Test Intervals for Sample System**

The sensors are calibrated once a year and are tested once a year through the logic. However, the entire system is never tested end to end. This results, in this example, in a specific contact never being tested during the life of the facility. Figure 5-3 focuses on this situation.

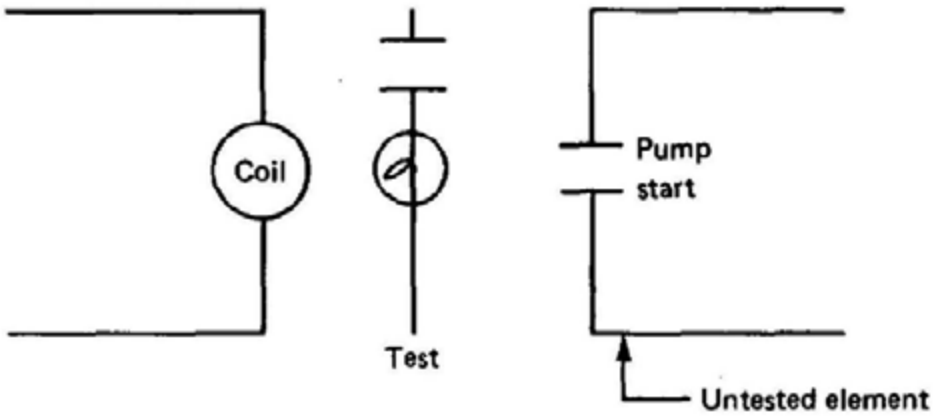



**Figure 5-3. Interface Schematic**

The logic testing verifies that the coil is energized when the test contact closes and the light is illuminated. However, the contact for pump start is not tested. The analyst then must decide on a value of $\tau$ for this contact that is not directly tested during the life of the facility. Please recall that $\tau$ represents the fault or failure mode exposure time for the analysis. Indeed, it may be deemed appropriate to assign a $\tau$ of 40 years. However, in this case a 40-year value for $\tau$ is inappropriate, because the contact is part of a relay that is tested in part and has an associated mean time to failure, thus, the relay will be periodically replaced and the untested contact will be renewed. It is therefore suggested that the $\tau$ for the untested element be the reciprocal of the mean time to failure of the tested elements in the relay combined through an OR operation.

In the present example, assume that the coil has a mean time to failure of 20 years and the tested contact has a mean time to failure of 5 years. These can be combined by adding the failure rate, defined to be the reciprocal of the mean time to failure, and then inverting the result, that is, $\tau = [(1/20) + (1/5)]^{-1} = 4$ years. Thus, it would be appropriate to use $\tau = 4$ years for the contact that is not directly tested.

After determining an appropriate $\tau$ for each component that is modeled to fail in time during standby, it is necessary to define the unavailability due to each component's random-failure distribution in time. The expression for the availability of a component that fails in time over a period $\tau$ is given by the cumulative distribution function of the time-to-failure distribution for that component. For example, if a component is found to have an exponential failure density function (i.e., $f(t) = \lambda e^{-\lambda t}$) where t is time and $\lambda$ is the associated failure mode failure rate (events per unit time), then the unavailability is given by:

$$U(t) = 1 - e^{-\lambda t}$$

However, the demand on the safety systems and components occurs randomly in time. Thus, it is necessary to evaluate the unavailability function during the fault-exposure time $\tau$. If it is assumed that the demand can occur with equal likelihood at any point in the $\tau$ interval, as it usually does, the unavailability that should be used is the frequency-weighted unavailability† over the time period $\tau$. Thus,

$$\overline{U} = \frac{1}{\tau}\int_0^{\tau} U(t)\, dt$$

or, for the exponential considered above,

$$\overline{U} = \frac{1}{\tau}\int_0^{\tau} \left(1 - e^{-\lambda t}\right) dt$$

$$= 1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$$

$$= \frac{\lambda\tau}{2!} - \frac{(\lambda\tau)^2}{3!} + \frac{(\lambda\tau)^3}{4!} - \cdots$$

$$\approx \frac{\lambda\tau}{2}$$

Note that the often-used approximation for the frequency-weighted component unavailability assumes that (1) the failure density function is exponential and (2) higher-order terms of the exponential are negligible.

*Failure in Time: Annunciated*

For some components, failure is detected immediately; e.g., an annunciated failure. The probability that such a component is not available if needed is related to the frequency of failure and the average time needed to return the component to service. This unavailability is given by:

$$U = \frac{\lambda T}{1 + \lambda T}$$

where $\lambda$ is the failure rate and T is the average total time to respond to the failure, repair the component, and return it to service. Note that if $\lambda T$ is much smaller than unity, the unavailability may be approximated:

$$U \approx \lambda T$$

† The term "frequency-weighted unavailability" is used here to distinguish between this quantity and a similar quantity, average (un)availability. See a reliability text, such as that by Barlow and Proschan (Reference 5-10), for the definition and use of the term "average availability".

*Failure in Time after Successful Start*

It is often necessary to evaluate the probability of a component's starting successfully but failing in time before completing its mission. The mission time is here designated $\tau^*$. The probability that a component fails before $\tau^*$ is given by the cumulative distribution function. For the exponential case,

$$R(\tau^*) = 1 - e^{-\lambda\tau^*}$$

$$\approx \lambda\tau^*$$

It should not be assumed that the failure rate λ in this case is the same as the failure rate in standby. Indeed, in estimating the rate for failures occurring after a successful start, the analyst must take into account any adverse environment as well as recognize differences between the rates of standby and operation failures.

Often, failure to start on demand and failure to run for some time $\cdot\tau^*$ are both included in the tree. It must be noted that failure to run is dependent on a successful start; that is, the probability of failure to run for $\tau^*$ hours must be modified by the probability of successful start. There are two possible approaches to modeling this combination in the fault trees: (1) as dependent events or (2) as one event.

If failure to start and failure to continue running after starting are separate events, they should be modeled as mutually exclusive events (see Figure 5-4).

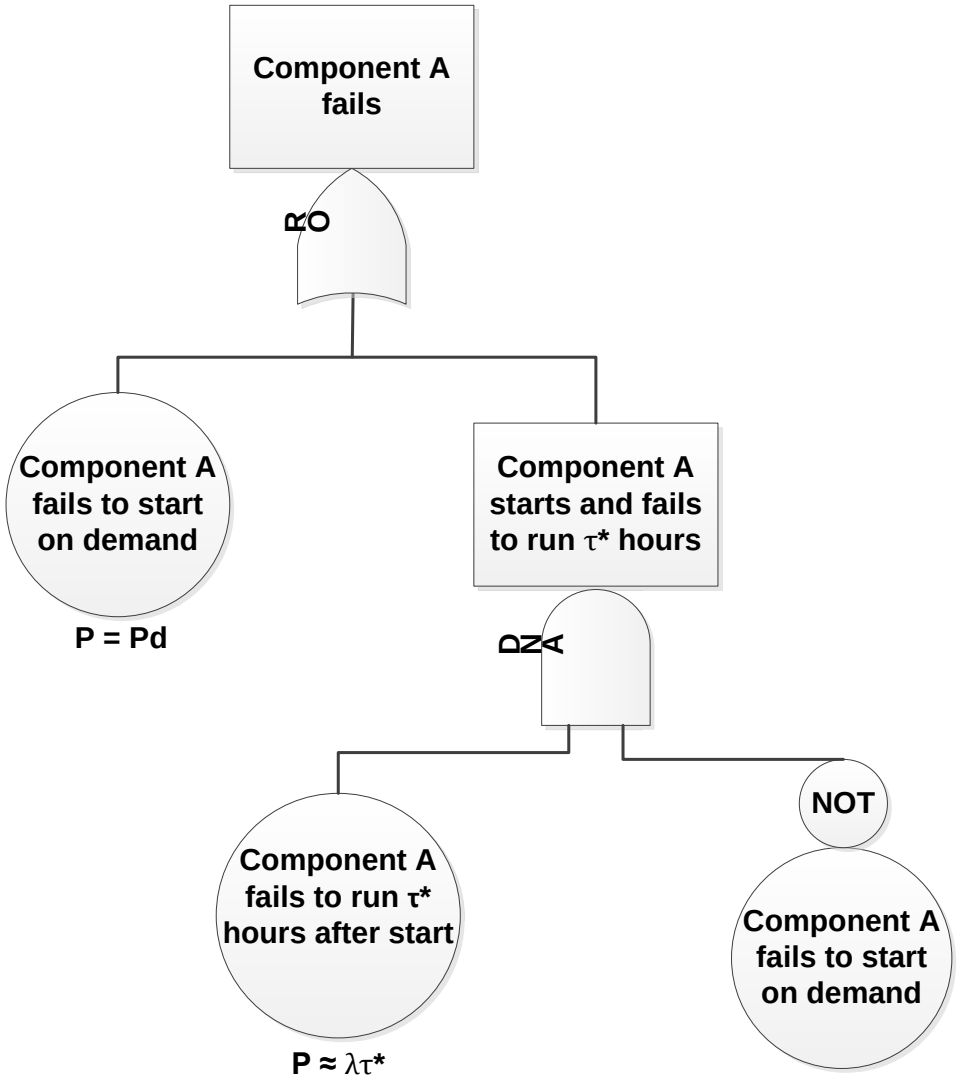



**Figure 5-4. Modeling of Mutually Exclusive Events**

If both modes are treated as one event, then

$$P_E = P_F + (1 - P_F)\lambda\tau^*$$

That is, the model accounts for the probability of failure to start on demand plus the probability of a successful start and failure to run for $\tau^*$ hours.

*Recovery*

It is possible that some events can be reversed in time to prevent loss of fuel inventory control. There are data that provide recovery times for the loss of offsite power (LOOP) and emergency power. For accident sequences that are initiated by a loss of offsite power and the subsequent failure of all emergency diesels, recovery within a specified time can prevent loss of fuel inventory control.

Such events can be broken into two parts: (1) frequency of loss or failure and (2) probability of recovery by time t, given loss or failure. This process is illustrated by the example given below, using point estimates. The data used in this example should not be taken for an actual assessment, though the results should be comparable with those of an actual assessment.

*Example: Total Loss of AC Power (station blackout)*

**Loss of Offsite Power.** The distribution for the duration of an offsite-power loss is given below. The data were collected from 46 sites where 45 losses occurred in 313.03 site-years, the rate of loss being .144 per site-year.

| Duration (hours) | Percentage of Events |
|---|---|
| <2 | 70 |
| 2 to 4 | 3 |
| 4 to 8 | 15 |
| >8 | 12 |

**Diesel Failure.** Data from 36 facilities were used to estimate the failure of diesel generators to start. If a configuration of three diesels is assumed and one diesel is needed for an adequate supply of power, the relevant probabilities for failure to start are as follows:

$$P(\text{diesel 1 fails to start}) = .0261$$

$$P(\text{diesel 2 fails to start} \mid \text{diesel 1 has failed}) = .234$$

$$P(\text{diesel 3 fails to start} \mid \text{diesels 1 and 2 have failed}) = .552$$

$$P(\text{all three diesels fail to start}) = .00337$$

The repair-time probabilities are

$$P(\text{diesel not repaired within 2 hours}) = .66$$

$$P(\text{diesel not repaired within 4 hours}) = .47$$

$$P(\text{diesel not repaired within 8 hours}) = .23$$

**Probability of Station Blackout Given Duration.** First we define the following:

D = duration of station blackout

L = duration of loss of station power

G = duration of diesel unavailability

S = event station blackout occurs in a year

Then for some period of time t,

$$P(D > t|S) = P(L > t \text{ AND } G > t|S)$$

$$= P(L > t|S)P(G > t|S) \text{ (assuming independence)}$$

If $F_D$ is the failure of all diesels on demand and $F_L$ is the loss of offsite power in a year, then assuming independence between diesel and offsite-power failures,

$$P(S) = P(F_D)P(F_L)$$

The probabilities being

$$P(F_L) = .144$$

$$P(F_D) = .0034$$

and

$$P(S) = 4.9 \times 10^{-4}\text{yr}^{-1}$$

Then

$$P(S \text{ and } D > t) = P(D > t|S)P(S)$$

For t = 2 hours:

$$P(S \text{ and } D > t) = (.30)(.66)(4.9 \times 10^{-4})$$

$$= 9.7 \times 10^{-5}\text{yr}^{-1}$$

For t = 4 hours:

$$P(S \text{ and } D > t) = (.27)(.47)(4.9 \times 10^{-4})$$

$$= 6.2 \times 10^{-5}\text{yr}^{-1}$$

For t = 8 hours:

$$P(S \text{ and } D > t) = (.12)(.23)(4.9 \times 10^{-4})$$

$$= 1.3 \times 10^{-5}\text{yr}^{-1}$$

*5.3.1.2.2 Demand Model vs. Time-to-Failure Model*

Another type of model for describing component failures is the demand model. It is used to describe the failure of a component at the time of a demand for its use. The number

of failures in n trials is described by the binomial distribution, and the demand model is appropriate for components that are in a dormant state until the moment of need, when they are switched on. The underlying assumption is that at each demand, the probability of failure is independent of whether or not a failure occurred at any previous demand. The demand model is one that will be carried through this chapter and has been commonly used in QRVAs.

The equation for the binomial distribution is as follows:

$$\Pr(X \le r) = \sum_{x=0}^{r} \binom{n}{x} p^x (1-p)^{n-x} \quad (5.2)$$

It gives the probability of r or fewer failures in n independent trials, given the probability of failure in a single trial is p. The parameter needed in this model is p, the probability of failure at each demand. It is important to note that, in this example, to be consistent with NUREG/CR-2300, the P(S) values are presented in terms of "probability per year". These values can be more appropriately expressed as frequency values (in events per unit time or, in this case, events per year).

Several very important factors should be taken into account when using the demand model. If the event being considered really could occur before the demand, then using the demand model "lumps" the failure rate into the instantaneous time of the demand. Thus, for different demand rates the probability of failure would actually be different, and if the demand model is used, a reasonable estimate is obtained only if the demand rates are similar. A component that behaves exactly as the demand model will have the same probability of failure on demand whether the demand occurs once per hour or once per decade.

The relationship between a failure-on-demand model and a failure-in-time model (assuming a constant failure rate) can easily be seen mathematically. The following assumptions are typical of this situation:

1. Component failures can be detected only at tests that occur every $\tau$ hours.

2. Components found failed are immediately repaired or replaced, components found operable are returned to service in working condition.

The data from such a situation yield x failures in N tests. The probability of failure on demand is P = x/N. Note that the results from successive tests are independent and that the exponential distribution allows a component to be considered as good as new after the test. Thus the number of tests failed has a binomial distribution with parameters N and $1 - e^{-\lambda t}$. The maximum-likelihood estimate (MLE) of $1 - e^{-\lambda \tau}$ is x/N, and thus the MLE of λ is

$$\hat{\lambda} = \frac{1}{\tau} \ln(1 - P)$$

For small P, $\hat{\lambda} \approx P/T$, which is the usual estimate for $\hat{\lambda}$. However, this approximation is nonconservative. For example, if half the tests are failed,

$$\hat{\lambda} = \frac{\ln 2}{\tau} = \frac{0.69}{\tau}$$

where the approximation yields

$$\hat{\lambda} \approx 0.5/\tau$$

If it is necessary to obtain a new probability of failure on demand, $P_1$, for a new test period $\tau_1$, the above relationships must be considered. The new demand probability is

$$\hat{P_1} = 1 - \exp(-\hat{\lambda}\tau_1)$$

$$= 1 - \exp\left[-\frac{\tau_1}{\tau}\ln(1-P)\right]$$

$$= 1 - (1-P)^{\tau_1/\tau}$$

For example, if P = 1 x $10^{-2}$, $\tau$ = 720 hours (1 month), and $\tau_1$ is 1 year, then $\tau_1/\tau = 12$, and

$$\hat{P} = 1 - [1 - (1x10^{-2})]^{12} = 1.14x10^{-1}$$

*5.3.1.2.3 Test Contributions to Component Unavailability*

Some test activities render a component or group of components unavailable to the system should a demand occur. Such an activity should appear on the appropriate tree as a separate event.

The probability that a component will be in testing when a demand occurs is simply the frequency of the test multiplied by the average duration of the test, normalized by the time between the start of tests. For example,

$$P_T = \frac{(1\ \text{test/month})(L_T\ \text{hr})}{730\ \text{hr/month}}$$

Here $L_T$ is the average length of a test that occurs once every month.

The model often used in QRVAs for the time to complete a test is the lognormal distribution. Although this assumption has not been extensively tested, several studies have found the lognormal distribution to provide a reasonable fit (References 5-11 through 5-13).

The equation for the lognormal distribution is

$$C(t) = \frac{1}{\sigma\sqrt{(2\pi)}}\int_{-\infty}^{\ln t}\exp\left[-\frac{(y-\mu)^2}{2\sigma_2}\right]dy\ \sigma^2 \qquad (5.3)$$

This equation represents the cumulative probability that the event has been completed by time t. The parameters σ and μ can be expressed in other terms:

$$\mu = \ln M$$

$$\sigma = \frac{\ln(EF)}{1.64}$$

where the parameter M is the median time to completion and the error factor EF is the quantity that, when multiplied by the median, gives the time of completion that is equal to or longer than 95% of all times to complete the event.

Sections 5.5.1 and 5.5.2 of NUREG/CR-2300 show how to estimate the parameters of a lognormal time-to-completion distribution as either distributions or point estimates with confidence limits. Methods for propagating these uncertainty measures can be found in Chapter 12 of NUREG/CR-2300. These methods can be used to estimate the distribution or point estimate with confidence limits for $P_T$ from the parameter distributions or point estimates and confidence limits. The quantity $P_T$ is then the input required for the accident-sequence quantification discussed in Chapter 6 of NUREG/CR-2300. Depending upon facility-specific historical data, a normal distribution or triangular distribution can also be applied for the time to complete a test.

#### *5.3.1.2.4 Maintenance Contributions to Component Unavailability*

A maintenance act is considered to be any unscheduled activity that causes a component or system to be taken out of service. It may be expected that repair takes place, but this repair may vary from the very simple to the very complex.

The evaluation of the maintenance contribution is similar to that of testing, except that maintenance acts occur randomly in time, whereas for tests the time is fixed. The Reactor Safety Study (Reference 5-12), for example, found that the time of maintenance for all components could be modeled by a lognormal distribution with 5$^{th}$ and 95$^{th}$ percentile points of 1 and 12 months, respectively. In most cases, it may be expected that the frequency of maintenance will exceed the frequency of failure for a component in the fault tree because the number of component failures requiring maintenance far exceeds the number of failures that completely negate a component's ability to function in its safety role. A good example is a motor-operated valve that must open to successfully perform its safety role. Failure to open occurs less frequently than valve-stem leaks, which require the valve to be taken out of service for repacking, but do not directly negate the safety role of the valve.

The probability that a component is in maintenance when a demand occurs is shown below as:

$$P_M = \frac{f_M L_M}{1 + f_M L_M}$$

In this expression, $f_M$ is the average frequency of required maintenance and $L_M$ is the average length of the maintenance.

The lognormal distribution (see Equation [5.3]) can be used for the time to complete maintenance, while the frequency of occurrence may be lognormal or exponential. Sections 5.5.1 and 5.5.2 of NUREG/CR-2300 show how to estimate the parameters of both the lognormal and the exponential distributions as either distributions or point estimates with confidence limits. Chapter 12 of NUREG/CR-2300 gives the methods for propagating the distribution or point estimate with confidence limit parameters to the event $P_M$, which will then be a distribution or a point estimate with confidence limits. The quantity $P_M$, then, is the required input for accident-sequence quantification (Chapter 6 of NUREG/CR-2300). Depending upon facility-specific historical data, a normal distribution or triangular distribution can also be applied for the time to complete a maintenance action.

#### *5.3.1.3 Facility-Specific Data Collection, Review, and Interpretation*

At present, few complex facilities (except for nuclear power facilities) keep records of component reliability for the specific purpose of using them as data for risk assessments. The QRVAs that have been conducted to date have had to depend on other sources for facility-specific data. These sources include many facility records and procedures that may be available to the QRVA analysts. The usefulness of a particular source depends on the reliability models chosen to represent components in system fault trees. On the other hand, the availability (or the absence) of various data sources may affect the choice of models by a system analyst. Table 5-1 lists the most common parameters used to represent components, the data required to derive estimates of the parameters, and the potential sources of such data at facilities. How these sources can be used to extract needed information is briefly explained below.

**Table 5-1. Sources of Facility Data**

| Parameter | Data Requirements | Potential Sources |
|---|---|---|
| 1. Probability of failure on demand | a. Number of failures | Periodic test reports, maintenance reports, control-room log |
| | b. Number of demands | Periodic test reports, periodic test procedures, operating procedures, control-room log |
| 2. Standby failure rate[a] | a. Number of failures | See 1a above |
| | b. Time in standby | Control-room log |
| 3. Operating failure rate[a] | a. Number of failures | See 1a above |
| | b. Time in operation | Control-room log, periodic test reports, periodic test procedures |
| 4. Repair-time distribution parameters | Repair times | Maintenance reports, control-room log |
| 5. Unavailability due to maintenance and testing | Frequency and length of test and maintenance | Maintenance reports, control-room log, periodic test procedures, periodic test reports |
| 6. Recovery | Length of time to recover | Maintenance reports, control-room log |
| 7. Human errors[b] | a. Number of errors | Maintenance reports, control-room log, periodic test procedures, operating procedures |
| | b. Opportunities | |

[a] *See Section 5.3.1.2.1.*

[b] *While this chapter does not deal with the evaluation of human errors, it is likely that a search for facility-specific data would find human-error data to supplement the analysis methods described in Chapter 4 of NUREG/CR-2300.*

#### *5.3.1.3.1 Periodic Test Reports and Procedures*

Periodic test reports and procedures are a potential source of data on failures, demands, and operating time for components that are tested periodically. Test reports for key components or systems typically contain a description of the test procedure and a checklist to be filled out by the tester as the steps are performed. For example, in an operating test of an emergency diesel generator, the procedure may call for starting the diesel and running it for an hour. The record of a specific test would report whether or not the diesel started and whether it ran successfully for the entire hour. Another example is a test of emergency system performance, in which the procedure calls for the tester to give an emergency signal that should open certain flow paths by moving some motor-operated valves and starting one or more pumps. The position of the valves and the operation of the pump are then verified, giving records of whether the valves and

pumps responded successfully to the demands. As shown by these examples, records of periodic tests provide a self-contained tally of demands on some components, as well as the failure (and success) of the component given these demands.

When failures are reported in periodic tests, however, the failure mode should be examined carefully, if possible, before the failure is included in a failure-parameter estimate to be used in system fault trees. In the diesel-generator example, the report may note that the result of the test was unsatisfactory because the diesel tripped on a signal of low oil pressure, high oil temperature, or the like. If any of these trips are disabled by a facility-specific accident signal, such an event should not be counted in deriving a failure-parameter estimate for a fault tree that is part of that facility-specific accident sequence, even though the test report indicated an unsatisfactory performance by the diesel generator. If, on the other hand, the diesel would have failed if the trip was bypassed, it must be counted as a failure. Similarly, a test report on diesel-generator operability may log an unsatisfactory result due to an air-compressor failure. Such a failure would cause a diesel-generator failure to start only if it occurred in conjunction with a leak in the diesel air tank. In this instance, the test report indicates a failure even though no actual demand was placed on the diesel.

If the records of actual periodic tests are not readily available, the test procedures can be used to estimate the number of testing demands or the operating time during tests for a component over a period of time. To do this, the number of demands or the operating time of a single test can be multiplied by the frequency of the test and the pertinent calendar time. Of course, this approach is valid only if the tests are conducted at the prescribed frequency. Some tests may in fact be conducted at more frequent intervals than those stated in the procedures. Facility personnel should be interviewed to determine what adjustments are necessary.

If this approach is used, a count of failures must be obtained from different sources; e.g., maintenance reports. Since these sources may not indicate clearly which failures occurred during the periodic tests considered, the failure-parameter estimates derived by this approach are probably conservative. In order to correctly match failures with demands or operating time for a component, the number of demands or the duration of operating time occurring outside periodic tests must be obtained. Such information is usually much more difficult to extract from typically available data sources.

#### *5.3.1.3.2 Maintenance Reports*

Reports of maintenance on components are potential sources of data on failures, repair times after failure, and other unavailability due to maintenance. These reports typically include the following:

1. A facility identification number for the component undergoing maintenance and a description of the component.

2. A description of the reason for maintenance.

3. A description of the work performed.

4. An indication of the time required for the work or the duration of the component's unavailability.

The report may indicate that maintenance was needed because the component failed to operate adequately or was completely inoperable. Such an event may then be added to the count of component failures. The maintenance report often gives information about the failure mode and mechanism as well as the amount of time spent on repair after the failure was discovered.

Such information must be interpreted carefully, because the actual repair time may cover only a fraction of the time the component was unavailable between the detection of the failure and the completion of repairs. In addition, the repair time is often given in terms of man-hours, which means that the actual time spent on repair could be shorter, depending on the size of the work crew; the use of recorded man-hours would therefore lead to a conservative estimate of repair time. The complete out-of-service time for the component can, however, be derived, because the maintenance record often states the date on which the failure was discovered and the date on which the component was made available after repair.

Maintenance reports that record preventive maintenance can be used to estimate the contributions of these actions to component unavailability. Again, the report may show that a component was taken out of service on a certain date and restored some time later, giving a sample of the duration of maintenance. The frequency of these events can be derived from the number of preventive-maintenance reports in the calendar time considered.

Not all maintenance reports present all of the information listed above. Often, the descriptions of a component's unavailability or the work performed are unclear (or missing altogether), requiring engineering judgment as to whether an unfailed component was made unavailable by maintenance or whether the maintenance was the result of component failure. An additional problem that has already been mentioned is the difficulty in matching up the failures recorded in maintenance reports with the demands or operating times reported in other documents.

#### *5.3.1.3.3 Operating Procedures*

Operating procedures can be used to estimate the number of demands on certain components in addition to demands occurring during periodic tests. This estimate is obtained by multiplying the number of demands imposed on a component during a procedure by the number of times the procedure was carried out during the calendar time of interest. Unfortunately, the latter number is not always easily obtained. For procedures followed during facility fill or supply operations, the number of times the procedure was performed should be readily obtainable, but for procedures followed during operation, this information will be available only from the control-room log.

#### 5.3.1.3.4 Control-Room Log

Many of the gaps in a component-reliability database compiled from test and maintenance records can be filled by examining the control-room log, which is a chronological record of important events at the facility. For example, the log may have records of demands made (e.g., pumps and diesel generators) at times other than periodic tests. It may note the starting and stopping times for these components, thus supplying operating-time data. The log may also note the initiation of various operating procedures, thus adding to the information about demand. Furthermore, it may record periods when certain components and systems are out of service, and therefore this the log is often more accurate than the maintenance reports.

There is, however, a problem with using the control-room log as a source of component data: all events in the log are listed chronologically, without being separated by system, type of event, or any other category. The analyst must therefore search through many irrelevant entries to find those needed for the database. The additional accuracy that is supplied to the estimates of component-failure parameters by data from the log may not be worth the effort needed to search through several years of the facility history recorded in the log.

### 5.3.1.4 Bayesian Updating of Generic Data with Facility-Specific Evidence

After model selection, the parameters of the models can be estimated. Two methods of estimation are described in this chapter and are complemented by the relevant methods in Chapters 6 and 12 of NUREG/CR-2300: (1) classical methods and (2) Bayesian methods.

A Bayesian analysis allows the augmentation of available data by quantified personal judgment. The analyst quantifies his belief about the parameters (unknown constants) in the model, exclusive of the information in the data, by a probability distribution, that is, he not only models the occurrence of accidents probabilistically but also develops a probability model for his beliefs about such occurrences.

In a classical analysis, knowledge and expertise also play a role, but less formally, in general serving only as aids in choosing probability models and relevant data. For example, data obtained under normal operating conditions may or may not be applicable to accident conditions. An understanding of the situation is needed to resolve this question. Once such questions are resolved, a classical analysis lets the data “speak for themselves”. The users of a classical analysis must be aware that limited data can lead to imprecise estimates. Though the introduction of a quantified degree of belief can improve the apparent precision of risk estimates, it may be useful and informative to do both a Bayesian and a classical analysis for comparison purposes.

#### 5.3.1.4.1 Classical Estimation

##### 5.3.1.4.1.1 Point Estimation

Reliability and availability models involve a variety of parameters, such as component-failure rates and expected repair times that need to be estimated in order to estimate the probability of specific accident sequences. Choosing a point estimate can involve a

variety of considerations, depending on the information available. If data are available and it is desired to obtain estimates that are strictly functions of the data, then, for the models commonly used in risk analysis, point estimators are well established. The point estimators generally used for the binomial, Poisson, and lognormal models, and appropriate data, are given below.

**Binomial Distribution.** The data, parameter, and estimate for binomial models are as follows:

Data: f failures in n demands. The number of demands is known, the outcomes, success or failure, are statistically independent, and the failure probability is constant across these demands.

Parameter: p, the probability of failure on demand (dimensionless).

Estimate:

$$p^* = f/n$$

**Poisson Distribution.** For Poisson models, the data, parameter, and estimate are the following:

Data: f failures (or occurrences of an initiating event) in T time units. The quantity T is known; failures occur independently and at a constant rate in time and across different items, which may be combined to obtain the data.

Parameter: λ, the failure rate (number of failures per unit time).

Estimate:

$$\lambda^* = f/T$$

**Lognormal Distribution.** The data, parameters, and estimates for lognormal models are as follows:

Data: n independent positive observations, $x_1, x_2, \ldots, x_n$, such as failure rates, whose logarithms are modeled as being normally distributed.

Parameters: μ, the expected value of $t = \log_e(X)$ and $\sigma^2$, the variance of t.

Estimates:

$$\mu^* = \sum_{i=1}^{n} \frac{t_i}{n} = \bar{t} \text{ for the sample mean}$$

$$\sigma^{2*} = \frac{\sum(t_i - \bar{t})^2}{n-1} = s_t^2 \text{ for the sample variance}$$

All the estimates given here are unbiased, which means that, on the average, they equal the parameter being estimated. Moreover, all but $\sigma^{2*}$ are maximum-likelihood estimators. Additional details pertaining to these estimates are available in a text by Mann et al. (Reference 5-9), which also provides statistical estimators for other models,

such as the Weibull and gamma distributions, and other situations, such as a fixed number of failures/random operating-time estimates of the failure rate λ.

Classical point estimates are attempts to identify single parameter values indicated by the data. As such, they are data summaries, and information is necessarily lost in the summarization. The loss is serious in the case of point estimation because the amount of data going into the estimates is lost. For example, one failure in 10,000 hours yields the same point estimate of a failure rate as do ten failures in 100,000 hours, but clearly more information is present in the latter case. If this information is ignored or not communicated, an incomplete analysis results. Two classical methods by which the amount of information pertaining to parameters of interest can be conveyed are standard errors and statistical confidence intervals.

#### 5.3.1.4.1.2 Standard Errors

If the data-yielding process described above is repeated, the parameter estimates will vary; that is, in another n demands or T time units, the number of failures will vary (in a manner described by the probability models used to analyze those data). Furthermore, then repair times collected in the future would differ from those observed at present. The variance over such repetitions of the estimators described above provides a measure of the information contained in the point estimates obtained. The larger the variance, the less reliable the point estimate. In general, the variance of an estimator is not known, but it can be estimated in these cases. The square root of the estimated variance of an estimator is termed the "standard error of the estimate". For the parameters considered in the preceding section, the standard errors (s.e.) are as follows:

Binomial:

$$\text{s.e. } (p^*) = \left[\frac{p^*(1-p^*)}{n}\right]^{1/2}$$

Poisson:

$$\text{s.e. } (\lambda^*) = \left(\frac{\lambda^*}{T}\right)^{1/2}$$

Lognormal:

$$\text{s.e. } (\mu^*) = \frac{\sigma^*}{n^{1/2}}$$

$$\text{s.e. } (\sigma^{2*}) = \sigma^{2^*}\left(\frac{2}{n-1}\right)^{1/2}$$

(The information contained in an estimated variance is usually conveyed by reporting the degrees of freedom, n - 1 in the case considered here, rather than a standard error.)

One way in which standard errors are used is to obtain approximate classical confidence limits on the parameter of interest. For example, the point estimate plus or minus twice its standard error provides a crude 95-percent confidence interval on the parameter.

Thus, a large standard error, relative to the point estimate, indicates that the data do not provide a very clear indication of the parameter. If only a point estimate is given, this information about the data is lost, and an unwarranted and misleading aura of precision may result. Without standard errors, any comparison of point estimates, say for the purpose of ranking accident sequences, may be misleading.

#### 5.3.1.4.1.3 Interval Estimation

A given set of data, say f failures in T hours, can occur in sampling from a variety of Poisson distributions. That is, many other values of λ besides λ* = f/T can give rise to this particular outcome. Some values of λ, however, are more consonant with the data than others. This realization is the basis for classical confidence intervals, whose purpose is to identify ranges of parameter values that are consonant with the data to some specified extent. For example, suppose an upper 95% limit on λ is found to be $\lambda_{95} = 10^{-4}$ failures per hour. This means that, for λ values greater than $10^{-4}$, the observed data are in the extreme 5% of possible outcomes; such λ values are not very consistent with the data. Values of λ less than $10^{-4}$ are less inconsonant with the data. Both upper and lower confidence limits, at any specified confidence level, can be obtained, and the interval between these limits is termed a "classical confidence interval". Classical confidence intervals have the property that, in repeated sampling, the probability that the confidence interval will contain the parameter of interest is at least at the specified confidence level.

As indicated above, approximate confidence intervals on a parameter can be obtained from a point estimate and its standard error. For the three distributions considered here, though, exact confidence limits or better approximations can be readily obtained.

*Binomial Distribution*

The upper 100(1 - α)% confidence limit on p is obtained by solving

$$\alpha = \sum_{x=0}^{f} \binom{n}{x} p^x (1-p)^{n-x}$$

for p. The lower 100(1 - α)% confidence limit on p is obtained by solving

$$\alpha = \sum_{x=f}^{n} \binom{n}{x} p^x (1-p)^{n-x}$$

for p. Tables, calculators, and computer programs are available for solving these equations (References 5-14 and 5-15). A useful approximation for small f, large n is

$$P_U(1-\alpha) = \frac{\chi^2(2f+2;\,1-\alpha)}{2n}$$

$$P_L(1-\alpha) = \frac{\chi^2(2f;\,\alpha)}{2n}$$

where $P_U(1 - \alpha)$ and $P_L(1 - \alpha)$ are the upper and the lower 100(1 - α)% confidence limits, respectively, and $x^2(m, \gamma)$ denotes the 100 γ-percentile of the chi-squared distribution with m degrees of freedom. The interval between $P_L(\alpha)$ and $P_U(\alpha)$ constitutes a 100(1 - 2α)% confidence interval.

*Poisson Distribution*

The upper and the lower 100(1 - α)% confidence limits on λ are obtained by solving the following equations:

$$\lambda_U(1-\alpha) = \frac{\chi^2(2f+2;1-\alpha)}{2T}$$

$$\lambda_L(1-\alpha) = \frac{\chi^2(2f;\alpha)}{2T}$$

Note that, mathematically, confidence limits on a failure rate λ are similar to those on a failure probability p, with time units replacing the number of demands.

*Lognormal Distribution*

The upper and the lower 100(1 - α)% confidence limits on μ. are obtained from

$$\bar{t} \pm t(n-1,1-\alpha)\left(\sigma^*/n^{1/2}\right)$$

where t(f, γ) denotes the γ-percentile of the Student's t distribution with f degrees of freedom.

For the upper and the lower 100(1 - α)% confidence limits on $\sigma^2$, the following equations are used:

$$\sigma_U^2(1-\alpha) = \frac{(n-1)\sigma^{2*}}{\chi^2(n-1,\alpha)}$$

$$\sigma_L^2(1-\alpha) = \frac{(n-1)\sigma^{2*}}{\chi^2(n-1,1-\alpha)}$$

As already discussed, classical confidence intervals supplement point estimates as a summary of the database information about the parameters of a probability model. They also serve to provide guidance on the parameter ranges that should be covered in a sensitivity analysis (see Chapter 12 of NUREG/CR-2300). That is, if one is interested in the change in an accident-sequence probability that results from a change in a component parameter, confidence intervals provide a plausible range over which the component parameter should be varied.

Occasionally, in QRVAs classical confidence limits are misinterpreted as percentiles on a probability distribution of the parameter. Because confidence limits are derived under the assumption that these parameters are constants, not random variables, such an interpretation is unwarranted, except perhaps as a Bayesian degree-of-belief distribution, given a uniform prior distribution. One reason confidence limits are given a

distributional interpretation is to provide input to probabilistic uncertainty analyses (Chapter 12 of NUREG/CR-2300). One could view such an analysis as a mathematical device for obtaining approximate classical confidence limits on an accident-sequence probability, given data pertaining to the parameters in the accident model, but better methods are available (Chapters 6 and 12 of NUREG/CR-2300). One particular treatment of confidence limits that should be avoided is the fitting of distributions to classical confidence limits on failure rates or probabilities.

An example of the application of classical techniques is included in Section 5.5.2.5 of NUREG/CR-2300, where the result can be compared with Bayesian treatments of the same data.

#### *5.3.1.4.2 Bayesian Estimation*

The Bayesian approach is similar to the classical approach in that it yields "best" point estimates and interval estimates, the intervals representing ranges in which, we are confident, the parameter really lies. It differs in both practical and philosophical aspects, though. The practical distinction is in the incorporation of belief and information beyond that contained in the observed data; the philosophical distinction lies in assigning a distribution that describes the analyst's belief about the values of the parameter. This is the so-called prior distribution.

The prior distribution may reflect a purely subjective notion of probability, as in the case of a Bayesian degree-of-belief distribution, or any physically caused random variability in the parameter, or some combination of both. Physically caused random variations in a parameter like a failure rate may stem from facility and/or system effects, operational differences, maintenance effects, environmental differences, and the like. The distribution that describes this physically caused random variation in the parameter is sometimes referred to as the "population variability" distribution (Reference 5-16) and can be represented by a Bayesian prior distribution. However, such random variation in the parameter can also be modeled by classical methods, using compound distributions in which the population-variability distribution becomes the mixing distribution. On the other hand, if the prior distribution embodies subjective probability notions regarding the analyst's degree of belief about the parameter, the Bayesian method is the appropriate framework for making parameter estimates. A comparative discussion of both interpretations of the notion of probability, the subjective and the relative-frequency notions, is given by Parry and Winter (Reference 5-17).

Whether the analyst does or does not have objective relative-frequency data, he will often have other information based on engineering designs, related experience in similar situations, or the subjective judgment of experienced personnel. These more or less subjective factors will also be incorporated into the prior distribution—that is, into the description of his prior knowledge (or opinions) about the parameter.

The Bayesian method takes its name from the use of Bayes' theorem and the philosophical approach embodied in the 18$^{th}$-century work of the Rev. Thomas Bayes (Reference 5-18). Bayes' theorem (see Section 5.3.1.4.2.1.2) is used to update the prior distribution with directly relevant data. Here the term "generic data" will be used to refer to parameter-related information that is nonspecific to any particular facility or application, being an aggregation over more than one use condition. A prior distribution

is often based on such generic data sources (Reference 5-16). A QRVA for a particular facility, of course, requires not generic data but rather estimates that are specific to the facility or application. Bayes' theorem then updates the prior distribution with facility-specific evidence and has the effect of "specializing" the prior to the specific facility. The updated, or specialized, prior is called the "posterior distribution" because it can be derived only after the facility-specific evidence is incorporated. The prior reflects the analyst's degree of belief about the parameter before such evidence; the posterior represents the degree of belief after incorporating the evidence. Facility-specific estimates are then obtained from the posterior distribution as described in Sections 5.5.2.3 and 5.5.2.4 of NUREG/CR-2300.

#### 5.3.1.4.2.1 Essential Elements of the Bayesian Approach

This section considers the essential elements of the Bayesian approach to data reduction. It presents a brief discussion of Bayes' theorem, the basic notions of Bayesian point and interval estimation, and a step-by-step outline of the procedures for obtaining Bayesian estimates.

The main benefit in using the Bayesian approach to data reduction is that it provides a formal way of explicitly organizing and introducing into the analysis assumptions about prior knowledge. This knowledge may be based on past generic industry-wide data and experience, engineering judgment, expert opinion, and so forth, with varying degrees of subjectivity. The parameter estimates will then reflect this knowledge. Such prior information is often available to the extent that it may contribute more to knowledge about the parameter than does the more directly applicable (but sparse) facility-specific information.

##### *5.3.1.4.2.1.1 Bayes' Theorem*

The fundamental tool for use in updating the generic prior distribution to obtain facility- or application-specific parameter estimates is Bayes' theorem. If the parameter of interest is a failure rate λ (number of failures per unit time), Bayes' theorem states that

$$f(\lambda|E) = \frac{f(\lambda)\, L(E|\lambda)}{\int_0^\infty f(\lambda)\, L(E|\lambda)\, d\lambda} \tag{5.4}$$

where f(λ|E) is the posterior distribution, the probability density function of λ, conditional on the specific evidence E; f(λ) is the prior distribution, the probability density function of λ based on generic information but incorporating no specific evidence E; and L(E|λ) is the likelihood function, the probability distribution of the specific evidence E for a given value of λ.

If the parameter of interest is the probability of failure on demand, p, rather than a failure rate λ per unit time, then λ is simply replaced by p in Equation (5.4). However, the likelihood function will differ for the different cases, as shown in Sections 5.5.2.3.1 and 5.5.2.4 of NUREG/CR-2300.

In certain special cases, the integral on the right-hand side of Equation (5.4) can be done analytically to give a closed-form expression for the posterior distribution. The term

"conjugate prior" is used to describe the prior-distribution form that conveniently simplifies the integration.

For example, if the likelihood function is the Poisson distribution (see Section 5.5.2.4 of NUREG/CR-2300), then the gamma family represents the conjugate prior: the posterior distribution will be expressible in closed form as another gamma distribution. Section 5.3.1.4.2.2.3 will discuss this in more detail. In general, a closed-form integration will not be possible, and numerical techniques must be used; alternatively, the continuous prior distribution can be approximated by a discrete approximation and the integral replaced by a sum. An example of the latter approach has been given by Apostolakis et al. (Reference 5-16).

Numerical integration or a discrete approximation is often needed when the generic data include a precise description of a prior distribution, so that the analyst lacks the flexibility to choose a mathematically tractable form for it. For example, if a lognormal prior distribution is specified for λ and the likelihood is the Poisson distribution, then the posterior distribution cannot be obtained analytically in closed form. On the other hand, if we have incomplete information, this choice can be made from the conjugate family of distribution (see Section 5.3.1.4.2.2.3), which yields the mathematical convenience and resultant simplicity of a closed-form expression for the posterior distribution. Sensitivity studies can then be used to examine the effects of this choice.

The discrete form of Bayes' theorem is

$$f(\lambda|E) = \frac{f(\lambda_i)L(E|\lambda_i)}{\sum_{i=1}^{m} f(\lambda_i)L(E|\lambda_i)} \tag{5.5}$$

where $\lambda_i$ (I = 1, 2,…, m) is a discrete set of failure-rate values. The prior and posterior distributions are approximated by the discrete functions $f(\lambda_i)$ and $f(\lambda_i|E)$, respectively.

The discrete form of Bayes' theorem is mathematically convenient and is sometimes used as an approximation to the continuous form given by Equation (5.4) when the denominator in Equation (5.4) cannot be evaluated in closed form. In such cases, the range of the parameter is carved into a set of intervals and the probability content of each interval is then associated with a single point inside the interval.

There are two important issues that should be raised in conjunction with the discrete-prior approach. First, it sometimes happens that the use of a discretized approximation to a continuous prior does not produce a meaningful well-spread posterior distribution (see Reference 5-16, Examples 2 and 3). In such cases, the prior distribution must be finely spread in the appropriate region after the initial posterior distribution has been obtained. Thus, the method may require more than one iteration to produce a meaningful posterior, and such recursive procedures may be unacceptable.

Second, if continuous priors of a specified form (e.g., a lognormal distribution) are discretized, the results may be interpreted as a crude approximation to the integration in Equation (5.4). A better approximation is to use Equation (5.4) in conjunction with an appropriate numerical integration method, such as the Gauss quadrature, thus maintaining in effect a continuous prior distribution. This is the approach used by Ahmed et al. (Reference 5-19).

The denominator of either Equation (5.4) or Equation (5.5) can be thought of simply as a normalizing factor that makes the posterior distribution integrate or sum to unity. Thus, Bayes' theorem can be stated verbally as simply saying that the posterior distribution is proportional to the product of the prior distribution and the likelihood function.

*5.3.1.4.2.1.2 Bayesian Point and Interval Estimation*

The prior distribution summarizes the uncertainty in a parameter as reflected by prior judgment and/or the generic data sources on which the prior is based. Similarly, the posterior distribution summarizes the uncertainties in the facility-specific value of the parameter as reflected by the combined influence of both the prior distribution and the likelihood function. In either case, it is frequently desired to obtain either a point or an interval estimate of the underlying parameter.

A Bayesian point estimate is a single value that, in some precisely defined sense, best estimates or represents the unknown parameter. Two commonly used point estimates are the mean and the median (50$^{th}$ percentile) of the prior or the posterior distribution. The mean of a distribution is the Bayesian estimate that minimizes the average squared error of estimation (averaged over the entire population of interest), while the median is the one that minimizes the average absolute error. Thus, either the mean or the median of the prior distribution can be used as a point estimate of the unknown generic parameter, likewise, the mean or the median of the posterior distribution can be used as a point estimate of the unknown facility- or application-specific parameter. The properties of the two estimators are discussed by Martz and Waller (Reference 5-20). The mean or the median would be found by conventional statistical procedures using the prior distribution, the mean of a failure rate λ is given by

$$\mu_\lambda = \int_0^\infty \lambda f(\lambda)\, d\lambda \tag{5.6}$$

while the median is the solution to

$$F(\lambda) = \int_0^\lambda f(t)\, dt = .5 \tag{5.7}$$

F(λ) denoting the cumulative distribution function. Using the posterior distribution, the prior f(λ) would be replaced by the posterior f(λ|E) in Equations (5.6) and (5.7).

Now consider the problem of obtaining an interval estimate for λ, using either the prior or the posterior distribution, depending on whether one is concerned with a generic or a specific failure rate. Suppose we want a probability of (1 - γ) that the interval estimate really includes the unknown failure rate. (For example, γ = .05 for .95 probability.) We can obtain a 100(1 - γ)% two-sided Bayes probability interval estimate of λ by solving the two equations

$$\int_0^{\lambda_L} f(\lambda)\ d\lambda = \frac{\gamma}{2} \tag{5.8}$$

and

$$\int_{\lambda_U}^\infty f(\lambda)\ d\lambda = \frac{\gamma}{2} \tag{5.9}$$

for the lower end point $\lambda_L$ and the upper end point $\lambda_U$. It follows immediately that $P(\lambda_L < \lambda < \lambda_U) = 1 - \gamma$. Such an interval is often called a "Bayesian confidence interval"; we avoid that term here because it is not a confidence interval in the classical sense. The coefficient $(1 - \gamma)$ is the subjectively defined probability that the interval estimate ($\lambda_L$, $\lambda_U$) contains $\lambda$.

For a Bayesian interval estimate of an unknown facility-specific failure rate, the posterior distribution $f(\lambda|E)$ would replace the prior distribution $f(\lambda)$ in Equations (5.8) and (5.9). The interval estimate ($\lambda_L$, $\lambda_U$) would then be such that $P(\lambda_L < \lambda < \lambda_U \mid E) = 1 - \gamma$.

Analogous results hold when the parameter of interest is a failure-on-demand probability p rather than a failure rate $\lambda$.

*5.3.1.4.2.1.3 Step-by-Step Procedure for Bayesian Estimation*

The QRVA analyst goes through several steps in Bayesian data reduction. For estimating a parameter like a component-failure rate or a failure-on-demand probability, the steps are as follows:

1. Identify the sources and forms of generic information to be used in selecting an appropriate prior distribution for the parameter (see Section 5.3.1.4.2.2.1).

2. Select a prior-distribution family if none has been specified as part of the generic information (see Sections 5.3.1.4.2.2.2 and 5.3.1.4.2.2.3).

3. Choose a particular prior distribution by reducing and/or combining the generic data from Step 1 (see Sections 5.5.2.2.4 through 5.5.2.2.8 of NUREG/CR-2300).

4. Plot the prior and summarize it by determining its mean, variance, and selected summary percentiles.

5. If generic estimates are required, determine them from the prior as in Section 5.3.1.4.2.1.2.

6. If facility- or application-specific estimates are required, then—

    a. Obtain data representing operating experience with the specific component.

    b. Identify an appropriate form for the likelihood function (see Sections 5.5.2.3.1 and 5.5.2.4.1 of NUREG/CR-2300).

    c. Use Bayes' theorem to get the posterior distribution (see Section 5.4.2.1.1 of NUREG/CR-2300).

    d. Plot the posterior distribution on the same page with the prior and summarize the posterior in the same manner as in Step 4.

e. Compare the prior and the posterior distributions to see the effect of the specific data.

f. Obtain the desired estimates from the posterior distribution.

7. Investigate the sensitivity of the results to the prior distribution.

#### 5.3.1.4.2.2 Determining Prior Distributions

A fundamental part of any Bayesian estimation procedure is the selection and fitting of a prior distribution. This section considers "generic" data that can be used to determine a prior distribution, including sample sources of such data, and then discusses some methods for reducing or combining such data in fitting a prior. Subsequently, several classes of priors that have been found useful in complex facility applications will be introduced. Particular emphasis is given to the class of noninformative prior distributions, useful when there are few or no prior generic data. Lognormal, gamma, and beta prior distributions are presented for possible use when prior generic data are available.

##### *5.3.1.4.2.2.1 Sources of Data for Use in Bayesian Estimation*

Three types of information about the reliability parameter of interest are often available: (1) engineering knowledge about the design, construction, and performance of the component, (2) the past performance of similar components in similar environments, and (3) the past performance of the specific component in question. The first two types constitute the "generic" information (or data) and may include varying degrees of subjective judgment. The third type, constituted of objective data, is the "facility- or application-specific" information (or data).

There are several sources of facility- or application-specific data that can be used via Bayes' theorem to determine posterior distributions suitable for application-specific estimates. Facility-specific equipment history reports or databases and corrective maintenance reports or databases are usually good sources of information to support determination of Bayesian posterior distributions.

##### *5.3.1.4.2.2.2 Noninformative Prior Distributions*

"Noninformative" prior distributions are a class of priors that loosely minimize the relative importance of the prior (compared with the data) in generating a posterior estimate. There are many ways of precisely quantifying this basic notion and hence a variety of classes of noninformative priors and corresponding methods for their attainment in practice. The notion adopted here for the noninformative prior is that of Martz and Waller (Reference 5-20), in which, roughly speaking, a prior is said to be noninformative if the facility-specific data serve only to change the location of the corresponding likelihood and not its shape. This and other notions have also been discussed by Jeffreys (Reference 5-21), and a summary of the relevant literature on this subject has been presented by Parry and Winter (Reference 5-17).

Noninformative priors are useful when little or no generic prior information is available, they should not be used when there is such information, because they deliberately

downgrade its role in the estimation process. Frequently, Bayesian estimates from noninformative priors are identical with, or very close to, the classical estimates, a fact illustrating the versatility of the Bayesian method. However, interval estimates generated by their use are probability intervals, not classical confidence intervals. Section 5.5.2.3.2 of NUREG/CR-2300 presents the noninformative prior for failure-on-demand probabilities, and Section 5.5.2.4.2 of NUREG/CR-2300 does so for failure rates. Since noninformative priors contain no generic information, it may be preferable to avoid their use when even minimal generic prior data are available.

#### *5.3.1.4.2.2.3 Natural Conjugate Prior Distributions*

Natural conjugate prior distributions have the property that, for a given likelihood function, the posterior and prior distributions are members of the same family of distributions. In such cases, the posterior distribution has a closed-form analytical representation (at least to the extent that the prior does), and accordingly the expressions for computing the Bayesian point and interval estimates can usually be represented in terms of well-defined probabilities. This can be seen in Sections 5.5.2.3.3 and 5.5.2.4.3 of NUREG/CR-2300. The parameters of such priors are often especially easy to interpret, playing the role of prior failure data entirely analogous to the specific data used in the likelihood function. This is also illustrated in Sections 5.5.2.3.3 and 5.5.2.4.3 of NUREG/CR-2300. Such families of priors are often rich enough and flexible enough to permit the analyst to model reasonably a wide range of prior data that may be encountered (Reference 5-20). Finally, there are well-developed methods for fitting natural conjugate priors to generic prior data. Some of these are discussed in Sections 5.5.2.2.6 and 5.5.2.2.7 of NUREG/CR-2300.

For these reasons, natural conjugate priors have found application in complex facility QRVAs (see, for example, Reference 5-22). Their use is recommended (see, for example, Reference 5-19) whenever the exact form of the prior has not been specified as part of the generic prior data, but the data are sufficient to determine a reasonable member of the natural conjugate family. If incomplete information exists on the prior, as often happens, the analyst will have the flexibility to select the form of the distribution, and the conjugate prior is often the natural selection. However, a sensitivity analysis should be performed to confirm this choice.

### 5.3.2 Common Cause Failure Analysis

Several terms have been used to describe specific types of dependent failures. Common-mode failures[‡] are multiple, concurrent, and dependent failures of identical equipment that fails in the same mode. Propagating failures occur when equipment fails in a mode that causes sufficient changes in operating conditions, environments, or requirements to cause other items of equipment to fail. Common cause failures are failures of multiple equipment items occurring from some single cause that is common to all of them. While a great many dependent failures are due to a common cause, not all can be categorized as such, propagating failures being a case in point.

[‡] In the Reactor Safety Study (Reference 5-12), the term “common-mode failure” was used in a broader sense to include all the types of dependent failures defined in Section 3.7.2 of NUREG/CR-2300.

Unfortunately, the above three categories of dependent failures are neither mutually exclusive nor exhaustive. This has resulted in much confusion in the literature. For our purposes, the term "dependent-failure analysis" will be used to describe the assessment of all multiple, concurrent, and dependent failures. A survey of the various definitions that have been proposed for common-cause and common-mode failures has been published by Smith and Watson (Reference 5-23).

### *5.3.2.1 Definition of Dependent Failures*

A number of authors have developed extensive lists of categories of dependent failures with the primary objective of design improvement. One of the more comprehensive classifications is that by Watson and Edwards (Reference 5-24). The purpose here, however, is to help risk analysts select methods for their analysis, and therefore the simplified classification scheme described below is adequate.

**Type 1. Common Cause Initiating Events (external events):** external and internal events that have the potential for initiating a facility transient and increase the probability of failure in multiple systems. These events usually, but not always, cause severe environmental stresses on components and structures. Examples include fires, floods, earthquakes, losses of offsite power, aircraft crashes, and gas clouds.

**Type 2. Intersystem Dependences:** events or failure causes that create interdependences among the probabilities of failure for multiple systems. Stated another way, intersystem dependences cause the conditional probability of failure for a given system along an accident sequence to be dependent on the success or failure of systems that precede it in the sequence. There are several subtypes of interest in risk analysis.

**Type 2A. Functional Dependences:** dependences among systems that follow from the facility design philosophy, system capabilities and limitations, and design bases. One example is a system that is not used or needed unless other systems have failed; another is a system that is designed to function only in conjunction with the successful operation of other systems.

**Type 2B. Shared-Equipment Dependences:** dependences of multiple systems on the same components, subsystems, or auxiliary equipment. Examples are (1) a collection of pumps and valves that provide both a coolant-injection and a coolant-recirculation function when the functions appear as different events in the event tree and (2) components in different systems fed from the same electrical bus.

**Type 2C. Physical Interactions:** failure mechanisms, similar to those in common-cause initiators that do not necessarily cause an initiating event but nonetheless increase the probability of multiple system failures occurring at the same time. Often they are associated with extreme environmental stresses created by the failure of one or more systems after an initiating event. For example, the failure of a set of sensors in one system can be caused by the excessive temperature resulting from the failure of a second system to provide cooling.

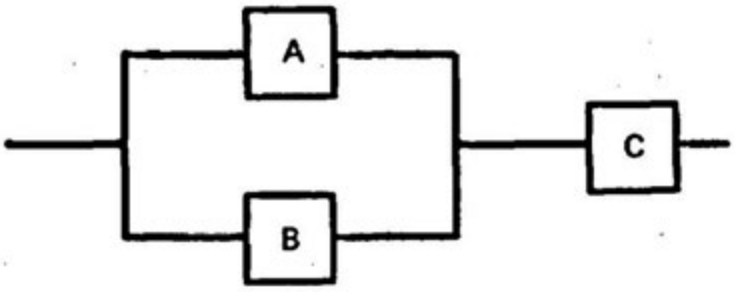
**Type 2D. Human-Interaction Dependences:** dependences introduced by human actions, including errors of omission and commission. The persons involved can be

anyone associated with a facility-life-cycle activity, including designers, manufacturers, constructors, inspectors, operators, and maintenance personnel. A dependent failure of this type occurs, for example, when an operator turns off a system after failing to correctly diagnose the condition of the facility.

**Type 3. Intercomponent Dependences:** events or failure causes that result in a dependence among the probabilities of failure for multiple components or subsystems. The multiple failures of interest in risk analysis are usually within the same system or the same minimal cut set that has been identified for a system or an entire accident sequence. Subtypes 3A, 3B, 3C, and 3D are defined to correspond with Subtypes 2A, 2B, 2C, and 2D, respectively, except that the multiple failures occur at the subsystem and component level instead of at the system level.

*5.3.2.1.1 Analysis of Intercomponent Dependences (common cause failures)*

Once the intersystem dependences are accounted by means of one of the methods described in the preceding section, the facility logic has been developed to a level of detail corresponding with basic component-failure modes. Before the quantification of the event and fault trees can be completed, it is necessary to analyze the possibilities for dependences among the basic component failures (Type 3 intercomponent dependences). A well-known category of dependent failures involving multiple components is common cause failure (CCF): the occurrence of multiple component failures induced by a single, shared cause. The importance of CCF in system-failure analysis can be seen from the following simple example of a system with three components, A, B, and C. Suppose that the reliability block diagram for this system is given by:




The corresponding system unavailability Q can be expressed as

$$Q = P(A \text{ AND } B) + P(C) - P(A \text{ AND } B \text{ AND } C)$$

or alternatively as

$$Q = P(A) \bullet P(B|A)[1 - P(C|A \text{ AND } B)] + P(C)$$

where P(x) is the availability of Component x and P(y|z AND t) is the unavailability of Component y given Components z and t are failed.

The significance of common-cause failures in this example is as follows: any cause of failure that affects any pair or all three components at the same time (or, in general, any

multiple set of components in the system) will have an effect on system unavailability. When Equation 3-2 of NUREG/CR-2300 is used, these common causes show up as dependences in that the conditional component unavailabilities—for example, P(B|A)—are different from, and often significantly greater than, the respective unconditional unavailabilities, in other words, P(B|A) >> P(B). It is a well-known characteristic of common-cause failures that, if the cause or causes are shared by two or more components in the same minimal cut set, the assumption that the component unavailabilities are independent leads to optimistic predictions of system reliability. It is not so well known that, if the dependence exists between two or more units in a series system (i.e., in different minimal cut sets), the assumption of independent failures can lead to conservative predictions, depending on how the data are analyzed. However, the former effect is more important and can lead to considerably larger errors in calculations for highly reliable redundant systems.

The magnitude of the errors that result from neglecting common-cause failures can be seen by developing the model of the above three-component system in terms of sets of explicit causes of component failure. Suppose that each of the three components can fail through independent causes, denoted by A', B', and C', and further that there are additional causes of failure, denoted by D, common to Components A and B, and a final set of causes, denoted by E, that are common to Components B and C.

The causes of single and multicomponent failures can be represented in the format of a fault tree (see Figure 5-5) where the causes appear at the level below the basic component-failure modes.

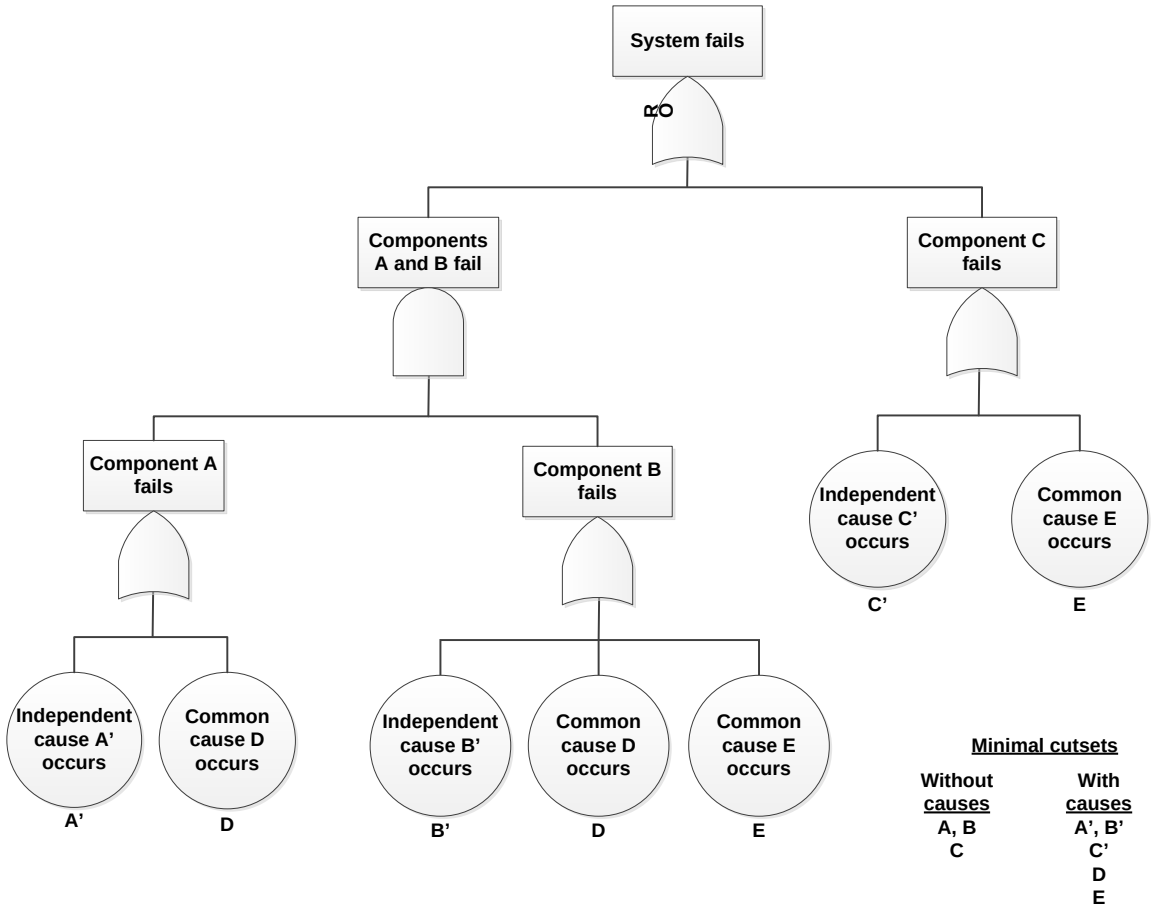



**Figure 5-5. Fault Tree for a Three-Component System with Independent and Common Causes**

An alternative approach is to develop the failure causes for each component-failure set in the form of a cause table (see Section 3.6.2 of NUREG/CR-2300), separately from the fault tree or the reliability diagram, which is left in terms of basic component-failure modes. In Table 5-2 this fault tree is quantified under the assumption that all the causes of single and multi-component failures are independent for the different cases chosen to illustrate the effect of the common causes. The tree can then be quantified in the normal way with the aid of the minimal cut sets of causes rather than the minimal cut sets of component-failure modes, both of which are indicated in Figure 5-5.

## Table 5-2. Effect of Two Types of Common Causes on Fault-Tree Quantification[a]

| Parameter | Fault-Tree Quantification Case | | | |
|---|---|---|---|---|
| | Case 1 | Case 2 | Case 3 | Case 4 |
| | No Common Cause, No Single Failures | Common Causes A and B, No Single Failures | No Redundancy, No Common-Cause Failure | No Redundancy, Common Causes B and C |
| $P(A^1)$ | $1.0 \times 10^{-3}$ | $9.9 \times 10^{-4}$ | 1 | 1 |
| P(B') | $1.0 \times 10^{-3}$ | $9.9 \times 10^{-4}$ | $1.0 \times 10^{-3}$ | $5.0 \times 10^{-4}$ |
| $P(C^1)$ | 0 | 0 | $1.0 \times 10^{-3}$ | $5.0 \times 10^{-4}$ |
| P(D) | 0 | $1.0 \times 10^{-5}$ | 0 | 0 |
| P(E) | 0 | 0 | 0 | $5.0 \times 10^{-4}$ |
| Q | $1.0 \times 10^{-6}$ | $1.1 \times 10^{-5}$ | $2.0 \times 10^{-3}$ | $1.5 \times 10^{-3}$ |

[a] *see Figure 5-5 for the fault tree.*

Cases 1 and 2 are selected to illustrate the well-known result of a common cause shared by redundant components, in this case, A and A. In each of these cases the component unavailability is held fixed at $1 \times 10^{-3}$ but is distributed differently between the independent and the common causes. As the common-cause contribution is varied from 0 to 1 percent (essentially the same as varying the component beta factor from 0 to .01), the system unavailability is increased by more than a factor of to. Of course, there are examples in which the effect of common cause is many orders of magnitude. However, these values were selected to help view the problem from a different perspective, as explained in the discussion that follows.

Let us examine Case 1—the typical situation in which the component unavailabilities are known and it is assumed that the component-failure modes are independent. This assumption implies that all the causes of component failure, which presumably are not known in most cases, are also independent. A comparison of Cases 1 and 2 shows that, in order for the result of Case 1 to be "correct", it is necessary to establish that all causes of failure, which contribute to more than 99% of the component unavailability, are independent. (Even if only 0.1 percent of the failure-cause contribution is common, the result of Case 1 is still off by a factor of 10.) This result can be generalized to the statement that, whenever independence is claimed between subsystems highly reliable redundancy, it is necessary to have an extraordinarily high level of confidence in asserting that all causes of subsystem failure are independent. The level of confidence that the independence assumption is correct must exceed the complement of the unavailability claimed for the redundant subsystem. This result is compounded for higher levels of redundancy.

Cases 3 and 4 illustrate a result that is not so well known: for a given fixed level of component unavailability, common cause failures actually tend to improve the reliability of a system of components in series; i.e., components not in the same minimal cut set. In these two cases, the redundancy is eliminated (P[A] = 1) and the unavailabilities of Components B and C are held fixed, again at $10^{-3}$. As the common cause contribution to component unavailability increases from 0 to 50% (i.e., as the beta factor increases from 0 to 0.50), the system unavailability decreases by 30%. In most cases the common cause fraction would be expected to be less than 50%, in which case the effect on the series system unavailability would be smaller. Hence, this type of common cause can usually be ignored with a small error on the conservative side. However, this example points to the fact that the existence of any cause common to any set of components in a system changes the unavailability of the system. The situation becomes even more complicated in the multisystem or facility-level models encountered in risk analysis.

The simple model and examples described above are also useful in describing some of the interrelationships between common cause failures and their analysis—and the related issues of human reliability, data, and completeness. The role of completeness should be obvious from the quantification cases just described. The sensitivity of reliability predictions to the assumption that component failures are independent has been shown to be strongly related to the completeness of the model. Only in the ideal case, when essentially all the causes of component unavailability are identified and shown to be independent, can we be assured that the error resulting from the assumption of independence is negligible. In realistic cases, in which only some of the causes are explicitly identified, the assumption of independent failures, particularly in the case of multiple equipment items in the same cut set, should be suspect. Hence, the more complete the models are in terms of the identification of causes, the better the treatment of common cause failures.

The relationship between human actions and common cause failures arises from the fact that all types of system and component failures are either caused or induced by human actions. Design errors and other human acts during manufacture, installation, operation, and maintenance are among the chief causes of multiple as well as single component failures. Of particular interest in the analysis of common cause failures is the fact that a substantial number of human errors and shortcomings affect the entire system—or at least multiple components, as opposed to individual components singly. The dependence among error rates in a sequence of human actions is recognized as an important factor in the technique for predicting the rates of human error, which is discussed in Chapter 4 of NUREG/CR-2300.

The limitations and uncertainties associated with attempts to analyze common cause failures can be largely attributed to a lack or a scarcity of data. For example, if sufficient applicable data were available at the system level, the unavailability and other reliability characteristics of the system could be estimated directly from the data without analyzing the system through various combinations of cause failures. The analysis of field-experience data is also the most effective and defensible way to establish the degree of dependence among the causes of multiple failures, to estimate the conditional frequencies of common cause failures (e.g., beta factors), or to estimate multiple-failure frequencies directly, depending on the type of the model. However, many problems and limitations are associated with currently published data sources and “banks” in the

context of common cause analysis. These are discussed in Chapter 5 of NUREG/CR-2300.

There are basically three approaches to analyzing and quantifying the effects of common-cause failures in a system-failure analysis. One is to develop the causes of failure explicitly in the fault trees or the cause tables. The second and third approaches are the beta-factor and the binomial-failure-rate methods, which use parameters to quantify the effect of common causes without explicitly enumerating the causes. All three approaches require the collection and analysis of CCF experience data, as described in Chapter 5 of NUREG/CR-2300. A brief discussion and a limited comparison of the three methods are presented below.

#### *5.3.2.1.2 Fault-Tree Analysis of Common-Cause Failures*

One approach to the analysis of common-cause failures is to model them directly in the system fault tree or as specific entries in the cause table. The basic concepts of fault-tree construction and cause-table analysis are discussed in Sections 3.5 and 3.6.2 of NUREG/CR-2300, respectively. This approach seeks to apply experience data at the greatest level of detail available. Specific details of the modeled system-failure modes are compared with the common cause failures experienced in similar systems to determine their applicability. The analyst must exercise judgment in this task because rarely are the systems exactly alike. For example, suppose a dependence induced two of two redundant trains to fail in one system, but the system to be analyzed has three redundant trains. The analyst must decide whether to model the cause as affecting all three trains or just two, depending on the details of the experienced event in relation to the design of the system being analyzed. While some design changes may have been specifically introduced to eliminate observed dependent failures, it is recognized that these same changes may introduce new common cause failures as yet not experienced. The review of past experience is therefore often augmented by systematic searches for dependences between the components of the system. Two or more components may share the same operating environment or require the same periodic maintenance actions.

These qualitative searches for sources of common cause failure are useful for the task of design improvement but, when performed in the absence of CCF experience data, are difficult to quantify without resorting to the assignment of subjective probabilities. However, a systematic search for the common causes of failure would greatly enhance the basis for such subjective assessments. The computer-aided procedures described in Section 3.7.3.9 of NUREG/CR-2300 are useful in carrying out such systematic searches for common-cause failures.

As indicated in the sample fault-tree analysis of causes in Section 5.3.2.1.1, the chief weakness of this approach is the tendency to underestimate the frequencies of common-cause failures because of the incomplete enumeration of causes. If the systematic search identified the common causes of failure for each of the lowest order of minimal cut sets for the system, it would be easier to establish that the most important CCF events were accounted for. As indicated in examples given below, it would be extremely difficult to establish that any redundant system is not susceptible to common-cause failures.

It is of interest to examine some actual occurrences of dependent failures and to determine whether the search procedures would have identified them. Table 5-1 and Table 5-4 describe two classes of dependent failures: those due to generic causes and those due to special conditions. The generic causes are defined as out-of-tolerance operating conditions; the special conditions refer to conditions or attributes that may be common to a number of system components. These causes and conditions form the basis for a search for dependent failures.

**Table 5-3. Generic Causes of Dependent Failures**

| Generic Cause | Example of Source |
|---|---|
| Impact | Pipe whip, water hammer, missiles, earthquakes, structural failure |
| Vibration | Machinery in motion, earthquake |
| Pressure | Explosion, out-of-tolerance system changes (pump overspeed, flow blockage) |
| Grit | Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from control system |
| Moisture | Condensation, pipe rupture, rainwater |
| Stress | Thermal stress at welds of dissimilar metals |
| Temperature | Fire, lightning, welding equipment, cooling-system faults, electrical short-circuits |
| Freezing | Water freezing |
| Electromagnetic Interference | Welding equipment, rotating electrical machinery, lightning, power supplies, transmission lines |
| Conducting Medium | Conductive gases |
| Out-of-Tolerance Voltage | Power surge |
| Out-of-Tolerance Current | Short-circuit, power surge |
| Corrosion (acid) | Boric acid from chemical control system, acid used in maintenance for rust removal and cleaning |
| Corrosion (oxidation) | In a water medium or around high-temperature metals (e.g., filaments) |
| Other Chemical Reactions | Galvanic corrosion, complex interactions of fuel cladding, water, oxide fuel, and fuel chemicals |
| Biological Hazards | Poisonous gases, explosions, missiles |

## Table 5-4. Special Conditions

| Special Conditions | Example of Source |
|---|---|
| Calibration | Misprinted calibration instructions |
| Installation Contractor | Same subcontractor or crew |
| Maintenance | Incorrect procedure, inadequately trained personnel |
| Operator or Operation | Operator disabled or overstressed, faulty operating procedures |
| Proximity | Location of components in one cabinet (common location exposes all of the components to many unspecified common causes) |
| Test Procedure | Faulty test procedures that may affect all components normally tested together |

For example, failure data on page 3-88 of NUREG/CR-2300 show that, in the 11 instances of multiple failures, five were due to maintenance or operator error and one was due to improper installation. This emphasizes the importance of the noted special conditions. The search procedures may have been able to assign the cause of a multiple-failure event to a common inadequately trained maintenance team. This same maintenance team, however, would be responsible for much of the facility's systems. A great many dependences could be attributed to this condition alone. All such dependent-failure causes could not possibly be included in the system's fault tree. Yet several maintenance-related errors did lead to dependent failures.

How could the analyst determine beforehand which dependences to ignore and which to include? This reveals an important limitation associated with fault-tree cause analysis. In an effort to ensure completeness, an intractable number of dependences are identified. Taken separately, these dependences can often be discounted on the basis of a perceived low occurrence probability. Experience shows, however, that as a class they cannot be dismissed. There are many accounts of dependent-failure events involving dependences once thought to be highly improbable. Table 5-5 lists just a few.

## Table 5-5. Dependent Failures Involving Subtle Dependences

| Facility | Description |
|---|---|
| Facility 1 | Dropped light bulb led to shorted instrument bus, leading to a scram and a severe transient |
| Facility 2 | Maintenance error: valves in auxiliary feedwater system left closed |
| Facility 3 | Gasket rupture on service-water liner; resulting spray failed a pressure switch |
| Facility 4 | Improper installation of insulation led to failure of three ADS valves through overheating |
| Facility 5 | Maintenance error: lifted electrical lead prevented automatic pump start |
| Facility 6 | Mechanic maintaining one service-water pump accidentally broke an adjacent pump |

*5.3.2.1.3 Common Cause Failure Analysis Parametric Methods*

This section provides a detailed description of the various parametric models applied in common cause failure analysis, develops a set of estimators for their parameters, and describes the implication of the assumptions made in developing the estimators. The estimators presented here are point estimators. Appendix D of NUREG/CR-5485 discusses the representation of the statistical uncertainty in the values of these estimates. The models are described by showing how each model is used to calculate the probability of occurrence of the various common cause basic events. It is therefore helpful to review the definition of common cause basic events and other key concepts prior to the discussion of the models. This section is an adaptation of information provided in Appendix A of NUREG/CR-5485.

As described in Section 5.1 of NUREG/CR-5485, a common cause basic event is defined as "an event representing multiple failures of (usually similar) components due to a shared cause."

Thus, in modeling a system of three components A, B, and C as in Section 5.2 of NUREG/CR-5485, in addition to the basic events $A_1$, $B_1$, and $C_1$ representing unavailability or failure of one and only one component, it is necessary to consider the common cause basic events $C_{AB}$, $C_{BC}$ and $C_{AC}$, $C_{ABC}$. When defined in this way, events are clearly interpreted as specifying the impact of the underlying causes of failure. In the same way that the single component basic events represent the sum of contributions from many causes, so do the common cause basic events.

When constructing system models, not taking common cause failures into account, the basic events representing unavailability of different component are regarded as independent. The question arises whether, since the common cause basic events form a partition of the failure space of the components, these basic events can be defined as being independent. To investigate this further, it is necessary to decompose the events into the contributions from root causes.

Define

$$A_I = \sum_i A_I^{(i)} + \sum_j A_{C_i}^{(j)} \tag{5.10}$$

where $A_I^{(i)}$ is a truly independent failure of Component A as a result of Cause I, and $A_{C_1}^{(j)}$ is a failure of Component A and only A as a result of the occurrence of a common cause trigger j. In this context, the common cause trigger implies the occurrence of some root cause of failure and also the existence of a coupling mechanism.

Similarly, define

$$C_{AB} = \sum_i C_{AB(C_2)}^{(i)} \tag{5.11}$$

where $C_{AB(C_2)}^{(i)}$ is a failure of Components A and B from the occurrence of a common cause, I, which resulted in the two failures only. In the notation used, $(C_2)$ indicates that the common cause event involved two components only. Similar expansions can be developed for $B_I$ and $C_{BC}$.

If these events are regarded as being independent, the following (cause level) cut set expansions of the system cut sets result:

$$A_I \bullet B_I = \sum_i A_I^{(i)} \bullet \sum_j B_I^{(j)} + \sum_i A_I^{(i)} \bullet \sum_j B_{C_1}^{(j)} + \sum_i A_{C_1}^{(i)} \bullet \sum_j B_I^{(j)} + \sum_i A_{C_1}^{(i)} \bullet \sum_j B_{C_1}^{(j)} \quad (5.12)$$

$$C_{AB} \bullet C_{BC} = \sum_i C_{AB(C_2)}^{(i)} \bullet \sum_j C_{BC(C_2)}^{(j)} \quad (5.13)$$

Looking at the causal cut sets more closely, it can be seen that among them there exist cut sets of the type:

$$A_I^{(k)} \cdot B_I^{(k)}$$

$$A_{C_1}^{(k)} \cdot B_{C_1}^{(k)}$$

$$C_{AB(C_2)}^{(k)} \cdot C_{BC(C_2)}^{(k)}$$

The first of these is logically correct given that the causes indicated by a subscript I are independent. Then the two failures may by chance occur simultaneously. However, when the failures result from a common cause, cut sets such as $A_{C_1}^{(k)} \cdot B_{C_1}^{(k)}$ would be indistinguishable from $C_{AB(C_2)}^{(k)}$, and should be classified as the latter. Similarly, $C_{AB(C_2)}^{(k)} \cdot C_{BC(C_2)}^{(k)}$ would be indistinguishable from $C_{ABC(C_3)}^{(k)}$. Thus, when the common cause failures are introduced into the model at the impact level (i.e., by evaluating the functional state of components involved and not the specific causes), the basic events can no longer be regarded as truly independent since this may cause logical inconsistencies with the system model.

A convenient approach to properly model common cause failure events is to define the Events $A_I$, $C_{AB}$, $C_{AC}$, and $C_{ABC}$ to be mutually exclusive, since they partition the failures space of A according to the explicit impact on other components in the common cause group.

Such a definition implies that cut sets of the type $C_{AB} \bullet C_{AC}$ are identically zero. This definition has particular implications for the analysis of event data in that events in which three components fail, must be identified as one or another of the combinations $A_IC_{BC}$, $A_IB_IC_I$,$C_{ABC}$, and other permutations, but excluding $C_{AB} \bullet C_{BC}$. This, and the observation made earlier about indistinguishability, guarantees mutual exclusivity of the partition of the failure space of each components. It should be noted that in this report the $A_I$, $B_I$, and $C_I$ are still regarded as independent events even though the common cause contribution to these events, the $A_{C_1}^{(j)}$ in Equation A.1 from NUREG/CR-2300, can lead to some cut sets at the cause level, which have the same problem concerning indistinguishability as the multiple component cut sets discussed previously. The contribution of the latter is considered to be insignificant.

Once the basic events are defined, a simplifying assumption is made to reduce the number of probabilities that need to be estimated. According to this assumption, the

probabilities of similar basic events involving similar types of components are the same (symmetry assumption). For example, if A, B, and C are identical components, then

$$P(A_I) = P(B_I) = P(C_I) = Q_1$$
$$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2$$
$$P(C_{ABC}) = Q_3 \quad (5.14)$$

Note that, with the symmetry assumption, the probability of failure of any given common cause basic event involving similar components depends only on the number and not on the specific components in that basic event. This number is indicated as a subscript to the letter Q used to represent the probabilities of basic events. Therefore, $Q_2$, for example, is the probability of basic events involving failure of two and only two components due to a shared cause.

It should be mentioned at this point that, as will be seen shortly, the probability of the basic event $Q_k$ changes with "m", the total number of components in the common cause component group.[§]

Therefore, the general representation of the probabilities of basic events is the following:

$Q_k^{(m)}$ = probability of a basic event involving k specific components (l ≤ k ≤ m) in a common cause component group of size m (5.15)

And, the general,

$$Q_k^{(m)} \neq Q_k^{(l)} \quad l \neq m \quad (5.16)$$

The above discussion provides the necessary background for the following presentation of the various parametric models for calculating the probabilities of common cause basic events.

#### 5.3.2.1.3.1 Parametric Models

Parametric models refer to different ways in which the probabilities of the basic events in terms of a set of parameters are calculated. Numerous parametric models have been proposed over the past two decades, and some have been widely used in risk and reliability analyses. The models presented in Section 5 and Appendix A of NUREG/CR-5485, cover a wide range of such models. The main characteristics of these models are summarized in Table 5-6.

[§] A common cause component group is a set of (usually identical) components considered to be susceptible to common cause failure (see also Sections 3 and 4 of NUREG/CR-5485).

## Table 5-6. Key Characteristics of Some Popular Parametric Models

| Estimation Approach | | | Model | Model Parameters* | General Form for Multiple Component Failure Frequency** |
|---|---|---|---|---|---|
| Nonshock Models | Direct | | Basic Parameter | $Q_1^{(m)}, Q_2^{(m)}, \cdots, Q_m^{(m)}$ | $Q_k^{(m)} = Q_k^{(m)} \quad k = 1,2,\cdots,m$ |
| Nonshock Models | Indirect | Single Parameter | Beta Factor | $Q_t, \beta$ | $Q_k^{(m)} = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$ |
| Nonshock Models | Indirect | Multiparameter | Multiple Greek Letters | $Q_t, \beta, \gamma, \delta, \cdots$ | $Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \binom{k}{\pi \rho_t}_{t=1} (1-\rho_{k+1})Q_t$ <br> $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \cdots, \rho_{m+1} = 0$ |
| Nonshock Models | Indirect | Multiparameter | Alpha Factor | $Q_t, \alpha_1, \alpha_2, \cdots, \alpha_m$ | Non-Staggering Test <br> $Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \cdots, m$ <br> $\alpha_t = \sum_{k=1}^{m} k\alpha_k$ |
| Shock Models | | | Binomial Failure Rate | $Q_1, \mu, \rho, \omega$ | $Q_k^{(m)} = \begin{cases} Q_1 + \mu\rho(1-\rho)^{m-1} & k = 1 \\ \mu\rho^k(1-\rho)^{m-k} & 2 \le k < m \\ \mu\rho^m + \omega & k = m \end{cases}$ |

* *Refer to the text for definition of various parameters.*

** *Formulae are presented for the basic events in a common cause component group of size m. For the Alpha Factor Model equations are shown for the non-staggered test scheme (see discussion in Section A-3 of Reference 1 of NUREG/CR-5485).*

Table 5-6 also provides a categorization of these models based on how each of the basic event probabilities is estimated.

The two major categories are:

- Shock Models
- Nonshock Models

A "shock model" recognizes two failure mechanisms: (1) failures due to random independent causes of single component failures and (2) failures of one or more components due to common cause "shocks" that impact the systems at a certain frequency. The shock models, therefore, develop the frequency of the second type of failure as the product of the frequency of shocks and the conditional probability of failure of components, given the occurrence of shocks.

The nonshock models estimate basic event probabilities without postulating a model for the underlying failure process. The Basic Parameter model is used to estimate the basic event probabilities directly. The other models discussed here, namely, the Beta Factor, Multiple Greek Letter (MGL), and Alpha Factor models, are reparameterizations of the basic parameter model. They are used whenever common cause failure probabilities are estimated by using estimates of the ratios or probabilities from one source of data, and independently a total failure rate or probability from another source. For example, facility-specific data may be used to estimate a total failure probability but, as there is insufficient data to estimate multiple failure probabilities, a generic source may be used to estimate ratios of multiple to single components failure events.

*Basic Parameter Model*

The basic parameter model (Reference 5-25) refers to the straightforward definition of the probabilities of the basic events as given by Equation (5.15). Depending on the system modeling requirements, $Q_k^{(m)}{}'s$ can be defined as demand-based (frequency of failures per demand) or time-based (rate of failures per unit time). The latter can be defined both for the standby failure rates as well as for the rate of failures during operation.

In terms of the basic specific parameters defined in Equation (5.15), the total failure probability, $Q_t$, of a component in a common cause group of m components is

$$Q_t = \sum_{\kappa=1}^{m} \binom{m-1}{\kappa-1} Q_\kappa^{(m)} \tag{5.17}$$

where the binomial term

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(m-k)!\,(k-1)!} \tag{5.18}$$

represents the number of different ways that a specified component can fail with (k-1) other components in a group of m similar components. In this formulation, the events $Q_k^{(m)}$, $Q_j^{(m)}$ are mutually exclusive for all k, j. If the events $Q_k^{(m)}$ were not defined as being mutually exclusive, but independent, Equation (5.17) is still valid under the rare event approximation.

*Beta Factor Model*

The beta factor model (Reference 5-26) is a single parameter model; that is, it uses one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. It was the first model to be applied to common cause events in risk and reliability studies. The model assumes that a constant fraction (p) of the component failure probability can be associated with common cause events shared by other components in that group. Another assumption is that whenever a common cause event occurs, all components within the common cause component group fail. Therefore, for a group of m components, all $Q_k^{(m)}{}'s$ defined in Equation (5.15) are zero except $Q_l^{(m)}$ and $Q_m^{(m)}$. The last two quantities are written as

$$Q_l^{(m)} = (1-\beta)Q_t$$

$$Q_m^{(m)} = \beta Q_t \tag{5.19}$$

This implies that

$$\beta = \frac{Q_m^{(m)}}{Q_l^{(m)} + Q_m^{(m)}} \tag{5.20}$$

Note that $Q_t$, the total failure probability of one component, is given as

$$Q_t = Q_l^{(m)} + Q_m^{(m)} \tag{5.21}$$

which is the special case of Equation 2-17 of NUREG/CR-5485 when $Q_2^{(m)} = Q_3^{(m)} = \cdots = Q_{m-1}^{(m)} = 0$.

Therefore, using the beta factor model, the frequencies of various basic events in a common cause group of m components are

$$Q_k^{(m)} = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases} \tag{5.22}$$

As can be seen, the beta factor model requires an estimate of the total failure rate of the components, which is generally available from generic data sources, and a corresponding estimate for the beta factor. The estimators of beta do not explicitly depend on system or component success data, which are not generally available. Also, estimates of the beta parameter for widely different types of components do not appear to vary appreciably. These two observations and the simplicity of the model are the main reasons for its wide use in risk and reliability studies.

It should be noted that relaxing the requirement for data on demands or time in operation (success data) requires making specific assumptions concerning the interpretation of data. This and several related issues regarding the assumptions behind the various models and the implications of the assumptions are discussed later in this section.

The questions about interpretation of data and its impact on the form of estimators led to the development of a single parameter model known as the C-factor model (Reference 5-27) which is different from the beta factor model only in the way the data are used to estimate the single parameter of the model.

Although historical data collected from the operation of facilities indicate that common cause events do not always fail all redundant components, experience from using this simple model reveals that, in some cases, it gives reasonably accurate (only slightly conservative) results for redundancy levels up to about three or four. However, beyond such redundancy levels, this model generally yields results that are conservative. When interest centers on specific contributions from third or higher order trains, more general parametric models are recommended.

*Multiple Greek Letter Model*

The MGL model (Reference 5-28) is the most general of a number of recent extensions of the beta-factor model. The MGL model was the one used most frequently in the International Common Cause Failure Reliability Benchmark Exercise (Reference 5-29). In this model, other parameters in addition to the beta factor are introduced to account more explicitly for higher order redundancies and to allow for different probabilities of failures of subgroups of the common cause component group.

The MGL parameters consist of the total component failure probability, $Q_t$, which includes the effects of all independent and common cause contributions to that component failure, and a set of failure fractions, which are used to quantify the conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components in the same group, given component failure has occurred. For a group of m redundant components and for each given failure mode, m different parameters are defined. For example, the first four parameters of the MGL model are, as before

$Q_t$ = total failure probability of each component due to all independent and common cause events.

plus

$\beta$ = conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.

$\gamma$ = conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or some additional components, given that two specific components have failed.

$\delta$ = conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components given that three specific components have failed.

The general equation that expresses the probability of k specific component failures due to common cause, $Q_k$, in terms of the MGL parameters, is consistent with the above definitions. The MGL parameters are defined in terms of the basic parameter model parameters for a group of three similar components as

$$Q_t = Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)} \tag{5.23}$$

$$\beta^{(3)} = \frac{2Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)}}$$

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2Q_2^{(3)} + Q_3^{(3)}} \tag{5.24}$$

$\delta$ and higher order terms are identically zero.

For a group of four similar components, the MGL parameters are

$$Q_t = Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)} \tag{5.25}$$

$$\delta^{(4)} = \frac{Q_4^{(4)}}{3Q_3^{(4)}+Q_4^{(4)}} \tag{5.26}$$

It is important to note that the integer coefficients in the above definitions are a function of m, the number of components in the common cause group. Therefore, it is generally inappropriate to use MGL parameters that were quantified for an m unit group in an l unit group, m ≠ l. The same comment applies to the other similar multi-parameter methods.

The following equations express the probability of multiple component failures due to common cause, $Q_k$, in terms of the MGL parameters for a three-component common cause group:

$$\begin{aligned} Q_1^{(3)} &= (1-\beta)Q_t \\ Q_2^{(3)} &= \frac{1}{2}\beta(1-\gamma)Q_t \\ Q_3^{(3)} &= \gamma\beta Q_t \end{aligned} \tag{5.27}$$

For a four-component group, the equations are

$$\beta^{(4)} = \frac{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}$$

$$\gamma^{(4)} = \frac{3Q_3^{(4)}+Q_4^{(4)}}{3Q_2^{(4)}+3Q_3^{(4)}+Q_4^{(4)}} \tag{5.28}$$

$$Q_1^{(4)} = (1-\beta)Q_t$$

$$Q_2^{(4)} = \frac{1}{3}\beta(1-\gamma)Q_t$$

$$Q_3^{(4)} = \frac{1}{3}\beta\gamma(1-\delta)Q_t$$

$$Q_4^{(4)} = \beta\gamma\delta Q_t$$

The generalization of this is given by

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} \rho_1 \, (1-\rho_{k+1}) Q_t \quad (k = 1, \cdots, \rho_{m+1} = 0) \tag{5.29}$$

where

$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$

*Alpha-Factor Model*

As explained in Appendix D of NUREG/CR-5485, rigorous estimators for the beta factor and the MGL model parameters are fairly difficult to obtain, although approximate methods have been developed and used in practice (Reference 5-30). A rigorous approach to estimating beta factors is presented in Reference 5-31 by introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference 5-32 uses the multi-parameter generalizations of event-based parameters directly to estimate the common cause basic event probabilities. This multi-parameter common cause model is called the alpha factor model.

Alpha factor parameters are estimated from observable data from a sampling scheme. The MGL parameters cannot be directly related to any known sampling scheme and observable data. This difference and its implications are described more fully in Appendix D of NUREG/CR-5485.

The alpha factor model defines common cause failure probabilities from a set of failure frequency ratios and the total component failure frequency, $Q_T$. In terms of the basic event probabilities, the alpha factor parameters for non-staggered testing are defined as

$$Q_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}} \tag{5.30}$$

where $\binom{m}{k} Q_k^{(m)}$ is the frequency of events involving k component failures in a common cause group of m components, and the denominator is the sum of such frequencies. In other words,

$\alpha_k^{(m)}$ = probability that when a common cause basic event occurs in a common cause group of size m, it involves failure of k components.

For example, for a group of three similar components we have

$$\alpha_1^{(3)} = \frac{3Q_1^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_2^{(3)} = \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_3^{(3)} = \frac{Q_3^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} \tag{5.31}$$

and $\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1$ as expected.

Using Equations (5.17) and (5.30), we can see that the basic event probabilities can be written as a function of $Q_t$ and the alpha factors as follows:

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} Q_t \tag{5.32}$$

where

$$\alpha_t \equiv \sum_{k=1}^{m} k\alpha_k^{(m)} \tag{5.33}$$

To see how Equation (5.32) is obtained from Equations (5.17) and (5.30), note that Equation (5.30) can also be written as

$$\frac{k}{m}\left\{\sum_{k=1}^{m}\binom{m}{k}Q_k^{(m)}\right\}\alpha_t^{(m)} = \binom{m-1}{k-1}Q_k^{(m)}$$

By summing both sides over k we get

$$\frac{1}{m}\left\{\sum_{k=1}^{m}\binom{m}{k}Q_k^{(m)}\right\}\sum_{k=1}^{m}k\alpha_t^{(m)} = \sum_{k=1}^{m}\binom{m-1}{k-1}Q_k^{(m)}$$

or

$$\sum_{k=1}^{m}\binom{m}{k}Q_k^{(m)} = \frac{m}{\alpha_t}Q_t$$

where we have used Equations (5.17) and (5.33). By using the above equation in Equation (5.30) and solving for $Q_k^{(m)}$ we get Equation (5.32).

The parameters of the α-factor and the MGL models are related through a set of simple relations. For example, for a common cause component group of size three, the MGL (Non-Staggered Testing) parameters are

$$\beta^{(3)} = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$$

$$\gamma^{(3)} = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3} \tag{5.34}$$

Similarly, the alpha factor (Staggered Testing) model parameters for the same group are written as

$$\alpha_1^{(3)} = (1-\beta)$$

$$\alpha_2^{(3)} = (1-\gamma)\beta$$

$$\alpha_3^{(3)} = \beta\gamma \tag{5.35}$$

The form of these relations depends on assumptions regarding the particular testing scheme (staggered vs. non-staggered) applied to the system as described in Section 5.3.2.1.3.2. Table 5-7, Table 5-8, and Table 5-9 list such conversion equations for common cause component groups of up to size m = 8, under both staggered and non-staggered testing schemes.

## Table 5-7. MGL to Alpha Factor Conversion Formulae for Staggered Testing

| m | MGL to Alpha Factor | Alpha Factor to MGL |
|---|---|---|
| 2 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = \beta$ | $\beta = 1 - \alpha_1 = \alpha_2$ |
| 3 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = \beta\gamma$ | $\beta = \alpha_2 + \alpha_3$<br>$\gamma = \frac{\alpha_3}{\alpha_2 + \alpha_3}$ |
| 4 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = (1 - \delta)\beta\gamma$<br>$\alpha_4 = \beta\gamma\delta$ | $\beta = \alpha_2 + \alpha_3 + \alpha_4$<br>$\gamma = \frac{\alpha_3 + \alpha_4}{\alpha_2 + \alpha_3 + \alpha_4}$<br>$\delta = \frac{\alpha_4}{\alpha_3 + \alpha_4}$ |
| 5 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = (1 - \delta)\beta\gamma$<br>$\alpha_4 = (1 - \epsilon)\beta\gamma\delta$<br>$\alpha_5 = \beta\gamma\delta\epsilon$ | $\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5$<br>$\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5}$<br>$\delta = \frac{\alpha_4 + \alpha_5}{\alpha_3 + \alpha_4 + \alpha_5}$<br>$\epsilon = \frac{\alpha_5}{\alpha_4 + \alpha_5}$ |
| 6 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = (1 - \delta)\beta\gamma$<br>$\alpha_4 = (1 - \epsilon)\beta\gamma\delta$<br>$\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$<br>$\alpha_6 = \beta\gamma\delta\epsilon\mu$ | $\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6$<br>$\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}$<br>$\delta = \frac{\alpha_4 + \alpha_5 + \alpha_6}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}$<br>$\epsilon = \frac{\alpha_5 + \alpha_6}{\alpha_4 + \alpha_5 + \alpha_6}$<br>$\mu = \frac{\alpha_6}{\alpha_5 + \alpha_6}$ |

**Table 5-7. MGL to Alpha Factor Conversion Formulae for Staggered Testing (Continued)**

| m | MGL to Alpha Factor | Alpha Factor to MGL |
|---|---|---|
| 7 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = (1 - \delta)\beta\gamma$<br>$\alpha_4 = (1 - \epsilon)\beta\gamma\delta$<br>$\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$<br>$\alpha_6 = (1 - \nu)\beta\gamma\delta\epsilon\mu$<br>$\alpha_7 = \beta\gamma\delta\epsilon\mu\nu$ | $\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7$<br>$\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$<br>$\delta = \frac{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$<br>$\epsilon = \frac{\alpha_5 + \alpha_6 + \alpha_7}{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$<br>$\mu = \frac{\alpha_6 + \alpha_7}{\alpha_5 + \alpha_6 + \alpha_7}$<br>$\nu = \frac{\alpha_7}{\alpha_6 + \alpha_7}$ |
| 8 | $\alpha_1 = 1 - \beta$<br>$\alpha_2 = (1 - \gamma)\beta$<br>$\alpha_3 = (1 - \delta)\beta\gamma$<br>$\alpha_4 = (1 - \epsilon)\beta\gamma\delta$<br>$\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$<br>$\alpha_6 = (1 - \nu)\beta\gamma\delta\epsilon\mu$<br>$\alpha_7 = (1 - \kappa)\beta\gamma\delta\epsilon\mu\nu$<br>$\alpha_8 = \beta\gamma\delta\epsilon\mu\nu\kappa$ | $\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8$<br>$\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$<br>$\delta = \frac{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$<br>$\epsilon = \frac{\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$<br>$\mu = \frac{\alpha_6 + \alpha_7 + \alpha_8}{\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$<br>$\nu = \frac{\alpha_7 + \alpha_8}{\alpha_6 + \alpha_7 + \alpha_8}$<br>$\kappa = \frac{\alpha_8}{\alpha_7 + \alpha_8}$ |

## Table 5-8. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing

| m | Alpha Factor to MGL |
|---|---|
| 2 | $\beta = 1 - \alpha_1 = \alpha_2$ |
| 3 | $\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$<br>$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3}$ |
| 4 | $\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4}$<br>$\gamma = \frac{3\alpha_3 + 4\alpha_4}{2\alpha_2 + 3\alpha_3 + 4\alpha_4}$<br>$\delta = \frac{4\alpha_4}{3\alpha_3 + 4\alpha_4}$ |
| 5 | $\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$<br>$\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$<br>$\delta = \frac{4\alpha_4 + 5\alpha_5}{3\alpha_3 + 4\alpha_4 + 5\alpha_5}$<br>$\epsilon = \frac{5\alpha_5}{4\alpha_4 + 5\alpha_5}$ |
| 6 | $\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$<br>$\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$<br>$\delta = \frac{4\alpha_4 + 5\alpha_5 + 6\alpha_6}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$<br>$\epsilon = \frac{5\alpha_5 + 6\alpha_6}{4\alpha_4 + 5\alpha_5 + 6\alpha_6}$<br>$\mu = \frac{6\alpha_6}{5\alpha_5 + 6\alpha_6}$ |

## Table 5-8. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing (Continued)

| m | Alpha Factor to MGL |
|---|---|
| 7 | $\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$<br>$\gamma = 2\frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$<br>$\delta = \frac{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$<br>$\epsilon = \frac{5\alpha_5 + 6\alpha_6 + 7\alpha_7}{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$<br>$\mu = \frac{6\alpha_6 + 7\alpha_7}{5\alpha_5 + 6\alpha_6 + 7\alpha_7}$<br>$\nu = \frac{7\alpha_7}{6\alpha_6 + 7\alpha_7}$ |
| 8 | $\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\delta = \frac{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\epsilon = \frac{5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\mu = \frac{6\alpha_6 + 7\alpha_7 + 8\alpha_8}{5\alpha_5 + 6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\nu = \frac{7\alpha_7 + 8\alpha_8}{6\alpha_6 + 7\alpha_7 + 8\alpha_8}$<br>$\kappa = \frac{8\alpha_8}{7\alpha_7 + 8\alpha_8}$ |

## Table 5-9. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing

| m | MGL to Alpha Factor |
|---|---|
| 2 | $\alpha_1 = \frac{2(1-\beta)}{2-\beta}$<br>$\alpha_2 = \frac{\beta}{2-\beta}$ |
| 3 | $\alpha_1 = \frac{6(1-\beta)}{6-\beta(3+\gamma)}$<br>$\alpha_2 = \frac{3\beta(1-\gamma)}{6-\beta(3+\gamma)}$<br>$\alpha_3 = \frac{2\beta\gamma}{6-\beta(3+\gamma)}$ |
| 4 | $\alpha_1 = \frac{12(-1+\beta)}{-12+\beta(6+(2+\delta)\gamma)}$<br>$\alpha_2 = \frac{6\beta(-1+\gamma)}{-12+\beta(6+(2+\delta)\gamma)}$<br>$\alpha_3 = \frac{4\beta(-1+\delta)\gamma}{-12+\beta(6+(2+\delta)\gamma)}$<br>$\alpha_4 = \frac{3\beta\gamma\delta}{-12+\beta(6+(2+\delta)\gamma)}$ |
| 5 | $\alpha_1 = \frac{12(-1+\beta)(5+4\epsilon)}{D}$<br>$\alpha_2 = \frac{6\beta(5+4\epsilon)(-1+\gamma)}{D}$<br>$\alpha_3 = \frac{4\beta(-1+\delta)(5+4\epsilon)\gamma}{D}$<br>$\alpha_4 = \frac{3\beta\gamma\delta(-5+\epsilon)}{D}$<br>$\alpha_5 = \frac{12\beta\gamma\delta\epsilon}{D}$<br>where<br>$D = -60+30\beta-48\epsilon+24\beta\epsilon+10\beta\gamma+5\beta\gamma\delta+8\beta\epsilon\gamma+7\beta\delta\epsilon\gamma$ |

**Table 5-9. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing (Continued)**

| m | MGL to Alpha Factor |
|---|---|
| 6 | $\alpha_1 = \frac{12(-1+\beta)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_2 = \frac{6\beta(-1+\gamma)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_3 = \frac{4\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$<br>$\alpha_4 = \frac{3\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$<br>$\alpha_5 = \frac{12\beta\gamma\delta\epsilon(-1+\mu)}{D}$<br>$\alpha_6 = \frac{10\beta\gamma\delta\epsilon\mu}{D}$<br>where<br>$D = 60 - 30\beta + 48\epsilon - 24\beta\epsilon - 10\beta\gamma - 5\beta\gamma\delta - 8\beta\epsilon\gamma - 7\beta\delta\epsilon\gamma - 48\epsilon\mu + 24\beta\epsilon\mu + 8\beta\epsilon\gamma\mu + 2\beta\delta\gamma\epsilon\mu$ |
| 7 | $\alpha_1 = \frac{84(-1+\beta)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_2 = \frac{42\beta(-1+\gamma)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_3 = \frac{28\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$<br>$\alpha_4 = \frac{21\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$<br>$\alpha_5 = \frac{84\beta\gamma\delta\epsilon(-1+\mu)}{D}$<br>$\alpha_6 = \frac{70\beta\gamma\delta\epsilon\mu(-1+\nu)}{D}$<br>$\alpha_7 = \frac{60\beta\gamma\delta\epsilon\mu\nu}{D}$<br>where<br>$D = -420 + 210\beta - 336\epsilon + 168\beta\epsilon - 70\beta\gamma + 35\beta\gamma\delta + 56\beta\epsilon\gamma + 49\beta\delta\epsilon + 336\epsilon\mu - 168\beta\epsilon\mu - 56\beta\epsilon\gamma\mu - 14\beta\delta\gamma\epsilon\mu + 10\beta\gamma\delta\epsilon\mu\nu$ |

**Table 5-9. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing (Continued)**

| m | MGL to Alpha Factor |
|---|---|
| 8 | $\alpha_1 = \frac{84(-1+\beta)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_2 = \frac{42\beta(-1+\gamma)\left(-5+4\epsilon(-1+\mu)\right)}{D}$<br>$\alpha_3 = \frac{28\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$<br>$\alpha_4 = \frac{21\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$<br>$\alpha_5 = \frac{84\beta\gamma\delta\epsilon(-1+\mu)}{D}$<br>$\alpha_6 = \frac{70\beta\gamma\delta\epsilon\mu(-1+\nu)}{D}$<br>$\alpha_7 = \frac{60\beta\gamma\delta\epsilon\mu\nu(-1+\kappa)}{D}$<br>$\alpha_8 = \frac{105\beta\gamma\delta\epsilon\mu\nu\kappa}{2D}$<br>where<br>$D = -420 + 210\beta - 336\epsilon + 168\beta\epsilon + 70\beta\gamma + 35\beta\gamma\delta + 56\beta\epsilon\gamma + 49\beta\delta\epsilon\gamma + 336\epsilon\mu - 168\beta\epsilon\mu - 56\beta\epsilon\gamma\mu - 14\beta\delta\gamma\epsilon\mu + 10\beta\gamma\delta\epsilon\mu\nu + 60\beta\gamma\delta\epsilon\mu\nu\kappa$ |

*Binomial Failure Rate (BFR) Model*

The Binomial Failure Rate model (Reference 5-33) considers two types of failures. The first represents independent component failures; the second type is caused by shocks that can result in failure of any number of components in the system. According to this model, there are two types of shocks: lethal and nonlethal. When a nonlethal shock occurs, each component within the common cause component group is assumed to have a constant and independent probability of failure. For a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution, hence the name Binomial Failure Model. When originally presented and applied, the model only included the nonlethal shock.

Because of its structure, the model tended to underestimate the probabilities of failure of higher order groups of components in a highly redundant system; therefore, the concept of lethal shock was included. This version of the model is the one recommended.

When a lethal shock occurs, all components are assumed to fail with a conditional probability of unity. Application of the BFR model with lethal shocks requires the use of the following set of parameters:

$Q_I$ = independent failure frequency for each component.

μ = frequency of occurrence of nonlethal shocks.

P = conditional probability of failure of each component, given a nonlethal shock.

Ω = frequency of occurrence of lethal shocks.

Thus, the frequency of basic events involving k specific components is given as

$$Q_k^{(m)} = \begin{cases} Q_I + \mu\rho(1-\rho)^{m-1} & k = 1 \\ \mu(\rho)^k(1-\rho)^{m-k} & 2 \le k < m \\ \mu\rho^m + \omega & k = m \end{cases} \quad (5.36)$$

It should be noted that the basic formulation of the BFR model was introduced in terms of the rate of occurrence of failures in time, such as failure of components to continue running while in operation. Here, consistent with our presentation of other models, the BFR parameters are presented in terms of general frequencies that can apply to both failures in time and to failure on demand for standby components.

#### *5.3.2.1.3.1.1 Some Estimators for Parameters of the Common Cause Models*

In order to estimate a parameter value, it is necessary to find an expression that relates the parameters to measurable quantities. This expression is called an estimator.

There are several possible estimators that can be used for a given parameter. Estimators presented in this section are the maximum likelihood estimators and are presented here for their simplicity. However, the mean values obtained from probability distribution characterizing uncertainty in the estimated values are more appropriate for point value quantification of system unavailability. These mean values are presented in the context of developing uncertainty distributions for the various parameters in Appendix D of NUREG/CR-5485.

The estimators of this section are also based on assuming a particular component and system testing scheme. More specifically, it is assumed that, for the facilities in the data base, in each test or actual demand, the entire system (or common cause component group) and all possible combinations of multiple components are challenged. This corresponds to the non-staggered testing scheme. However, if this assumption is changed (e.g., if a staggered testing scheme is assumed), the form of the estimators will also change, resulting in numerically different values for the parameters. The estimators presented in this section are the more conservative, given a fixed $Q_T$. A more detailed discussion of the effects of various assumptions including alternative strategies is given in Section 5.3.2.1.3.2.

Estimators for Basic Parameters

The maximum likelihood estimator for $Q_k$ is given as

$$\widehat{Q}_k = \frac{n_k}{N_k} \tag{5.37}$$

where

$n_k$ = number of events involving k components in a failed state,

and

$N_k$ = number of demands on any k component in the common cause group.

If it is assumed that each time the system is operated, all of the m components in the group are demanded, and this number of demands is $N_D$, then

$$N_k = \binom{m}{k} N_D \tag{5.38}$$

The binomial term $\binom{m}{k}$ represents the number of groups of k components that can be formed from m components. We, therefore, have

$$\widehat{Q}_k^{(m)} = \frac{n_k}{\binom{m}{k} N_D} \tag{5.39}$$

Thus, Equation (5.39) assumes that the data are collected from a set of $N_D$ system demands for which the state of all m components in the common cause group is checked. It is simply the ratio of the number of basic events involving k components, divided by the total number of times that various combinations of k components are challenged in $N_D$ system demands. This is represented by the binomial term in the denominator of Equation (5.39). Similar estimators can be developed for rate of failure per unit time by replacing $N_D$ with T, the total system operating time.

Replacing $Q_k$ in Equation (5.17) with the corresponding estimator yields the following estimator for the total failure probability for a specific component:

$$\widehat{Q}_t = \frac{1}{m N_D} \sum_{k=1}^{m} k n_k \tag{5.40}$$

Estimator for the β-Factor Model Parameter

Although the β-factor was originally developed for a system of two redundant components and the estimators that are often presented in the literature also assume that the data are collected from two-unit systems, a generalized β-factor estimator can be defined for a system of m redundant components.

Such an estimator is based on the following general definition of the β-factor (identical to the way it is defined in the more general MGL model).

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k \tag{5.41}$$

Using the estimator of $Q_k^{(m)}$, given by Equation (5.39), and $Q_t$, given by Equation (5.40), in the above equation results in the following estimator for β.

$$\beta = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{5.42}$$

For a two-unit system (m = 2), the above estimator reduces to the familiar estimator of the β-factor.

$$\beta = \frac{2n_2}{n_1 + 2n_2} \tag{5.43}$$

Note that the estimator β is developed from maximum likelihood estimators of $Q_k$'s. An alternative estimator can be developed directly from the distribution of the beta factor based on its definition in Equation (5.41).

Estimators for the MGL Parameters

In the following we develop estimators for the first three parameters of the MGL model for a system of m components. Estimators for the higher order parameters can be developed in a similar fashion. Based on the definition of the MGL parameters,

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \tag{5.44}$$

$$\gamma = \frac{1}{\beta Q_t} \sum_{k=3}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \tag{5.45}$$

$$\delta = \frac{1}{\beta \gamma Q_t} \sum_{k=4}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \tag{5.46}$$

Therefore, by using Equations (5.39) and (5.40) in the above expressions, the following estimators are obtained:

$$\hat{\beta} = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{5.47}$$

$$\hat{\gamma} = \frac{\sum_{k=3}^{m} k n_k}{\sum_{k=2}^{m} k n_k} \tag{5.48}$$

$$\hat{\delta} = \frac{\sum_{k=4}^{m} k n_k}{\sum_{k=3}^{m} k n_k} \tag{5.49}$$

For instance, for a three-unit system (m = 3), we have

$$\hat{\beta} = \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \tag{5.50}$$

Similarly,

$$\hat{\gamma} = \frac{3n_3}{2n_2 + 3n_3} \tag{5.51}$$

As can be seen from the above estimators, the MGL parameters are essentially the ratios of the number of component failures in various basic events. For instance in Equation (5.51), the numerator ($3n_3$ is the total number of components failed in common cause basic events that fail three components ($n_3$). This is in contrast with estimates of the α-factor model, which are in terms of the ratios of events rather than component states, and is demonstrated in the following section.

Estimators for the α-factor Model Parameters

An estimator for each of the α-factor parameters ($\alpha_k$) can be based on its definition as the fraction of total failure events that involve k component failures due to common cause. Therefore, for a system of m redundant components,

$$\hat{\alpha}_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{5.52}$$

It is shown in Appendix D of NUREG/CR-5485 that $\hat{\alpha}_k's$ correspond to the maximum likelihood estimate of the distribution of $\alpha_k's$.

Estimators for the BFR Model

The main parameters of the model are $Q_I$, μ, ω, and ρ. To develop estimators for these parameters, several other quantities are defined as:

$\lambda_t$ ≡ rate of nonlethal shocks that cause at least one component failure

$n_t$ ≡ total number of common cause failure events

$$n_t = \sum_{k=1}^{m} n_k \tag{5.53}$$

where, as before, $n_k$ is the number of basic events involving k components, and

$n_L$ = the number of occurrences of lethal shocks

$n_I$ = the number of individual component failures, not counting failures due to lethal and nonlethal shocks

The maximum likelihood estimators for the four parameters $Q_I$, $\lambda_t$, ω, and ρ, as presented in Appendix D of NUREG/CR-5485, are

$$\hat{Q}_I = \frac{n_I}{mN_D} \tag{5.54}$$

$$\hat{\lambda}t = \frac{n_t}{N_D} \tag{5.55}$$

$$\hat{\omega} = \frac{n_L}{N_D} \tag{5.56}$$

and $\hat{\rho}$ is the solution of the following equation:

$$\hat{s} = \hat{\rho}\frac{mn_t}{1-(1-\rho)^m} \tag{5.57}$$

where

$$\hat{s} = \sum_{k=1}^{m} kn_k \tag{5.58}$$

Based on the above estimators, an estimator for μ can be obtained from the following equation:

$$\lambda_t = \mu[1 - (1 - \rho)^m] \tag{5.59}$$

which is based on the definition of $\lambda_t$ at the rate of nonlethal shocks that cause at least one component failure. Therefore,

$$\hat{\mu} = \frac{\hat{\lambda}_t}{1-(1-\hat{\rho})^m} \tag{5.60}$$

#### 5.3.2.1.3.2 The Effect of Testing Schemes on Estimators

The testing scheme to which the system (or common cause component group) is subjected has an impact on the form of the statistical estimator of some model parameters. It also affects the conversion relations between various parametric models such as those shown in Table 5-7 through Table 5-9.

For example, in the estimator for $Q_k$ in the basic parameter model, the number of times a group of k components is challenged ($N_k$) is derived from the number of test episodes, $N_D$, using the following relation:

$$N_{k=}\binom{m}{k}N_D \tag{5.61}$$

This means that all such combinations are assumed to be challenged in each episode. Note that $N_D$ in this case is the same as $N_{TS}$, the number of tests of each of the redundant trains (components) as specified by facility technical specifications:

However, assuming a staggered testing scheme results in different values of $N_k$; the value depends on the response to the failure observed. Suppose that a given failure is observed in the single component tested in a particular test episode, all the other components are tested immediately, then $N_k$ can be evaluated in terms of the number of test episodes $N_D^*$ follows. (Note that in this case the number of test episodes is denoted as $N_D^*$. This is done to avoid an equivalence being made with the number of test episodes of the non-staggered testing case. In fact, for the same technical specifications or frequency of testing of a component, the value of $N_D^*$ in any given calendar time period would be related to $N_{TS}$ by $N_D^* = mN_{TS}$, since in each of the test episodes for non-staggered testing all components in the group are tested at a test episode whereas unless there is a failure, in the staggered case only one is tested in a test episode.)

Each successful test results in demonstrating that for $\binom{m-1}{k-1}$ groups of k components there was no common cause failure. In addition, each time the component ailed the test, all other components are tested and this leads to $\binom{m-1}{k-1}$ tests on any group of k components.**

Neglecting the second order effects arising from the complication that if k + 1 components are failed this modifies the number of feasible tests on k components; the number of demands on a group of k components can be expressed as

$$N_k = \left(N_D^* - \sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1} + \left(\sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1} = N_D^*\binom{m-1}{k-1} = mN_{TS}\binom{m-1}{k-1} \quad (5.62)$$

The number of single component demands is given by

$$N_D^* + \sum_{j=1}^{m} n_j \bullet (m-1) \quad (5.63)$$

with the above estimates of $N_k$ for different testing schemes, the following estimators for the probability of basic events involving k components are derived:

For a non-staggered testing scheme, using Equation (5.61),

$$Q_k^{NS} = \frac{n_k}{\binom{m}{k} N_{TS}} \quad (5.64)$$

For a staggered testing scheme, using Equation (5.62),

$$Q_k^{S} = \frac{n_k}{m\binom{m-1}{k-1} N_{TS}} \quad (5.65)$$

Therefore, $Q_k^S \leq Q_k^{NS}$ because

$$\frac{Q_k^S}{Q_k^{NS}} = \frac{1}{k} \quad (5.66)$$

In light of the above difference, we can now see that estimates of beta-factor, for example, are different depending on what testing scheme is assumed. To show this we recall that, for a two component system,

$$\beta = \frac{Q_2}{Q_1 + Q_2} \quad (5.67)$$

Therefore,

$$\beta^S = \frac{Q_2^S}{Q_1^S + Q_2^S} \quad (5.68)$$

** In this example, it is assumed that we are estimating $Q_k$, and not specifically a common cause failure probability. If we were identifying combinations of multiple and independent failures such as $Q_I \bullet Q_k$ at each testing episode, this term would be $\binom{m}{k}$. However, since the $n_j's$ are collectively usually much smaller than $N_D^*$, this subtle distinction will make little difference.

and

$$\beta^{NS} = \frac{Q_2^{NS}}{Q_1^{NS}+Q_2^{NS}} \tag{5.69}$$

thus,

$$\beta^{NS} = \frac{2Q_2^{S}}{Q_1^{S}+2Q_2^{S}} \cong 2\frac{Q_2^{S}}{Q_1^{S}+Q_2^{S}} = 2\beta^{S} \tag{5.70}$$

where we assumed, as it is true in most cases, that $Q_2 << Q_1$. The staggered-based estimator is approximately a factor of 2 smaller.

The estimator presented by Equation (5.68) is similar in form to the estimator of a single parameter model called the C-factor model (Reference 5-27). In this respect, C-factor is another estimator of the β-factor under the assumptions leading to Equation (5.68). It should be mentioned, however, that the C-factor method was developed to try to use the event report summary data to provide estimates of common cause failure probabilities. It essentially involved an interpretation of data on historical events based on an assessment of root cause. The potential of each observed root cause for being a cause of multiple failures at the facility in question was judged on engineering grounds, taking into account such aspect as facility design, maintenance, philosophy, etc. The estimator (the C-factor) was the fraction of observed root causes of failure that either did, or were judged to have the potential to, result in multiple failure. The spectrum of root causes used comes from both single and multiple failure events. Since it is the occurrence of the root cause that is important and the common cause root causes are assumed to result in this model in totally coupled failures, the multiple failure events, if applicable, are only counted once (not multiplied by the number of components failed).

#### *5.3.2.1.4 Evaluation of Common Cause Events and Dependences*

Fault tree linking provides a structure that can be used to perform the common cause analysis described in Section 3.7 of NUREG/CR-2300. The dependent-failure approach and the qualitative common cause search can be applied to the fault tree directly or to the minimal cut sets of the accident-sequence fault tree. The approach taken depends primarily on the number of minimal cut sets generated by the accident-sequence fault tree since the solution and enumeration of large numbers of cut sets are impractical.

If the dependent-failure approach is to be used for quantifying common cause events, there are at least two distinct methods for applying it. Typically with small fault tree models generating hundreds of cut sets, the beta-factor method can be applied on a cut set basis. This approach requires that all the minimal cut sets for the fault tree be generated (i.e., no probability truncation) and that each cut set be individually examined to determine whether a dependent-failure probability should be applied to increase the cut set frequency or probability. Since all the cut sets must be generated and examined, there is a limitation on the total number of cut sets that can be analyzed. While it may prove to be impractical to apply dependent-failure probabilities to all the cut sets of the accident sequence, it may be possible to apply them to the cut sets of independent subtrees within the accident-sequence fault tree, since the independent subtrees are quantified individually and replaced by primary events within the accident-sequence fault

tree. If the fault tree has been modularized, care must be taken that dependences between modules are calculated and included.

For accident-sequence fault trees that generate too many minimal cut sets for using dependent-failure probabilities on an individual basis, Section 3.7 of NUREG/CR-2300 describes a method for introducing dependent-failure probabilities as primary events in the system fault trees. This method uses solutions at intermediate gates of the accident-sequence fault tree to analyze portions of systems and derive dependent-failure probabilities from those solutions. The accident-sequence fault tree is then modified to include new primary even representing the dependent-failure probabilities, at the appropriate places. The modified fault trees are then solved in a normal typical fashion (including truncation) to yield a result with dependent-failure probabilities included.

Similarly, qualitative searches can be made for common-cause events on the accident sequence cut sets (References 5-34 through 5-36). As already discussed, if any cut sets were eliminated during the fault tree solution, the common-cause analysis is not complete, and the results of common cause searches may not include all significant common cause events. One way around this problem is to break the accident sequence fault tree into subtrees for which all the cut sets can be obtained. The cut sets for each subtree are then searched for common cause modes within that subtree and the results are propagated to the top of the accident-sequence fault tree (Reference 5-37). In this manner all the cut sets can be analyzed.

Another approach to the common-cause search is to use a transformation-of-variables technique to change the fault tree to a form reflecting the effects of common cause events; it has been described by Rasmuson et al. (Reference 5-38), Putney (Reference 5-39), and Worrell and Stack (Reference 5-36). Once the fault tree has been transformed, it can be solved to yield minimal cut sets containing one or more common cause events, combinations of common cause events, or cut sets containing common cause events. Combining multiple common cause events and combining common cause events with random-failure events have been shown to be important in past QRVAs.

### 5.3.3 Data Uncertainty Analysis

The data-development process, as presented herein, includes both classical and Bayesian viewpoints of uncertainty in parameter estimation. While these techniques treat, to some extent, the uncertainty that is related to the amount of data and the variability due to differences between data sources, there are other uncertainties that are not treated at all. This section briefly describes the potential sources of uncertainty and methods of judging their effects. In addition, Chapter 12 of NUREG/CR-2300 should be consulted for an overview of the treatment of uncertainty.

#### 5.3.3.1 Sources of Uncertainty

Before discussing sources of uncertainty, it is important to remember what one may be uncertain about. This chapter has so far presented methods for estimating the following:

1. The failure rate of components.

2. The probability that components (or systems) fail on demand.

3. The probability that components (or systems) are unavailable because of testing or maintenance.

This estimation process involves the use of various models and estimates of the parameters in these models. Thus, there may be uncertainty in the models and/or the parameters.

Since the analyst first chooses a model for the data items, there is obviously some uncertainty in that selection, as no physical occurrence exactly fits a mathematical model. Next, there is uncertainty in the parameter of that model, even given that the model is correct. The sources for parameter uncertainty include (1) the amount of data, (2) the diversity of data sources, and (3) the accuracy of data sources.

#### 5.3.3.2 Procedures for Treating Modeling Uncertainties

The first source of uncertainty mentioned above is that of model choice. The best way to determine the effect of this choice is to try another model—that is, perform a sensitivity assessment. The difference in the point estimate and confidence interval can then be reported. It is not expected that this will be an important contribution to uncertainty, and hence these extra evaluations need be done only for dominant events where the model does not seem to fit well.

#### 5.3.3.3 Procedures for Treating Parameter Uncertainties

Uncertainty in the data parameters is already treated explicitly in the data process for certain sources by including uncertainty due to the amount of data. In addition, the data process can include differences between sources of data—that is, variability of an event's rate (or probability) of occurrence from one facility to another. In addition, the data process can be used to incorporate inaccuracies in the data sources. Of course, judgment is likely to enter into the process at this point. For example, in using data from event reports, the number of demands is often estimated. Instead of treating this estimate as constant, the Bayesian approach could treat it as a random variate, while the classical approach could treat this value as a point estimate with error bounds.

### 5.3.4 QRVA Database Development

An important aspect of developing the data for accident-sequence evaluation is to document the various steps of the process. This includes not only the final numbers but also the various assumptions and sources of information. The reader should be able to

trace each data item from the fault tree or event tree back to the source, with each assumption and calculation apparent.

Documentation should include the output of the data process (i.e., the numbers used in quantification) and the general database used in the QRVA. These two types of documentation are discussed below.

#### 5.3.4.1 Documentation of the General Database

The general database for the QRVA includes all work from the source of data through the numerical results for the general types of events evaluated.

#### 5.3.4.2 Documentation of Data Applied to Each Model

The basic inputs to the task of accident-sequence quantification, and the outputs of the data process, are the numerical representations of each event. Forms like those shown in Figure 5-6 and Figure 5-7 should be used to tie the specific events to the general database.

Figure 5-6 is an example of a data table for hardware events. The first two columns, event name and description, come from the fault tree or the event tree. They give the alphanumeric code for an event and a brief description. The third column, the failure rate or probability of failure on demand, gives the data from the general database for the type of event modeled. Note that the type of distribution and the parameters are included. The fault exposure time or mission time applies to events that occur as a function of time (either failure in time after a successful start or failure in time during standby). This time, then, is the length of time the component must survive to ensure success or the time between tests.

An example of tabular format for documenting test or maintenance acts is shown in Figure 5-7. The first column gives the event name as it appears in the fault tree or event tree. The second column is a brief description of the event. The third and fourth columns list the model used for act frequency and the model for the duration of the act. Note that these values could be average values, distributions, or point estimates with error factors. The fifth column contains a list of all the components included in the one act. For a test, this is often several components. This list helps to indicate the level in the tree where the act is modeled. Also included is a column for indicating the source of the information used to develop the act models.

The most important column in the tables is the quantification model. This column is the output of the data section and the input to sequence quantification. It includes the distribution and mean (or point estimate and interval estimates) for each specific event.

Note that for time-dependent events it is a function of $\tau$ and the failure rate (see Section 5.5 of NUREG/CR-2300).

| Basic Events: Hardware | | | | | | |
|---|---|---|---|---|---|---|
| **Event Name** | **Description** | **Failure Rate or Failure-on-Demand Probability** | **Fault Exposure Time or Mission Time (τ)** | **Data Source** | **Quantification Model** | **Comments** |
| EVLV12 | Valve Fails to Open | Lognormal<br>1 x $10^{-3}$ per demand<br>Error Factor = 3 | NA | Reactor Safety Study | Distribution:<br>Lognormal<br>1 x $10^{-3}$ (3)<br>Mean:<br>1.3 x $10^{-3}$ | |
| EPM12F | Pump Fails to Start | Lognormal<br>1 x $10^{-3}$ per demand<br>Error Factor = 3 | NA | Reactor Safety Study | Distribution:<br>Lognormal<br>1 x $10^{-3}$ (3)<br>Mean:<br>1.3 x $10^{-3}$ | |
| EPM12D | Pump Discontinues Running after Start | Lognormal<br>3 x $10^{-5}$ per hour<br>Error Factor = 10 | 24 Hr | Reactor Safety Study | Distribution:<br>Lognormal<br>7.2 x $10^{-4}$ (10)<br>Mean:<br>1.9 x $10^{-3}$ | |
| ECL12D | Clutch Fails during Mission | Lognormal<br>1 x $10^{-6}$ per hour<br>Error Factor = 20 | 24 Hr | Reactor Safety Study | Distribution:<br>Lognormal<br>2.4 x $10^{-5}$ (20)<br>Mean:<br>1.3 x $10^{-4}$ | |

**Figure 5-6. Example of Data Table for Hardware**

| Basic Events: Test and Maintenance Acts | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Event Name** | **Description** | **Frequency-of-Act Model** | **Duration-of-Act Model** | **Components in Act Block** | **Data Source** | **Quantification Model** | **Comments** |
| EHPIMA | Maintenance of HPI Leg A | 1/3 Month | Lognormal<br>4 Hr<br>Error Factor = 1.5 | Manual<br>Valve 11,<br>MOV-12, Pump | Plant Data | Distribution:<br>Lognormal<br>$1.8 \times 10^{-3}$ (1.5)<br>Point Estimate:<br>$1.9 \times 10^{-3}$ | |

**Figure 5-7. Example of Data Table for Test or Maintenance Acts**

#### 5.3.4.3 *Assurance of Technical Quality*

The term "assurance of technical quality", as used here, refers only to the quality of the database that results from the procedures given in this chapter. Many factors affect the quality of the database, including the overall programming, planning, and scheduling, as well as budget limitations such items are discussed in Chapter 2, Section 2.3.3, of NUREG/CR-2300. The objective of this section is to address the items that will enhance the data quality within the program constraints.

The most beneficial activities to maximize quality are reviews and checks. As each data quantity is produced, it should be checked against other databases. Major discrepancies should be justified. Other staff members should review the event quantifications for their models and cross-compare with others with the same type of events. Finally, the team leader should review the data, using his experience to look for unusual results. Of course, outside peer review is an important part of the review process, though feedback for revision via this path usually takes longer than does feedback within the study.

Documentation is the key to the quality of the database. The data analyst should keep a notebook to document his decisions and assumptions. This notebook will make final documentation easier and make the data traceable from event results back to the source. It is also important to carefully document computer runs so that, if necessary, the runs producing particular results can be found. Often a keypunch error can result in an incorrect result.

## 5.4 Initiating Events Data

### 5.4.1 Introduction

The initiating events data for this QRVA consists primarily of acute event sequence loss-of-fuel-inventory-control precursor events such as main fuel storage tank leaks or ruptures, fuel handling piping, valves, and pumps leakage or ruptures, and fuel tank overfill events, and chronic event sequence loss-of-fuel-inventory-control precursor events such as very small main fuel storage tank leakage that is effectively too small to be effectively detected and/or managed via the automated fuel handling equipment (AFHE) System or via operator manual monitoring and control. For acute event sequences, a single-stage or two-stage Bayesian update process is applied to develop initiating event frequencies. For the chronic event sequences, simple estimates of reasonable loss rates per storage tank are applied.

### 5.4.2 Initiating Events Analysis Bayesian Update Process

The methodology of the data analysis is based on the Bayesian interpretation of probability and the concept of "probability of frequency" (Reference 5-40). In this context, component failure rates are treated as measurable quantities whose uncertainty is dependent on the state of knowledge of the investigation. The "state of knowledge" is presented in the form of a probability distribution over the range of possible values of that quantity. The probability associated with a particular numerical value of an uncertain but measurable quantity indicates the likelihood that the numerical value is the correct one.

A key issue in developing state of knowledge for the parameters of the probabilistic risk assessment (PRA) models is to ensure that the information regarding each parameter, its relevance, and its value as viewed by the analyst are presented correctly, and that various pieces of information are integrated coherently. "Coherence" is preserved if the final outcome of the process is consistent with every piece of information used and all assumptions made. This is done by using the fundamental tool of probabilistic inference; i.e., Bayes' theorem. Mathematically, Bayes' (Reference 5-41) theorem is written as:

$$P(x|E,E_0) = F^{-1}L(E|x,E_0)P(x|E_0) \tag{5.71}$$

where

$P(x|E,E_0)$ ≡ probability of x being the true value of an unknown quantity in light of new evidence, E, and prior body of knowledge, $E_0$.

$L(E|x,E_0)$ ≡ likelihood of the new evidence, E, given that the true value is x.

$P(x|E_0)$ ≡ probability of x being the true value of the unknown quantity based on the state of knowledge, $E_0$, prior to receiving E.

Finally, F is a normalizing factor defined as:

$$F \equiv \int_{allx} L(E|x,E_0)\,P(x|E_0)dx \tag{5.72}$$

In the context of a site-specific PRA, three types of information are available for the frequency of elemental events:

- **Type 1.** The historical information from other similar sites.
- **Type 2.** General engineering knowledge such as design and manufacture of equipment sometimes expressed as expert estimate of parameter values or their uncertainty distributions.
- **Type 3.** The past experience in the specific site being studied.

The information of Types 1 and 2 together constitute the "generic" information, and Type 3 is the "site-specific" or "item-specific" information. The synthesis of information Types 1 and 2 to develop generic distributions is explained in Section 2.

### *5.4.2.1 Synthesis of Generic Distributions*

To discuss the way in which the failure rate distributions were developed based on different types of information, we consider the following information types:

- **Type 1.** Failure data from operating experience at various sites.
- **Type 2.** Failure rate estimates or distributions contained in various industry compendia, such as WASH-1400 (Reference 5-42) and IEEE-500 (Reference 5-43).

By Type 1 information, we mean failure and success data collected from the performance of similar equipment in various sites. Type 2 information, which could be called processed data, is estimates ranging from the opinion of experts with engineering knowledge about the design and manufacturing of the equipment to estimates based on observed performance of the same class of equipment in various applications.

Normally, Type 2 data are either a point estimate, usually referred to as the "best estimate," or a range of values centered about a "best estimate." In some cases, a distribution is provided covering a range of values for the failure rate with the mean or median representing the "best estimate" of the source. For instance, IEEE-500 provides a "low," "high," or "recommended" value for the failure rates under normal conditions and a "maximum" value under extreme environments. WASH-1400, on the other hand, assesses a probability distribution for each failure rate to represent the variability of the available data from source to source. Such distributions are normally centered about a median value judged to be most representative of the equipment in question for nuclear applications.

The methodology used to develop generic failure rate data uses both types of information to generate generic probability distribution for the failure rates. Such distributions represent variability of the failure rates, from source to source (for Type 2 information) and/or from site to site (for Type 1 information). Obviously, as applied to any specific site, these distributions are in fact, our state of knowledge curves for the failure rate of components. The following discussion helps to clarify the distinction and serves as a prelude to the discussion of the methodology.

#### *5.4.2.1.1 The Meaning of Generic Distributions*

Suppose that we have 100 sites and that for each site the exact value of the failure rate of a particular type of pump is known. Let $\lambda_i$ be the failure rate of the pump at the ith site. Suppose further that the $\lambda_i$'s can be grouped into a limited number of discrete values, say $\lambda_1^*$ through $\lambda_5^*$, with 20 of the $\lambda_i$'s being equal to $\lambda_1^*$, 35 equal to $\lambda_2^*$, 25 equal to $\lambda_3^*$, 15 equal to $\lambda_4^*$, and finally, 5 equal to $\lambda_5^*$. The frequency distribution of the $\lambda_i$'s is then given by the histogram shown in Figure 5-8.

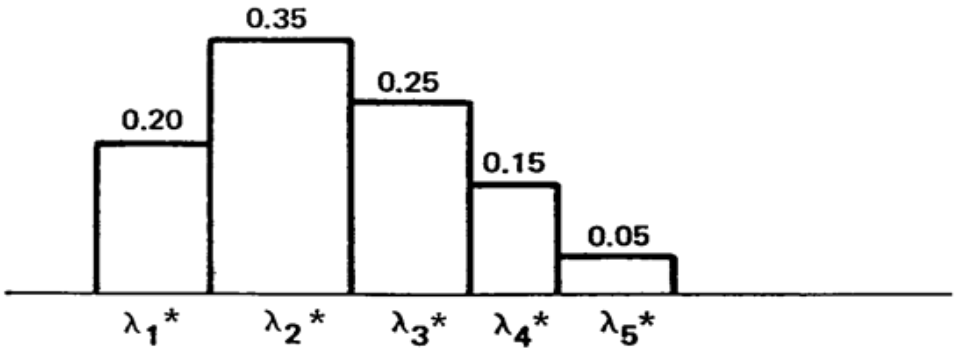



**Figure 5-8. Population Variability of the Failure Rate**

This histogram represents the "population variability" of the $\lambda_i$'s because it shows how the failure rate of the particular type of pumps under consideration varies from site to

site. It is an exact and true representation of the variability of the failure rate at the 100 sites in the population without any uncertainty or ambiguity because the distribution is based on presumed perfectly known failure rates at each and every site.

Consider now the case where only estimates, and not the exact values of the failure rates, are available for some, but not all, of the 100 sites in the population. With this state of knowledge, obviously we are not able to know the exact population variability distribution. The question is how one can use this more limited information to estimate the population variability curve and how close the estimate will be to the true distribution, as given in Figure 5-9.

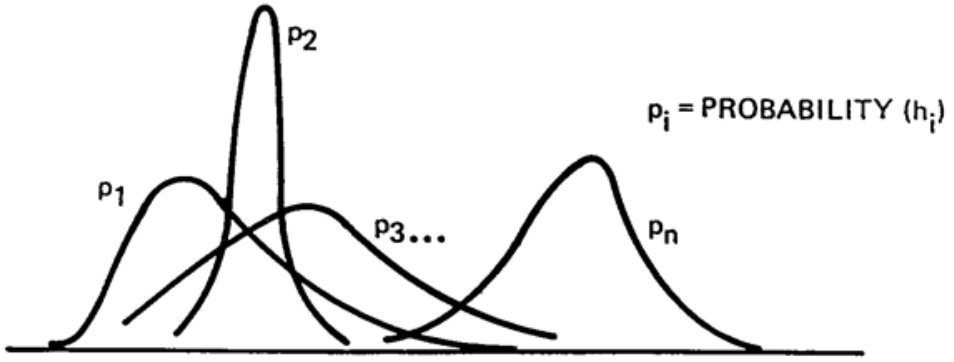



**Figure 5-9. State-of-Knowledge Distribution over the Set of Frequency Distributions**

To answer this question, first note that the desired distribution is a member of the set of all histograms. Because of our limited information, we are uncertain as to which member of that set is, in fact, the true distribution. This situation can be represented by a probability distribution over the set of all possible histograms expressing our state of knowledge about the nature of the true histogram.

For instance, if the entire space, H, of all possible histograms is composed of only n histograms; i.e., if:

$$\mathrm{H} \equiv \{\mathrm{h}_1, \mathrm{h}_2, \cdots, \mathrm{h}_\mathrm{n}\}$$

where $h_i$ represents the ith histogram, the evidence regarding the pump failure rates at different power sites can be used to assess a probability distribution over H as follows:

$$P(H) = \{p_1, p_2, \cdots, p_n\} \; with \sum_{i=1}^{n} p_i = 1 \tag{5.73}$$

where pi is the chance that hi is the true histogram.

Figure 5-9 depicts the situation in which the variable λ is considered to be continuous, and the desired distribution is a density function.

For a perfect state of knowledge, we would be able to say which hi is the true distribution; consequently, the corresponding $p_i$ would be equal to 1, and all others equal to 0. However, based on the state of knowledge expressed by Equation (5.73), our estimate of the true histogram is:

$$\bar{h} = \sum_{i=1}^{n} p_i h_i \tag{5.74}$$

that is called the "expected distribution". Another histogram of interest is one that is assigned the highest chance of being the true histogram. We call it the "most likely distribution," $h_m$, and we have:

$$p_m = \max\{p_i; i = 1, \cdots, n\} \tag{5.75}$$

The problem of obtaining P, as defined by Equation (5.71), is formulated in the Bayesian context as follows:

$$P(h_i|E) = F^{-1} L(E|h_i) P_0(h_i) \tag{5.76}$$

where $P_0(h)$ is the prior state of knowledge regarding the set H as defined by Equation (5.73), and $P(h_i|E)$ is the posterior state of knowledge in light of the evidence E. The evidence is incorporated via the likelihood term $L(E|h_i)$, which is the probability of observing the evidence, given that the true histogram is h. Finally, F is a normalizing factor defined as (see Equation [5.72]):

$$F = \sum_{i=1}^{n} L(E|h_i) P_0(h_i) \tag{5.77}$$

The expected distribution, Equation (5.74), is our estimate of the true population variability of the failure rate. It shows how the failure rates of similar pumps are distributed among sites in the population. Now, if all we know about a specific pump before we have any experience with it is that it is one member of the population, the population variability curve also becomes our state of knowledge distribution for the failure rate of that specific pump. In other words, generic distributions representing the population variability can also be used to predict the expected behavior of any member of the population, if no other information is available.

#### *5.4.2.1.2 Generic Distributions Based on Actual Performance Records (Type 1)*

The following discussion is based on the method presented in Reference 5-44. Consider the case where the following set of information is available about the performance of a generic component in N sites:

$$I_1 = \{\langle k_i, T_i \rangle; i = 1, \cdots, N\} \tag{5.78}$$

where $k_i$ is the number of failures of the component in the ith site during a specific period of time, $T_i$.

The desired information is $\phi(\lambda)$, the distribution of the failure rate of the component, λ, in light of evidence $I_1$. This distribution represents the variation of λ from one site to another, and is analogous to Figure 5-8.

Following the discussion at the beginning of Section 2, we would like to express a posterior state of knowledge about the true nature of the function $\phi(\lambda)$. To make matters practical, it is assumed that $\phi(\lambda)$ belongs to a particular parametric family of distributions. Let θ be the set of m parameters of $\phi(\lambda)$:

$$\theta = \{\theta_1, \cdots, \theta_m\} \tag{5.79}$$

For each value of θ, there exists a distribution $\phi(\lambda|\theta)$ and vice versa. Therefore, the state of knowledge distribution over the space of all possible $\phi(\lambda|\theta)$s is the state of knowledge over all possible values of θ and vice versa.

Bayes' theorem, in this case, is written as (see Equation [5.76]):

$$P(\theta|I_0 I_1) = F^{-1} L(I_1|\theta, I_0) P_0(\theta|I_0) \tag{5.80}$$

where

$P(\theta|I_0 I_1)$ = posterior state of knowledge about θ in light of evidence $I_1$ and prior information $I_0$.

$F^{-1} L(I_1|\theta, I_0)$ = the likelihood of evidence $I_1$ given that the actual set of parameters of $\phi(\lambda)$ is θ.

$P_0(\theta|I_0)$ = prior state of knowledge about θ based on general engineering knowledge $I_0$.

and F is a normalizing factor:

$$F = \int_\theta (I_0|\theta, I_0)\, P_0(\theta|I_0) d\theta$$

The likelihood term is the (conditional) probability of observing the evidence, $I_1$, given that the data are based on an underlying population variability curve $\phi(\lambda|\theta)$ with θ as the value of its parameters:

$$L = P(\langle k_i, T_i \rangle; i = 1, \cdots, N|\theta, I_0) \tag{5.81}$$

Note that L is also conditional on the prior state of knowledge $I_0$.

If we assume that the length of operating hours, $T_i$'s, at different sites is independent of one another and that the observed failures, $k_i$'s, also have no dependence (according to our model, each $k_i$ is based on a different underlying failure rate), the joint probability distribution given by Equation (5.81) can be reduced to the product of the marginal distributions as follows:

$$L(I_1|\theta, I_0) = \prod_{i=1}^{N} P_i(k_i, T_i|\theta, I_0) \tag{5.82}$$

where $P_i(k_i, T_i|\theta, I_0)$ is the probability of observing $k_i$ failures of the equipment in question during the period $T_i$ in the ith site assuming that the set of parameters of the underlying population variability curve is θ.

If the failure rate, $\lambda_i$, at the ith site is known exactly, using a Poisson model, the likelihood of observing $k_i$ in $T_i$ can be calculated from:

$$P_i(k_i, T_i|\lambda_i) = \frac{(\lambda_i T_i)^{k_i}}{k_i!}\exp(-\lambda_i T_i) \tag{5.83}$$

However, $\lambda_i$ is not known. All we know is that $\lambda_i$ is one of possibly many values of variable λ that represents the variation of the failure rate from site to site. In addition, according to our model, λ is distributed according to $\phi(\lambda|\theta)$, with θ being unknown. For this reason, we calculate the probability of observing the evidence, $\langle k_i, T_i\rangle$, by allowing the failure rate to assume all possible values. This is achieved through averaging Equation (5.83) over the distribution of λ:

$$P_i(k_i, T_i|\theta, I_0) = \int_0^\infty P_i(k_i, T_i|\lambda)\phi(\lambda|\theta)d\lambda \tag{5.84}$$

$$= \int_0^\infty \frac{(\lambda T_i)^{k_i} e^{-\lambda T_i}}{k_i!}\phi(\lambda|\theta)d\lambda$$

Depending on the parametric family chosen to represent $\phi(\lambda|\theta)$, the integration in Equation (5.84) can be carried out analytically or by numerical techniques. For example, if $\phi(\lambda_i|\theta)$ is assumed to be a gamma distribution that has the following form:

$$\phi(\lambda|\alpha, \beta) = \frac{\beta^\alpha}{\Gamma(\alpha)}\lambda^{\alpha-1}e^{-\beta\lambda} \tag{5.85}$$

with α and β, both nonnegative, as its parameters, the integral can be done analytically resulting in (Reference 5-45):

$$P_i(k_i, T_i|\alpha, \beta) = \frac{T_i^{k_i}}{k_i!}\frac{\beta^\alpha}{\Gamma(\alpha)}\frac{\Gamma(\alpha+k_i)}{(\beta+T_i)^{\alpha+k_i}} \tag{5.86}$$

In developing failure rate distributions, $\phi(\lambda|\theta)$ is assumed to be lognormally distributed with μ as the median and σ as the standard deviation of the underlying normal. Then,

$$\phi(\lambda|\mu,\sigma) = \frac{1}{\sqrt{2\pi}\sigma\lambda}\exp\left\{-\frac{1}{2}\left(\frac{\ell n\lambda-\mu}{\sigma}\right)^2\right\} \tag{5.87}$$

In this case, Equation (5.84) is calculated numerically.

The total likelihood for all N sites can now be found by using Equation (5.84) in Equation (5.82):

$$L(I_i|\theta,I_0) = \prod_{i=1}^{N}\left\{\int_0^\infty \phi(\lambda|\theta)\frac{(\lambda T_i)^{k_i}}{k_i!}\exp(-\lambda T_i)d\lambda\right\} \tag{5.88}$$

The posterior distribution resulting from using the likelihood of Equation (5.88) in Bayes' theorem, Equation (5.80), is a probability distribution over the m-dimensional space of θ. Any point, θ, in this space has a one-to-one correspondence with a distribution, $\phi(\lambda_i|\theta)$, in the space of $\phi(\lambda|\theta)$. Figure 5-10 is an example of $P(\theta|I_0,I_1)$ constructed for $\theta = \{\alpha,\beta\}$, the two parameters of gamma distribution based on the pump data from all U.S. nuclear power plants (Reference 5-46).

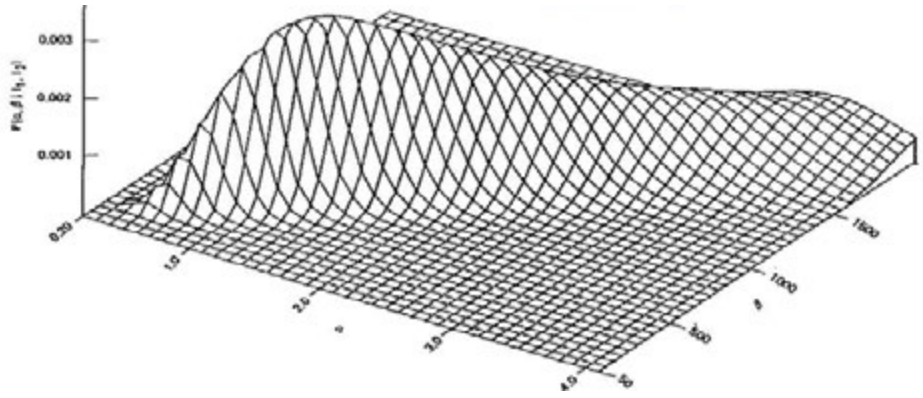



**Figure 5-10. Posterior Distribution for the Parameters of the Distribution of Pumps' Failure to Start on Demand Rates**

The "expected distribution" is obtained from (see Equation [5.74]):

$$\bar{\phi}(\lambda) = \int_\theta \theta(\lambda|\theta)P(\theta|I_0,I_1)\,d\theta \tag{5.89}$$

The quantity $\bar{\phi}(\lambda)$ "summarizes" the information about λ and is used in this study as the model for generic failure distributions.

Sometimes it is also useful to obtain the "most likely distribution" (see Equation [5.74]). According to the definition, the most probable distribution of λ is the one whose

parameters maximize $P(\theta|I_0, I_1)$. These parameters are therefore the solution of the following system of m equations:

$$\frac{\partial P(\theta|I_0, I_1)}{\partial \theta_i}\Big|\theta_{i,max} = 0; i = 1, \cdots, m \quad (5.90)$$

The methodology discussed above also applies to failure on demand-type data where the evidence is of the form:

$$I_1 = \{\langle k_i, D_i\rangle, i = 1, \cdots, N\} \quad (5.91)$$

where $k_i$ and $D_i$ are the number of failures and demands in the ith site, respectively. This can be done if the Poisson distribution used in Equation (5.84) is replaced by the binomial distribution:

$$P(k_i, D_i|\lambda) = \frac{D_i!}{k_i!(D_i - k_i)!}\lambda^{k_i}(1-\lambda)^{D_i - k_i} \quad (5.92)$$

**Example**

For motor-operated valve failure to start on demand, the following data from six sites were available:

| Site | Number of Failures (k) | Number of Demands (D) |
|---|---|---|
| 1 | 10 | 1.65E+3 |
| 2 | 14 | 1.13E+4 |
| 3 | 7 | 1.73E+3 |
| 4 | 42 | 6.72E+3 |
| 5 | 3 | 1.26E+3 |
| 6 | 31 | 9.72E+3 |

These data, which form a set of Type 1 information, $I_1$, were evaluated through the data module of RISKMAN (Reference 5-47), which calculates Equations (5.84) and (5.88) and generates $\phi(\lambda)$ based on Equation (5.89). The result was a 20-bin discrete probability distribution with the following characteristics:

| Parameter | Value |
|---|---|
| 5th Percentile | 7.56E-04 |
| 50th Percentile | 3.22E-03 |
| 95th Percentile | 1.59E-02 |
| Mean | 4.83E-03 |

### 5.4.2.2 *Generic Distributions Using Estimates of Available Sources of Generic Data (Type 2)*

As mentioned earlier, generic data frequently are not in the fundamental form given by Equations (5.78) and (5.91). Rather, most sources report point or interval estimates, or even distributions for failure rates (Type 2 information). These estimates are either judgmental (expert opinion), or based on standard estimation techniques used by the analysts to translate original data into point or interval estimates, and sometimes into a full distribution.

An example of such estimation techniques is the well-known maximum likelihood estimator given by:

$$\lambda_M = \frac{k}{T} \tag{5.93}$$

where k is the total number of failures in T units of operating time. Most data sources report $\lambda_M$, and not k and T.

To develop a model for constructing generic distributions using this type of data, the following cases are considered.

#### *5.4.2.2.1 Estimating an Unknown Quantity Having a Single True Value*

The following method is adopted from Reference 5-48. Suppose that there are M sources, each providing its own estimate of λ, which has a single true, but unknown, value, $\lambda_t$. An example is the failure rate of a particular component at a given site. The true value of that failure rate, $\lambda_t$, will be known at the end of the life of the component. Before then, however, the failure rate may be estimated by one or more experts familiar with the performance of the component. Let:

$$I_2^* = \{\lambda_i^*; i = 1, \cdots, M\} \tag{5.94}$$

be the set of such estimates where $\lambda_i^*$ is the estimate of the ith expert for $\lambda_t$.

The objective is to use information $I_2^*$ and obtain a state of knowledge distribution for $\lambda_t$. Obviously, when everything is known about $\lambda_t$, such a state of knowledge distribution is a delta function centered at $\lambda_t$.

$$P(\lambda|\text{PerfectKnowledge}) = \delta(\lambda - \lambda_t) \tag{5.95}$$

Note that in Equation (5.95), λ is used as a variable representing the unknown failure rate.

Assuming a prior state of knowledge, $P_0(\lambda)$, about the quantity λ, Bayes' theorem can be used to incorporate information $I_2^*$ into the prior and to obtain an "updated" state of knowledge about λ.

$$P(\lambda|\lambda_1^*, \cdots, \lambda_N^*) = k^{-1} L(\lambda_1^*, \cdots, \lambda_N^*|\lambda) P_0(\lambda) \tag{5.96}$$

For N independent sources of information, the likelihood term, $L(\lambda_1^*, \cdots, \lambda_N^* | \lambda)$ can be written as:

$$L(\lambda_1^*, \cdots, \lambda_N^* | \lambda) = \prod_{i=1}^{N} P_i(\lambda_i^* | \lambda) \tag{5.97}$$

where $P_i(\lambda_i^* | \lambda)$ is the probability that the estimate of the ith source is $\lambda_i^*$, when the true value of the unknown quantity is λ.

The case of dependent sources of information is discussed in Reference 5-48. Obviously, if the ith source is a perfect one,

$$P_i(\lambda_i^* | \lambda) = \delta(\lambda_i^* - \lambda) \tag{5.98}$$

which means that the estimate, $\lambda_i^*$, is the true value. The posterior, $P(\lambda | \lambda_i^*, \cdots, \lambda_N^*)$, in this case, will be entirely determined by the estimate of this source:

$$P(\lambda | \lambda_1^*, \cdots, \lambda_N^*) = \delta(\lambda - \lambda_i^*) \tag{5.99}$$

In another extreme, when it is believed that the source is totally unreliable,

$$P_i(\lambda_i^* | \lambda) = C \tag{5.100}$$

where C is a constant. This means that if the true value is λ, the estimate of the ith source can be anything. Using a likelihood of this form in Equation (5.97) will show that the estimate of this source, as expected, has no effect on shaping the posterior state of knowledge.

The likelihood term in this approach is the most crucial element. It reflects the analyst's degree of confidence in the sources of information, their accuracy, and the degree of applicability of their estimates to the particular case of interest.

As can be seen, the subjective nature of evaluating and "weighting" of the evidence from different sources fits very well in the above formulation. This becomes clearer in discussing the following models for the likelihood functions in Equation (5.97).

Suppose that in estimating the true value of $\lambda_t$, the ith source makes an error of magnitude E. Two simple models relating $\lambda_t$, E, and $\lambda_i^*$ are:

$$\lambda_i^* = \lambda_t + E \tag{5.101}$$

$$\lambda_i^* = \lambda_t \times E \tag{5.102}$$

In the model of Equation (5.101), if a normal distribution is assumed for the error term of the estimate of each source, the likelihood function will be a normal distribution with mean equal to $\lambda_t + b_i$, where bi is the expected error, or, in other words, a "bias" term about which the error of the ith source is propagated.

Formally, we have:

$$P(\lambda_i^* | \lambda_t) = \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left\{-\frac{1}{2}\left(\frac{\lambda_i^* - (\lambda_t - b_i)}{\sigma_i}\right)^2\right\} \quad (5.103)$$

The variance of the likelihood, $\sigma_i^2$, is the variance of the error distribution. Values of $b_i$ and $\sigma_i$ are subjectively assessed by the data analyst, and reflect the credibility and accuracy of the source as viewed by the data analyst. Sometimes, certain information provided by the source, such as the uncertainty bound for the estimate, can be used to assess $\sigma_i$.

If, in addition to a normal likelihood function, a normal prior distribution representing the state of knowledge of the data analyst is assumed for $\lambda_t$ with mean $\lambda_0$ and variance $\sigma_0^2$, the posterior distribution in Equation (5.96) will also be normal with mean, $\sigma_p$, given by:

$$\lambda_p = \sum_{i=0}^{N} w_i (\lambda_i^* - b_i) \quad (5.104)$$

and variance

$$\sigma_p^2 = \left(\sum_{i=0}^{N} \frac{1}{\sigma_i^2}\right)^{-1} \quad (5.105)$$

where $w_i$, defined as:

$$w_i = \left(\frac{\sigma_p}{\sigma_i}\right)^2 \quad (5.106)$$

is the weight given to the ith source.

Note that:

$$\sum_{i=0}^{N} w_i = 1 \quad (5.107)$$

The mean therefore is a weighted average of the individual estimates after correcting for their expected biases. Also, as can be seen from Equation (5.106), smaller values of $\sigma_i$ result in higher weights, implying that the source that is believed to make errors of smaller magnitudes ($\sigma_i$ is the variance of E) is assigned a higher weight, which is intuitively expected. Extreme cases are when $\sigma_i = 0$ (highest degree of confidence in the ith estimate), for which $w_i = 1$, and when $\sigma_i = \infty$ (no confidence at all) for which $w_i = 0$.

If, instead of the model of Equation (5.101), the model of Equation (5.102) is applied and the logarithm of the error is assumed to be normally distributed, the likelihood function for the ith source becomes a lognormal distribution:

$$P_i(\lambda_i^*|\lambda_t) = \frac{1}{\sqrt{2\pi}\sigma_i\lambda_i^*}\exp\left\{-\frac{1}{2}\left(\frac{\ell n\lambda_i^* - (\ell n\lambda_t + \ell nb_i)}{\sigma_i}\right)^2\right\} \quad (5.108)$$

where $\ell nb_i$ is the logarithmic mean error about the logarithm of the true value, $\ell n\lambda_t$, and $\sigma_i$ is the multiplicative standard deviation. Again, $P_i(\lambda_i^*|\lambda_t)$ is the probability that the estimate of the ith source is $\lambda_i^*$ when the true value of the failure rate is $\lambda_t$. Some evidence in support of the lognormality of $P_i(\lambda_i^*|\lambda_t)$ is provided in References 5-45 and 5-48.

By using the model of Equation (5.108) for individual likelihoods in Bayes' theorem, Equation (5.96), and assuming a lognormal prior distribution for $\lambda_t$, the posterior state of knowledge will also be a lognormal with the following median value:

$$\lambda_{50,p} = \sum_{i=0}^{N}\left(\frac{\lambda_i^*}{b_i}\right)^{w_i} \quad (5.109)$$

where $w_i$ is defined, as in Equation (5.106).

The median, then, is a weighted geometric average of the individual estimates after correcting for the multiplicative biases. Note that the usual arithmetic and geometric average methods frequently used in the literature are special cases of these Bayesian normal and lognormal models. For instance, Reference 5-43 uses the following geometric average of the estimates provided by several experts:

$$\bar{\lambda} = \left(\sum_{i=1}^{N}\lambda_i\right)^{1/N} \quad (5.110)$$

which assumes equal weights ($w_i = 1/N$), no bias ($b_i = 1$), no prior information, and does not show any uncertainty about the resulting value.

**Example**

Reference 5-46 provides a point estimate of 4.60E-3 for the demand failure rate of motor-operated valves. We would like to use this estimate and obtain a state of knowledge distribution for the MOV failure rates. We use the lognormal model of Equation (5.108) to express our confidence in the estimated value:

$$P(\lambda_i^*|\lambda_t) = \frac{1}{\sqrt{2\pi}\sigma_1\lambda_1^*}\exp\left\{-\frac{1}{2}\left(\frac{\ell n\lambda_1^* - (\ell n\lambda_t + \ell nb_1)}{\sigma_1}\right)^2\right\} \quad (5.111)$$

where $\lambda_1^*$ is the estimate (5.60E-3), and $\lambda_t$ is the assumed true value of the failure rate that remains an unknown variable at this point. Our subjective judgment about the

magnitude of error of the data source is expressed by assigning numerical values to the "bias" term $b_1$ and the logarithmic standard deviation $\sigma_1$.

We assume that there is no systematic bias ($b_1 = 1$). We estimate $\sigma_1$ with the aid of range factor, which is a more understandable quantity. Unless otherwise indicated, the range factor here is defined as the ratio of the 95th to the 50th percentiles of the lognormal distribution.

Therefore, given the range factor, the value of $\sigma_1$ is obtained from the following equation:

$$\sigma_1 = \frac{\ell n RF}{1.645} \tag{5.112}$$

For our example, we assume a range factor of 3. Normally, such a range factor represents a relatively high degree of confidence and means that the source's estimate could be a factor of 3 higher or lower than the true failure rate and that such a statement is made with 90% confidence. Using this range factor in Equation (5.112) results in a value of 0.67 for $\sigma_1$.

If we now use the likelihood of Equation (5.111)in Bayes' theorem, Equation (5.96), and assume a flat prior distribution, $P_0(\lambda_t)$, the posterior distribution will be:

$$P(\lambda|\lambda_1^* = 5.6E-3) = 106.65 \exp\left\{-\frac{1}{2}\left(\frac{\ell n\lambda - \ell n 5.6E-3}{0.67}\right)^2\right\} \tag{5.113}$$

This has the following characteristics:

| Parameter | Value |
|---|---|
| 5th Percentile | 1.87E-3 |
| 50th Percentile | 5.60E-3 |
| 95th Percentile | 1.68E-2 |
| Mean | 7.01E-3 |

#### *5.4.2.2.2 Estimating Distributions Using Point Estimates of Various Sources*

We now go back to our original problem, which was estimating the generic failure rate distribution $\phi(\lambda|\theta)$. This time, however, we assume that instead of having the set of $\langle k_i, T_i \rangle$ defined in Equation (5.78) from various sites, we are given one estimate, $\lambda_i^*$, for each site. That is, the evidence is of the form:

$$I_2 = \{\lambda_i^* i = 1, \cdots, N\} \tag{5.114}$$

The model to be used is a combination of the methods presented previously and is fully discussed in References 5-44 and 5-48. A particular family of parametric distributions, $\phi(\lambda|\theta)$, is assumed for $\lambda$, and the information $I_2$ is used in Bayes' theorem to obtain a

posterior distribution over the entire set of possible values of q and consequently over all possible distributions $\phi(\lambda|\theta)$. Formally,

$$P(\theta|I_2, I_0) = F^{-1}L(I_2|\theta, I_0)P_0(\theta|I_0) \tag{5.115}$$

See the set of definitions immediately following Equation (5.80) for interpretation of the terms in Equation (5.115).

The total likelihood function in the present case when $\lambda_i$'s are independently estimated can be written as (see Equation [5.82]):

$$L(I_2|\theta, I_0) = \sum_{i=1}^{N} P_i(\lambda_i^*|\theta, I_0) \tag{5.116}$$

where

$$P_i(\lambda_i^*|\theta, I_0) \equiv \text{probability that the estimate provided for the ith site is } \lambda_i^* \text{ if the parameter of the population variability distribution of the failure rates is } \theta. \tag{5.117}$$

To make matters clearer, note that we are assuming that the ith source of data is providing an estimate for the failure rate at a particular site, and all we know is that failure rates vary from site to site according to the variability curve $\phi(\lambda|\theta)$. Each $\lambda_i$ therefore is an estimate of one point in that distribution. As a result, there are two sources of variability in the estimates. First, estimates of individual sources are not necessarily perfect; i.e., they could involve errors and biases, as discussed in the previous section. Second, even if all the sources were perfect, the estimates would still be different due to the actual variation of the failure rate from site to site.

Based on our discussion in the previous section, the confidence that we have in the accuracy of the estimate $\lambda_i^*$ for the failure rate at the ith site can be modeled by a lognormal distribution (see Equation [5.108]). Assuming no bias, we have:

$$P_i(\lambda_i^*|\lambda_i) = \frac{1}{\sqrt{2\pi}\sigma_1\lambda_1^*} \exp\left\{-\frac{1}{2}\left(\frac{\ell n\lambda_i^* - \ell n\lambda_i}{\sigma_i}\right)^2\right\} \tag{5.118}$$

where $\lambda_i$ is the true value of the failure rate at the ith site. Again, we really do not know $\lambda_i$, but we assume that it belongs to $\phi(\lambda|\theta)$, the distribution representing the variability of $\lambda_i$'s from site to site. The relationship between $P_i(\lambda_i^*|\theta, I_0)$ and $\phi(\lambda|\theta)$ is shown in Figure 5-11.

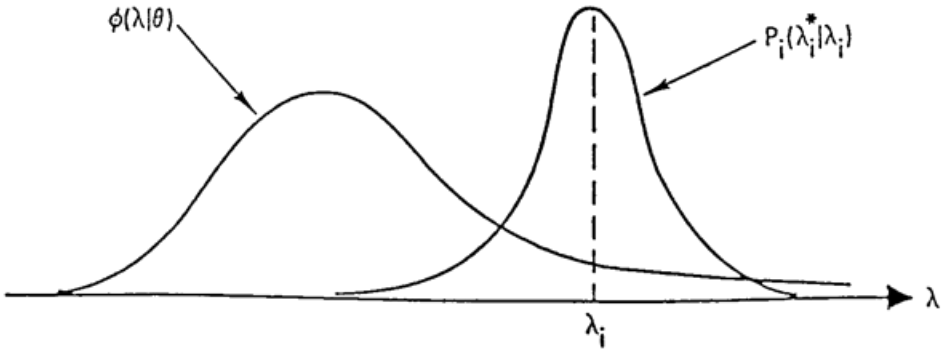



**Figure 5-11. The Relation between the Population Variability Curve and Uncertainty about Individual Estimates**

Therefore, as we did in the case of Equation (5.84), we can write:

$$P_i(\lambda_i^*|\theta, I_0) = \int_0^\infty P_i(\lambda_i^*|\lambda)\phi(\lambda|\theta)\, d\lambda \tag{5.119}$$

As mentioned earlier, in developing the failure rate distributions, $\phi(\lambda|\theta)$ is assumed to be lognormally defined by Equation (5.87).

With this assumption, the integration in Equation (5.49) can be done analytically, and the result is:

$$P_i(\lambda_i^*|\theta, I_0) = \frac{1}{2\pi\sqrt{\sigma_i^2+\sigma^2}\lambda_i^*}\exp\left\{-\frac{1}{2}\frac{(\ell n\lambda_i^*-\mu)^2}{\sigma_i^2+\sigma^2}\right\} \tag{5.120}$$

Equation (5.115), Bayes' theorem, is now written as:

$$P(\theta|\lambda_i^*,\cdots,\lambda_N^*) = F^{-1}\sum_{i=1}^{N} P_i(\lambda_i^*|\theta, I_0)P_0(\theta|I_0) \tag{5.121}$$

The most probable and expected distributions of λ can be found in the same way as discussed in Section 2.2. The expected distribution is calculated by using the result of Equation (5.118) in Equation (5.89). The parameters of the most likely distribution are shown to be solutions of the following system of equations:

$$\mu = \sum_{i=0}^{N}\frac{(\sigma_i^2+\sigma^2)^{-1}}{\sum_{i=0}^{N}(\sigma_i^2+\sigma^2)^{-1}}\ell n\lambda_i^* \tag{5.122}$$

$$\sum_{i=1}^{N}\left[\frac{1}{\sigma_i^2+\sigma^2}-\left(\frac{(\ell n\lambda_i^*-\mu)^2}{\sigma_i^2+\sigma^2}\right)\right] = 0 \tag{5.123}$$

For perfect sources of information (i.e., $\sigma_i = 0$), the above equations simplify and result in the following solution:

$$\mu = \ell n\left(\prod_{i=1}^{N} \lambda_i^*\right)^{1/N} \tag{5.124}$$

$$\sigma^2 = \frac{1}{N}\sum_{i=0}^{N} (\ell n\lambda_i^* - \mu)^2 \tag{5.125}$$

Note that Equations (5.124) and (5.125) are similar to the conventional results for fitting a lognormal distribution to a set of estimates. It should also be mentioned that the results of this section apply to any set of failure rate estimates from various sources where a true variability is suspected to exist among the actual values being estimated by each source. For instance, if several generic sources of data provide estimates for a particular type of equipment and it is known or suspected that each source's estimate is based on a different subset of the population, the methods of this section can be applied to obtain a generic distribution representing the "source to source" variability of the failure rate.

**Example**

The following set of estimates is available for the demand failure rate of MOVs:

| Source | Estimate |
|---|---|
| WASH-1400 (Reference 5-42) | 1.00E-3 |
| NUREG/CR-1363 (Reference 5-46) | 5.60E-3 |
| GCR (Reference 5-49) | 1.00E-3 |

To use the model of this section, we need to assign range factors to each source as a measure of our confidence in the estimate provided by that source. In this way, we will be able to determine $P_i(\lambda_i^*|\lambda_i)$, Equation (5.118), for each source.

Following our discussion in the previous example, we assign a range factor of 3 to the estimate of NUREG/CR-1363. For the estimate of WASH-1400, we assign a range factor of 5, which results in a broader likelihood, $P_i(\lambda_i^*|\lambda_i)$, for that source and represents a lesser degree of confidence as compared to NUREG/CR-1363. This is due to the fact that the estimate of NUREG/CR-1363 appears to be based on a larger sample of MOV failures in nuclear applications than does the estimate of WASH-1400. The latter provides a range factor of 3 for the lognormal distribution whose median (1.00E-3) we have taken as the estimate. Assigning a larger range factor of 5 also means that we believe that WASH-1400 has overstated its confidence in the estimated median value.

The idea of broadening some WASH-1400 distributions when used as generic curves was introduced in an early site-specific PRA study (References 5-50 and 5-51) where the WASH-1400 curves (as given) were used as generic prior distributions. It was then found that several posterior distributions, reflecting the evidence of the specific site, lay in the tail region of the prior distributions on the high side. These results led us to the conclusion that the generic curves had to be broadened to reflect greater uncertainty.

References 5-52 and 5-53 provide further support to our decision. In Reference 5-52, the authors reviewed experimental results that test the adequacy of probability assessments, and concluded that "the overwhelming evidence from research on uncertain quantities is that people's probability distributions tend to be too tight. The assessment of extreme fractiles is particularly prone to bias." Referring to the Reactor Safety Study, they state, "The research reviewed here suggests that distributions built from assessments of the 0.05 and 0.95 fractiles may be grossly biased."

Commenting on judgmental biases in risk perception, Reference 5-53 states:

> A typical task in estimating uncertain quantities like failure rates is to set upper and lower bounds such that there is a 98% chance that the true value lies between them. Experiments with diverse groups of people making many different kinds of judgments have shown that, rather than 2% of true values falling outside the 98% confidence bounds, 20% to 50% do so [Reference 5-52]. Thus, people think that they can estimate such values with much greater precision than is actually the case.

The numerical effect of using a larger range factor is illustrated in the following table:

| Distribution | 5th Percentile | Median | Mean | 95th Percentile | Range Factor |
|---|---|---|---|---|---|
| WASH-1400 | 3.3E-4 | 1.0E-3 | 1.2E-3 | 3.0E-3 | 3 |
| Broadened Distribution | 2.0E-4 | 1.0E-3 | 1.6E-3 | 5.0E-3 | 5 |

We see here that the medians are the same and that the mean value increases slightly reflecting the extension of the high side tail of the curve.

For the cases where WASH-1400 was the only source used for a failure rate, the above methodology was used to generate a broader generic curve from the distribution of WASH-1400. The applied range factor, however, was not necessarily the same for each

case. For the estimates from the three sources listed previously, the range factors are assigned as follows:

| Source | Range Factor |
|---|---|
| WASH-1400 | 5 |
| NUREG/CR-1363 | 3 |
| GCR | 10 |

The above values and the estimates from the three sources were used as input to Mode 2 of the Data Analysis module of RISKMAN, which evaluates Equations (5.118) through (5.121) and obtains an expected distribution based on an integration similar to Equation (5.89).

The resulting histogram has the following characteristics:

| Parameter | Value |
|---|---|
| 5th Percentile | 3.05E-4 |
| 50th Percentile | 2.34E-3 |
| 95th Percentile | 1.67E-2 |
| Mean | 4.43E-3 |

#### *5.4.2.2.3 Generic Distributions Based on a Mix of Type 1 and Type 2 Data*

An obvious extension of the situations discussed in the previous sections is the case where a mix of Types 1 and 2 information is available.

In this case, the equivalent of Equations (5.80) and (5.115) is:

$$P(\theta|I_2, I_1, I_0) = F^{-1}L(I_2, I_1|\theta, I_0)P_0(\theta|I_0) \quad (5.126)$$

If $I_1$ and $I_2$ are independent pieces of information,

$$L(I_2, I_1|\theta, I_0) = L(I_2|\theta, I_0)L(I_1|\theta, I_0) \quad (5.127)$$

where the terms in the right side of the equation are defined by Equations (5.80) and (5.116).

The expected distribution of L can now be found from:

$$\bar{\phi}(\lambda) = \int_0^\infty \phi(\lambda|\theta)\, P(\theta|I_2, I_1, I_0)d\theta \quad (5.128)$$

**Example**

As an example, we use the combination of the data given in the examples in the previous sections. This information was used as the main input to the Data Analysis module of RISKMAN, which calculates Equations (5.126) through (5.128). The resulting discretized distribution has the following characteristics:

| Parameter | Value |
|---|---|
| 5th Percentile | 8.13E-4 |
| 50th Percentile | 3.07E-3 |
| 95th Percentile | 1.37E-2 |
| Mean | 4.29E-3 |

A summary of the Types 1 and 2 evidence and the results of this example are presented in Figure 5-12.

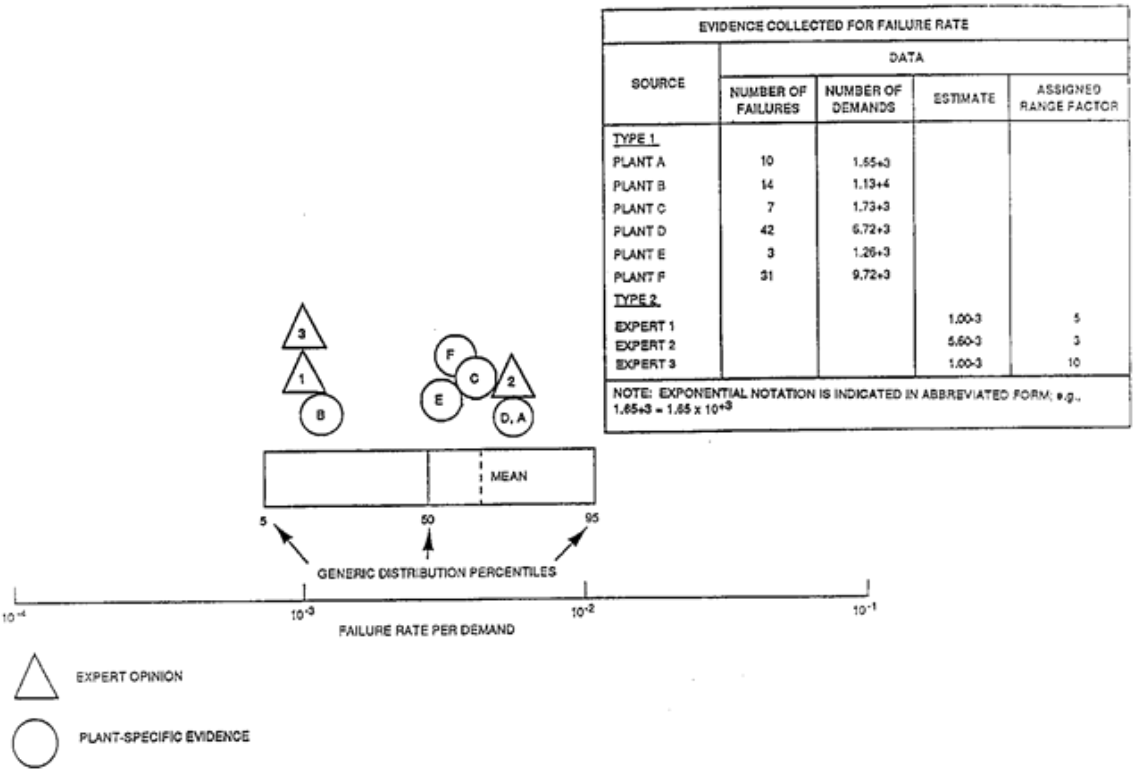



**Figure 5-12. Application of RISKMAN to Develop Generic Distribution for MOV Failure Rates**

### 5.4.2.3 Incorporation of Site-Specific Evidence

Data specialization, or the development of site-specific failure rate distribution, is achieved by applying Bayes' theorem as follows:

$$P(\lambda|E_2) = F^{-1}L(E_2|\lambda)P_0(\lambda) \quad (5.129)$$

where $P(\lambda|E_2)$ is the site-specific failure rate distribution reflecting the site-specific experience $E_2$, and the generic distribution $P_0(\lambda)$ is the prior state of knowledge about the failure rate of the component in question. The likelihood term, $L(E_2|\lambda)$, takes the form of a Poisson distribution when λ is the rate of failure per unit time and the evidence $E_2$ is k failures in T time units:

$$P(k, T|\lambda) = \frac{(\lambda T)^k}{k!} e^{-\lambda T} \quad (5.130)$$

If λ is a demand failure frequency and $E_2$ is k failures in D demands, then $L(E_2|\lambda)$ is a binomial distribution:

$$P(k, T|\lambda) = \frac{D!}{(D-k)!k!}(1-\lambda)^{D-k}\lambda^k \quad (5.131)$$

It should be noted that, when developing a distribution for λ that is specific to a certain site (the "two-stage" Bayesian procedure is described in Reference 5-41), the data for that site should not be incorporated into the first stage of the analysis; i.e., when developing the expected population variability curve via Modes 1, 2, or 3. The use of these data in the first stage leads to a "double counting" of the evidence in the second stage.

### 5.4.2.4 Advantage of Using a Bayesian Approach

The magnitude of the effect of adding site-specific data depends on the relative strength of the data compared with the prior level of confidence expressed in the form of the spread of the prior distribution. Typically, both the location and the spread of the posterior or updated distribution are affected by the site-specific evidence. The mean value of the updated distribution could be higher or lower than the mean of the generic prior, but adding the site-specific data normally reduces the spread of the distribution, as shown in the following example. The generic distribution for the valve failure to operate on demand frequency is updated with 15 failures in 5,315 demands. Calculations were performed using RISKMAN. The following table compares some basic characteristics for the generic prior and updated distributions:

| Distribution | Mean (per demand) | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|
| Generic | 4.29E-3 | 8.13E-4 | 3.07E-3 | 1.37E-2 |
| Updated | 2.87E-3 | 1.79E-3 | 2.80E-3 | 4.12E-3 |

Another example of how the Bayesian procedure is used to incorporate site-specific data is illustrated in Figure 5-13. In this example, for motor-operated valves, suppose that the site-specific evidence revealed that there was 1 failure in 1,000 demands (Posterior 1) at the specific site being analyzed. As can be seen in this figure, the weight of this evidence pulls down the mean of the posterior distribution toward 1.0E-3, the point estimate of the site-specific evidence.

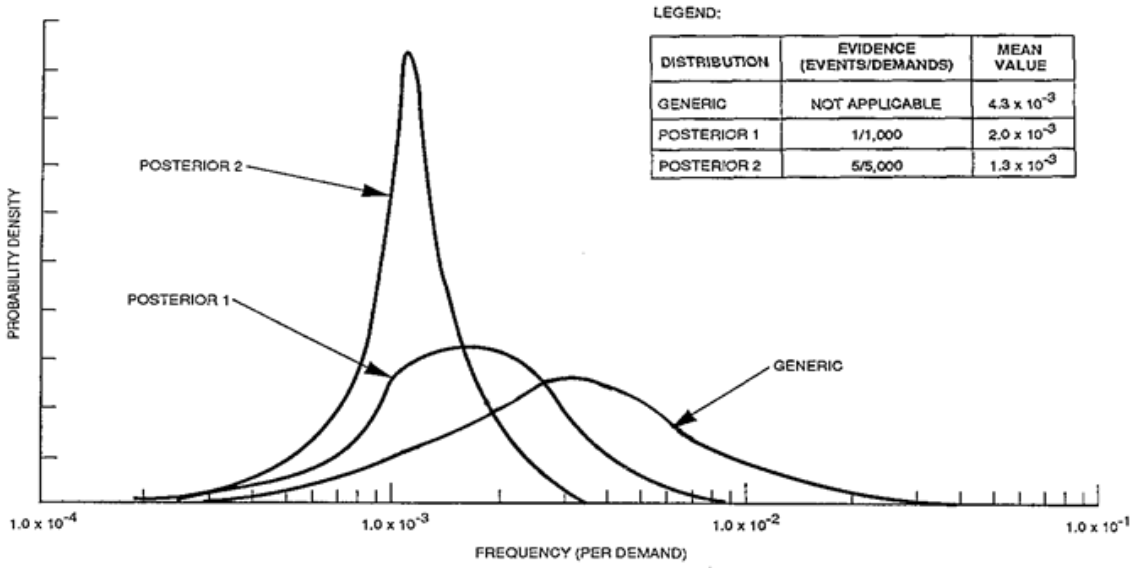



**Figure 5-13. Updating Generic Distributions with Site-Specific Evidence**

One useful property of Bayes' theorem is that it automatically weights the respective roles of the prior distribution and the evidence according to the amount of evidence applied. So, for example, if five times as much data that happen to be consistent with a point estimate of 1.0E-3 (i.e., 5 failures in 5,000 demands) were collected from the specific site being analyzed, the updated distribution (Posterior 2) would become very peaked about the point estimate of the evidence such that the role of the prior distribution becomes unimportant. The use of this approach eliminates the need to make and to document difficult and arbitrary decisions about when to use generic and when to use site-specific data. Even for a site with much experience, there are insufficient data for some of the rare events that are important (e.g., small loss of coolant accident frequency) to eliminate the need for both sources of data.

Another useful property of Bayes' theorem is that it provides a consistent treatment of any type of evidence, even when that evidence is made up from experience data in which no failures were observed. Suppose that we are using Bayes' theorem to evaluate the failure rate of a pump, l, at a specific site that tests the pump N times and observes no failures. Using Bayes' theorem, the probability that the failure rate of the pump is equal to any particular value, say,

$$p(\lambda^*|E) = F^{-1}L(E|\lambda^*)p_0\lambda^* \qquad (5.132)$$

where

F = $\int_0^\infty L(E|\lambda)\, p_0(\lambda) d\lambda$

$L(E|\lambda^*)$ = likelihood of observing evidence E, given that the failure rate is $\lambda^*$.

If we are quantifying a demand-based failure rate, the appropriate likelihood function is the binomial distribution. If the failure rate on demand is λ, the likelihood of observing exactly k failures in N demands is:

$$L(\text{kfailuresinNdemands}) = \binom{N}{k} \lambda^k (1-\lambda)^{N-k} \quad (5.133)$$

So, for zero failures in N demands,

$$L(0\text{failuresinNdemands}) = (1-\lambda)^N \quad (5.134)$$

This likelihood function is plotted in Figure 5-14 for different values of N and λ.

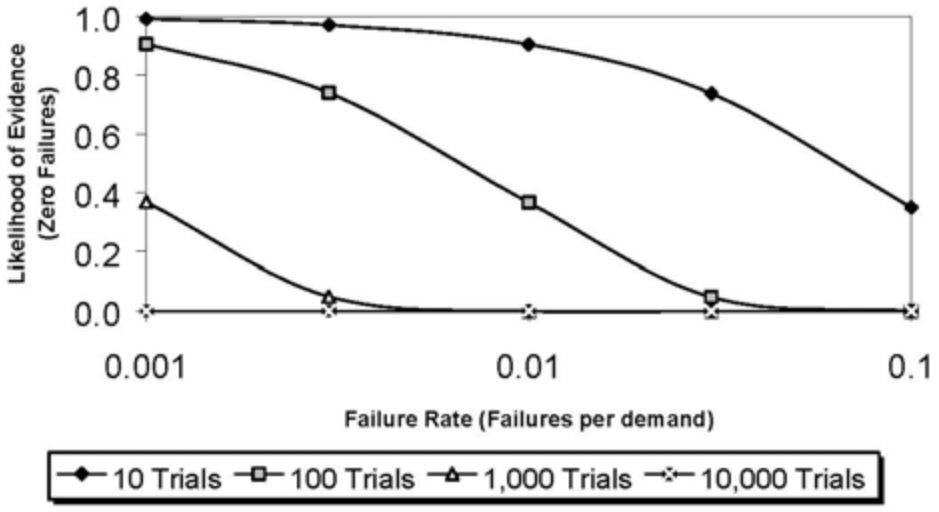



**Figure 5-14. Treatment of Zero Failures Using Binomial Likelihood Function**

To see how Bayes' theorem works for this kind of evidence, assume that λ can take on only one of five discrete values: {1, .03, .01, .003, or .001} and that the prior distribution is uniform over these values; i.e., a "flat distribution". Application of Bayes' theorem for zero failures in N demands is illustrated in the following table. As can be seen in this table, the posterior distribution is heavily influenced by the prior distribution for N = 10 demands, indicating rather weak evidence. However, for N = 1,000 demands, the posterior essentially vanishes for values of λ in excess of 3.00E-3 because of the influence of the likelihood function. Thus, zero failures does not pose any problems for the Bayesian approach, and the results are a strong function of the quantity of evidence; i.e., the number of successful demands.

| Application of Bayes' Theorem for Case of Zero Failures | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| λ | Prior Distribution | | | Binomial Likelihood Function for Zero Failures $(1-\lambda)^N$ | | | Posterior Distribution $p(\lambda \mid 0\ failure\ in\ N\ demands)$ | | |
| | $p_0(\lambda)$ | N = 10 | N = 100 | N = 1,000 | N = 10,000 | N = 10 | N = 100 | N = 1,000 | N = 10,000 |
| .1 | .2 | .35 | 2.6E-5 | 1.8E-46 | 0.00 | .088 | 1.3E-5 | 4.2E-46 | 0.00E+00 |
| .03 | .2 | .74 | .047 | 5.9E-14 | 0.00 | .187 | .023 | 1.4E-13 | 0.00E+00 |
| .01 | .2 | .90 | .37 | 4.3E-5 | 2.25E-44 | .229 | .178 | 1.0E-4 | 4.98E-40 |
| .003 | .2 | .97 | .74 | .049 | 8.95E-14 | .246 | .36 | .12 | 1.98E-09 |
| .001 | .2 | .99 | .90 | .37 | 4.52E-05 | .251 | .44 | .88 | 1.00E+00 |

### 5.4.3 RHBFSF Tank Acute Initiating Events Analysis

For acute event sequences, the analysis, three main sources of information were applied as follows: generic tank leak data for large and small leaks taken from NUREG/CR-6928; atmospheric storage tank leak frequencies taken from Oil & Gas Producers (OGP) Risk Assessment Data Directory Report No. 434-3 (References 5-54 and 5-55); leak data for Navy fuel tanks other than RHBFSF tanks provided by NAVFAC; and RHBFSF tank leak history data obtained from computer files provided by the Navy and EPA. The Bayesian update process for the data analysis was performed applying the RISKMAN Version 14.4 computer software, specifically via a RISKMAN model archived in a file named RHBFSF1.zip. [redacted]

A historical review of Red Hill Bulk Fuel Storage Tank (RHBFST) leak incidents was conducted to determine the potential for RHBFST leakage events going forward. This review considered:

1. Unverified RHBFST leak histories beginning in 1943 and ending in 1983 (References 5-56 to 5-75).

2. A series of emails by Whitacre, which repeat much of the unverified RHBFST leak histories, but include some additional information from later years (References 5-76 to 5-84).

3. Navy Audit Report – Department of the Navy Red Hill and Upper RHBFST Farm Fuel Storage Facilities N2010-0049, 2010 (Reference 5-85).

4. EPA report to the Board of Water Supply, July 20, 2015 (Reference 5-86).

5. Unverified Histories: Releases vs Tell-tales AND Verified Reporting: Since 1988 RHBFST (Reference 5-87).

6. AFHE Pearl Harbor RHBFST 0105 Findings RHBFST (Reference 5-88).

7. Individual RHBFST inspection reports, beginning in 1998 and ending in 2010 (Reference 5-89 to 5-99).

The above references often overlap in the resources materials they rely on. For example, the EPA report makes extensive use of the references in the first three bullets. The Navy verified RHBFST leak histories using Red Hill facility records that were not directly available at the time of the EPA review.

The unverified RHBFST leak histories and emails transmitted by Whitacre contain chronological histories for each of the 20 RHBFSTs. These RHBFST histories, beginning with RHBFST construction and operation in 1943, are uneven in the descriptions provided. In general they document records of fuel leaks detected while in operation, the dates of their occurrence, estimated amounts of fuel leaked in each incident, and often list fuel leak rates while the RHBFST still contained fuel. Often the fuel level at the time the leak was detected is also recorded. If the leakage was via the

RHBFST's tell-tale system, this is also noted. The dates of successful repair and initiation of RHBFST refilling are usually recorded. These RHBFST chronologies also describe to some extent the activities while undergoing inspections and repairs. Major RHBFST upgrades performed throughout the Red Hill facility history are also noted, for the years covered; i.e., up to 1983.

The Navy audit report provides RHBFST inspection records and a record of maintenance intervals; i.e., when they occurred and what was planned at the time for future RHBFST inspections. It does not include a summary of the RHBFST leak incidents.

The EPA report provides a site chronology which includes records of RHBFST leak incidents from the sources noted.

The NAVFAC comments on RHBFST leak histories contain additional information not available in the unverified histories. In some cases the leakages referred to involved water that was used specifically to test for leaks prior to filling the RHBFSTs. These are then excluded as fuel leakage events. The comments also contain records of the types and amounts of fuel determined to have been released in gallons. The durations of the leak events recorded are also noted.

The individual RHBFST inspection reports are generally not directly associated with individual Red Hill leak incidents, but rather document the periodic RHBFST inspections, especially the findings as to what anomalies were found. The records for inspections prior to those in 1998 are not available. The inspections documented in 1998 only thoroughly inspected approximately 10% of the RHBFST's steel liner, although a sampling in each of the major areas of the RHBFST liner were inspected; i.e., from among the lower dome, barrel, expansion, extension, and upper dome.

## Table 5-10. Surface Area Covered by Inspections

| Tank | API Document | Percent Surface Area of Tank Inspected |
|---|---|---|
| 1 | | |
| 2 | 2008 Oct 13_API 653 - Final Report_Red Hill Tank 2.pdf<br>RedHill_API653Report_Tank02_OCT08.pdf | 99.40% |
| 3 | | |
| 4 | | |
| 5 | RedHill_Tank05InspectionReport_18NOV10.pdf | 100% |
| 6 | Final API 653 Inspection Report-Tk 6_2007.pdf<br>RedHill_API653Report_Tank06_JAN07.pdf | 80% |
| 7 | RedHill_Tank07InspectionReport_1998.pdf | Not listed |
| 8 | RedHill_Tank08InspectionReport_1998.pdf | Not listed |
| 9 | | |
| 10 | RedHill_Tank10InspectionReport_1998.pdf | Not listed |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | API-653 Inspection Report-Tk15_2007.pdf<br>RedHill_API653Report_Tank15_JAN07.pdf | 83% |
| 16 | Tank 16 API 653 Final Inspection Report_2007.pdf<br>RedHill_API653Report_Tank16_JAN07.pdf | 79% |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | RedHill_API653Report_Tank20_05DEC08.pdf | 100% |
| **Total:** | **9** | - |

The QRVA requires model input parameters from knowledge of the RHBFST experience for use in quantifying the accident sequence models. These parameter inputs, from the references noted above, include the following:

1. A disposition of the historically observed fuel leakage incidents, as applicable to operation of the Red Hill facility in future years.

2. Information on the number of RHBFST outages and the years out of service for each RHBFST.

3. During RHBFST operation, the frequencies per RHBFST year of detected fuel leakage incidents within the range of fuel leakage rates historically experienced; i.e., small leakage rate incidents.

4. During RHBFST operation, the frequencies per RHBFST calendar year of fuel leakage incidents with fuel leakage rates larger than those historically experienced; i.e., large leakage rate incidents.

5. The probability of a leak incident occurring while filling the RHBFST during a return to service event following an extended maintenance period.

6. The probability of an undetected, above-fuel-level hole for use with overfill events during operation.

7. Probability of a hole below the realistic fuel maximum operating level for use with chronic leakage estimates.

8. Distribution of through hole locations.

#### *5.4.3.1 A Disposition of the Historically Observed Fuel Leakage Incidents, as Applicable to Operation of the Red Hill Facility in Future Years*

Based on the sources of Red Hill facility data available, a total of 65 leakage incidents were identified. [redacted] Of these, 10 were determined to involve leakage of water during tests and indicated in the NAVFAC comments on the RHBFST incident data. Of the 55 involving fuel leakage, the leakage incidents were divided into three groups:

- Fuel leaks during RHBFST operation detected by the tell-tale systems; 25 incidents.

- Fuel leaks during RHBFST operation detected not via the tell-tale systems but by changes in RHBFST liquid level, inventory changes determined from mass balances, or visually due to fuel external to the RHBFST; 15 incidents.

- Potential leaks from holes detected during API 653 RHBFST inspections that were judged large enough that they would have been detected if they were below the fuel level. The test inspection repair maintenance (TIRM) reports for RHBFST 2 (Reference 5-100) lists two through holes within the operating height range, and for RHBFST 15 (Reference 5-95) lists one through hole within the operating height

range. These three through holes were discovered during the inspection, but did not lead to a detectable fuel leak during RHBFST operation.

- Fuel leaks detected during RHBFST filling when returning to service from an extended outage; 12 incidents.

Of course, there are no fuel leakage events while the RHBFST is empty for inspection or repairs.

Key assumptions in the identification and disposition of the historical leakage incidents are:

- If a leakage incident is clearly reported in the unverified histories or Whitacre e-mails, but is not identified in the incidents recorded by NAVFAC, then the incident is counted as a RHBFST fuel leak unless the NAVFAC comments conclude that it was a leakage of water. There were nine incidents of this type that were included.

- The 25 incidents detected by the RHBFST tell-tale systems were removed from the count of fuel leakage incidents during operation. The tell-tale systems in RHBFSTs 1 through 16 were removed and patched over prior to 1984. The incidents detected by tell-tale systems prior to this time involved fuel leakage through the tell-tale leak detection system in the Lower Access Tunnel. This fuel leakage is directed to the drainage system in the Lower Access Tunnel, and not to the surrounding rock. Once the RHBFST tell-tale systems were removed and patched over, the frequency of fuel leakage incidents during operation dropped dramatically. The earlier tell-tale detected leaks have been attributed to fuel leakage via the tell-tale system pipes themselves, located inside and at the bottom of the RHBFSTs; i.e., not from the RHBFST liners. Corrosion of the tell-tale pipes at these locations by seawater in the years prior to their removal explains these early leak occurrences. That the rate of leak incidents have fallen off since their removal, and since ships offloading fuel are no longer susceptible to seawater splashing into the fuel cargo holes, its judged this is an adequate explanation for the reduction in leak incident frequency in later years; i.e., the incidents in earlier years detected via the tell-tales systems are no longer viable for operation going forward.

- The periods of RHBFST refilling following extended maintenance outages (i.e., returns to service) are judged to have a higher frequency per hour of detecting a leak than RHBFSTs in normal operation. These periods of RHBFST filling are judged to be best represented by assigning a probability of leak for the refill operation, and to exclude them from the fuel leakage rate to be used for other periods of operation. Twelve such leak incidents have been identified from Red Hill facility records, including the RHBFST 5 event in 2014.

- The undetected through holes discovered only during API 653 RHBFST inspections were located between 200’ to 212’ in the RHBFST, which is below the current realistic maximum operating limits. However, the size and relatively high height of these through holes suggests that the RHBFSTs were not operating with fuel levels above these through holes prior to discovery during the inspections. In the future it is expected that through holes at these elevations would be detected during the annual

leak tightness test. Therefore, these through holes are included in the incident count for the assessment of fuel leakage during operation.

#### 5.4.3.2 *Information on the Number of RHBFST Outages and the Years Out of Service for Each RHBFST*

One or more RHBFSTs may be out of service (i.e., empty of fuel) at a given time and therefore not susceptible to fuel leaks during these times. In order to better characterize the frequency of RHBFST leaks, and to match up the derived frequencies with RHBFST operating conditions in the future, it was decided to compute the frequencies of RHBFST leaks per RHBFST operating year rather than by calendar years. By definition, the frequency per RHBFST operating year is higher than that per calendar year since not every RHBFST is in service every year in its entirety.

Not every RHBFST outage (i.e., period when it is empty of fuel) is recorded in the Red Hill data, but enough of them are to provide a reasonable basis for estimating each RHBFST's number of extended outages and total outage durations over the life of the facility. The number of RHBFST outages is inferred from the reported leak incidents, inspections, design improvements, and repairs. A total of 91 such RHBFST outages are identified, which is slightly more than one RHBFST per year. The total number of RHBFST returns to service varies by RHBFST, the fewest having two (i.e., RHBFSTs 2 and 20) and the most (RHBFST 1 which is now permanently out of service) experiencing nine.

These RHBFST outages also correspond to the number of RHBFST fillings during returns to service.

Not all outage durations are accurately reported and so assumptions must be made. The total number of RHBFST operating years is estimated at 1,389 years, or about 111 RHBFST years were unavailable for operation because the RHBFST was empty of fuel and in an outage.

Key assumptions in deriving these inputs are:

- The historical references noted above were reviewed and only those where there is reference to a RHBFST outage were counted. This includes those references where the RHBFST number and dates of service were explicitly listed, and also general references indicating a group of RHBFSTs upgraded as a batch; e.g., RHBFSTs 1 through 16 had their tell-tale system removed and patched over. In other words, more RHBFST outages are counted in this total than are explicitly listed in the unverified RHBFST chronologies.

- RHBFST outages due to simple cleaning are not included in these outage totals since extensive repairs to the liners were not performed. These outages in the distant past are also relatively short and so their omission is not expected to be significant.

- Through the years, the outage records indicate there are more RHBFST outages involving repairs to the RHBFST liners in the early 1960s, early 1970s, early 1980s, around 1998, and in the years following 2005, than prior to 1960. By contrast there

are relatively few reported outages in the 1940s, 1950s, and late 1980s. When the durations for known outages are not explicitly reported, durations consistent with other RHBFST outages in the same period of years are used to estimate the RHBFST durations.

Considering these records of RHBFST years out of service, the years of service of each individual RHBFST can be estimated and trends in different time intervals can be developed.

#### *5.4.3.3 During RHBFST Operation, the Frequencies per RHBFST Year of Detected Leakage Incidents within the Range of Fuel Leakage Rates Historically Experienced (i.e., small leakage rate incidents)*

As described in Section 5.4.3.1, there have been 15 fuel leakage incidents that were detected during normal operation and did not involve tell-tale leakages to the Lower Access Tunnel. Leakage incidents detected during RHBFST filling while returning to service are excluded from this total and instead treated separately. Recorded leakage rates for all incidents were compiled. For some incidents only an estimate of the total amount of fuel leaked and the duration of the leakage are recorded from which an average leak rate can be determined. No RHBFST leakage rate greater than 1.8 gpm has ever been recorded and most of the 15 were much smaller. The 1.8 gpm peak leakage rate was estimated from one pause interval in the filling of RHBFST 5 during the 2014 incident. All other individual pause intervals and the average leak rate over the period of detected leakage for that incident were at lower flow rates, as measured by changes in the fuel level. A flow rate of 1.5 gpm is selected as representative of all historically observed leakage events and to be considered small in size.

Even though there were no fuel leaks recorded for the three holes discovered during RHBFST 2 and RHBFST 15 inspections, these holes are treated conservatively as potential leak incidents and are added to the actual leakage incidents. The two through holes discovered during the inspection of RHBFST 2 were conservatively counted as two leakage events. These additions increased the number of leak incidents during RHBFST operation from 15 to 18. The TIRM reports for RHBFST 2 (Reference 5-100) lists two through holes and the TIRM report for RHBFST 15 (Reference 5-95) lists one through hole.

The frequency of such small leakage rate incidents during normal operation for RHBFSTs can be estimated in several ways. A point estimate of the average RHBFST frequency can be obtained directly from the assessed incidents and RHBFST operating years recorded; i.e., 18/1316 RHBFST operating years = 1.37E-02 events per operating RHBFST year.

A more formal approach, which addresses uncertainties in these estimates, uses a mathematical technique of Bayesian updating. But there are several ways Bayesian methods can be applied depending on what is selected as the best representation of the prior evidence before updating with the Red Hill-specific evidence. Three approaches are described below.

1. The preferred Bayesian approach is to use Navy data for its underground storage tanks from six different locations. This data is used to create a two-stage prior distribution reflecting the variation in leak frequencies at different locations, excluding the Red Hill facility data. When this distribution is updated with 18 small leakage rate incidents in 1,316 RHBFST years, the mean of the posterior distribution is 1.24E-2 per RHBFST year of operation. By contrast, the Navy underground storage tank location, other than at Red Hill, with the highest point estimate frequency for leaks had an average underground storage tank leakage frequency at its location of 1.43E-3 leak incidents per tank year.

**Table 5-11. Empirical Evidence of Small Leaks from Six Navy Underground Storage Tank Locations**

| Empirical Data from 6 Navy UST (small leaks < 1.5 gpm) | | |
|---|---|---|
| **Plant Name** | **Events** | **Years** |
| Sasebo-Akasaki | 0 | 100 |
| Sasebo-Iorizaki | 0 | 128 |
| Sasebo-Yokose | 1 | 229 |
| Hakozaki | 6 | 998 |
| NB Guam | 1 | 1658 |
| FLC Puget Sound | 0 | 2530 |
| NAS Lemoore | 0 | 748 |
| Guantanamo Bay | 2 | 659 |
| **Total** | **10** | 7050 |

**Table 5-12. RISKMAN Two-Stage Prior Distribution for Small Leaks from Six Navy Underground Storage Tank Locations**

| Navy UST (small leaks < 1.5 gpm) Two-Stage Prior in RISKMAN | | | | | | |
|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Mean λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** |
| NGRID | Two-Stage Prior | 1.43E-03 | 3.81E-06 | 2.26E-05 | 4.58E-03 | 34.6 |

## Table 5-13. Bayesian Update of Navy UST Small Leaks with All RHBFST Evidence

| All Red Hill Tanks – Small < 1.5 gpm Two-Stage Posterior (prior NGRID) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Events** | **Tank Years** | **Mean λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **1 Incident/ n Yrs.** |
| LTKS | Two-Stage Posterior | 18 | 1315.6 | 1.24E-02 | 6.78E-03 | 1.11E-02 | 1.67E-02 | 1.57 | 81 |

## Table 5-14. Bayesian Update of Navy UST Small Leaks with Individual RHBFST Evidence

| Red Hill Specific Data for Tanks 1–20 Two-Stage Posterior (prior NGRID) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Events** | **Tank Years** | **Mean λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **1 Incident/ n Yrs.** |
| RH1S2 | Tank 1 External Leak Small | 6 | 45.4 | 7.61E-02 | 2.60E-02 | 7.13E-02 | 1.07E-01 | 2.01 | 13 |
| RH2S2 | Tank 2 External Leak Small | 2 | 68.7 | 9.60E-03 | 1.20E-04 | 5.74E-03 | 2.63E-02 | 14.80 | 104 |
| RH3S2 | Tank 3 External Leak Small | 1 | 71.7 | 4.34E-03 | 2.02E-05 | 1.49E-03 | 1.21E-02 | 24.50 | 230 |
| RH4S2 | Tank 4 External Leak Small | 0 | 72.0 | 1.03E-03 | 3.76E-06 | 1.94E-05 | 3.08E-03 | 28.60 | 971 |
| RH5S2 | Tank 5 External Leak Small | 1 | 64.6 | 4.51E-03 | 2.14E-05 | 1.63E-03 | 1.27E-02 | 24.20 | 222 |
| RH6S2 | Tank 6 External Leak Small | 1 | 64.2 | 4.52E-03 | 2.15E-05 | 1.64E-03 | 1.28E-02 | 24.40 | 221 |
| RH7S2 | Tank 7 External Leak Small | 0 | 69.4 | 1.04E-03 | 3.76E-06 | 1.95E-05 | 3.12E-03 | 28.80 | 962 |
| RH8S2 | Tank 8 External Leak Small | 0 | 70.6 | 1.03E-03 | 3.76E-06 | 1.95E-05 | 3.10E-03 | 28.70 | 971 |
| RH9S2 | Tank 9 External Leak Small | 1 | 70.9 | 4.36E-03 | 2.03E-05 | 1.50E-03 | 1.21E-02 | 24.50 | 229 |
| RH10S2 | Tank 10 External Leak Small | 1 | 64.8 | 4.50E-03 | 2.13E-05 | 1.62E-03 | 1.27E-02 | 24.40 | 222 |
| RH11S2 | Tank 11 External Leak Small | 1 | 71.1 | 4.36E-03 | 2.03E-05 | 1.50E-03 | 1.21E-02 | 24.50 | 229 |
| RH12S2 | Tank 12 External Leak Small | 0 | 64.5 | 1.05E-03 | 3.76E-06 | 1.97E-05 | 3.19E-03 | 29.10 | 952 |

## Table 5-14. Bayesian Update of Navy UST Small Leaks with Individual RHBFST Evidence (Continued)

| Red Hill Specific Data for Tanks 1–20 Two-Stage Posterior (prior NGRID) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Events** | **Tank Years** | **λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **1 Incident/ n Yrs.** |
| RH13S2 | Tank 13 External Leak Small | 1 | 65.0 | 4.47E-03 | 2.11E-05 | 1.60E-03 | 1.26E-02 | 24.40 | 224 |
| RH14S2 | Tank 14 External Leak Small | 1 | 70.9 | 4.34E-03 | 2.01E-05 | 1.49E-03 | 1.21E-02 | 24.50 | 230 |
| RH15S2 | Tank 15 External Leak Small | 0 | 67.8 | 1.04E-03 | 3.76E-06 | 1.96E-05 | 3.14E-03 | 28.90 | 962 |
| RH16S2 | Tank 16 External Leak Small | 1 | 68.4 | 4.42E-03 | 2.07E-05 | 1.55E-03 | 1.24E-02 | 24.40 | 226 |
| RH17S2 | Tank 17 External Leak Small | 1 | 70.3 | 4.35E-03 | 2.02E-05 | 1.50E-03 | 1.21E-02 | 24.50 | 230 |
| RH18S2 | Tank 18 External Leak Small | 0 | 71.0 | 1.03E-03 | 3.76E-06 | 1.95E-05 | 3.09E-03 | 28.70 | 971 |
| RH19S2 | Tank 19 External Leak Small | 0 | 33.3 | 1.19E-03 | 3.78E-06 | 2.09E-05 | 3.71E-03 | 31.30 | 840 |
| RH20S2 | Tank 20 External Leak Small | 0 | 71.0 | 1.03E-03 | 3.76E-06 | 1.95E-05 | 3.09E-03 | 28.70 | 971 |

2. A second approach is to use the frequency of leak incidents from the OGP (References 5-54 and 5-55) data for atmospheric tanks fixed roofs to construct the prior distribution. The frequency for all leaks is historically estimated to be 2.8E-03 per tank year. However, there is no estimate of uncertainty provided for this frequency. A constrained (by the mean) non-informative gamma distribution is therefore assumed for the OGP (References 5-54 and 5-55) prior data. This approach likely over estimates the actual uncertainty in this leakage frequency. Updating with the Red Hill-specific evidence of 18 incidents in 1,316 RHBFST years of operation yields a posterior mean of 1.24E-2 incidents per RHBFST operating year.

**Table 5-15. OGP Atmospheric Storage Tanks Small Leak Data**

| **OGP<br>Report No. 434 – 3<br>March 2010 (References 5-54 and 5-55)** | | | |
|---|---|---|---|
| **2.0 Summary of Recommended Data** | | | |
| Tank Description | Failure Mode | Leak Frequency (per tank year) | Leak Frequency (per hour) |
| Atmospheric Storage Tanks Fixed/Floating Roof | Liquid Spill outside Tank | 2.80E-03 | 3.19E-07 |
| **4.0 Review of Data Sources** | | | |
| Failure experience was reviewed from a number of sources: | | | |
| • [3] includes 122 cases of atmospheric storage tank fires world-wide during 1965-89. | | | |
| • [4] lists 69 such events during 1981-96. | | | |
| • [5] lists 107 events during 1951-95 (see [1] App I). | | | |

## Table 5-16. RISKMAN Two-Stage Prior Distribution from OGP Atmospheric Storage Tanks Small Leak Data

| Generic Distribution from OGP – Report No. 434 – 3 (References 5-54 and 5-55), in RISKMAN (prior) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Distribution Type** | **Mean (failures/ Year)** | **1 Incident/ n Yrs.** | **5th** | **Median** | **95th** | **Range Factor** |
| OGPS | Liquid Spill outside Tank | Gamma | 2.81E-03 | 355.9 | 9.29E-06 | 1.16E-03 | 9.91E-03 | 32.60 |

## Table 5-17. Bayesian Update of OGP Tank Small Leak Data with All RHBFST Evidence

| OGPS Updated with Red Hill Data | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Distribution Type** | **Mean (failures/ year)** | **1 Incident/ n Yrs.** | **5th** | **Median** | **95th** | **Range Factor** |
| RHOGPS | Small Tank Leaks | One-Stage Update Prior OGPS | 1.24E-02 | 80.6 | 7.96E-03 | 1.20E-02 | 1.71E-02 | 1.47 |

3. A third approach is to construct a prior by pooling all Navy underground tank leak incident data as another simple constrained (by the mean) non-informative prior (1.43E-3/tank year) and then to update this alternative prior with the Red Hill data of 18 incidents in 1,316 years of RHBFST operation. This approach yields a posterior mean of 1.11E-2 per RHBFST operating year. The pooling of data from all locations, rather than using the two-stage prior distribution approach, artificially lowers the posterior mean slightly, as compared to the first approach.

## Table 5-18. RISKMAN Non-Informative Prior for Small Leaks Data from Six Navy Underground Storage Tank Locations Pooled

| Navy UST – Small < 1.5 gpm | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Events** | **Alpha** | **Beta** | **λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **Source** |
| NAVYSG | Gamma | 0 | 0.5 | 352 | 1.43E-03 | 4.73E-06 | 5.88E-04 | 5.04E-03 | 32.6 | Navy Bulk Tank Spill Releases Data |

## Table 5-19. Bayesian Update of Pooled Navy UST Small Leak Data with All RHBFST Evidence

| All Red Hill Tanks – Small < 1.5 gpm Two-Stage Posterior | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Events** | **Tank Years** | **λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **1 Incident/ n Yrs.** |
| RHNGPR | One-Stage Update Prior NAVYSG | 18 | 1316.0 | 1.11E-02 | 7.14E-03 | 1.08E-02 | 1.54E-02 | 1.47 | 90 |

It is seen that each approach yields roughly the same small leakage frequency. This indicates that the amount of small leakage incident evidence from Red Hill is robust enough to make the specific choice of the prior insignificant.

Key assumptions in deriving these inputs are:

- The fuel leakage rates for the 18 incidents recorded in the entire history of Red Hill are all less than 1.8 gpm. An average fuel leakage rate of all such leakage incidents is much less than 1.8 gpm. A representative leakage rate of 1.5 gpm is selected as representative for the small fuel leakage event category. For tell-tale leakage events, the largest leak rate reported was also just 1.49 gpm.

- Fuel leakage incidents with leakage rates greater than what has been observed to date at Red Hill are considered separately.

- The Red Hill small leakage incidents included in this estimate are those detected during RHBFST API 653 inspections or during RHBFST operation, excluding those detected as tell-tale leakages, or as identified as leakage events involving water.

- Small leakage incidents detected during filling operations (i.e., while returning a RHBFST to service) are treated separately.

- Chronic leakage events that go undetected, are excluded from the small leakage frequency estimate; i.e., they are treated separately.

- The frequency of small leakage incidents is assumed constant throughout the history of Red Hill facility operation. The trends show a small decline, specifically over the latter part of the life of the facility. [redacted] These charts exclude the holes during returns to service since these holes are maintenance and repair related. Those are considered separately under Item 5.

- The average frequency of small leakage incidents is assumed to apply to all RHBFSTs in operation. Only RHBFST 1 has recorded more than 2 of the 18 small leakage incidents in the history at Red Hill. It recorded six incidents prior to its permanent shutdown in 2005. All other RHBFSTs recorded one or no leak incidents. While RHBFST 1 is clearly an outlier, none of the other RHBFSTs are. Although RHBFST 1 will not be operated in the future, use of the average frequency for RHBFST small leakages, including the six incidents that did occur at RHBFST 1, is judged acceptable.

- The most applicable prior with which to characterize evidence of Navy underground storage leakage frequencies other than at Red Hill is the world-wide Navy UST data, provided the location to location variability is captured.

- None of the leakage incidents recorded at Navy UST, other than Red Hill, identified flow rates greater than those experienced at Red Hill.

- The small leakage frequency is assumed to occur during periods of RHBFST operation. None of the 18 leakage incidents recorded occurred when the affected RHBFST was undergoing a planned fuel movement (i.e., issue, receipt or transfer between RHBFSTs) or shortly thereafter. This is likely because fuel movement periods are only a small fraction of the total RHBFST operation time.

#### *5.4.3.4 During RHBFST Operation, the Frequencies per RHBFST Year of Fuel Leakage Incidents with Fuel Leakage Flow Rates Larger than Those Historically Experienced (i.e., "large" leakage rate incidents)*

No RHBFST fuel leakage incidents with leakage rates greater than 1.8 gpm have historically been observed at Red Hill facility. Larger rates due to random RHBFST leaks (i.e., not due to external factors) are feasible and so still of interest. A 1.5 gpm leak corresponds to an equivalent hole at the bottom of a full (i.e., filled to the current maximum level of 213') RHBFST of roughly .072" in diameter; i.e., less than 0.1 inches. All hole sizes greater than 0.072" equivalent diameter are from now on called "large".

Larger through holes have been found via RHBFST inspections at Red Hill but these were judged to be above the operating fuel level and most were well above the fuel level; i.e., in the upper dome sections. The largest single through hole discovered to date was in RHBFST 5 in 2010. It was 0.75" in diameter. This hole was discovered in the second row of plates from the top of the upper dome; i.e., well above the maximum fuel level. This size hole, if it instead suddenly developed at the bottom of a RHBFST, would have a leakage rate of approximately 160 gpm. Since this maximum size hole was found near the top of the RHBFST, even if the RHBFST was completely full, the actual external leakage rate would have been much less. Further, such larger holes do not develop suddenly, as indicated by 75 years of Red Hill facility operating data. Much smaller holes can be detected well before they grow to 0.75". There are four relatively large through holes that have been detected above the fuel level in RHBFSTs that underwent thorough inspections; i.e., sizes of 0.125", 0.25", 0.5", and 0.75" in diameter. The average of the flow of these four through hole sizes is chosen as the representative hole size for "large" leakage events, none of which have yet occurred below the fuel level at Red Hill. Therefore a 0.5" diameter hole is selected as representative for "large" holes, and corresponds to a leak rate of 72 gpm if it was located at the bottom of the RHBFST. By contrast, if the hole were only 20' below the liquid level, the corresponding flow rate would be about 22 gpm.

The frequency of a large hole, leakage rate incidents during normal operation for RHBFSTs can again be estimated in several ways. A point estimate of the frequency cannot be obtained directly since there have been no reported occurrences of hole sizes greater than 0.072" below the liquid level. If we instead count zero incidents as 1/3 of an incident, the point estimate large leak frequency would be 0.33/1316 RHBFST operating years = 2.5E-4 large leakage events per operating RHBFST year.

Bayesian methods are again used with different representations of the prior evidence before updating with the Red Hill-specific evidence. Three approaches are described below.

1. The preferred Bayesian approach is to again use the Navy UST data from the six different locations. This is for zero large leakage incidents in 7,050 tank years. This data is used to create a two-stage prior distribution reflecting the variation in large leak frequencies at different locations, excluding the Red Hill facility data. When this prior distribution is updated with zero large leakage rate incidents in 1,316 RHBFST years, the mean of the posterior distribution is 6.65E-5 per RHBFST year of operation.

**Table 5-20. Empirical Evidence of Large External Leaks from Six Navy Underground Storage Tank Locations**

| Empirical Data from Six Navy UST (large leaks > 1.5 gpm) | | |
|---|---|---|
| **Plant Name** | **Events** | **Years** |
| Sasebo-Akasaki | 0 | 100 |
| Sasebo-Iorizaki | 0 | 128 |
| Sasebo-Yokose | 0 | 229 |
| Hakozaki | 0 | 998 |
| NB Guam | 0 | 1658 |
| FLC Puget Sound | 0 | 2530 |
| NAS Lemoore | 0 | 748 |
| Guantanamo Bay | 0 | 659 |
| **Total** | **0** | **7050** |

## Table 5-21. RISKMAN Two-Stage Prior Distribution for Large External Leaks from Six Navy UST Locations

| RM Dist. | Distribution Type | λ/Yr. | 5th | Median | 95th | Range Factor |
|---|---|---|---|---|---|---|
| NAVYLG | Two-Stage Prior | 7.63E-5 | 8.7E-7 | 2.77E-05 | 1.36E-04 | 12.5 |

## Table 5-22. Bayesian Update of Navy UST Large Leaks with All RHBFST Evidence

| All Red Hill Tanks – Small > 1.5 gpm Two-Stage Posterior (prior NAVYLG) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| RM Dist. | Distribution Type | Events | Tank Years | λ/Yr. | 5th | Median | 95th | Range Factor | 1 Incident/ n Yrs. |
| RHLNG | Two-Stage Posterior | 0 | 1315.6 | 6.65E-05 | 8.70E-07 | 2.26E-05 | 1.34E-04 | 12.4 | 15,038 |

2. A second approach is to use the frequency of tank rupture incidents from the OGP (References 5-54 and 5-55) data for atmospheric tanks fixed roofs to construct the prior distribution for large leaks. The frequency for all leaks is historically estimated to be 3.01E-6 events per tank year. However, there is no estimate of uncertainty provided for this frequency. A constrained (by the mean) non-informative gamma distribution is therefore assumed for the OGP (References 5-54 and 5-55) prior. This approach overestimates the actual uncertainty in this leakage frequency. Once updated with the Red Hill-specific evidence of zero incidents in 1,316 RHBFST years of operation yields a posterior mean of 2.99E-6 incidents per RHBFST operating year.

**Table 5-23. OGP Atmospheric Storage Tanks Large Leak Data**

| **OGP<br>Report No. 434 – 3<br>March 2010 (References 5-54 and 5-55)** | | | |
|---|---|---|---|
| **2.0 Summary of Recommended Data** | | | |
| Tank Description | Failure Mode | Leak Frequency (per tank year) | Leak Frequency (per hour) |
| Atmospheric Storage Tanks Fixed/Floating Roof | Tank Rupture | 3.01E-06 | 3.42E-10 |
| **4.0 Review of Data Sources** | | | |
| Failure experience was reviewed from a number of sources: | | | |
| • [3] includes 122 cases of atmospheric storage tank fires world-wide during 1965-89. | | | |
| • [4] lists 69 such events during 1981-96. | | | |
| • [5] lists 107 events during 1951-95 (see [1] App I). | | | |

## Table 5-24. RISKMAN Two-Stage Prior Distribution from OGP Atmospheric Storage Tanks Large Leak Data

| Generic Distribution from OGP – Report No. 434 – 3 (References 5-54 and 5-55), in RISKMAN (prior) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Distribution Type** | **Mean (failures/year)** | **1 Incident/ n Yrs.** | **5th** | **Median** | **95th** | **Range Factor** |
| OGPL | Tank Rupture | Gamma | 3.01E-06 | 332,225.9 | 9.96E-09 | 1.24E-06 | 1.06E-05 | 32.60 |

## Table 5-25. Bayesian Update of OGP Tank Large Leak Data with All RHBFST Evidence

| OGPS Updated with Red Hill Data | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Failure Mode** | **Distribution Type** | **Mean (failures/year)** | **1 Incident/ n Yrs.** | **5th** | **Median** | **95th** | **Range Factor** |
| RHOGPL | Large Tank Leaks | One-Stage Update Prior OGPL | 2.99E-06 | 334,448.2 | 9.99E-09 | 1.23E-06 | 1.05E-05 | 32.60 |

3. A third approach is to construct a prior by pooling all underground tank Navy leak incident data as another simple constrained (by the mean) non-informative prior (7.13E-5/tank year) and then update this alternative prior with the Red Hill data of zero large leak rate incidents in 1,316 years of RHBFST operation. However, with zero large leak rate incidents the approximate prior mean is estimated 0.33/7050 RHBFST years = 4.7E-05 per tank year. Assuming this mean as defining the mean for the constrained non-informative prior, yields a posterior mean of 6.01E-5 large leakage events per RHBFST operating year.

**Table 5-26. RISKMAN Non-Informative Prior for Large Leaks Data from Six Navy Underground Storage Tank Locations Pooled**

| Tank 1–20 Releases – Large > 2 gpm | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Events** | **Tank Years** | **Alpha** | **Beta** | **λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **Source** |
| NAVYL | Gamma | 0 | 7050 | 0.5 | 7050 | 7.13E-05 | 2.36E-07 | 2.94E-05 | 2.52E-04 | 32.6 | Navy Bulk Tank Spill Releases Data |

**Table 5-27. Bayesian Update of Pooled Navy UST Large Leak Data with All RHBFST Evidence**

| All Red Hill Tanks – Small > 1.5 gpm Two-Stage Posterior | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Events** | **Tank Years** | **λ/Yr.** | **5th** | **Median** | **95th** | **Range Factor** | **1 Incident/ n Yrs.** |
| RHNVYL | One-Stage Update | 0 | 1316.0 | 6.01E-05 | 2.00E-07 | 2.48E-05 | 2.12E-04 | 32.6 | 16,639 |

For the frequency of large leak incidents, the specific choice of the prior is significant.

The first approach yields a large leak frequency noticeably lower than that obtained for small leak events. The second approach uses tank rupture data from a different industry which may not include consideration of all leaks greater than a 0.072" hole and so is judged too low. The third approach gives greater weight to the extensive tank years of experience from the other Navy USTs. This third approach is selected as most appropriate for estimating the large leakage event frequency at Red Hill.

Key assumptions in deriving this input are:

- The Red Hill large leakage incidents included in this estimate are those that would be detected during RHBFST operation.

- Large leakage incidents detected during filling operations (i.e., while returning a RHBFST to service) are treated separately.

- The average frequency of large leakage rate incidents is assumed to apply to all RHBFSTs in operation. There have been no large leaks at any RHBFST so use of the average frequency for RHBFST large leakage rates for each individual RHBFST is judged acceptable.

- The most applicable prior with which to characterize evidence of Navy underground storage leakage frequencies other than at Red Hill is the constrained non-informative prior using pooled world-wide Navy UST data.

- None of the leakage incidents recorded at NAVY UST, other than Red Hill, reported flow areas greater than the small leakage events experienced at Red Hill; i.e., assumed each of the 10 events in the Navy UST had equivalent hole sizes less than 0.072" in diameter.

- The large leakage frequency is assumed to occur during periods of RHBFST operation whether or not a planned fuel movement is also occurring; i.e., the occurrence of issues, receipts, or transfers between RHBFSTs has no effect on the frequency.

#### *5.4.3.5 The Probability of a Leak Incident Occurring while Filling the RHBFST during a Return to Service Event Following an Extended Maintenance Period*

The probability of a small leak during RHBFST filling as part of a return to service event following extended maintenance period, can be estimated from Red Hill experience data. There have been 12 small leak incidents at Red Hill while filling as part of a return to service from extensive maintenance. The number of such returns to service for all RHBFST over the life of the facility is 91. This yields a point estimate probability per return to service of 12/91 = 0.13.

**Table 5-28. Summary of RHBFST Maintenance Outages and Return to Service**

| Tank | Years of Service | Outage Total (yrs) | Outage Total (days) | Number of Outages | Tell-Tale Work Outage (yrs) |
|---|---|---|---|---|---|
| 1 | 45.37 | 15.63 | 5711 | 9 | 1 |
| 2 | 68.74 | 4.26 | 1556 | 5 | 1 |
| 3 | 71.72 | 2.28 | 834 | 4 | - |
| 4 | 71.98 | 2.02 | 740 | 2 | - |
| 5 | 64.59 | 7.41 | 2707 | 4 | 2 |
| 6 | 64.15 | 7.85 | 2868 | 6 | 2 |
| 7 | 69.43 | 3.57 | 1306 | 5 | 1 |
| 8 | 70.63 | 2.37 | 868 | 3 | 1 |
| 9 | 70.95 | 2.05 | 751 | 4 | 1 |
| 10 | 64.80 | 8.20 | 2998 | 6 | 1 |
| 11 | 71.10 | 2.90 | 1060 | 3 | - |
| 12 | 64.47 | 7.53 | 2752 | 4 | 2 |
| 13 | 65.01 | 7.99 | 2921 | 5 | 1 |
| 14 | 70.92 | 3.08 | 1126 | 5 | |
| 15 | 67.79 | 5.21 | 1903 | 4 | 1 |
| 16 | 68.40 | 4.60 | 1683 | 7 | 1 |
| 17 | 70.33 | 1.67 | 609 | 4 | 2 |
| 18 | 71.02 | 0.98 | 360 | 3 | 2 |
| 19 | 33.26 | 20.74 | 7579 | 6 | 1 |
| 20 | 71.00 | 1.00 | 366 | 2 | 2 |
| **Totals** | **1315.65** | **111.35** | **40698** | **91** | **-** |

Most of the recorded RHBFST returns to service occurred before 1984; i.e., 74 events or just a bit less than 2 per calendar year. In the 34 years since 1983, there have only been 12 returns to service identified, or roughly one RHBFST every 3 years. Two other RHBFSTs (i.e., RHBFSTs 1 and 19) were removed from service permanently during this later period. Based on the API 653 RHBFST inspections planned for future years, a RHBFST return to service rate of 1 RHBFST per year now seems reasonable going forward.

Since 1983, only one small leakage event has occurred during a return to service, that being the 2014 event at RHBFST 5; i.e., 1 out of 12 (1/12 = .08), which is reasonably close to the probability averaged over all years of Red Hill facility operation. It therefore is judged reasonable to assume the probability of a small leakage during a RHBFST

return to service averaged over the entire Red Hill facility (i.e., 0.13) also applies in future years.

Key assumptions in deriving this input are:

- The frequency of RHBFST returns to service in future years is once per calendar year.

- The probability of experiencing a small leak while in the process of RHBFST refilling as part of a return to service in future years is the same as has been experienced over the life of Red Hill facility; i.e., approximately 0.13. No credit or degradation is expected from the more elaborate API 653 inspections and repairs going forward.

- The leak rate experienced assuming a leak occurs while in the process of RHBFST refilling as part of a RHBFST return to service are consistent with the small leakage category for normal operation; i.e., a representative flow rate of 1.5 gpm.

- For the large leak frequency during a return to service, it is assumed that the small leak rate for returns to service, reduced by the ratio of frequencies for large to small leaks for liner leaks during normal operation is a reasonable assumption; i.e., a factor of 5.5E-3 reduction.

#### *5.4.3.6 Probability of an Above Fuel Level Hole for Use with Overfill Events during Operation*

In the event of a RHBFST overfill event (i.e., above the realistic maximum fuel RHBFST level, roughly 212', planned by plant operations and also at which annual leak tightness tests are performed), there is some probability of a hole in the RHBFST liner above the realistic maximum fuel level, in the RHBFST upper dome. RHBFST inspection experience is used to compute this probability and to investigate the probable sizes of such holes. These holes are above the fuel level and so do not result in RHBFST leaks during RHBFST operation.

Only the most recent, API 653 inspection reports are used to estimate the hole probability above the maximum operating level because only these inspections cover 100% of the RHBFST liner and the inspection findings are thoroughly documented. Findings from earlier inspections are not as informative. The RHBFST inspections, for example, documented in 1998 did not inspect the entire RHBFST liner. There are 10 inspection reports that are certified as API 653 however only 7 of them that were performed after 2005 have listed close to a 100% liner inspection.

Of the seven API 653 RHBFST inspections reported since 2005, five holes in four RHBFSTs were found to have through-liner holes above the maximum operating level. This yields a point estimate of 5/7 = 0.72 for the probability of a hole above the maximum operating level at the time of the RHBFST inspection. However, these holes are not expected to have been in place during the entire interval since the previous inspection. For the five RHBFSTs discovered to have holes, the prior RHBFST inspections took place years earlier; i.e., 26, 27, 24, and 26 years. It is believed that the through-liner holes would likely only have occurred in the second half of the inspection interval, and possibly much later in the interval. Nevertheless, it is assumed that if half the inspection

interval is greater than 25 years, then the through hole is assumed to have occurred after the first 25 years. With this assumption, the years in which holes may have been present sum to (26+27+24+26)/2 = 51.5 RHBFST years. For the three RHBFST inspections without any holes above the maximum operating level, these RHBFSTs were last inspected 25 years (RHBFST 1), 25 years (RHBFST 6), and 66 years (RHBFST 20) prior. Therefore, the total years at risk of an overfilling event from these seven RHBFSTs that were thoroughly inspected since 2005 sum to 219 years. The probability of a through hole above the maximum operating level for a random occurrence of an overfilling event during normal operation, averaged over the seven RHBFST inspection intervals, is then 51.5/219 = 0.235.

**Table 5-29. Above-Maximum-Fuel-Level Holes Detected during Inspections**

| RHBFST | Years since Last Inspection | Undetected Through Holes above Maximum Fuel Level |
|---|---|---|
| 1 | 25 | |
| 2 | 26 | 1 |
| 5 | 27 | 1 |
| 6 | 25 | |
| 15 | 24 | 2 |
| 16 | 26 | 1 |
| 20 | 66 | |
| **Total** | **219** | |

Four of the RHBFST API 653 inspections documented holes of substantial sizes; i.e., hole diameters of roughly 1/8", 1/4", 1/2", and 3/4". The 1/4" and 3/4" holes were both found in RHBFST 5 as part of the same API 653 inspection. The holes found in two of the RHBFSTs were much smaller, likely just pinhole, though there were several through liner pinholes. For purposes of the QRVA, a representative size hole is obtained by averaging the flow areas of the four large hole sizes. An equivalent through hole diameter of roughly 0.5" is selected as representative of such holes.

A judgment based uncertainty distribution was created to model the occurrence of a hole to aid in computing a probability of an above maximum operating level hole. Three discrete probability distributions (DPD) were created to represent the probability of a hole developing in 24 years (RHBFST 15), in 26 years (RHBFST 16), and in 27 years (RHBFST 5). The probability of a hole is assumed 0.0 at time 0.0 and ends in 1.0 at the $24^{th}$, $26^{th}$, and $27^{th}$ year, respectively. The three distribution were averaged to create a final DPD distribution representing the occurrence of a hole above the maximum operating level.

**Table 5-30. Probability of an Undetected Hole above the Fuel Level**

| Probability of an Undetected Hole above the Fuel Level | | | | | | |
|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Probability** | **5th** | **Median** | **95th** | **Range Factor** |
| PUDHA3 | DPD | 8.19E-2 | -- | 9.17E-2 | 1.06E-1 | -- |

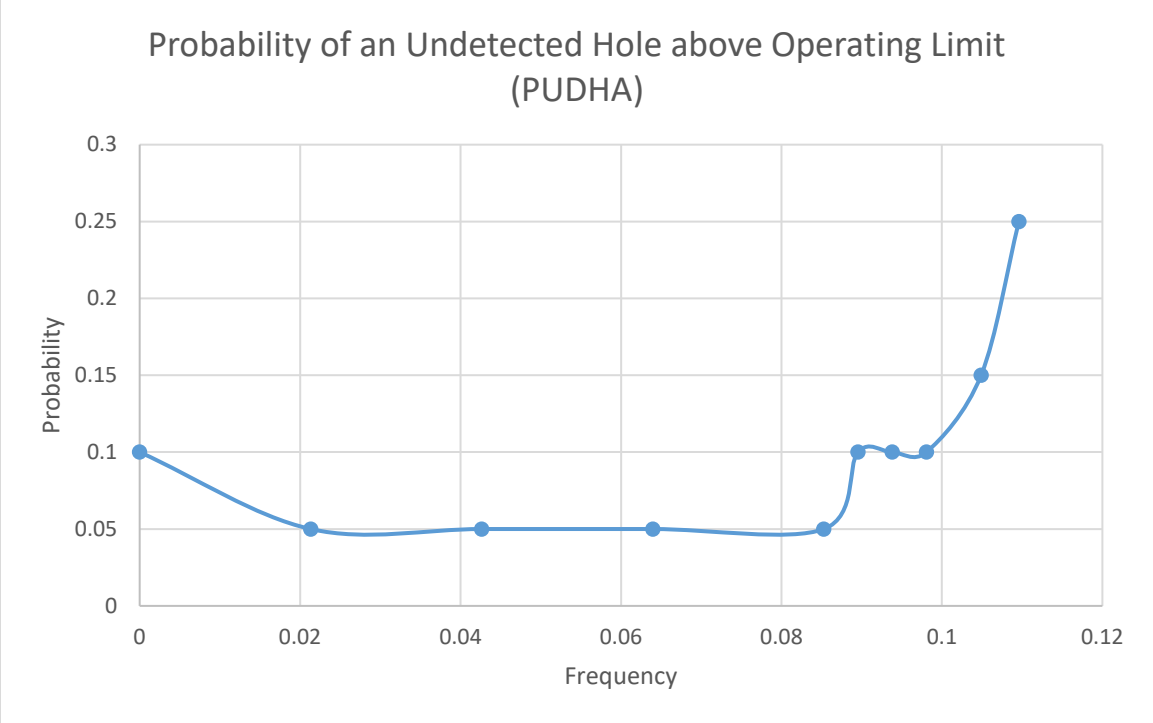



**Figure 5-15. Plot of Probability of an Undetected Hole above the Fuel Level Distribution**

Key assumptions in deriving this input are:

- Only RHBFST API 653 inspection findings of seven RHBFSTs with 100% liner inspection are used; i.e., those RHBFST inspections conducted since 2005.
- The origination of the through-liner holes detected is assumed to occur at half the time interval between RHBFST inspections, not to exclude more than 25 years. Implicitly, it is assumed that such relatively large through holes present during the prior RHBFST inspection would have been detected before their return to service.
- The representative through hole size to be used in sequence modeling is conservatively estimated by averaging the four largest flow areas found at the final RHBFST inspection; i.e., at the end of the inspection interval.

### 5.4.3.7 Probability of a Below Maximum Operating Level Hole for Use in Undetected Leakage Estimates

Estimates of undetected fuel leakage from RHBFSTs are in part determined by the accuracy of annual leak tightness tests and by fuel level monitoring performed during RHBFST operation. But, just because the leakage rate may be below detection levels, does not necessarily indicate that fuel leakage is in fact occurring. Another controlling factor is whether a through-liner hole develops during RHBFST operation that is located below the realistic maximum operating fuel level, thereby providing a path for fuel leakage.

Similar to determining the probability of a hole above the realistic maximum operating fuel level, the findings from the same seven RHBFST API 653 inspection reports with 100% liner inspection are used to investigate holes below the maximum liquid level. Only two of the seven API 653 inspections reported observed through-liner holes below the realistic maximum operating fuel level. Several through-liner pinholes (flow areas not specified and believed to be very small) were observed in the barrel of RHBFST 15 in the inspections of 2005 and 2007. This yields a point estimate of 2/7 = 0.285 for the probability of a through hole below the maximum operating level at the end of the RHBFST inspection interval. However, these through-liner holes are not expected to have been in place during the entire inspection interval. For the two RHBFST (RHBFST 2 and 15) discovered to have below fuel level through holes, the prior RHBFST inspection took place 26 and 24 years earlier. It's believed that the through-liner holes would likely only have occurred in the second half of the 26- and 24-year inspection interval, and possibly much later in the interval. With this assumption, the RHBFST years in which holes below the maximum operating level may been present (i.e., only in RHBFST 2 and 15) total just 26/2+24/2 = 25 RHBFST years.

The other RHBFSTs subject to API 653 with 100% liner inspections after 2005 did not find any through-liner holes below the maximum operating level, even though through-liner holes above that level were observed. For the five RHBFST inspections without any holes observed below the maximum operating level, these RHBFSTs were last inspected 25 (RHBFST 1), 27 (RHBFST 5), 25 (RHBFST 6), 26 (RHBFST 16), and 66 (RHBFST 20) years earlier. Therefore the total years at risk in these seven RHBFST inspection intervals is (24 +25+26+27+25 +26+66) = 219 RHBFST years. Therefore, the fraction of the operating years for these seven RHBFSTs during which an undetected leakage may have occurred due to a hole below the maximum operating level is estimated as 25/219 = 0.114.

## Table 5-31. Below-Maximum-Fuel-Level Holes Detected during Inspections

| RHBFST | Years since Last Inspection | Undetected Through Holes below Maximum Fuel Level |
|---|---|---|
| 1 | 25 | |
| 2 | 26 | 2 |
| 5 | 27 | |
| 6 | 25 | |
| 15 | 24 | 1 |
| 16 | 26 | |
| 20 | 66 | |
| **Total** | **219** | |

A judgment based uncertainty distribution was created to model the time of hole occurrence since the previous tank inspection given that a hole was detected in the most recent 100% inspection. This uncertainty distribution makes the assumption that there is a 10% chance that the hole actually originated before the prior inspection. With this uncertainty distribution for time of hole occurrence the point estimate calculation can be repeated for each point on the uncertainty distribution to determine an uncertainty distribution for the fraction of time that a very small and therefore undetected, below maximum operating, hole is present.

## Table 5-32. Probability of an Undetected Hole below Maximum Fuel Level

| Probability of an Undetected Below-Maximum-Operating-Level Hole | | | | | | |
|---|---|---|---|---|---|---|
| **RM Dist.** | **Distribution Type** | **Probability** | **5th** | **Median** | **95th** | **Range Factor** |
| PUDHB3 | DPD | 8.73E-2 | -- | 9.64E-2 | 1.14E-1 | -- |

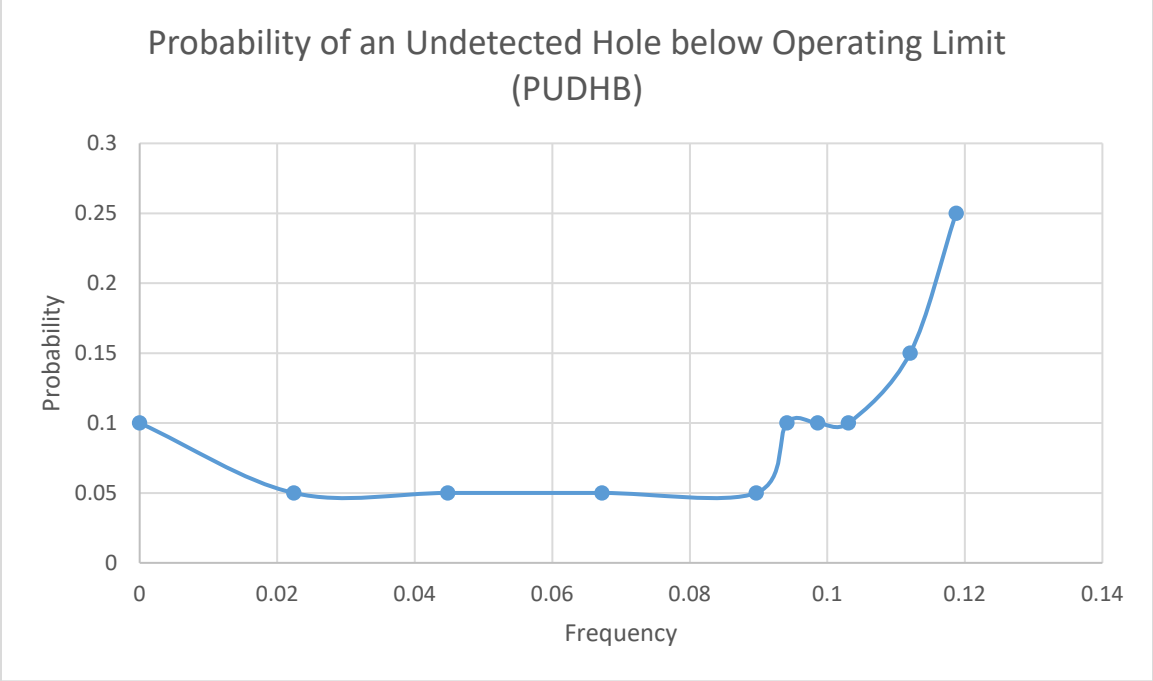



**Figure 5-16. Plot of Probability of an Undetected Hole below Maximum Fuel Level Distribution**

Key assumptions in deriving this input are:

- Only the seven RHBFST API 653 inspection findings on which 100% liner coverage below the realistic maximum fuel levels are used; i.e., those RHBFST inspections conducted during and since 2005.

- The maximum operating fuel level is at 212'. Therefore, the through hole locations of interest are those in the lower dome, barrel, expansion areas or lower row of the upper dome. Through holes located further up in upper dome are excluded.

- For RHBFST 15, a 1/8" hole was also found in the RHBFST's expansion area; i.e., just below the 212' level. It is expected that such a hole would have easily been detected during normal operations if the fuel level had covered the hole. It is therefore assumed that the hole was not detected before shutting down for inspection because the actual fuel level did not cover it after the hole formed, or that the actual leakage rate did not exceed the minimum detectable leakage rate because the hole was only barely below the liquid level. Nevertheless, the through hole detected by the RHBFST 15 inspection was counted as having a hole below the fuel level due to other through-liner holes at the level of the lower dome and RHBFST barrel.

- The representative, undetected hole size is assumed to be a distribution of sizes ranging below the minimum detectable in the annual leak tightness tests as these would not be detected during RHBFST operation.

### 5.4.3.8 Distribution of Hole Locations

The current Red Hill facility data shows 23 approximate through hole locations for all incidents recorded, which includes 18 through holes during RHBFST inspections and 5 incidents during normal operations. Please note that there have been 18 leak incidents during normal operations, however, only 5 of the incidents have a location recorded. The following table presents the through hole locations within each range of fuel levels simulated as leak locations in the QRVA. This table is for through holes occurring randomly during RHBFST operation. The last column of the table also shows the distribution by liner area for RHBFST return to service (RTS) events.

**Table 5-33. Distribution of Hole Locations**

| Height Range | Holes Detected during Inspection by Tank Sections | Holes Detected during Operation by Tank Sections | Total | % Distributed by RHBFST Experience | % Distribution by Liner Area below 212' for RTS |
|---|---|---|---|---|---|
| 175'–212' | 6 | 4 | 10 | 43% | 17.5% |
| 140'–175' | 5 | 0 | 5 | 22% | 16.5% |
| 70'–140' | 2 | 1 | 3 | 13% | 33% |
| 0'–70' | 5 | 0 | 5 | 22% | 33% |
| **Total** | **18** | **5** | **23** | 100% | 100% |

The "% Distributed by RHBFST Experience" column is simply the sum of "Total" number of holes by "Height Range" divided by the total holes for the entire tank. For example, the "% Distributed by RHBFST Experience" for the "Height Range" of 175'–212' is (10 / 23) * 100 = 43%.

### 5.4.3.9 RHBFST Operating Years

Total RHBFST operating years was estimated in Table 5-34 by accounting for all RHBFSTs' start of service to either their end of service or the present (Year 2017) and subtracting any downtime due to maintenance. The estimated total RHBFST operating experience is 1,315.6 years.

## Table 5-34. RHBFST Operating Years

| RHBFST | Start of Service Year | End of Service Year | Work on Tell-Tale | Tell-Tale Work Outage (yrs.) | TIRM and Repairs Outage (yrs.) | # of Outages/RTS | RHBFST Years |
|---|---|---|---|---|---|---|---|
| 1 | 1943 | 2005 | (1978/84) | 1 | **15.63** | 10 | 45.4 |
| 2 | 1943 | 2017 | (1978/84) | 1 | **4.26** | 6 | 68.7 |
| 3 | 1943 | 2017 | | | **2.28** | 4 | 71.7 |
| 4 | 1943 | 2017 | | | **2.02** | 2 | 72.0 |
| 5 | 1943 | 2017 | (1971/73) (1978/84) | 2 | **7.41** | 6 | 64.6 |
| 6 | 1943 | 2017 | 1964 (1971/73) | 2 | **7.85** | 8 | 64.2 |
| 7 | 1943 | 2017 | (1978/84) | 1 | **3.57** | 6 | 69.4 |
| 8 | 1943 | 2017 | (1978/84) | 1 | **2.37** | 4 | 70.6 |
| 9 | 1943 | 2017 | (1978/84) | 1 | **2.05** | 5 | 70.9 |
| 10 | 1943 | 2017 | (1978/84) | 1 | **8.20** | 7 | 64.8 |
| 11 | 1943 | 2017 | | | **2.90** | 3 | 71.1 |
| 12 | 1943 | 2017 | (1971/73) (1978/84) | 2 | **7.53** | 6 | 64.5 |
| 13 | 1943 | 2017 | (1978/84) | 1 | **7.99** | 6 | 65.0 |
| 14 | 1943 | 2017 | | | **3.08** | 5 | 70.9 |
| 15 | 1943 | 2017 | 1981 | 1 | **5.21** | 5 | 67.8 |
| 16 | 1943 | 2017 | 1976 | 1 | **4.60** | 8 | 68.4 |

## Table 5-34. RHBFST Operating Years (Continued)

| RHBFST | Start of Service Year | End of Service Year | Work on Tell-Tale | Tell-Tale Work Outage (yrs.) | TIRM and Repairs Outage (yrs.) | # of Outages/RTS | RHBFST Years |
|---|---|---|---|---|---|---|---|
| 17 | 1943 | 2017 | (1960/63) (1978/84) | 2 | **1.67** | 6 | 70.3 |
| 18 | 1943 | 2017 | (1960/63) (1978/84) | 2 | **0.98** | 5 | 71.0 |
| 19 | 1943 | 1998 | (1960/63) | 1 | **20.74** | 7 | 33.3 |
| 20 | 1943 | 2017 | (1960/63) (1978/84) | 2 | **1.00** | 4 | 71.0 |
| **Total** | | | **22** | | | **113** | **1315.6** |

### 5.4.4 Tank Overfill Initiating Events

When assessing potential tank overfill initiating events at the RHBFSF, the QRVA team, through discussions with the FLC Fuels Department operations staff, and through review of system information, discovered that the following general chain of events must occur to create a realistic tank overfill event:

- Operations orders are developed and implemented for all fuel movements.
- Operators check tank ullage before initiating fuel movements to ensure adequate tank volume exists for the planned fuel movement.
- A high-high level alarm sounds, cueing operators to act.
- A high level switch is activated, which automatically
  - Deactivates all facility pumps.
  - Activates a timer to allow time to secure system.
  - Closes the skin valve to the affected tank.

The chain of events is initiated by a challenge for overfill leak which has been modelled as a constrained non-informative gamma distribution based on the assumption that once per year each RHBFST is filled to the operating limit as part of preparing for its annual leak tightness test.

**Table 5-35. Challenge for Overfill Leak to Rock**

| Challenge for Overfill Leak to Rock (per hour) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **IE Name** | **Type** | **Alpha** | **Beta** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| OVRFIL | Gamma | 0.5 | 4.40E+3 | 1.14E-4 | 3.78E-7 | 4.71E-5 | 4.03E-4 | 32.60 |

For each operating RHBFST an overfill initiator was modeled using the above “OVRFIL” data variable distribution multiplied by the hours in a year (8,766) to compute a frequency per year for “Challenge for overfill leak to rock per year”. The uncertainty distribution is broadened to account for other times during the year that the fuel level would be at risk to overfilling.

The system response to this initiating event in the form of operator actions, alarms, and automatic deactivation of pumps have been modeled as an event tree (OVERFILL) and documented in Section 6 of this report.

### 5.4.5 Piping, Valve, and Connection Leakage Fuel Release Initiating Events

As the RHBFSF piping is not buried piping, because it runs through large or small tunnels where it can be monitored and where leakage would most likely be effectively contained and directed back to Joint Base Pearl Harbor-Hickam sumps via designed drainage paths, the impact of piping leakage could be considered to be of minimal impact in the QRVA. However, generic pipe leakage data is prudently included within the scope of this data analysis. As the Navy has not, to date, provided facility-specific information regarding pipe leakage or pipe break events, generic pipe leakage data from Pipeline Risk Management Manual (Reference 5-1) is applied in the QRVA. The generic pipe leakage data to be applied in the QRVA is:

- For small leaks (0 to 50 gallons per minute), a gamma distribution with the following characteristics: mean value 4.16E-12 events per hour-foot, alpha 0.500, beta 1.21E+11.

- For large leaks (> 50 gallons per minute), a gamma distribution with the following characteristics: mean value 6.75E-13 events per hour-foot, alpha 0.5, beta 7.45E+11, and range factor 32.6.

The piping leakage failure rate data is assumed to subsume associated relevant connection (e.g., flanges, welds, etc.) failures.

Table 5-36 lists the pipeline lengths for segments considered as part of the initiating event frequency computations.

## Table 5-36. RHBFSF Pipeline Length by Section

| Section | Length (mi.) | Length (ft.) |
|---|---|---|
| A UGPH to ADIT 2Y | 0.25 | 1,320.00 |
| B ADIT 2Y to ADIT 3Y | 2.3 | 12,144.00 |
| C ADIT 3Y to first sectional valves (154, 158, 162) at RH (~0.16m from first sectional valve to corner of lower access tunnel, plus ~0.2m to ADIT 3Y) (0.16m is obtained via subtracting length of tank gallery from 0.5 miles) Additional 0.1m from the Oil-Tight Door to ADIT 3Y | 0.46 | 2,428.80 |
| *Section D* | | |
| D F24 (8*200) (first Sectional Valves 0162 to T15,16) Blue (16") | 0.30 | 1,600.00 |
| D F24 (2.5*100ft) Tank Gallery Cross Tank | 0.047 | 250.00 |
| D JP5 (5.5*200) (first Sectional Valve 158 to Mid-sectional Valve 163) Gold 18" | 0.21 | 1,100.00 |
| D JP5 (2*100ft) Tank Gallery Cross Tank | 0.038 | 200.00 |
| D F76 (5.5*200) (first Sectional Valve 154 at RH to Mid-sectional Valve 164) Green 32" | 0.21 | 1,100.00 |
| *Section E* | | |
| E JP5 (6*200) (Mid-sectional Valve 163 to Tank 19 & 20) Gold 18" | 0.23 | 1,200.00 |
| E JP5 (3.5*100ft) Tank Gallery Cross Tank | 0.066 | 350.00 |
| E F76 (3*200) (Mid-sectional Valve 164 to Tank 15 & 16) Green 32" | 0.11 | 600.00 |
| E F76 (100ft) Tank Gallery Cross Tank F76 | 0.019 | 100.00 |
| *Lower Dome Pipes* | | |
| F24 - 8" Pipe - 65'-5" for Each Active Tank (65*5) | 0.062 | 325.00 |
| F24 - 18" Pipe - 65'-3" for Each Active Tank (65*5) | 0.062 | 325.00 |
| F24 - 32" Pipe - 53'-6" for Each Active Tank (54*5) | 0.051 | 270.00 |
| JP5 - 8" Pipe - 65'-5" for Each Active Tank (65*11) | 0.135 | 715.00 |
| JP5 - 18" Pipe - 65'-3" for Each Active Tank (65*11) | 0.135 | 715.00 |
| JP5 - 32" Pipe - 53'-6" for Each Active Tank (54*11) | 0.113 | 594.00 |
| F76 - 8" Pipe - 65'-5" for Each Active Tank (65*2) | 0.025 | 130.00 |
| F76 - 18" Pipe - 65'-3" for Each Active Tank (65*2) | 0.025 | 130.00 |
| F76 - 32" Pipe - 53'-6" for Each Active Tank (54*2) | 0.020 | 108.00 |
| Total Distance from T20 to UGPH | 3.45 | 18,192.80 |
| Total Pipe Length from T20 to UGPH | 10.19 | 53,828.40 |

Valve external leakage data from Table 5-55 is applied for valve leakage initiating events. For example, for motor-operated valves, the generic leakage data from NUREG/CR-6928 to be applied in the QRVA is:

- For small external leaks (0 to 50 gallons per minute), a gamma distribution with the following characteristics: mean value 1.41E-08 events per hour, alpha 0.500, beta 3.557E+07, and error factor 8.4.

- For large external leaks (> 50 gallons per minute), a gamma distribution with the following characteristics: mean value 9.84E-10 events per hour, alpha 0.300, beta 3.049E+08, and error factor 18.8.

#### *5.4.5.1 Lower Dome Leak to Rock Initiators*

The total pipe length in the lower dome area is approximately the same for all active RHBFSTs, 65 feet of 8-inch pipe, 65 feet of 18-inch pipe, and 54 feet of 32-inch pipe totaling 184 feet.

For the lower dome large leak to rock initiator, the pipe segment length of 184 feet multiplied by the large leak pipe failure frequency of 6.75E-13 events per hour-foot, multiplied by 8,766 hours/year, yields 1.09E-6 failures per year.

For the lower dome small leak to rock initiator, the pipe segment length of 184 feet multiplied by the large leak pipe failure frequency of 4.16E-12 events per hour-foot, multiplied by 8,766 hours/year, yields 6.7E-6 failures per year.

Although the pipe segment length and pipe failure frequencies are approximately the same, lower dome piping for each tank has been modeled independently for purposes of identifying the leak location.

## Table 5-37. Lower Dome Leak to Rock Initiators Frequencies

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| *Large Leaks* | | | |
| DRTK02 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 002 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK03 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 003 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK04 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 004 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK05 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 005 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK06 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 006 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK07 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 007 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK08 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 008 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK09 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 009 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK10 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 010 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK11 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 011 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK12 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 012 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK13 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 013 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK14 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 014 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK15 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 015 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK16 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 016 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK17 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 017 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK18 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 018 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |
| DRTK20 | Lower dome RUPTURE pipe to ROCK per tank year applies to RHBFST 020 | (PSEGLD*LPIPE)*YEAR | 1.09E-06 |

## Table 5-37. Lower Dome Leak to Rock Initiators Frequencies (Continued)

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| *Small Leaks* | | | |
| LDTK02 | Lower dome 0.5” pipe leaks to ROCK per tank year applies to RHBFST 002 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK03 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 003 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK04 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 004 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK05 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 005 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK06 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 006 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK07 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 007 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK08 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 008 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK09 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 009 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK10 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 010 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK11 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 011 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK12 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 012 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK13 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 013 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK14 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 014 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK15 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 015 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK16 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 016 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK17 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 017 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK18 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 018 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |
| LDTK20 | Lower dome 0.5" pipe leaks to ROCK per tank year applies to RHBFST 020 | (PSEGLD*SPIPE)*YEAR | 6.70E-06 |

### 5.4.5.2 Nozzle Leak to Lower Access Tunnel (LAT) Initiators

The nozzle leak to LAT initiator considers the approximately 6 inches of pipe that is exposed to the LAT and the skin valve associated with it. RHBFSTs 2 to 16 have three such nozzles, a 12-inch-diameter pipe segment with an MOV, a 20-inch-diameter pipe segment with an MOV, and a 4-inch-diameter pipe segment with a manual-operated valve (XVM). RHBFSTs 17 and 18 have three such nozzles, a 12-inch-diameter pipe segment with a manual operated valve, a 20-inch-diameter pipe segment with an MOV, and a 6-inch-diameter pipe segment with a manual operated valve. RHBFST 20 has two such nozzles, a 20-inch-diameter pipe segment with an MOV, and a 6-inch-diameter pipe segment with a manual-operated valve. To further refine the nozzle leakage frequency, only the part of the valve that is exposed to the head pressure has been considered.

For the nozzle large leak to the LAT from RHBFSTs 2 to 16, the large leakage yearly failure frequency of the three pipe segments is added to the sum of the yearly failure frequency of two MOVs large external leak and one XVM large external leak. The result of this computation is 2.24E-5 failures per year.

For the nozzle large leak to the LAT from RHBFSTs 17 to 18, the large leakage yearly failure frequency of the three pipe segments is added to the sum of the yearly failure frequency of one MOV large external leak and two XVM large external leak. The result of this computation is 3.19E-5 failures per year.

For the nozzle large leak to the LAT from RHBFST 20, the large leakage yearly failure frequency of the two pipe segments is added to the sum of the yearly failure frequency of one MOV large external leak and one XVM large external leak. The result of this computation is 1.81E-5 failures per year.

For the nozzle small leak to the LAT from RHBFSTs 2 to 16, the small leakage yearly failure frequency of the three pipe segments is added to the sum of the yearly failure frequency of two MOVs small external leak and one XVM small external leak. The result of this computation is 3.2E-4 failures per year.

For the nozzle small leak to the LAT from RHBFSTs 17 to 18, the large leakage yearly failure frequency of the three pipe segments is added to the sum of the yearly failure frequency of one MOV small external leak and two XVM small external leak. The result of this computation is 4.55E-4 failures per year.

For the nozzle small leak to the LAT from RHBFST 20, the small leakage yearly failure frequency of the two pipe segments is added to the sum of the yearly failure frequency of one MOV small external leak and one XVM small external leak. The result of this computation is 2.58E-4 failures per year.

Although the pipe segment length and valve failure frequencies are the same for some of the RHBFSTs, each RHBFST has been modeled independently for purposes of identifying the leak location.

## Table 5-38. Nozzle Leak to LAT Initiators Frequencies

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| *Large Leaks* | | | |
| NLTK02 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valve and RHBFST 002 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK03 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valve and RHBFST 003 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK04 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 004 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK05 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 005 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK06 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 006 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK07 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 007 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK08 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 008 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |
| NLTK09 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 009 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))*YEAR | 2.24E-05 |

## Table 5-38. Nozzle Leak to LAT Initiators Frequencies (Continued)

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| NLTK10 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 010 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK11 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 011 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK12 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 012 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK13 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 013 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK14 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 014 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK15 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 015 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK16 | NOZZLE RUPTURE to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 016 | ((PNOZL*(LPIPE*3))+(FMOVEL*((2*MOVELL)+XVMELL)))* YEAR | 2.24E-05 |
| NLTK17 | NOZZLE RUPTURE to LAT per tank year, i.e., between 1 MOV and 2 XVM skin valves and RHBFST 017 | ((PNOZL*(LPIPE*3))+(FMOVEL*(MOVELL+(2*XVMELL))))* YEAR | 3.19E-05 |
| NLTK18 | NOZZLE RUPTURE to LAT per tank year, i.e., between 1 MOV and 2 XVM skin valves and RHBFST 018 | ((PNOZL*(LPIPE*3))+(FMOVEL*(MOVELL+(2*XVMELL))))* YEAR | 3.19E-05 |

## Table 5-38. Nozzle Leak to LAT Initiators Frequencies (Continued)

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| NLTK20 | NOZZLE RUPTURE to LAT per tank year, i.e., between 1 MOV and 1 XVM skin valves and RHBFST 018 | ((PNOZL*(LPIPE*3))+(FMOVEL*(MOVELL+XVMELL)))*YEAR | 1.81E-05 |
| NSTK02 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 002 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |
| NSTK03 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 003 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |
| NSTK04 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 004 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.21E-04 |
| NSTK05 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 005 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |
| NSTK06 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 006 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |
| NSTK07 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 007 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 6.19E-05 |
| NSTK08 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 008 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |
| NSTK09 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 009 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS)))*YEAR | 3.20E-04 |

## Table 5-38. Nozzle Leak to LAT Initiators Frequencies (Continued)

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| NSTK10 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 010 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK11 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 011 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK12 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 012 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK13 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 013 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK14 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 014 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK15 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 015 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK16 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 2 MOV and 1 XVM skin valves and RHBFST 016 | ((PNOZL*(3*SPIPE))+(FMOVEL*((2*MOVELS)+XVMELS))) *YEAR | 3.20E-04 |
| NSTK17 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 1 MOV and 2 XVM skin valves and RHBFST 017 | ((PNOZL*(3*SPIPE))+(FMOVEL*(MOVELS+(2*XVMELS)))) *YEAR | 4.55E-04 |

## Table 5-38. Nozzle Leak to LAT Initiators Frequencies (Continued)

| Initiating Event Name | Description | Equation | Frequency/ Year |
|---|---|---|---|
| NSTK18 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 1 MOV and 2 XVM skin valves and RHBFST 018 | ((PNOZL*(3*SPIPE))+(FMOVEL*(MOVELS+(2*XVMELS)))) *YEAR | 4.55E-04 |
| NSTK20 | RHBFST Nozzle 0.5" leak to LAT per tank year, i.e., between 1 MOV and 1 XVM skin valves and RHBFST 020 | ((PNOZL*(2*SPIPE))+(FMOVEL*(MOVELS+XVMELS)))*YEAR | 2.59E-04 |

#### 5.4.5.2.1 *RHBFSF Experience with Motor-Operated (MOV) and Manual Valves (XVM)*

In order to incorporate the RHBFSF's MOV and XVM facility experience, Bayesian methods are used to update the generic MOV and XVM external leak (MOVEL, XVMEL) failure frequencies obtained from NUREG/CR-6928 (Reference 5-2) (Table 5-39). RHBFSF's MOV experience includes zero external leak failure for 64 MOVs and 23 XVMs. Please see Table 5-40 for the tabulation of these valves. The number of years used in this computation is an average of RHBFST operating years (from Section 5.4.3.9) for the 20 RHBFSTs (1315.6/20 = 65.8). The RHBFSF's evidence as presented in Table 5-40 was used to perform the Bayesian update presented in Table 5-41 for small external leaks. Table 5-42 then scales the resulting mean of the distribution to obtain the updated distribution for large external leaks, accounting for RHBFSF specific experience. The scaling method described in NUREG/CR-6928 (Reference 5-2) was used to perform this scaling which is: Gamma (ELS * 0.07, LL).

## Table 5-39. Small External Leak for MOV and XVM from Industry Data

| Generic/Industry Data for MOV and XVM (NUREG/CR-6928) Small Leak | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Failure Mode** | **Type** | **Alpha** | **Beta** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| MVELS | Gamma | 0.5 | 3.56E+07 | 1.41E-08 | 4.67E-11 | 5.82E-09 | 4.98E-08 | 32.60 |
| XVELS | Gamma | 0.5 | 1.12E+07 | 4.49E-08 | 1.49E-10 | 1.85E-08 | 1.58E-07 | 32.60 |

## Table 5-40. Small External Leak Evidence for MOV and XVM from RHBFSF

| RHBFSF Specific Evidence for Valve External Leakage | | | | |
|---|---|---|---|---|
| **Bayesian Evidence MOVs** | | | **Bayesian Evidence XVMs** | |
| Skin Valves | 18 | | Slop Valves | 20 |
| Second Skin Valves | 17 | | Extra Manual Valves | 3 |
| Ball Valves | 18 | | | |
| Sectional Valves | 11 | | | |
| MOVs Total | 64 | | XVM Valves Total | 23 |
| Years | 65.8 | | Years | 65.8 |
| Hours per Year | 8766 | | Hours per Year | 8766 |
| MOV Hours at Risk | 3.69E+07 | | XVM Hours at Risk | 1.33E+07 |
| Updated Mean | 6.92E-09 | | Updated Mean | 2.05E-08 |

## Table 5-41. Bayesian Update of Small External Leak for MOV and XVM Using RHBFSF Evidence

| Updated Data for MOV and XVM Based on RHBFSF Evidence – Small Leak | | | | | | |
|---|---|---|---|---|---|---|
| **Failure Mode** | **Type** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| MOVELS | One-Stage Update | 6.92E-09 | 2.30E-11 | 2.85E-09 | 2.44E-08 | 32.60 |
| XVMELS | One-Stage Update | 2.05E-08 | 6.81E-11 | 8.46E-09 | 7.24E-08 | 32.60 |

## Table 5-42. Bayesian Update of Large External Leak for MOV and XVM

| Scaled (Mean by 0.07 and Alpha = 0.3) Data for MOV and XVM – Large Leak | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Failure Mode** | **Type** | **Alpha** | **Beta** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| MOVELL | Gamma | 0.3 | 6.20E+08 | 4.88E-10 | 3.94E-14 | 1.02E-10 | 2.01E-09 | 22.60 |
| XVMELL | Gamma | 0.3 | 2.10E+08 | 1.44E-09 | 1.16-13 | 3.02E-10 | 5.92E-09 | 22.60 |

### 5.4.5.3 Pipeline Leak to Lower Access Tunnel Initiators

Pipeline leak to LAT initiators consider the length of pipe segments as per Table 5-36, and associated sectional valves for the three fuel pipelines. The following Table 5-43 list each initiator along with a short description, equation used to compute the failure frequency and the resulting failure frequency per year.

## Table 5-43. Pipeline Leak to Lower Access Tunnel Initiators Frequencies

| Initiator | Description | Equation | Failure Frequency/ Year |
|---|---|---|---|
| *Large Leaks* | | | |
| SF24AL | Blue F24 16" line from Sectional Valve 160 at ADIT 2Y down to Sectional Valve 159 at PH59 Large leak pipe rupture | ((PSEGA*LPIPE)+MOVELL)*YEAR | 1.64E-05 |
| SF24BL | Blue F24 16" line from normally closed Sectional Valve 161 at ADIT 3Y down to Sectional Valve 160 at ADIT 2Y Large leak pipe rupture | ((PSEGB*LPIPE)+MOVELL)*YEAR | 8.04E-05 |
| SF24CL | Blue F24 16" line from Sectional Valve 162 below Tanks 1&2 to normally closed Sectional Valve 161 at ADIT 3Y Large leak pipe rupture | ((PSEGC*LPIPE)+MOVELL)*YEAR | 2.30E-05 |
| SF24DL | Blue F24 16" line from line blind above Tanks 15&16 down to Sectional Valve 162 below Tanks 1&2 Large leak pipe rupture | ((PSEGD1*LPIPE)+MOVELL)*YEAR | 1.81E-05 |
| SF76AL | Green F76 32" line from Sectional Valve 152 at ADIT 2Y to Sectional Valve 151 at PH59 Large leak pipe rupture | ((PSEGA*LPIPE)+MOVELL)*YEAR | 1.64E-05 |
| SF76BL | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y Large leak pipe rupture | ((PSEGB*LPIPE)+MOVELL)*YEAR | 8.04E-05 |
| SF76CL | Green F76 32" line from Sectional Valve 154 below Tanks 1&2 down to normally closed Sectional Valve 153 at ADIT 3Y Large leak pipe rupture | ((PSEGC*LPIPE)+MOVELL)*YEAR | 2.30E-05 |
| SF76DL | Green F76 32" line from Sectional Valve 164 below Tanks 11&12 down to Sectional Valve 154 below Tanks 1&2 Large leak pipe rupture | ((PSEGD1*LPIPE)+MOVELL)*YEAR | 1.81E-05 |
| SF76EL | Green F76 32" line from blind above Tanks 15 & 16 down to Sectional Valve 164 below Tanks 11&12 Large leak pipe rupture | ((PSEGE3*LPIPE)+MOVELL)*YEAR | 1.22E-05 |
| SJP5AL | Gold JP5 18" line from Sectional Valve 156 at ADIT 2Y down to Section Valve 155 at PH59 Large leak pipe rupture | ((PSEGA*LPIPE)+MOVELL)*YEAR | 1.64E-05 |

## Table 5-43. Pipeline Leak to Lower Access Tunnel Initiators Frequencies (Continued)

| Initiator | Description | Equation | Failure Frequency/ Year |
|---|---|---|---|
| SJP5BL | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y Large leak pipe rupture | ((PSEGB*LPIPE)+MOVELL)*YEAR | 8.04E-05 |
| SJP5CL | Gold JP5 18" line from Sectional Valve 158 below Tanks 1&2 down to normally closed Sectional Valve 157 at ADIT 3Y Large leak pipe rupture | ((PSEGC*LPIPE)+MOVELL)*YEAR | 2.30E-05 |
| SJP5DL | Gold JP5 18" line from Sectional Valve 163 below Tanks 11&12 down to Sectional Valve 158 below Tanks 1&2 Large leak pipe rupture | ((PSEGD3*LPIPE)+MOVELL)*YEAR | 1.51E-05 |
| SJP5EL | Gold JP5 18" line from blind above Tanks 19&20 down to Sectional Valve 163 below Tanks 11&12 Large leak pipe rupture | ((PSEGE1*LPIPE)+MOVELL)*YEAR | 1.57E-05 |
| *Small Leaks* | | | |
| SJP5ES | Gold JP5 18" line from blind above Tanks 19&20 down to Sectional Valve 163 below Tanks 11&12 Small Leak 0.5" | ((PSEGE1*SPIPE)+MOVELS)*YEAR | 1.67E-04 |
| SF24AS | Blue F24 16" line from Sectional Valve 160 at ADIT 2Y down to Sectional Valve 159 at PH59 Small Leak 0.5" | ((PSEGA*SPIPE)+MOVELS)*YEAR | 1.72E-04 |
| SF24BS | Blue F24 16" line from normally closed Sectional Valve 161 at ADIT 3Y down to Sectional Valve 160 at ADIT 2Y Small Leak 0.5" | ((PSEGB*SPIPE)+MOVELS)*YEAR | 5.66E-04 |
| SF24CS | Blue F24 16" line from Sectional Valve 162 below Tanks 1&2 to normally closed Sectional Valve 161 at ADIT 3Y Small Leak 0.5" | ((PSEGC*SPIPE)+MOVELS)*YEAR | 2.12E-04 |
| SF24DS | Blue F24 16" line from line blind above Tanks 15&16 down to Sectional Valve 162 below Tanks 1&2 Small Leak 0.5" | ((PSEGD1*SPIPE)+MOVELS)*YEAR | 1.82E-04 |
| SF76AS | Green F76 32" line from Sectional Valve 152 at ADIT 2Y to Sectional Valve 151 at PH59 Small Leak 0.5" | ((PSEGA*SPIPE)+MOVELS)*YEAR | 1.72E-04 |
| SF76BS | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y Small Leak 0.5" | ((PSEGB*SPIPE)+MOVELS)*YEAR | 5.66E-04 |

## Table 5-43. Pipeline Leak to Lower Access Tunnel Initiators Frequencies (Continued)

| Initiator | Description | Equation | Failure Frequency/ Year |
|---|---|---|---|
| SF76CS | Green F76 32" line from Sectional Valve 154 below Tanks 1&2 down to normally closed Sectional Valve 153 at ADIT 3Y Small Leak 0.5" | ((PSEGC*SPIPE)+MOVELS)*YEAR | 2.12E-04 |
| SF76DS | Green F76 32" line from Sectional Valve 164 below Tanks 11&12 down to Sectional Valve 154 below Tanks 1&2 Small Leak 0.5" | ((PSEGD1*SPIPE)+MOVELS)*YEAR | 1.82E-04 |
| SF76ES | Green F76 32" line from blind above Tanks 15 & 16 down to Sectional Valve 164 below Tanks 11&12 Small Leak 0.5" | ((PSEGE3*SPIPE)+MOVELS)*YEAR | 1.46E-04 |
| SJP5BS | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y Small Leak 0.5" | ((PSEGB*SPIPE)+MOVELS)*YEAR | 5.66E-04 |
| SJP5AS | Gold JP5 18" line from Sectional Valve 156 at ADIT 2Y down to Section Valve 155 at PH59 Small Leak 0.5" | ((PSEGA*SPIPE)+MOVELS)*YEAR | 1.72E-04 |
| SJP5CS | Gold JP5 18" line from Sectional Valve 158 below Tanks 1&2 down to normally closed Sectional Valve 157 at ADIT 3Y Small Leak 0.5" | ((PSEGC*SPIPE)+MOVELS)*YEAR | 2.12E-04 |
| SJP5DS | Gold JP5 18" line from Sectional Valve 163 below Tanks 11&12 down to Sectional Valve 158 below Tanks 1&2 Small Leak 0.5" | ((PSEGD3*SPIPE)+MOVELS)*YEAR | 1.64E-04 |

### 5.4.6 Chronic Fuel Release Initiating Events – Undetected Through Holes in the RHBFST Liners

It has been postulated that there may be through holes in the RHBFST's liners that are too small to detect but which nevertheless release fuel from the liner, through the pre-stressed grout, 4.5' to 5' of concrete, a thin red earth layer, and to the surrounding rock. Each RHBFST is continuously monitored for fuel level and these levels are recorded electronically for manual trending analysis. This continuous monitoring is also synchronized with low level setpoints to provide audio alarms in the control room. In addition, each RHBFST is manually top gauged at least once per month, and after each fuel movement, to confirm the electronic monitoring indications. These low level alarms are discussed more later on in subsequent sections. One difficulty with the electronic continuous level indication system is that the level setpoints must be reset after each fuel movement, since the amount of fuel discharged or received, and often if different temperatures, cannot be measured exactly.

In addition to continuous monitoring of fuel levels, annual leak tightness tests are performed on each RHBFST. These tests are performed over a 1-week period with the RHBFST in idle conditions and using an alternate, and more accurate, fuel mass measuring system. For leak tightness tests performed on or before 2013, the leak tightness test accuracy was stated to be within 0.7 gallons per hour. The tests reports for 2015 (tests were previously performed biennially) changed this to claim the tests were accurate to at least 0.5 gallons per hour, and possibly even more accurate to 0.2 gallons per hour. Some have argued that due to the accuracy limits of the RHBFST leak tightness test's accuracy, that undetected holes below the fuel level may be leaking fuel continuously at the rates in the following table.

| Leak Detection Accuracy (gallons per hour) | Gallons per RHBFST-Year | Facility Gallons per Year (18 RHBFSTs) |
|---|---|---|
| 0.7 | 6,136 | 110,449 |
| 0.5 | 4,383 | 78,892 |
| 0.2 | 1,753 | 31,557 |

It is important to recognize that these postulated fuel leakage rates involve a number of conservative assumptions, which make the estimates likely to be overstated. These assumptions include:

1. Each RHBFST has an existing through-liner hole(s), and for the right-most column, all operating RHBFSTs have existing through-liner hole(s).

2. The flow rate via the through-liner hole(s), is just large enough to match the annual leak tightness test detection accuracy, and no more.

3. The through-liner hole(s) do not grow in size leading to increasing flow rates with passing time, so that the through-liner hole(s) go undetected for multiple years.

4. The cause or mechanism for creating these postulated through-liner holes is not discussed.

The assumptions listed above are addressed in the alternative fuel leakage rate model developed in the following subsections. The model developed accounts for information gleaned from RHBFST API 653 inspection reports, and from the knowledge that in 54 RHBFSTs leak tightness tests formally reported to date, none have detected fuel leakage in excess of the test accuracy.

Leakage events have historically been reported for about two-thirds of the RHBFSTs. Past investigations have concluded that petroleum stains have been found under 19 of the 20 RHBFSTs, including under RHBFSTs 4, 8, 14, 18, and 20 for which no release events were reported. This information suggests that fuel leakage from one RHBFST can end up below other RHBFSTs, or that there have been fuel leakage events for the above RHBFSTs that were not detected or reported. It's feasible that very slow fuel leaks have occurred but that were too slow to be detected by available methods, including by the now annual leak tightness tests. This section discusses the available data on this issue and provides an estimate of the annual leakage from such otherwise undetected through-liner holes.

#### *5.4.6.1 Review of the Data*

Since 2008, there have been leak tightness tests performed on the RHBFSTs. These tests last for about 1 week for each RHBFST. Each test involves a 2-day period in which the RHBFST is allowed to settle, and then for the following 5 days, mass measurements are repeatedly taken. These mass measurements are a surrogate for fuel level and volume release. In 2008, 2 RHBFSTs were first tested, then 7 in 2009, 16 in 2011, 15 in 2013, and again 14 RHBFSTs were tested in 2015. The total number of leak tightness tests formally reported so far is 54. It is understood that the RHBFST leak tightness tests are now performed annually, though only the results up to and including 2015 were available for this study. The RHBFSTs not yet leak tightness tested are 1 and 19 which are permanently out of service, and RHBFSTs 5 and 17 which have been temporarily out of service from 2008 to date. Two of the leak tightness tests were performed on RHBFSTs which, for operational reasons, the fuel levels were less than 150'. Most leak tightness tests reported have been performed with fuel levels between 211' and 212'. Since leakage from otherwise undetected through holes can only be detected below the fuel level of the leak tightness tests, these two tests at lower fuel levels are not considered in the discussion below.

From 2008 through 2015, all RHBFSTs passed their leak tightness tests. The test reports indicated that the accuracy was within 0.7 gallons per hour (GPH) tests up to and through the 2013 tests. For 2015, the final report (Reference 5-101) indicates that the test data is accurate to within 0.5 GPH at 95% confidence, and claims that realistically an accuracy of 0.2 GPH is statistically achievable. In the 2015 report, plots display the measured fuel levels as a function of time for the entire week of testing on each of 14 RHBFSTs. These plots are displayed with major grid lines separated by just .002'; i.e., a very fine level of resolution. Close examination of these 2015 plots indicates no

discernible changes in fuel level over the duration of the tests; i.e., the least squares regression lines are flat. The rates of change of fuel level, and by inference the indicated rates of leakage, were not reported.

The accuracy of these leak tightness tests have been the subject of debate. The RHBFSTs are so large in cross-sectional area that leakage at these flow rates during such a 120-hour test would only change the fuel level by .0014' if leaking at 0.7 GPH, .001' at 0.5 GPH, and just .0004' at 0.2 GPH. The plots with indicated measurement points do suggest that level differences less than 0.001' is achievable.

Additional information about such low leak rate test systems is provided in Reference 5-102. Reference 5-102 claims a level measuring precision of 0.0002 inches (or .0024') compensating for the thermal expansion and contraction of the fuel. Independent third-party tests were performed on a 122.5'-diameter, 2.1-million-gallon bulk underground storage tank at the Navy's Point Loma Fueling Facility in San Diego, California, in 2000. The LRDP-24 (low range differential pressure system) product data sheet in Appendix C of Reference 5-102 indicates that for a 100-foot-diameter tank, such as for the RHBFSTs, a test accuracy of 0.2 GPH can be achieved by performing just five sequential tests, as are performed in the RHBFST annual leak tightness tests over a 120-hour period. This conclusion is based on scaling results for 12 tests performed on tanks with a diameter of 122.5 feet for which the minimum detectable leak rate of 0.2 GPH leak rate detection capability was confirmed.

For this study, based on the above information, the following probabilities are assigned as to the likely actual level of accuracy these now annual RHBFST leak tightness tests can achieve:

- 0.7 GPH, Probability of 0.3
- 0.5 GPH, Probability of 0.6
- 0.2 GPH, Probability of 0.1

Key parameters in the estimation of undetected leakage from RHBFSTs due to undetected through holes include the probability of an undetected through hole developing, and the growth rate of such holes once they are formed.

Section 5.4.3.7 develops an uncertainty distribution for the probability of below maximum fuel operating level hole for use in undetected leakage estimates. That probability distribution (identified as Data Variable PUDHB3 with a mean of 0.087) is adopted here.

RHBFST liner corrosion rates have been estimated as leaving 0.1" in liner thickness after 86 years of RHBFST operation; i.e., corrosion away 0.15" from the initial 0.25"-thick liner in 86 years. The estimated corrosion rate is then .001744" per calendar year. This assumed corrosion rate has been used to justify the 20-year interval between RHBFST inspections. It is understood that RHBFST liner corrosion rates are being evaluated by detailed inspections of multiple RHBFSTs.

This corrosion rate is not so useful for through hole initiation. This rate would indicate that such liner through holes should not be expected, although some localized holes in the liner have been detected via tank inspections while empty, especially higher in the RHBFST upper dome areas, well above the normal operating fuel levels. Even so,

application of this liner corrosion rate is proposed as a nominal estimate of the through-hole radial growth rate in existing through holes for purposes of this assessment. An allowance for growth rate uncertainty is also proposed.

Six different linear through-hole radial growth rates are assumed. These are specified as multiplicative factors, M, on a nominal through-hole growth rate of 0.001744" per calendar year. The probabilities of each multiplicative rate, as applied to through-hole radial growth rates are summarized below.

- M = 4, Probability of .05
- M = 2, Probability of 0.2
- M = 1.0, Probability of .4
- M = 0.5, Probability of 0.2
- M = 0.25, Probability of 0.1
- M = 0.1, Probability of 0.05

The above probability distribution for through-hole radial growth rates is skewed to the low side. Even at four times the nominal tank corrosion rate of .001744" per year, the through-hole radial size would grow to an equivalent flow rate that would exceed the 0.7 GPH leak tightness test accuracy in just half of a year. Such through hole sizes should be easily detectable by the annual leak tightness tests, but none have been observed.

The leakage flow rates detected in the annual leak tightness tests may result from one hole or from two or more smaller holes whose flow areas sum to the same equivalent leakage rate. For this study, a single through hole in a RHBFST is assumed to be the source of the leakage postulated. The holes are assumed to be round so that through-hole radial growth can be easily modeled. If instead, two or more smaller holes were to be assumed totaling the same initial leakage area, the total leakage rate from multiple through holes, assuming the same radial through-hole growth rate (i.e., rate of increase of the diameter in inches per year), would grow more quickly than does leakage from a single through hole. This is just a question of geometry. However, it will be seen later that smaller flow rate increases with time take longer to detect and therefore are projected to result in greater overall releases of fuel before detection. Therefore, the single through-hole model is judged appropriate.

Table 5-44 displays the average number of years between through-hole origination and leak detection by leak tightness testing, the average gallons released during the same period, and the through-hole leakage rate in GPH. These values for gallons released are from the time of through-hole origination, up until the time that the through-hole leak rate is high enough for the next leak tightness test to detect it. The fuel releases, in gallons, do not yet account for the additional leakage from the detection time until the leaking RHBFST is taken out of service.

**Table 5-44. Average Hole Growth, Cumulated Gallons of Fuel Released, and Leak Rate at Time of Detection for Annual Leak Tightness Tests**

| Annual Leak Tightness Test Accuracy GPH | Hole Growth Rate Multiplier, M | Average Gallons Released at Detection | Ave Years Growth @ Detection | Leak Rate (GPH) @ Detection |
|---|---|---|---|---|
| 0.2 | 4 | 6,025 | 0.75 | 2.15 |
| 0.2 | 2 | 2,702 | 0.95 | 0.82 |
| 0.2 | 1 | 2,099 | 1.45 | 0.46 |
| 0.2 | 0.5 | 2,350 | 2.45 | 0.32 |
| 0.2 | 0.25 | 3,414 | 4.45 | 0.26 |
| 0.2 | 0.1 | 6,595 | 10.25 | 0.22 |
| 0.5 | 4 | 8,167 | 0.85 | 2.69 |
| 0.5 | 2 | 5,582 | 1.25 | 1.37 |
| 0.5 | 1 | 5,605 | 2.05 | 0.89 |
| 0.5 | 0.5 | 6,987 | 3.55 | 0.66 |
| 0.5 | 0.25 | 11,302 | 6.65 | 0.58 |
| 0.5 | 0.1 | 24,804 | 15.95 | 0.53 |
| 0.7 | 4 | 10,810 | 0.95 | 3.29 |
| 0.7 | 2 | 8,396 | 1.45 | 1.82 |
| 0.7 | 1 | 8,324 | 2.35 | 1.17 |
| 0.7 | 0.5 | 11,098 | 4.15 | 0.90 |
| 0.7 | 0.25 | 18,555 | 7.85 | 0.81 |
| 0.7 | 0.1 | 40,925 | 18.85 | 0.74 |

To obtain an average for each parameter, the calculations were repeated assuming the through-hole origination occurs at different times between the annual leak tightness tests; i.e., every one-tenth of a year, assigned a 0.1 probability of being the time at which the through hole originates, and then averaged to obtain the results in Table 5-44. These three results are presented for each of the 18 combinations of modeling assumptions concerning test accuracy in GPH and the through-hole growth rate parameter, M. The highest through-hole leak rates occur for through-hole growth rate parameter M is 4.

The leak tightness tests have been repeated on most of the RHBFSTs now in operation. In 2015, 14 of the 18 RHBFSTs still nominally in operation, were tested. The remaining four were not tested (i.e., 5, 14, 17, and 18) because they were temporarily out of service. RHBFST 16 was tested in 2015, but at a reduced fuel level (59') so it is not counted. However, it was tested in 2013.

By pooling the data for all RHBFST leak tightness tests performed so far, it is proposed to obtain estimates on the through-hole origination rates per year (for a hole-growth model) given different assumptions about the through-hole size growth rates and the accuracy of the leak tightness test. Since none of the RHBFSTs subjected to leak tightness tests to date revealed the presence of otherwise undetected through holes, it is reasonable to pool the available data and thereby assume that such estimated through-hole origination rates apply to all RHBFSTs.

On first thought, one may assume that the last year of a successful leak tightness test ensures that the RHBFST is without undetected through holes and that they have not experienced any in previous years since they likely would have grown even larger as time goes on. However, when RHBFSTs are taken out of service for repairs and inspections it is conceivable that these activities may introduce such through holes or to have introduced conditions which could promote the formation of such through holes in the future, possibly at a different rate than in the past. Therefore, the count of RHBFST-successful test years is limited for each tank to the last time the RHBFST underwent inspection. Since the through-hole origination rate may also be changing with time, this analysis also limits the RHBFST-test success years to only the last 25 years. Periods when the RHBFSTs are out of service or in-service are counted the same since backside liner corrosion properties are still at work even when the RHBFST is empty of fuel. For example, RHBFST 2 was last taken out of service for inspection in 2010, but then was returned to service and was leak tightness tested in both 2013 and 2015. The more recent 2015 test is controlling, yielding a successful test count of 5 years for RHBFST 2. RHBFSTs like 17, which have never been leak tightness tested, are assigned an RHBFST-successful test year count of 0. Still other RHBFSTs have been recently tested and have not been taken out of service for inspection in the last 25 years; e.g., 18. The overall count for all RHBFSTs, as of 2015, numbered 254 RHBFST-successful test years.

A successful leak tightness test does not mean there is no through hole, it only means the flow rate from any postulated through hole in the RHBFST is not large enough to be detected. By conservatively assuming that a through hole does originate, just prior to when the last leak tightness test can detect it, the last one or more years of RHBFST-successful test years should be removed from that RHBFST's count. During these most recent removed years, the through hole may exist, but does not have a large enough leakage flow rate to be detected.

The time between through-hole origination and the ability of a future leak tightness test to detect it, depends on assumptions made for the through-hole growth rate multiplicative factor, M, and the leak tightness test accuracy in GPH. Table 5-45 lists the mean of a distribution of probabilities for through-hole origination per year for each of the 18 assumption combinations; i.e., the same assumption combinations as in Table 5-44. As seen in Table 5-45, none of the 18 assumption combinations are credited with the full 254 RHBFST successful test years. One year is subtracted from the successful test years of each RHBFST since a new through hole is not likely to be detected within its first year of growth. The smallest number of RHBFST successful test years is 26. This count applies to the extreme assumption set combination when the leak tightness test accuracy is at its least effective (0.7 GPH) and the growth rate multiplicative factor, M, is its smallest (M=0.1). This case also has the longest average growth time to detection and the highest probability of through-hole origination per year. The probability

distribution for the probability of through-hole origination per year was obtained for each assumption set combination assuming a non-informative Jeffrey's prior (gamma distribution) with Parameter A set to 0.5, and Parameter B set to the number of successful test years for that combination. The probability of a through hole then originating during the average number of years between through-hole origination and leak detection is approximately equal to the product of the average through-hole growth years to detection and the through-hole originate rate in years; i.e., see the last column of Table 5-45.

**Table 5-45. Probability of Through-Hole Origination per Year**

| Detection Accuracy, GPH | Hole Growth Multiplier, M | Average Hole Growth Years to Detect | Successful Test Years | Mean Probability of Through Hole/ Year | Probability of Through Hole during Average Growth Years |
|---|---|---|---|---|---|
| 0.2 | 4 | **0.75** | 238 | 2.11E-03 | 1.58E-03 |
| 0.2 | 2 | **0.95** | 222 | 2.26E-03 | 2.14E-03 |
| 0.2 | 1 | **1.45** | 222 | 2.26E-03 | 3.27E-03 |
| 0.2 | 0.5 | **2.45** | 206 | 2.44E-03 | 5.96E-03 |
| 0.2 | 0.25 | **4.45** | 174 | 2.89E-03 | 1.28E-02 |
| 0.2 | 0.1 | **10.25** | 99 | 5.08E-03 | 5.07E-02 |
| 0.5 | 4 | **0.85** | 238 | 2.11E-03 | 1.79E-03 |
| 0.5 | 2 | **1.25** | 222 | 2.26E-03 | 2.82E-03 |
| 0.5 | 1 | **2.05** | 206 | 2.44E-03 | 4.99E-03 |
| 0.5 | 0.5 | **3.55** | 190 | 2.65E-03 | 9.36E-03 |
| 0.5 | 0.25 | **6.65** | 146 | 3.44E-03 | 2.26E-02 |
| 0.5 | 0.1 | **15.95** | 44 | 1.14E-02 | 1.66E-01 |
| 0.7 | 4 | **0.95** | 238 | 2.11E-03 | 2.00E-03 |
| 0.7 | 2 | **1.45** | 222 | 2.26E-03 | 3.27E-03 |
| 0.7 | 1 | **2.35** | 206 | 2.44E-03 | 5.72E-03 |
| 0.7 | 0.5 | **4.15** | 174 | 2.89E-03 | 1.19E-02 |
| 0.7 | 0.25 | **7.85** | 134 | 3.75E-03 | 2.90E-02 |
| 0.7 | 0.1 | **18.85** | 26 | 1.93E-02 | 3.05E-01 |

The probabilities in Table 5-45 of a through hole having developed during the most recent years when a through hole may have originated and grew to be detected, is low for each assumption combination. This indicates that the approach of removing the average through-hole growth years from the successful test years is conservative; i.e., the count of successful test years should be higher, and the probabilities of through-hole origination per year would then be correspondingly even lower. A full

simulation calculation would likely be needed to relax this conservative assumption, so the current approach is retained in this study.

Idle RHBFSTs are constantly monitored by the AFHE system while a RHBFST is filled with fuel. RHBFST fuel levels and temperatures are continuously monitored. If while idle, fuel levels fall by more than 0.5", an AFHE warning alarm is sounded in the main control room. This 0.5" drop in fuel level corresponds to a leakage of approximately 2,456 gallons. A second AFHE critical alarm is sounded if the overall fuel level falls by more than 0.75".

In addition to the RHBFST leak tightness tests, now performed annually, and the levels continuously recorded by the AFHE system, the facility staff record RHBFST fuel levels continuously. At a leak rate of 0.7 GPH, the change in RHBFST fuel level would take approximately 146 days to initiate the low level warning alarm. However, RHBFST fuel levels would be drifting down before this time. A level drop of just 3/16" would be reached in 55 days. A fuel level drop of 3/16", which is just outside the accuracy of manual top gauging, could be considered significant and worthy of additional investigation after the RHBFST is checked and found to be fully isolated. However, facility staff indicates that no action would be taken to move the fuel at a level decrease of just 3/16". Rather, the staff would wait until the low level warning alarm is received.

On the other hand, as soon as the idle RHBFST undergoes a fuel movement, the fuel level initial conditions are then reset and the time to reach the AFHE warning alarm would start over. Facility staff has indicated that during long periods when a RHBFST is idle, fuel sampling and possibly water drainage from the lower dome, may take place, which would complicate the interpretation of the significance of a 3/16" drop in fuel level.

#### *5.4.6.2 Assembly of Undetected Through-Hole Growth and No-Growth Leakage Models*

Table 5-46 summarizes alternative assumption sets for estimating yearly fuel leakage from undetected through holes in RHBFST liners. There are two parts to the table. The first part is for through-hole no-growth assumption sets. The second part is for through-hole linear radial growth assumption sets.

**Table 5-46. Modeling Assumption Set Probabilities and Total Fuel Releases for 18 RHBFSTs per Year**

| # | Hole Growth Model | Growth Model Probability (1) | Leak Test Detection Accuracy in GPH (a) | Probability of Leak Test Accuracy in GPH (2) | Hole Growth Rate Multiplier | Hole Flow Rate as a Fraction of Detection Flow Rate (b) | Probability of Hole Flow Rate % (3) | Probability of Hole since Last Test | Effective Leak Rate (GPH) per RHBFST (a)*(b) | Gallons Leaked per Year for a Single RHBFST with Hole | Gallons Released per Year after Hole Detected | Facility Gallons Leaked per Year if Probability of Hole Is 1.0 | Probability of Modeling Assumptions (1)* (2)* (3) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | No Growth | 0.1 | 0.2 | 0.1 | N/A | 1 | 0.2 | 1 | 0.2 | 1,753 | N/A | 31,558 | 0.00200 |
| 2 | No Growth | 0.1 | 0.2 | 0.1 | N/A | 0.8 | 0.2 | 1 | 0.16 | 1,403 | N/A | 25,246 | 0.00200 |
| 3 | No Growth | 0.1 | 0.2 | 0.1 | N/A | 0.6 | 0.2 | 1 | 0.12 | 1,052 | N/A | 18,935 | 0.00200 |
| 4 | No Growth | 0.1 | 0.2 | 0.1 | N/A | 0.4 | 0.2 | 1 | 0.08 | 701 | N/A | 12,623 | 0.00200 |
| 5 | No Growth | 0.1 | 0.2 | 0.1 | N/A | 0.2 | 0.2 | 1 | 0.04 | 351 | N/A | 6,312 | 0.00200 |
| 6 | No Growth | 0.1 | 0.5 | 0.6 | N/A | 1 | 0.2 | 1 | 0.5 | 4,383 | N/A | 78,894 | 0.01200 |
| 7 | No Growth | 0.1 | 0.5 | 0.6 | N/A | 0.8 | 0.2 | 1 | 0.4 | 3,506 | N/A | 63,115 | 0.01200 |
| 8 | No Growth | 0.1 | 0.5 | 0.6 | N/A | 0.6 | 0.2 | 1 | 0.3 | 2,630 | N/A | 47,336 | 0.01200 |
| 9 | No Growth | 0.1 | 0.5 | 0.6 | N/A | 0.4 | 0.2 | 1 | 0.2 | 1,753 | N/A | 31,558 | 0.01200 |
| 10 | No Growth | 0.1 | 0.5 | 0.6 | N/A | 0.2 | 0.2 | 1 | 0.1 | 877 | N/A | 15,779 | 0.01200 |
| 11 | No Growth | 0.1 | 0.7 | 0.3 | N/A | 1 | 0.2 | 1 | 0.7 | 6,136 | N/A | 110,452 | 0.00600 |
| 12 | No Growth | 0.1 | 0.7 | 0.3 | N/A | 0.8 | 0.2 | 1 | 0.56 | 4,909 | N/A | 88,361 | 0.00600 |
| 13 | No Growth | 0.1 | 0.7 | 0.3 | N/A | 0.6 | 0.2 | 1 | 0.42 | 3,682 | N/A | 66,271 | 0.00600 |
| 14 | No Growth | 0.1 | 0.7 | 0.3 | N/A | 0.4 | 0.2 | 1 | 0.28 | 2,454 | N/A | 44,181 | 0.00600 |
| 15 | No Growth | 0.1 | 0.7 | 0.3 | N/A | 0.2 | 0.2 | 1 | 0.14 | 1,227 | N/A | 22,090 | 0.00600 |

**Table 5-46. Modeling Assumption Set Probabilities and Total Fuel Releases for 18 RHBFSTs per Year (Continued)**

| # | Hole Growth Model | Growth Model Probability (1) | Leak Test Detection Accuracy in GPH | Probability of Leak Test Accuracy in GPH (2) | Hole Growth Rate Multiplier | Probability of Growth Rate Multiplier (3) | Average Years to Hole Detection | Rate of Hole Origination (events/ RHBFST-yr.) | Gallons Leaked before Detection for Single RHBFST with Hole | Probability of Through-Hole Origination/ Year * (18 RHBFSTs) | Facility-Wide Gallons Leaked per Year up to the Time of Leak Detection | Leak Rate (GPH) at Time of Detection | Gallons Released after Hole Detected | Total Annual Gallons Released | Probability of Modeling Assumptions (1)* (2)* (3) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Linear Growth | 0.9 | 0.2 | 0.1 | 4 | 0.05 | 0.75 | 2.11E-03 | 6,025 | 0.038 | 229 | 2.15 | 4,007 | 381 | 0.00450 |
| 2 | Linear Growth | 0.9 | 0.2 | 0.1 | 2 | 0.2 | 0.95 | 2.26E-03 | 2,702 | 0.041 | 110 | 0.82 | 3,048 | 234 | 0.01800 |
| 3 | Linear Growth | 0.9 | 0.2 | 0.1 | 1 | 0.4 | 1.45 | 2.26E-03 | 2,099 | 0.041 | 85 | 0.46 | 2,784 | 199 | 0.03600 |
| 4 | Linear Growth | 0.9 | 0.2 | 0.1 | 0.5 | 0.2 | 2.45 | 2.44E-03 | 2,350 | 0.044 | 103 | 0.32 | 2,685 | 221 | 0.01800 |
| 5 | Linear Growth | 0.9 | 0.2 | 0.1 | 0.25 | 0.1 | 4.45 | 2.89E-03 | 3,414 | 0.052 | 178 | 0.26 | 2,643 | 315 | 0.00900 |
| 6 | Linear Growth | 0.9 | 0.2 | 0.1 | 0.1 | 0.05 | 10.25 | 5.08E-03 | 6,595 | 0.091 | 603 | 0.22 | 2,614 | 842 | 0.00450 |
| 7 | Linear Growth | 0.9 | 0.5 | 0.6 | 4 | 0.05 | 0.85 | 2.11E-03 | 8,167 | 0.038 | 310 | 2.69 | 4,392 | 477 | 0.02700 |
| 8 | Linear Growth | 0.9 | 0.5 | 0.6 | 2 | 0.2 | 1.25 | 2.26E-03 | 5,582 | 0.041 | 227 | 1.37 | 3,445 | 367 | 0.10800 |
| 9 | Linear Growth | 0.9 | 0.5 | 0.6 | 1 | 0.4 | 2.05 | 2.44E-03 | 5,605 | 0.044 | 246 | 0.89 | 3,100 | 382 | 0.21600 |
| 10 | Linear Growth | 0.9 | 0.5 | 0.6 | 0.5 | 0.2 | 3.55 | 2.65E-03 | 6,987 | 0.048 | 333 | 0.66 | 2,933 | 473 | 0.10800 |
| 11 | Linear Growth | 0.9 | 0.5 | 0.6 | 0.25 | 0.1 | 6.65 | 3.44E-03 | 11,302 | 0.062 | 700 | 0.58 | 2,872 | 878 | 0.05400 |
| 12 | Linear Growth | 0.9 | 0.5 | 0.6 | 0.1 | 0.05 | 15.95 | 1.14E-02 | 24,804 | 0.205 | 5,090 | 0.53 | 2,839 | 5,672 | 0.02700 |
| 13 | Linear Growth | 0.9 | 0.7 | 0.3 | 4 | 0.05 | 0.95 | 2.11E-03 | 10,810 | 0.038 | 411 | 3.29 | 4,825 | 594 | 0.01350 |
| 14 | Linear Growth | 0.9 | 0.7 | 0.3 | 2 | 0.2 | 1.45 | 2.26E-03 | 8,396 | 0.041 | 342 | 1.82 | 3,770 | 495 | 0.05400 |
| 15 | Linear Growth | 0.9 | 0.7 | 0.3 | 1 | 0.4 | 2.35 | 2.44E-03 | 8,324 | 0.044 | 366 | 1.17 | 3,299 | 510 | 0.10800 |
| 16 | Linear Growth | 0.9 | 0.7 | 0.3 | 0.5 | 0.2 | 4.15 | 2.89E-03 | 11,098 | 0.052 | 577 | 0.90 | 3,106 | 739 | 0.05400 |

**Table 5-46. Modeling Assumption Set Probabilities and Total Fuel Releases for 18 RHBFSTs per Year (Continued)**

| # | Hole Growth Model | Growth Model Probability (1) | Leak Test Detection Accuracy in GPH | Probability of Leak Test Accuracy in GPH (2) | Hole Growth Rate Multiplier | Probability of Growth Rate Multiplier (3) | Average Years to Hole Detection | Rate of Hole Origination (events/ RHBFST-yr.) | Gallons Leaked before Detection for Single RHBFST with Hole | Probability of Through-Hole Origination/ Year * (18 RHBFSTs) | Facility-Wide Gallons Leaked per Year up to the Time of Leak Detection | Leak Rate (GPH) at Time of Detection | Gallons Released after Hole Detected | Total Annual Gallons Released | Probability of Modeling Assumptions (1)* (2)* (3) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 17 | Linear Growth | 0.9 | 0.7 | 0.3 | 0.25 | 0.1 | 7.85 | 3.75E-03 | 18,555 | 0.068 | 1,252 | 0.81 | 3,036 | 1,457 | 0.02700 |
| 18 | Linear Growth | 0.9 | 0.7 | 0.3 | 0.1 | 0.05 | 18.85 | 1.93E-02 | 40,925 | 0.347 | 14,217 | 0.74 | 2,990 | 15,256 | 0.01350 |

*(1), (2), (3) These columns contain probabilities from a discrete probability distribution that the values in the previous column are the correct values of that distribution. These probabilities are multiplied in the last column to obtain the overall probability that the assumption set represented by that row is the correct assumption set.*

#### 5.4.6.2.1 No-Growth Assumption Sets

The first 15 assumption set combinations in Table 5-46 are termed "no-growth" models. In the 15 assumption set combinations, a through hole is postulated to always be present in each RHBFST and to have a through-hole size that permits fuel leakage at rates that are not detectable by the annual leak tightness tests. No through-hole radial growth is assumed with time so that the leakage flow rates remain undetectable for all years.

The no-growth assumption sets are assigned a low probability (0.1) of representing the correct model for leakage via undetected through holes. Instead, the linear growth models, as a surrogate for all hole radial growth models, are judged to be more likely (0.9) to correctly represent the leakage flows from initially very small through holes in the liner of a RHBFST.

A second uncertainty in the no-growth assumption sets is the assumed annual leak tightness detection accuracy; i.e., 0.2 GPH, 0.5 GPH, or 0.7 GPH. The assumed distribution of these leak rates was presented in Section 5.4.6.1.

A third uncertainty is the assumed size of the postulated through hole knowing that its leak rate is less than detection accuracy. It would be conservative to assume that the postulated through-hole leak rate is the same as the leak tightness test accuracy. For this realistic analysis, a uniform discrete probability distribution of flow rates is assumed with flow rates varying from 20% to 100% of the leak test accuracy (GPH). The mean of this discrete uniform distribution is 0.6.

#### 5.4.6.2.2 Linear Growth Assumption Sets

As noted in the preceding section, through-hole linear growth models, used as an approximation for all through-hole time-dependent growth models, are judged to be more likely (0.9) to correctly represent the leakage flows from initially very small through holes in a RHBFST than are the no-growth models presented in the previous section.

For the linear growth model assumptions, 18 assumption set alternatives are presented in the lower portion of Table 5-46. In addition to the 0.9 probability, two additional assumptions consider the uncertainties in the leak tightness test flow rate detection accuracy (in GPH) and the through-hole growth rate multiplier, M. The probability of a through hole originating per year of RHBFST operation is also considered. Each assumption set further assumes that the initiation probability of through holes, growth multipliers, and leak tightness test detection flow rate accuracy, are shared by all fuel types and individual RHBFST; i.e., all RHBFSTs are judged to behave similarly for purposes of estimating the impacts of undetected through holes, which is consistent with pooling the leak tightness test data.

The probability of a through hole originating in a RHBFST since the last annual leak tightness test is equal to the through-hole origination rate in events per year. Through holes that might have originated in earlier years but could not have been detected by the current leak tightness tests were not credited in the computation of successful test years, for this reason. The remaining successful test years were used to evaluate the rates of

through-hole origination per year for years when the through holes could have been detected but were not found.

The Table 5-46 column titled “Gallons Leaked per Year for a Single RHBFST with a Hole” represents the total quantity of fuel released in gallons from through-hole origination until detection at a leak tightness test. For assumption sets with high values of the multiplicative factor (M = 4) for through-hole growth, all of the fuel release events may be detected that same year. For assumption sets with low values of the multiplicative factor (M = 0.1) for through-hole growth, the fuel release may be spread out over many years; i.e., up to 18.85 years, on average, for Linear Growth Assumption Set 18 in Table 5-18.

In the Table 5-18 column labeled “Probability of Through-Hole Origination/Year * (18 RHBFSTs)”, is the probability of a through hole originating per year multiplied by the number of RHBFSTs nominally in service (18), to obtain the facility-wide probability of a through hole originating in the 1 year since the last annual leak tightness tests. It is this probability which is then multiplied by the conditional gallons leaked for a single RHBFST with a through hole in the next column to obtain the facility–wide gallons leaked per year up to the time of leak detection; i.e., in gallons per year. This value is a probabilistic sum of through holes that may have been initiated in the years prior to the current leak tightness test.

As an example, for Assumption Set 5, the fuel release is spread out over 5 years with an expected time from through-hole origination to leak detection being 4.45 years. Leakage in later years is larger, although the final year may have a smaller release than the previous year only because the through hole, on average, is detected prior to the end of the last year. The mean probability of a through hole originating per year was assumed constant for each of these 5 years and equally applicable to all 18 RHBFSTs in-service. The contribution to the total gallons released from through holes created earlier than the most recent leak tightness test is just the probability of a through hole for a single earlier year, multiplied by the leakage for that year, which is measured from the time of through-hole origination and summed over the applicable years for that assumption set. Mathematically then, the probability weighted total gallons released from earlier years sums to also equal the total release per through hole, multiplied by the yearly probability of through-hole origination.

Table 5-47 shows how the total fuel released from a single leaking RHBFST is apportioned by year, measured from the time of through-hole origination for a given assumption set. The fuel release would be spread out over the time from through-hole origination to eventual leak detection. These releases are a function of the through-hole growth rate and the leak tightness test detection accuracy and therefore are different for each assumption set. For all but three of the 18 linear growth assumption set combinations, the growing through hole is detected, on average, by an annual leak tightness test within 8 years so that the leakage is terminated for that RHBFST by 8 years. The gallons leaked after detection until the time the leaking RHBFST is emptied is considered separately.

After the through hole grows in size sufficiently to be detected by a leak tightness test, there would also be fuel leaked until the leaking RHBFST is emptied of fuel. There has not been a RHBFST leak tightness test that detected a leak, and a procedure for what to

do is not available. It is expected that if a leak was discovered, that it would take some time to formally compile the results of the leak tightness test and that during this time, additional fuel release would occur. For purposes of calculating the post-test release, it is assumed that the leaking RHBFST would be maintained as is until the AFHE warning alarm was activated. The change in RHBFST level at the warning alarm setpoint is equivalent to a release of about 2,456 gallons of fuel. Another 30 days is also assumed before the decision to empty the leaking tank is made and the leaking tank is emptied. For this extra 30-day period, the leak rate is assumed equal to that at the time of the leak tightness test. The quantity of gallons released after leak detection differs depending on the leak rate at detection and so also with differing assumption sets. This additional period of leakage could occur over a 2-month period, since the time to reach the low level alarm setpoint itself is at least 32 days, even for the highest leak rate expected at the time of detection; i.e., for Assumption Set 13.

**Table 5-47. Fuel Released Each Year Following Though-Hole Origination in One RHBFST for Different Linear Growth Assumption Sets**

| # | Leak Test Detection Accuracy in GPH | Hole Growth Rate Multiplier | Average Years to Hole Detection | Mean Probability of Through Hole/ Year | Total Gallons Leaked before Detection | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.2 | 4 | 0.75 | 2.11E-03 | 6,025 | 6,025 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0.2 | 2 | 0.95 | 2.26E-03 | 2,702 | 2,702 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0.2 | 1 | 1.45 | 2.26E-03 | 2,099 | 619 | 1,480 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0.2 | 0.5 | 2.45 | 2.44E-03 | 2,350 | 155 | 1,074 | 1,121 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0.2 | 0.25 | 4.45 | 2.89E-03 | 3,414 | 39 | 268 | 728 | 1,415 | 964 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0.2 | 0.1 | 10.25 | 5.08E-03 | 6,595 | 6 | 43 | 117 | 226 | 373 | 556 | 776 | 1,033 | 1,325 | 1,655 | 485 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0.5 | 4 | 0.85 | 2.11E-03 | 8,167 | 9,909 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0.5 | 2 | 1.25 | 2.26E-03 | 5,582 | 2,477 | 3,105 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0.5 | 1 | 2.05 | 2.44E-03 | 5,605 | 619 | 4,299 | 687 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0.5 | 0.5 | 3.55 | 2.65E-03 | 6,987 | 155 | 1,074 | 2,910 | 2,848 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0.5 | 0.25 | 6.65 | 3.44E-03 | 11,302 | 39 | 268 | 728 | 1,415 | 2,331 | 3,476 | 3,045 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0.5 | 0.1 | 15.95 | 1.14E-02 | 24,804 | 6 | 43 | 117 | 226 | 373 | 556 | 776 | 1,033 | 1,325 | 1,655 | 2,022 | 2,424 | 2,863 | 3,340 | 3,853 | 4,192 | 0 | 0 | 0 |
| 13 | 0.7 | 4 | 0.95 | 2.11E-03 | 10,810 | 10,810 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0.7 | 2 | 1.45 | 2.26E-03 | 8,396 | 619 | 7,777 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0.7 | 1 | 2.35 | 2.44E-03 | 8,324 | 2,477 | 5,847 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0.7 | 0.5 | 4.15 | 2.89E-03 | 11,098 | 155 | 1,074 | 2,910 | 5,659 | 1,300 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0.7 | 0.25 | 7.85 | 3.75E-03 | 18,555 | 39 | 268 | 728 | 1,415 | 2,331 | 3,476 | 4,850 | 5,448 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0.7 | 0.1 | 18.85 | 1.93E-02 | 40,925 | 6 | 43 | 117 | 226 | 373 | 556 | 776 | 1,033 | 1,325 | 1,655 | 2,022 | 2,424 | 2,863 | 3,340 | 3,853 | 4,401 | 4,988 | 5,610 | 5,314 |

### 5.4.6.3 Conclusions

The 33 assumption set probability weighted, mean estimate of fuel release from undetected holes is 5,803 gallons per year. See Table 5-48. This includes probability weighted contributions from the no-growth (5,018 gallons per year) and linear growth models (786 gallons per year). The no-growth model contribution dominates the calculated release of fuel per year despite its assigned low probability of being the correct model. The linear growth models average release (786 gallons per year) is made up of two parts. The average fuel release prior to leak detection is 630 gallons per year. The added contribution from leakage after detection until the RHBFST is emptied in order to stop the release, weighted by the frequency of such detections in any of the 18 RHBFSTs, is just 156 gallons per year. The fuel release for a single event of leak tightness test leak detection is a function of the final leakage rate and the time to empty the RHBFST. None of the leak tightness tests reported to date have detected fuel leakage in excess of the test accuracy.

**Table 5-48. Contribution to Mean Gallons of Fuel Release per Year**

| Contribution to Mean Gallons of Fuel Release per Year | Gallons per Year |
|---|---|
| No Growth Models Probability Weighted - 18 RHBFSTs = | 5,018 |
| Linear Growth Probability Weighted -18 RHBFSTs Leakage up to Detection = | 630 |
| Linear Growth Probability Weighted - 18 RHBFSTs Leakage before and after Detection = | 786 |
| Probability Weighted Total Release - Sum of No-Growth and Linear Growth Models = | 5,803 |

The uncertainty distribution for the fuel release in gallons per year is shown in Figure 5-17. The figure displays the probability of exceeding a given amount of fuel released per year versus the number of gallons released per year. Figure 5-17 represents the uncertainty in evaluating the mean gallons released per year accounting for the different assumption probabilities used in the calculation. This figure does not represent the variation in quantity of fuel released from year to year. As more information is gathered as to leak tightness test detection accuracy, through-hole size growth rates, and the probabilities of through-hole origination as it relates to the performance of leak tightness tests, these modeling uncertainties are expected to be reduced.

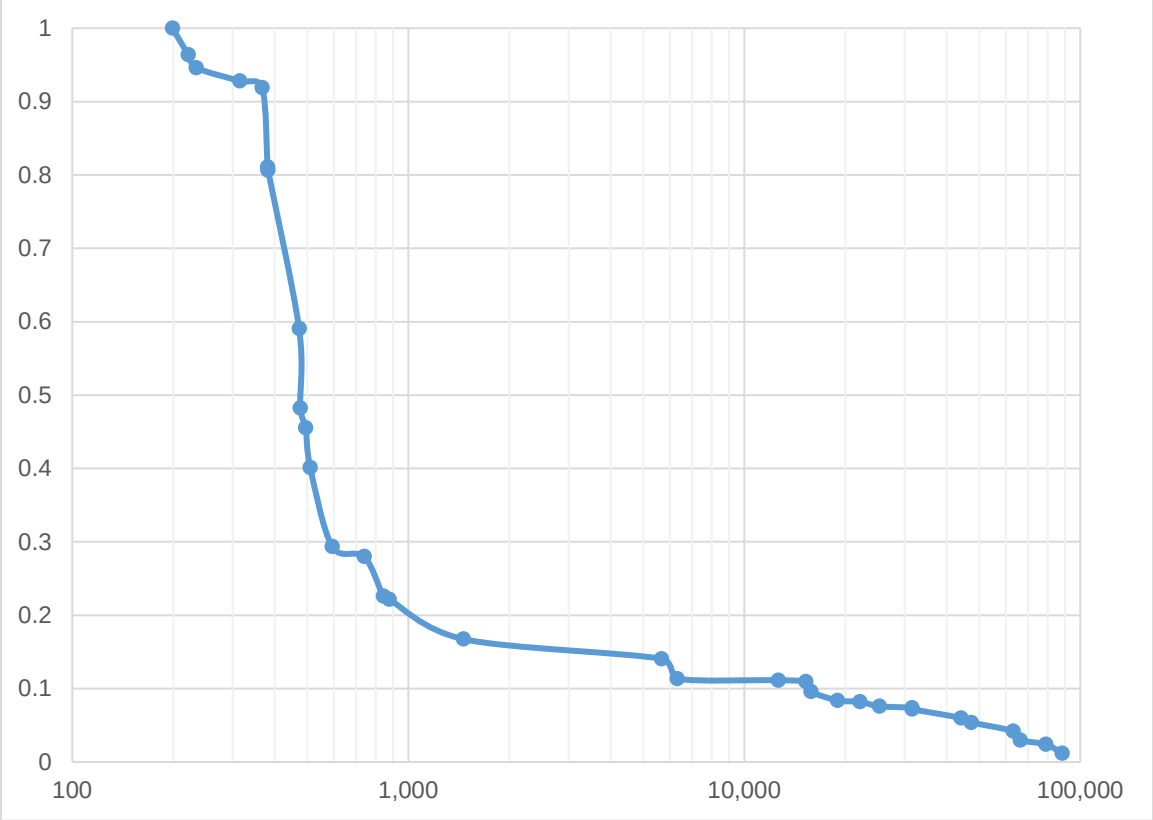



**Figure 5-17. Probability of Facility-Wide Chronic Releases Being Greater than Gallons per Year Shown on X-Axis**

Given a through hole is assumed, the linear growth models do estimate a conditional through-hole release of fuel in gallons for the year of through-hole detection that exceeds the corresponding release for the no-growth assumption sets; i.e., the leak rates at the time of detection exceed the leak test flow detection accuracy levels. It is the lower probability of through-hole initiation for the linear growth models (i.e., much lower than 1.0) that limits the time-averaged facility fuel releases to less than the corresponding first 15 no-growth assumption sets. It is also observed that the linear growth assumptions yielding the highest releases are those with lower through-hole growth rates. For these assumption sets, the leakage flow rates are lower, but the times to detection (i.e., within the accuracy of the leak tightness tests) can be years longer than if the through holes grow faster. This can lead to higher cumulative fuel releases.

The no-growth model results in Table 5-49, conservatively assume that the probability of an undetected hole being present in each operating RHBFST is 1.0. This is in contrast to the linear growth model in which the assessment provides estimates of the probability of such holes for each assumption set, assuming the holes growth with time.

As a sensitivity study, the mean of the uncertainty distribution developed in Section 5.4.3.7 for the probability of a below maximum fuel operating level hole is applied to the no-growth model results. The mean of the uncertainty distribution is 0.087. The summary results displayed in Table 5-48 then become as shown in Table 5-49. In the sensitivity case, once the probability of undetected holes is included

in the assessment, the no-growth model results are comparable to the mean gallons per year developed for the linear growth model. Of course, these results still include a subjective probability weighting that the linear-growth model is more likely correct (0.9) than is the no-growth hole model (0.1). If instead the no-growth model, with the probability of a below maximum fuel operating level of 0.87 included, was assumed the correct model (1.0) and the linear growth model not correct (0.), then the total mean chronic fuel release would be 4,370 gallons per year.

**Table 5-49. Summary of Sensitivity Results with Hole Probability Included in No-Growth Model**

| Contribution to Mean Gallons of Fuel Release per Year | Gallons per Year |
|---|---|
| No Growth Models Probability Weighted - 18 RHBFSTs with 0.087 Hole Probability = | 437 |
| Linear Growth Probability Weighted - 18 RHBFSTs Leakage up to Detection = | 630 |
| Linear Growth Probability Weighted - 18 RHBFSTs Leakage before and after Detection = | 786 |
| Probability Weighted Total Release - Sum of No Growth and Linear Growth Models = | 1,222 |

### 5.4.7 Maintenance Induced Leakage Fuel Release Initiating Events

The RHBFSF piping runs through the LAT and Harbor Tunnel where it can be monitored and maintained. In addition to the random leakage events for piping, valves, and other connections discussed in Section 5.4.5, maintenance errors can lead to leakage from these same components. There is no anecdotal evidence of such an event having occurred in the entire 75-year history of the Red Hill facility. Such events are postulated to most likely occur when a fuel line is slacked and the line is opened in a given pipe section to perform component maintenance or piping inspections, and possibly piping replacement. Such events are of special interest because the size of the inadvertent opening could be large, approaching the full diameter of the piping section.

Data for the frequency of such events was not available for this study. It is judged that the three fuel lines in the LAT and Harbor Tunnel are each opened approximately once every 10 years; i.e., three times in 10 years for the facility as a whole. Most likely, the entire fuel line is not drained for these maintenance activities. Rather, a fuel line section is slacked, and the piping section being maintained is isolated from other sections in the same fuel line by closure of the sectional valve above the opened pipe section where the maintenance is to be performed.

Two classes of maintenance errors for such maintenance activities are considered:

1. Inadvertent opening of the above sectional valve from an already slacked fuel line whose piping integrity has already been breached; i.e., the component or piping to be replaced or maintained has been removed. In this class of events, once the sectional valve is opened, flow from the still full fuel line sections upgrade are released to the slacked section and released to the tunnel via the opening.

2. Selection of the wrong component or piping segment to be removed, which is on a different fuel line from the one already slacked. In this class of events, fuel would be released at the time the component or piping removal is attempted.

In the first class of events identified above, any sectional valve would only be opened at the direction of, or by the control room crew. It would be unusual to have to open a sectional valve because when a fuel line is in service, the sectional valves are all normally open. Therefore, the very need to open a sectional valve indicates that the line is being restored from maintenance and extra care should be taken to ensure the proper steps are followed. The status of each of the three available fuel lines is well illustrated in the control room, making such an error very unlikely. Even if such an error occurred, the fuel released would be limited by the contents of the above sectional valve; i.e., no fuel movement from a RHBFST could be taking place. Further, inadvertent opening of the piping line from a RHBFST to the open fuel line section would require the opening of both the RHBFST's skin and ball valves; i.e., two errors. The operational orders needed to align a RHBFST by opening the two valves for a planned fuel movement would further have to specify the wrong fuel line, the one currently being maintained. This class of events is judged quite unlikely, and so not considered further.

In the second class of events, one fuel line section is isolated in preparation to be opened for planned maintenance. For this assessment, it is postulated that a ball valve has been identified to be removed for corrective maintenance. The ball valve would first be tagged for maintenance by the Red Hill staff, but the actual maintenance would be performed by a subcontractor to the Navy. The subcontractor also has the responsibility to tag-out the correct component. Before physically opening the line, the subcontractor would be in communication with the control room staff as a further check. Note that the body of the ball valve is at an elevated location in the tank gallery. The inadvertent opening of a ball valve on the wrong fuel line also seems unlikely because it requires a combination of three errors. It is still considered here as a representative maintenance error leading to release.

The first error is for Red Hill staff to tag the wrong valve for the planned maintenance. Red Hill staff is very familiar with the location of all ball valves so this error is very unlikely. Nearly all the lines exiting the RHBFSTs are the same 12"-diameter piping; i.e., 15 of the 18 RHBFSTs in service have cross-tie lines which are 12"-diameter piping. RHBFSTs containing F24 and JP5 fuel types all have 12" cross-tie lines with one exception; i.e., that for RHBFST 2. Though unlikely, there could be some confusion, for example, between the ball valve for RHBFST 6, which holds F24, and the ball valve for the adjacent RHBFST 8, which holds JP5 fuel. It's assumed that the correct ball valve to be maintained is 108C on RHBFST 8, but that Ball Valve 106C on RHBFST 6, aligned to the F24 16" main fuel line is erroneously tagged for service.

The 2017 master operational schematic for AFHE shows the spectral flanges for JP5 RHBFSTs aligned to the 18" main fuel line and the F24 RHBFSTs aligned to the 16" main fuel line. An apparent error in this drawing, however, shows the spectral flange position for RHBFSTs 3 and 4, which hold F24, actually aligned to the 18" JP5 main fuel line. While this drawing would not be used for the development of operational orders at Red Hill, this just highlights the potential for the initial error assumed in this assessment.

The second error would require that the subcontractor tasked with removing the 108C ball valve does not catch that the 106C ball valve tagged for service is the incorrect one. This action to tag-out the correct valve is to be performed independent of the Red Hill staff tagging, but some dependence of the subcontractor's action on the earlier error is assumed.

Before opening the line, the subcontractor would also be in contact with the control room, again checking that the correct valve is to be removed. Therefore a third error, this one involving both the subcontractor and the control room staff, is required. Once given the go-ahead, the subcontractor is assumed to open the line in to remove the valve. Once the bolts are loosened some leakage is to be expected. It is conservatively assumed, however, that the size of the resulting opening is bounded by the full pipe diameter of 12". Once fuel is released, the subcontractor staff is assumed to exit the tunnel quickly.

In the event the incorrectly selected fuel line is undergoing a fuel movement, this may be detected by the subcontractor personnel; i.e., via noise from the moving fuel in the line, or since the skin and ball valves should be indicating open. However, the fuel movement may be from a different RHBFST where these indications are not available. Therefore, it is assumed that they would proceed not knowing of the fuel movement. Whether the line is idle or undergoing fuel movement, no credit is given for the subcontractors closing the opening afterwards.

There is no sectional valve in the tank gallery for the 16", F24 main fuel line to which 106C is aligned, so the fuel line contents would be spilled through the opening. If a fuel movement was in progress at the time of the event, then control room staff would need to take action to isolate the skin valve of the F24 RHBFST that is undergoing the fuel movement.

The maintenance errors described above that may lead to a release to the LAT were modeled using fault trees to compute the frequency of occurrence of maintenance induced fuel release initiating events. The following table lists the 12 such initiating events and associated fault trees. [redacted]

## Table 5-50. Maintenance Induced Leakage Fuel Release Initiating Events

| Initiating Event Name | Description | Top Event/ Fault Tree | Failure Frequency/ Year |
|---|---|---|---|
| SF24I | Maintenance error on F24 Ball Valve 102C while idle; leading to release to LAT | OME24I | 7.83E-06 |
| SF24IS | Maintenance error on F24 Skin Valve 102B while idle; leading to release to LAT | OME24IS | 2.35E-07 |
| SF24M | Maintenance error on F24 Ball Valve 102C while fuel moving; leading to release to LAT | OME24M | 5.07E-08 |
| SF24MS | Maintenance error on F24 Skin Valve 102B while fuel moving; leading to release to LAT | OME24MS | 1.66E-09 |
| SF76I | Maintenance error on F76 Ball Valve 115C while idle; leading to release to LAT | OME76I | 8.82E-06 |
| SF76IS | Maintenance error on F76 Skin Valve 115B while idle; leading to release to LAT | OME76IS | 2.65E-07 |
| SF76M | Maintenance error on F76 Ball Valve 115C while moving fuel; leading to release to LAT | OME76M | 2.08E-08 |
| SF76MS | Maintenance error on F76 Skin Valve 115B while moving fuel; leading to release to LAT | OME76MS | 6.83E-10 |
| SJP5I | Maintenance error on JP5 Ball Valve 108C while idle; leading to release to LAT | OMJP5I | 9.54E-06 |
| SJP5IS | Maintenance error on JP5 Skin Valve 108B while idle; leading to release to LAT | OMJ5IS | 3.13E-07 |
| SJP5M | Maintenance error on JP5 Ball Valve 108C while moving fuel; leading to release to LAT | OMJP5M | 3.32E-08 |
| SJP5MS | Maintenance error on JP5 Skin Valve 108B while moving fuel; leading to release to LAT | OMJ5MS | 1.09E-09 |

### 5.4.8 Fuel Movement Data

Fuel evolutions were reviewed for a 90-day period starting from January 1, 2017, to March 31, 2017, to ascertain the frequency and duration of fuel movement at the RHBFSF. Table 5-51 summarizes the fuel movement by fuel type and RHBFST.

**Table 5-51. Summary of Fuel Movement by Fuel Type and RHBFST**

| Fuel Type | RHBFST | # Issues | Total Issue Hours | Issue Barrels | # Receipts | Total Receipt Hours | Received Barrels |
|---|---|---|---|---|---|---|---|
| F24 | 102 | 0 | 0.0 | 0 | 3 | 14.4 | 47,601 |
| F24 | 103 | 6 | 79.8 | 204,160 | 3 | 86.1 | 143,458 |
| F24 | 104 | 2 | 33.6 | 100,832 | 2 | 61.3 | 295,820 |
| F24 | 105 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| F24 | 106 | 2 | 34.0 | 128,864 | 4 | 63.7 | 187,910 |
| F76 | 115 | 4 | 24.8 | 51,279 | 2 | 53.3 | 84,027 |
| F76 | 116 | 12 | 44.9 | 65,143 | 2 | 27.5 | 49,958 |
| JP5 | 107 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 108 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 109 | 1 | 28.6 | 42,389 | 3 | 49.9 | 6,882 |
| JP5 | 110 | 0 | 0.0 | 0 | 3 | 126.7 | 118,107 |
| JP5 | 111 | 1 | 1.9 | 7,586 | 1 | 14.1 | 87,520 |
| JP5 | 112 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 113 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 114 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 117 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |
| JP5 | 118 | 1 | 19.8 | 106,054 | 0 | 0.0 | 0 |
| JP5 | 120 | 0 | 0.0 | 0 | 0 | 0.0 | 0 |

For inter-RHBFST fuel transfers, Table 5-52 lists the assumed number of transfers and durations over a 10-year period.

**Table 5-52. Number of Inter-Tank Fuel Transfers**

| Fuel Type | # of Transfers per Year | Average Duration |
|---|---|---|
| F24 | 4 | 10 |
| JP5 | 4 | 10 |
| F76 | 2 | 10 |

Table 5-53 lists the result distributions on fuel movement frequencies.

Table 5-54 lists the result distributions on fuel movement durations.

## Table 5-53. Distributions of Fuel Movement Frequencies

| Fuel Movement Frequencies by Fuel Type and Evolution Type | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Name** | **Evolution Type** | **Distribution Type** | **Median** | **Range Factor** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| FIF24 | Issue | Log-Normal Median Range Factor | 40 | 1.2 | 4.02E+1 | 3.32E+1 | 3.98E+1 | 4.75E+1 | 1.2 |
| FIF76 | Issue | Log-Normal Median Range Factor | 64 | 1.2 | 6.44E+1 | 5.31E+1 | 6.36E+1 | 7.61E+1 | 1.2 |
| FIJP5 | Issue | Log-Normal Median Range Factor | 12 | 1.3 | 1.22E+1 | 9.17E+0 | 1.19E+1 | 1.54E+1 | 1.3 |
| FRF24 | Receipt | Log-Normal Median Range Factor | 36 | 1.2 | 3.62E+1 | 2.99E+1 | 3.58E+1 | 4.28E+1 | 1.2 |
| FRF76 | Receipt | Log-Normal Median Range Factor | 12 | 1.3 | 1.22E+1 | 9.17E+0 | 1.19E+1 | 1.54E+1 | 1.3 |
| FRJP5 | Receipt | Log-Normal Median Range Factor | 21 | 1.2 | 2.11E+1 | 1.74E+1 | 2.09E+1 | 2.50E+1 | 1.2 |
| FXF24 | Inter-Tank Transfer | Log-Normal Median Range Factor | 4 | 1.5 | 4.12E+0 | 2.64E+0 | 3.95E+0 | 5.87E+0 | 1.49 |
| FXF76 | Inter-Tank Transfer | Log-Normal Median Range Factor | 2 | 1.5 | 2.06E+0 | 1.32E+0 | 1.98E+0 | 2.94E+0 | 1.49 |
| FXJP5 | Inter-Tank Transfer | Log-Normal Median Range Factor | 4 | 1.5 | 4.12E+0 | 2.64E+0 | 3.95E+0 | 5.87E+0 | 1.49 |

## Table 5-54. Distributions of Fuel Movement Durations

| Fuel Movement Durations (in hours) by Fuel Type and Evolution Type | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Name** | **Evolution Type** | **Distribution Type** | **Median** | **Range Factor** | **Mean** | **5th** | **Median** | **95th** | **Range Factor** |
| DIF24 | Issue | Log-Normal Median Range Factor | 14.7 | 1.2 | 1.48E+1 | 1.22E+1 | 1.46E+1 | 1.75E+1 | 1.2 |
| DIF76 | Issue | Log-Normal Median Range Factor | 4.4 | 1.2 | 4.43E+0 | 3.65E+0 | 4.38E+0 | 5.23E+0 | 1.2 |
| DIJP5 | Issue | Log-Normal Median Range Factor | 16.8 | 1.3 | 1.70E+1 | 1.28E+1 | 1.67E+1 | 2.15E+1 | 1.3 |
| DRF24 | Receipt | Log-Normal Median Range Factor | 18.8 | 1.2 | 1.89E+1 | 1.56E+1 | 1.87E+1 | 2.23E+1 | 1.2 |
| DRF76 | Receipt | Log-Normal Median Range Factor | 20.2 | 1.3 | 2.05E+1 | 1.54E+1 | 2.00E+1 | 2.59E+1 | 1.3 |
| DRJP5 | Receipt | Log-Normal Median Range Factor | 27.2 | 1.2 | 2.74E+1 | 2.26E+1 | 2.7E+1 | 3.23E+1 | 1.2 |
| DXF24 | Inter-Tank Transfer | Log-Normal Median Range Factor | 10 | 1.4 | 1.02E+1 | 7.08E+0 | 9.9E+0 | 1.37E+1 | 1.39 |
| DXF76 | Inter-Tank Transfer | Log-Normal Median Range Factor | 10 | 1.4 | 1.02E+1 | 7.08E+0 | 9.9E+0 | 1.37E+1 | 1.39 |
| DXJP5 | Inter-Tank Transfer | Log-Normal Median Range Factor | 10 | 1.4 | 1.02E+1 | 7.08E+0 | 9.9E+0 | 1.37E+1 | 1.39 |

### 5.4.9 Accounting for Potential of Corrosion Rates Increasing with Time

Some outside our QRVA team have suggested that over the long term (i.e., for the next 100 years), the QRVA should account for the potential of corrosion rates increasing with time in the QRVA risk calculations. While we understand, very well, the concept of potential failure rate acceleration with aging, we do not feel it is appropriate to apply that concept in this QRVA for the following reasons:

- This concept includes the implicit assumption that tank, pipe, and valve failures leading to fuel release are dominated by the corrosion failure mechanism. While we agree that corrosion is an important contributing factor to many failure events, we have strong evidence that it is not the exclusive failure mechanism in place at the RHBFSF. For example, we know that the major Tank 5 event in early 2014 had nothing to do with corrosion but was clearly dominated by cascading human errors in the inspection/repair and associated tank return-to-service process. Via our review of the known fuel release events (and precursor events) at the RHBFSF, we are confident that corrosion, while a factor in some events, is not the exclusive failure mechanism at work and is likely not the dominating failure mechanism when considering the complete spectrum of historical and potential future causal factors or root causes of fuel release events.

- If accelerating corrosion rates were dominating fuel releases at the RHBFSF, we would expect to be able to see evidence of the associated failure rate acceleration trend over the history of the facility, as this facility already has significant history (over 70 calendar years or 1,400 tank-years). The general failure trend [redacted] does not indicate significant evidence of accelerating failure rates over time.

- We feel that a strong reason for why we do not see evidence of corrosion rate acceleration at the RHBFSF is that there is an effective continuous “renewal” process in place for the tanks and supporting flow path components. This renewal process occurs via the regular tank inspection and repair processes in practice at the facility, specifically the commitment that all tanks will be inspected with 100% area coverage at least once every 20 years, and that as a result of these inspections there is a process in place for replacement of tank liner sections or plates where actual breeches in continuity are discovered or where impending breeches are predicted to cause through-wall leakage prior to the next inspection. Similarly, most facility piping and valves are effectively continuously monitored via direct roving watch observation and via control room operator monitoring of AFHE parameters, such as pipe pressure levels and tank levels.

- The probability of tank through-wall failure over time without renewal, can be characterized by the following equation: P(t) = the integral of the function (1-exp(-1*a*λ*t)) from time 0 to the time t where P(t) is the probability over time interval t (in years) that a through-wall failure exists; λ is the conventional failure rate for all failure causes (in failures per year, assumed constant) postulated via a Bayesian update of generic failure rate data with observed facility and/or industry failure history; and where a is the unitless failure rate acceleration factor (= 1+ X(t) * t where X(t) is the fraction increase in λ at each time, t, due to aging, and t is, again, in

years). In such a model, we would need to know the value of X(t) to account for failure rate acceleration with age. The QRVA team has no data or analysis to support the value of X(t) or a in this model other than treating it as 0, which is the standard practice in QRVA unless evidence to the contrary can be provided. No analysis or data supporting a non-zero value of X(t), or the average value of X(t) over the preceding life of the facility has been provided by the Navy or other experts for this QRVA, and such analyses or data has not been identified in the literature by the QRVA team for this facility risk assessment.

- One could argue that, in the case of the RHBFSF tanks, we might expect there to actually be a failure rate deceleration factor at play over the remainder of facility life. This could be supported by our reasonable expectations that, in the future over time, tank inspection processes designed to discover problematic corrosion and other failure mechanisms will improve (we have certainly seen that over the current history of the facility). Therefore our ability to find actual and impending failures will improve. Also, we might even expect that tank repair and liner section replacement processes could be enhanced in the future. These aspects of tank inspection and repair processes bolster the argument for the renewal effect that would counteract any hypothetical corrosion rate acceleration.

Therefore, the conventional QRVA assumption of constant failure rates is retained for this assessment.

### 5.4.10 Monitoring Well Data Review

To date, the QRVA team has performed a cursory review of RHBFSF monitoring well data to determine if and how spikes in detected levels of hydrocarbons in these wells may correlate with or relate to facility fuel release. While the team did note several spikes in this data over time, they could not correlate these heightened hydrocarbon levels directly with the 18 known acute fuel release incidents applied in the QRVA initiating event data. Similarly, monthly soil vapor sampling results for each RHBFST taken between January 24, 2014, and January 1, 2016, show a substantial volatile organic compounds peak under RHBFST 5 and to a lesser extent under RHBFST 3, beginning 3 months after the RHBFST 5 incident. However, RHBFST 5 was empty for all of those 3 intervening months.

The QRVA team has no expertise in the area of released fuel transport through rock and soil. This expertise resides within the AOC Sections 6 and 7 response teams. Based simply on the judgment of the QRVA team, there could be a significant variable amount of time between actual acute fuel release incidents and potentially associated specific monitoring well heightened hydrocarbon level detection observations. It is important to note that the monitoring well readings capable of detecting hydrocarbon level spikes were only taken quarterly in the past, and may currently be taken monthly, so, even if only based on recent readings, there could easily be an average of 2 weeks between any actual acute fuel release incident and hydrocarbon level observations from the monitoring wells. In the judgment of the QRVA team, time lags between acute fuel release incidents and elevated hydrocarbon readings from monitoring wells could be affected by fuel transport and potential “pooling” time associated with the amount of fuel released. Also, possibly even more likely, the monitoring well hydrocarbon level spikes could be associated with transport and pooling of fuel release from chronic, generally

undetected, fuel releases from the facility, which could also be affected by fuel transport and pooling time associated with the amount of fuel released. For a discussion of predicted chronic fuel release from the RHBFSF, please see Section 5.4.6 of this report.

## 5.5 Response Events Data

### 5.5.1 Response Equipment Failure Mode Failure Rate Data

In a QRVA, the facility response to initiating events takes the form of hardware and human actions. The analysis of human response actions and associated HFE HEP values is conducted in the QRVA HRA. The hardware or systemic response to initiating events requires the characterization of hardware failure rate data to be applied in event sequence quantification. The response events data analysis follows the same general Bayesian updating process as that described for initiating events. Ideally, generic data is updated in a first-stage update applying similar facility historical data, and this data is updated in a second-stage update applying facility-specific (in this case, RHBFSF-specific) historical data. To date, the Navy has not provided similar facility or facility-specific failure and corrective maintenance information for RHBFSF, or for similar Navy facility hardware. Therefore, given no such information is provided, the QRVA will apply industry generic data for response events. The following generic data sources were reviewed for this QRVA:

- NUREG/CR-6928 Data (2007) (Reference 5-2)
- OREDA 2015 Data (Reference 5-5)
- Process Equipment Reliability Data (1989) (Reference 5-103)
- IEEE Standard 500 Data (1984) (Reference 5-43)
- Westinghouse Savannah River Site Chemical Process Data (1993) (Reference 5-104)
- PLG-0500 Data (1989) (Reference 5-105)
- Lees' Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control (2012) (Reference 5-106)
- OGP Risk Assessment Data Directory, Report No. 434, March 2010 (434.PDF) (Reference 5-54)
- OGP Risk Assessment Data Directory, Report No. 434-3 March 2010 (434-03.PDF) (Reference 5-55)

Based on this review, the QRVA team selected NUREG/CR-6928 (Table 5-1) data as the best generic data source to support the RHBFSF QRVA response event data analysis. To support facility-specific hardware data analysis, it is necessary to determine what general types of components exist at the facility that could potentially be associated with the facility hardware response to initiating events in the QRVA. Additionally, the

QRVA team must determine what equipment failure modes may apply to the response event analysis for event sequence quantification. This is not the detailed FMEA performed within the systems analysis, but it is a general assessment of potential applicable component failure modes. Therefore, the QRVA team developed a list of equipment and associated failure modes as modeled in the QRVA. Table 5-55 presents this list of RHBFSF equipment and associated failure modes along with the linkage to NUREG/CR-6928.

## Table 5-55. RHBFSF Equipment Failure Mode Failure Rate Data for Response Event Data Analysis

| System/ Component Name | Data Source | Component Type Link (6928) | Failure Mode ID | Failure Rate Unit | Distribution Name | Description | Events | Time/ Demands | Priors | Prior Mean | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Automatic Bus Transfer Switch | NUREG/CR-6928 (Reference 5-2) | ABT | FTOP | d | ATFTOP | Automatic Bus Transfer Switch Fail to Operate | | | | N/A | 3.07E-03 | 1.01E-05 | 1.26E-03 | 1.08E-02 |
| Battery (DC) | NUREG/CR-6928 (Reference 5-2) | BAT | FTOP | d | BATFOP | Battery (DC) Fail to Operate | | | | N/A | 1.87E-06 | 2.42E-09 | 6.51E-07 | 6.93E-06 |
| Bus | NUREG/CR-6928 (Reference 5-2) | BUS | FTOP | d | BUSFOP | Bus Fail to Operate | | | | N/A | 4.35E-07 | 1.47E-09 | 1.80E-07 | 1.53E-06 |
| Door (characterized as solenoid valve) | NUREG/CR-6928 (Reference 5-2) | SOV | FTOP | d | DOOR | Oil Tight Door Failure to Close (SOV NUREG) | | | | N/A | 9.62E-04 | 1.33E-06 | 5.84E-05 | 2.41E-03 |
| Diesel Generator | NUREG/CR-6928 (Reference 5-2) | EDG STBY | FTLR | h | EDGFR2 | Emergency Diesel Generator (standby) Fail to Run after First Hour of Operation | | | | N/A | 8.49E-04 | 1.45E-04 | 6.86E-04 | 1.92E-03 |
| Diesel Generator | NUREG/CR-6928 (Reference 5-2) | EDG STBY | FTR>1H | h | EDGFTR | Emergency Diesel Generator Fail to Run during First Hour of Operation | | | | N/A | 2.90E-03 | 2.87E-04 | 2.14E-03 | 7.30E-03 |
| Diesel Generator | NUREG/CR-6928 (Reference 5-2) | EDG STBY | FTS | d | EDGFTS | Emergency Diesel Generator (standby) Fail to Start | | | | N/A | 4.55E-03 | 2.52E-04 | 3.05E-03 | 1.25E-02 |
| Elevator | Reference 5-4 | | | | ELEVD | Failure of Elevator on Demand | | | | N/A | 7.47E-03 | 2.65E-04 | 2.61E-03 | 2.48E-02 |
| Fan | NUREG/CR-6928 (Reference 5-2) | FAN RUN | FTR | h | FANFTR | Fan (running) Fail to Run | | | | N/A | 1.08E-05 | 1.26E-07 | 5.56E-06 | 3.51E-05 |
| Fan | NUREG/CR-6928 (Reference 5-2) | FAN RUN | FTS | d | FANFTS | Fan (running) Fail to Start | | | | N/A | 1.81E-03 | 1.46E-07 | 3.80E-04 | 7.45E-03 |
| Fan | NUREG/CR-6928 (Reference 5-2) | FANTM | | h | FANTM | Fan Test or Maintenance Unavailability (NUREG CR 6928 Table 6-1) | | | | N/A | 2.01E-03 | 6.69E-06 | 8.30E-04 | 7.08E-03 |
| Offsite Power | UI Listing.xlsx (Received 03/15/18) | | Loss of Offsite Power | h | LOOP | Grid Loss Frequency | | | | N/A | 1.00E+00 | 9.05E-01 | 9.95E-01 | 1.09E+00 |
| Pipe | “Pipeline Risk Management Manual Ideas, Techniques and Resources” (Reference 5-1) | | ELM | ft-hr | LPIPE | 6" Pipe Failure (Medium) per Ft-Hr (6–10 mm thick) | | | | N/A | 6.75E-13 | 2.23E-15 | 2.78E-13 | 2.38E-12 |
| Level Switch | IEEE 500 (Reference 5-43) | | FTOP | d | LSWFOP | Level Switch No Function with Signal (IEEE 500) | | | | N/A | 1.76E-06 | 3.14E-07 | 1.20E-06 | 4.52E-06 |
| RHBFST | Red Hill Evidence | | | | LTKM | Medium Leak 0.5" | 0 | 1315.6 | NAVYLG | 7.63E-05 | 6.65E-05 | 8.70E-07 | 2.26E-05 | 1.34E-04 |
| RHBFST | Red Hill Evidence | | | | LTKS | Small Leak 1.5 gpm | 18 | 1315.6 | NGRID | 1.43E-03 | 1.24E-02 | 6.78E-03 | 1.11E-02 | 1.67E-02 |
| Motor-Driven Compressor | NUREG/CR-6928 (Reference 5-2) | MDC RUN | FTR | h | MDCFTR | Motor-Driven Compressor (running) Fail to Run | | | | N/A | 9.18E-05 | 9.19E-06 | 6.80E-05 | 2.31E-04 |

## Table 5-55. RHBFSF Equipment Failure Mode Failure Rate Data for Response Event Data Analysis (Continued)

| System/ Component Name | Data Source | Component Type Link (6928) | Failure Mode ID | Failure Rate Unit | Distribution Name | Description | Events | Time/ Demands | Priors | Prior Mean | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Motor-Driven Compressor | NUREG/CR-6928 (Reference 5-2) | MDC RUN | FTS | d | MDCFTS | Motor-Driven Compressor (running) Fail to Start | | | | N/A | 1.36E-02 | 5.71E-06 | 3.86E-03 | 5.28E-02 |
| Motor-Operated Valve | Red Hill Evidence | | ELL | h | MOVELL | RH-Updated ELS Motor-Operated Valve External Leak Large | 0 | 37027584 | MVELL | 9.83E-10 | 4.88E-10 | 3.94E-14 | 1.02E-10 | 2.01E-09 |
| Motor-Operated Valve | Red Hill Evidence | | ELS | h | MOVELS | RH-Updated Motor-Operated Valve External Leak Small | 0 | 37027584 | MVELS | 1.41E-08 | 6.92E-09 | 2.30E-11 | 2.85E-09 | 2.44E-08 |
| Motor-Operated Valve | NUREG/CR-6928 (Reference 5-2) | MOV | FTO/C | d | MOVFOC | Motor-Operated Valve Fail to Open or Close | | | | N/A | 1.08E-03 | 8.87E-05 | 7.72E-04 | 2.79E-03 |
| Motor-Operated Valve | NUREG/CR-6928 (Reference 5-2) | MOV | ELL | h | MVELL | Motor-Operated Valve External Leak Large (NUREG/CR-6928) | | | | N/A | 9.83E-10 | 7.93E-14 | 2.06E-10 | 4.04E-09 |
| Motor-Operated Valve | NUREG/CR-6928 (Reference 5-2) | MOV | ELS | h | MVELS | Motor-Operated Valve External Leak Small (NUREG/CR-6928) | | | | N/A | 1.41E-08 | 4.67E-11 | 5.82E-09 | 4.98E-08 |
| Underground Storage Tank | NavyBulkTank_ SpillReleaseData | | ELL | h | NAVYLG | Navy UST Large Release | | | | N/A | 7.63E-05 | 8.70E-07 | 2.77E-05 | 1.36E-04 |
| Underground Storage Tank | NavyBulkTank_ SpillReleaseData | | ELS | h | NAVYS | Navy UST Small Releases | 10 | 7050 | OGPS | 2.81E-03 | 1.45E-03 | 7.90E-04 | 1.38E-03 | 2.21E-03 |
| Underground Storage Tank | NavyBulkTank_ SpillReleaseData | | | | NGRID | Navy UST Prior Grouped by Location | | | | N/A | 1.43E-03 | 3.81E-06 | 2.26E-05 | 4.58E-03 |
| Electrical Panel | IEEE 500 (Reference 5-43) | | | h | EPANEL | Electrical Control Panel Composite (IEEE 500) | | | | N/A | 8.31E-07 | 1.66E-09 | 6.37E-08 | 2.22E-06 |
| Pipe | "Pipeline Risk Management Manual Ideas, Techniques and Resources" (Reference 5-98) | | ELL | ft-hr | PIPEL | Large Pipe Leak per Foot | | | | N/A | 2.54E-11 | 2.55E-13 | 4.72E-12 | 8.29E-11 |
| Pipe | "Pipeline Risk Management Manual Ideas, Techniques and Resources" (Reference 5-1) | | ELS | ft-hr | PIPES | Small Pipe Leak per Foot | | | | N/A | 2.53E-10 | 1.24E-11 | 1.03E-10 | 8.21E-10 |
| Process Logic (level) | NUREG/CR-6928 (Reference 5-2) | PLL | FTOP | d | PLLFOP | Process Logic (level) Fail to Operate | | | | N/A | 6.29E-04 | 2.08E-06 | 2.59E-04 | 2.22E-03 |
| Pump | NUREG/CR-6928 (Reference 5-2) | PMP | FTR | h | PMPFTR | Pump Fail to Run | | | | N/A | 1.35E-04 | 1.30E-05 | 9.95E-05 | 3.42E-04 |

## Table 5-55. RHBFSF Equipment Failure Mode Failure Rate Data for Response Event Data Analysis (Continued)

| System/ Component Name | Data Source | Component Type Link (6928) | Failure Mode ID | Failure Rate Unit | Distribution Name | Description | Events | Time/ Demands | Priors | Prior Mean | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pump | NUREG/CR-6928 (Reference 5-2) | PMP | FTS | d | PMPFTS | Pump Fail to Start | | | | N/A | 2.70E-04 | 8.95E-07 | 1.11E-04 | 9.54E-04 |
| RHBFST | Red Hill Evidence | | ELL | h | RHLNG | RH Large Release, Updated from Navy Large UST | 0 | 1315.6 | NAVYLG | 7.63E-05 | 6.65E-05 | 8.70E-07 | 2.26E-05 | 1.34E-04 |
| Pipe | "Pipeline Risk Management Manual Ideas, Techniques and Resources" (Reference 5-1) | | ELS | ft-hr | SPIPE | 0.5" Pipe Failure (small) per Ft-Hr (6–10 mm thick) | | | | N/A | 4.16E-12 | 1.37E-14 | 1.71E-12 | 1.47E-11 |
| Sensor/ Transmitter (Level) | NUREG/CR-6928 (Reference 5-2) | STL | FTOP | d | STLFOP | Sensor/Transmitter (level) Fail to Operate | | | | N/A | 8.20E-04 | 2.71E-06 | 3.38E-04 | 2.89E-03 |
| Sensor/ Transmitter (level) | IEEE 500 (Reference 5-43) | | No Change of Output with Change of Input | h | STLSTK | Sensor/Transmitter (level) No Change of Output with Change of Input (IEEE 500) | | | | N/A | 4.60E-07 | 8.16E-08 | 3.14E-07 | 1.18E-06 |
| Strainer | NUREG/CR-6928 (Reference 5-2) | STR | PLG | h | STRPLG | Strainer Plug | | | | N/A | 7.44E-06 | 6.00E-10 | 1.56E-06 | 3.06E-05 |
| Transformer | NUREG/CR-6928 (Reference 5-2) | TFM | FTOP | h | TFFTOP | Transformer Fail to Operate | | | | N/A | 9.13E-07 | 1.12E-10 | 2.07E-07 | 3.70E-06 |
| Manual Valve | NUREG/CR-6928 (Reference 5-2) | XVM | ELL | h | XVELL | Manual Valve External Leak Large (NUREG/CR-6928) | | | | N/A | 3.15E-09 | 2.54E-13 | 6.60E-10 | 1.29E-08 |
| Manual Valve | NUREG/CR-6928 (Reference 5-2) | XVM | ELS | h | XVELS | Manual Valve External Leak Small (NUREG/CR-6928) | | | | N/A | 4.49E-08 | 1.49E-10 | 1.85E-08 | 1.58E-07 |
| Manual Valve | Red Hill Evidence | | ELL | h | XVMELL | RH-Updated Manual Valve External Leak Large | | | | N/A | 1.44E-09 | 1.16E-13 | 3.02E-10 | 5.92E-09 |
| Manual Valve | Red Hill Evidence | | ELS | h | XVMELS | RH-Updated Manual Valve External Leak Small | 0 | 13306788 | XVELS | 4.49E-08 | 2.05E-08 | 6.81E-11 | 8.46E-09 | 7.24E-08 |

#### *5.5.1.1 Elevator Reliability Data*

Elevator experience in Australia was obtained from 81 different high rise elevators over a 3-year period. See Reference 5-3. The study evaluated lift reliability, or availability, and found the 81 elevators exhibited reliabilities ranging from 0.957 to .999. Converting to unavailability, the full range for the 81 elevators was found to be between .001 and .043. The mean of the 81 elevators was found to be .007 with a corresponding median of .0028. A lognormal distribution named ELEVD is assigned to elevator unavailability for Red Hill with a median of .0028 and range factor of 10. This yields a mean value of 0.0076 and a 95% value for the unavailability of 0.025.

### 5.5.2 Equipment Common Cause Failure Data

As described in the data analysis methodology description (Section 5.3) of this report, equipment common cause failure analysis is performed to properly and rigorously account for the class of dependent failures called common cause failures in response event data analysis. Common cause failures occur when similar components in functionally-redundant trains or channels of response equipment fail closely in time due to the same general failure mechanisms and causes. The term “closely in time” in this definition generally applies to failures that occur within the normal or expected mean-time-to-restore or mean-time-to-repair of the equipment designated as being in the same common cause failure groups for QRVA logic models. Typically, in QRVA, common cause failure groups are defined for redundant active components, such as pumps, valves, instrumentation channels, electric power sources, etc., and not for passive components, such as tanks or pipes.

As part of the RHBFSF QRVA, system analysis common cause failure groups were identified and modeled for ventilation fans, cargo pump and sump pumps. The fault tree logic and the utilization of these common cause groups are documented in Section 7 of this report for Top Events “EFAN”, “TFAN”, “UFAN”, “CARGO”, “MSUMP” and “USUMP”. Table 5-56 provides the common cause alpha factors used (from CCF Parameter Estimations Reference 5-4) for each common cause group.

## Table 5-56. Common Cause Parameters

| Common Cause Group Description | Distribution Name | Description | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|
| Two Fans FTR | A1C2FR | CC2 Alpha Factor 1 for FAN Fail to Run | 9.93E-01 | 9.87E-01 | 9.94E-01 | 9.98E-01 |
| | A2C2FR | CC2 Alpha Factor 2 for FAN Fail to Run | 6.30E-03 | 2.01E-03 | 5.60E-03 | 1.19E-02 |
| Two Fans FTS | A1C2FS | CC2 Alpha Factor 1 for FAN Fail to Start | 9.95E-01 | 9.84E-01 | 9.97E-01 | 1.00E+00 |
| | A2C2FS | CC2 Alpha Factor 2 for FAN Fail to Start | 4.79E-03 | 1.03E-04 | 2.75E-03 | 1.47E-02 |
| Four Fans FTR | A1C4FR | CC4 Alpha Factor 1 for FAN Fail to Run | 9.95E-01 | 9.91E-01 | 9.95E-01 | 9.98E-01 |
| | A2C4FR | CC4 Alpha Factor 2 for FAN Fail to Run | 1.83E-03 | 3.54E-04 | 1.51E-03 | 4.00E-03 |
| | A3C4FR | CC4 Alpha Factor 3 for FAN Fail to Run | 1.97E-03 | 4.14E-04 | 1.64E-03 | 4.21E-03 |
| | A4C4FR | CC4 Alpha Factor 4 for FAN Fail to Run | 1.00E-03 | 7.47E-05 | 7.07E-04 | 2.64E-03 |
| Four Fans FTS | A1C4FS | CC4 Alpha Factor 1 for FAN Fail to Start | 9.88E-01 | 9.78E-01 | 9.90E-01 | 9.96E-01 |
| | A2C4FS | CC4 Alpha Factor 2 for FAN Fail to Start | 9.31E-03 | 2.63E-03 | 8.14E-03 | 1.83E-02 |
| | A3C4FS | CC4 Alpha Factor 3 for FAN Fail to Start | 1.17E-03 | 1.06E-06 | 3.83E-04 | 4.42E-03 |
| | A4C4FS | CC4 Alpha Factor 4 for FAN Fail to Start | 6.50E-04 | 1.98E-09 | 7.32E-05 | 2.88E-03 |
| Two Pumps FTR | A1C2MR | CC2 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 9.68E-01 | 9.24E-01 | 9.73E-01 | 9.94E-01 |
| | A2C2MR | CC2 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 3.12E-02 | 4.86E-03 | 2.51E-02 | 7.14E-02 |
| Two Pumps FTS | A1C2MS | CC2 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO START | 9.82E-01 | 9.70E-01 | 9.83E-01 | 9.92E-01 |
| | A2C2MS | CC2 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO START | 1.76E-02 | 7.95E-03 | 1.64E-02 | 2.91E-02 |

## Table 5-56. Common Cause Parameters (Continued)

| Common Cause Group Description | Distribution Name | Description | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|
| Three Pumps FTR | A1C3MR | CC3 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 9.66E-01 | 9.40E-01 | 9.68E-01 | 9.85E-01 |
| | A2C3MR | CC3 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 2.66E-02 | 9.45E-03 | 2.41E-02 | 4.83E-02 |
| | A3C3MR | CC3 Alpha Factor 3 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 7.13E-03 | 4.80E-04 | 4.96E-03 | 1.90E-02 |
| Three Pumps FTS | A1C3MS | CC3 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO START | 9.82E-01 | 9.74E-01 | 9.83E-01 | 9.90E-01 |
| | A2C3MS | CC3 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO START | 1.19E-02 | 5.96E-03 | 1.13E-02 | 1.89E-02 |
| | A3C3MS | CC3 Alpha Factor 3 Factor for MOTOR DRIVEN PUMP FAIL TO START | 5.23E-03 | 1.63E-03 | 4.63E-03 | 9.98E-03 |
| Five Pumps FTR | A1C5MR | CC5 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 9.67E-01 | 9.49E-01 | 9.68E-01 | 9.81E-01 |
| | A2C5MR | CC5 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 1.70E-02 | 6.89E-03 | 1.57E-02 | 2.95E-02 |
| | A3C5MR | CC5 Alpha Factor 3 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 9.63E-03 | 2.58E-03 | 8.36E-03 | 1.93E-02 |
| | A4C5MR | CC5 Alpha Factor 4 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 5.19E-03 | 6.64E-04 | 4.01E-03 | 1.24E-02 |
| | A5C5MR | CC5 Alpha Factor 5 Factor for MOTOR DRIVEN PUMP FAIL TO RUN | 7.29E-04 | 2.96E-09 | 8.67E-05 | 3.21E-03 |

## Table 5-56. Common Cause Parameters (Continued)

| Common Cause Group Description | Distribution Name | Description | Mean | 5th Percentile | Median | 95th Percentile |
|---|---|---|---|---|---|---|
| Five Pumps FTS | A1C5MS | CC5 Alpha Factor 1 Factor for MOTOR DRIVEN PUMP FAIL TO START | 9.83E-01 | 9.77E-01 | 9.84E-01 | 9.89E-01 |
| | A2C5MS | CC5 Alpha Factor 2 Factor for MOTOR DRIVEN PUMP FAIL TO START | 7.75E-03 | 4.05E-03 | 7.36E-03 | 1.20E-02 |
| | A3C5MS | CC5 Alpha Factor 3 Factor for MOTOR DRIVEN PUMP FAIL TO START | 5.10E-03 | 2.21E-03 | 4.73E-03 | 8.62E-03 |
| | A4C5MS | CC5 Alpha Factor 4 Factor for MOTOR DRIVEN PUMP FAIL TO START | 2.60E-03 | 7.08E-04 | 2.26E-03 | 5.17E-03 |
| | A5C5MS | CC5 Alpha Factor 5 Factor for MOTOR DRIVEN PUMP FAIL TO START | 7.66E-04 | 2.85E-05 | 4.81E-04 | 2.22E-03 |

## 5.6 Section 5 References


5-1 Muhlbauer, W. Kent, "Pipeline Risk Management Manual Ideas, Techniques and Resources," Third Edition, ELSEVIER.

5-2 NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, 2007.

5-3 Turhanlar, Daniel, Yaping He, and Glenn Stone, "The Use of Lifts for Emergency Evacuation – a reliability study," The 9th Asia-Oceania Symposium on Fore and Science Technology, www.sciencedirect.com, Procedia Engineering 62 (2013) 680-689, by School of Computing, Engineering and Mathematics, University of Western Sydney, Penrith NSW 2751, Australia.

5-4 U.S. Nuclear Regulatory Commission, "CCF Parameter Estimations, 2015 Update," October 26, 2015.

5-5 OREDA 2015 Handbook, Offshore and Onshore Reliability Database, 2015.

5-6 Kaplan, S., "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems (preprint), 1981.

5-7 Chhikara, R. S., and J. L. Folks, "The Inverse Gaussian Distribution as a Lifetime Model," Technometrics, Vol. 19, pp. 461–468, 1977.

5-8 Hahn, G. J., and S. S. Shapiro, Statistical Models in Engineering, John Wiley & Sons, Inc., New York, Chapter B, 1967.

5-9 Mann, N. R., R. E. Shafer, N. D. Singpurwalla, Methods for Statistical Analysis of Reliability and Life Data, John Wiley & Sons, Inc., New York, 1974.

5-10 Barlow, R. E., and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York, 1975.

5-11 Lapides, M. E., and E. L. Zebroski, Use of Nuclear Plant Operating Experience to Guide Productivity Improvement Programs, EPRI SR-26-R, Electric Power Research Institute, Palo Alto, California, 1975.

5-12 U.S. Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), Washington, D.C., 1975.

5-13 McClymont, A., and G. McLagan, Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis, EPRI NP-2433, Electric Power Research Institute, Palo Alto, California, 1982.

5-14 Green, A. E., and A. J. Bourne, Reliability Technology, Wiley-Interscience, New York, 1972.

5-15 Hald, A., Statistical Theory with Engineering Applications, John Wiley & Sons, Inc., New York, 1952.

5-16 Apostolakis, G., S. Kaplan, B. J. Garrick, and R. J. Duphily, "Data Specialization for Plant-Specific Risk Studies," Nuclear Engineering and Design, Vol. 56, pp. 321–329, 1980.

5-17 Parry, T. W., and P. W. Winter, "Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis," Nuclear Safety, Vol. 22, pp. 28–42, 1981.

5-18 Bayes, T., "Essay Toward Solving a Problem in the Doctrine of Chances" (reprinted), Biometrika, Vol. 45, pp. 293–315, 1958.

5-19 Ahmed, S., D. R. Metcalf, R. E. Clark, and J. A. Jacobsen, BURD – A Computer Program for Bayesian Updating of Reliability Data, NPGD-TM-582, Babcock & Wilcox, Lynchburg, Virginia, 1981.

5-20 Martz, H. F., and R. Waller, Bayesian Reliability Analysis, John Wiley & Sons, New York, 1982.

5-21 Jeffreys, H., Theory of Probability, 3rd ed., Clarendon Press, Oxford, England, 1961.

5-22 Apostolakis, G., and A. Mosleh, "Expert Opinion and Statistical Evidence: An Application to Reactor Core Melt Frequency," Nuclear Science and Engineering, Vol. 70, pp. 135–149, 1979.

5-23 Smith, A. M., and I. A. Watson, "Common Cause Failures – A Dilemma in Perspective," Reliability Engineering, Vol. 1, pp. 127–142, 1980.

5-24 Watson, J. A., and G. T. Edwards, A Study of Common-Mode Failures, R-146, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, London, England, 1979.

5-25 Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operation Experience Involving Dependent Events," Pickard Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

5-26 Fleming, K. N., "A Reliability Model for Common Mode Failure in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A1 3284, April 23–25, 1975.

5-27 Parry, G. W., "Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty," 1984 Annual Meeting of the Society for Risk Analysis.

5-28 Fleming, K. N., and A. M. Kalinowski, "An Extension of the Beta Factor Method to Systems with High Levels of Redundancy," Pickard, Lowe and Garrick, Inc., PLG-0289, June 1983.

5-29 Poucet, A., A. Amendola, and P. C. Carriabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Center Report, EUR-11054 EN, Ispra, Italy, 1987.

5-30 Mosleh, A., "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data," Nuclear Engineering and Design, August 1985.

5-31 Paula, H. M., "Comments on the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation," Nuclear Safety, Vol. 27, No. 2, April/June 1986.

5-32 Mosleh, A., and N. O. Siu, "A Multi-Parameter, Event-Based Common Cause Failure Model," Paper M7/3, Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, 1987.

5-33 Atwood, C. L., "Common Cause Fault Rates for Pumps," NUREG/CR-2098, prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.

5-34 Burdick, G. R., N. H. Marshall, and J. R. Wilson, "COMCAN – A Computer Program for Common Cause Failure Analysis," ERDA Report ANCR-1314, Aerojet Nuclear Company, 1976.

5-35 Rooney, J. J., and J. B. Fussell, "BACFIRE II – A Computer Program for Common Cause Failure Analysis of Complex Systems," Department of Nuclear Engineering, University of Tennessee, Knoxville, Tennessee, 1978.

5-36 Worrell, R. B., and O. W. Stack, "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, California, pp. 363–366, 1981.

5-37 Wagner, O. P., C. L. Cate, and J. B. Fussell, "Common Cause Failure Analysis for Complex Systems," in Nuclear Systems Reliability and Risk Assessment, J. B. Fussell and G. R. Burdick (editors), Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania, 1977.

5-38 Rasmuson, D. M., N. H. Marshall, J. R. Wilson, and G. R. Burdick, COMCAN II – A Computer Program for Automated Common Cause Failure Analysis, U.S. Department of Energy Report TREE-1361, EG&G Idaho, Inc., Idaho Falls, Idaho, 1979.

5-39 Putney, B. F., WAMCOM, Common Cause Methodologies Using Large Fault Trees, NP-1851, Electric Power Research Institute, Palo Alto, California, 1981.

5-40 Lindley, D. V., Introduction to Probability and Statistics. Part 1: Probability, Part 2: Inference, Cambridge University Press, 1970.

5-41 Kaplan, S., "On a 'Two-Stage' Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 1, January 1983.

5-42 U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG/75-014), October 1975.

5-43 Nuclear Power Engineering Committee of the IEEE Power Engineering Society, "IEEE Guide to the Collection and Presentation of Electrical, Electronic and Sensing Component Reliability Data for Nuclear Power Generation Stations," IEEE Std 500-1984, New York, New York, December 13, 1983.

5-44 Mosleh, A., and G. Apostolakis, "Models for the Use of Expert Opinions," Proceedings, Workshop on Low-Probability/High-Consequence Risk Analysis, Arlington, Virginia, June 15-17, 1982, Plenum Press, New York, 1983.

5-45 Dalkey, N. C., An Experimental Study of Group Opinion, The RAND Corporation, RM-5888-PR, Santa Monica, California, 1969.

5-46 Hubble, W. H., and C. F. Miller, "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants," NUREG/CR-1363, EGG-EA-5125, June 1980.

5-47 ABSG Consulting Inc., "RISKMAN™ for Windows Version 14.4 User Manual II: Data Analysis," Irvine, California, December 2015.

5-48 Mosleh, A., and G. Apostolakis, "Combining Various Types of Data in Estimating Failure Rate Distributions," Transactions of the 1983 Winter Meeting of the American Nuclear Society, San Francisco, California, 1983.

5-49 Hannaman, G. W., "GCR Reliability Data Bank Status Report," General Atomic Company, GA-A14839 UC-77, July 1978.

5-50 Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, September 1981.

5-51 Apostolakis, G., "Data Analysis in Risk Assessments," Nuclear Engineering and Design, Vol. 71, pp. 375-381, 1982.

5-52 Lichtenstein, S., B. Fischhoff, and L. D. Phillips, "Calibration of Probabilities: The State of the Art," Decision Making and Change in Human Affairs, J. Jungermann and G. de Zeeuw, editors, D. Reidel Publishing Co., Dordrecht, Holland, 1977.

5-53 Slovic, P., B. Fischhoff, and S. Lichtenstein, "Facts versus Fears: Understanding Perceived Risk," Societal Risk Assessment, R. C. Schwing and W. A. Albers, Jr., editors, Plenum Press, 1980.

5-54 OGP Risk Assessment Data Directory, Report No. 434, March 2010. (434.PDF)

5-55 OGP Risk Assessment Data Directory, Report No. 434-3 March 2010. (434-03.PDF)

5-56 RH_Tank1_UnverifiedHistory.pdf

5-57 RH_Tank 2_UnverifiedHistory.pdf

5-58 RH_Tank 3_UnverifiedHistory.pdf

5-59 RH_Tank 4_UnverifiedHistory.pdf

5-60 RH_Tank 5_UnverifiedHistory.pdf

5-61 RH_Tank 6_UnverifiedHistory.pdf

5-62 RH_Tank 7_UnverifiedHistory.pdf

5-63 RH_Tank 8_UnverifiedHistory.pdf

5-64 RH_Tank 9_UnverifiedHistory.pdf

5-65 RH_Tank 10_UnverifiedHistory.pdf

5-66 RH_Tank 11_UnverifiedHistory.pdf

5-67 RH_Tank 12_UnverifiedHistory.pdf

5-68 RH_Tank 13_UnverifiedHistory.pdf

5-69 RH_Tank 14_UnverifiedHistory.pdf

5-70 RH_Tank 15_UnverifiedHistory.pdf

5-71 RH_Tank 16_UnverifiedHistory.pdf

5-72 RH_Tank 17_UnverifiedHistory.pdf

5-73 RH_Tank 18_UnverifiedHistory.pdf

5-74 RH_Tank 19_UnverifiedHistory.pdf

5-75 RH_Tank 20_UnverifiedHistory.pdf

5-76 Whitacre 2014a.pdf

5-77 Whitacre 2014b.pdf

5-78 Whitacre 2014c.pdf

5-79 Whitacre 2014d.pdf

5-80 Whitacre 2014e.pdf

5-81 Whitacre 2014f.pdf

5-82 Whitacre 2014g.pdf

5-83 Whitacre 2014h.pdf

5-84 Whitacre 2014i.pdf

5-85 Audit Report – Department of the Navy Red Hill and Upper Tank Farm Fuel Storage Facilities N2010-0049, August 16, 2010.
(N2010-0049 Final Audit Report-16aug2010.pdf)

5-86 Board of Water Supply Comments on the Proposed Administrative Order on Consent (AOC) and Attachment A, Statement of Work (SOW) on the Red Hill Bulk Fuel Storage Facility, July 20, 2015.
(EPA-R09-UST-2015-0441-0559 (1).pdf)

5-87 Unverified Histories: Releases Vs Tell-tales AND Verified Reporting: Since 1988 (RH_CompUnverLeakHistories_DEC17-NAVFACcomments.xlsx)

5-88 AFHE Pearl Harbor Tank 0105 Findings, February 6, 2014. (Pearl Harbor Tank 0105 AFHE Findings_02_6_2014=chronology.pdf)

5-89 Administrative Order on Consent Statement of Work Section 2.4 TIRM Procedures Decision Document and Implementation, Red Hill Bulk Fuel Storage Facility, Joint Base Pearl Harbor-Hickam, Oahu, Hawaii, April 24, 2017.
(RH_AOC_Section2_TIRMDecisionDocument_24APR17-RHBFST5.pdf)

5-90 Final API 653 Inspection Report, PRL 03-12: Internal Inspection of Tank 6, Red Hill, FISC Pearl Harbor, Hawaii, January 2007.
(Final API 653 Inspection Report-Tk 6_2007.pdf)

5-91 RedHill_ Tank07InspectionReport_1998.pdf

5-92 RedHill_ Tank08InspectionReport_1998.pdf

5-93 RedHill_ Tank10InspectionReport_1998.pdf

5-94 Consolidated Construction Projects for FISC, Pearl Harbor, Hawaii, Clean and Repair Tanks 1 and 15, 6 and 16, Weld Repair As Built Record, June 2005.
(Tank 15 Repair As Built Jun05.pdf)

5-95 Final API-653 Inspection Report, PRL 99-21: Clean, Inspect, and Repair Tank 15, Red Hill, FISC Pearl Harbor, Hawaii, January 2007. (API-653 Inspection Report-Tk15_2007.pdf)

5-96 Final API 653 Inspection Report, PRL 02-11: Clean, Inspect, and Repair Tank 16, Red Hill, FISC Pearl Harbor, Hawaii, January 2007. (Tank 16 API 653 Final Inspection Report_2007.pdf)

5-97 Repair Tank, Red Hill, FISC Pearl Harbor, Hawaii, DESC Project PRL 98-9, August 1998. (Tank 19 Rpr.pdf)

5-98 Modified API-653 Out-of-Service, Tank 20, Red Hill, December 5, 2008.
(RedHill_API653Report_ Tank 20_05DEC08.pdf)

5-99 RHBFST 20, Engineering Review and Suitability, for Service Evaluation, API 653 Out-of-Service Tank Inspection by Others, January 2009. (SUMMARY Tank 20 Engineering Review - Final Report 01-27-09.pdf)

5-100 RHBFST 2 Repair Certification Report Clean, Inspect, and Repair Red Hill Storage Tank s Fleet and Industrial Supply Center Pearl Harbor, Revision 2, July 2010. (DO 31 Final, Rv2 Tank 2 Repair Certification Rpt.pdf)

5-101 Michael Baker Jr., Inc., "Final 2015 Biennial Leak Detection Testing Report of 14 Bulk Field-Constructed Underground Storage Tanks at Red Hill Underground Fuel Storage Facility," prepared for Defense Logistics Agency Energy, Ft. Belvoir, Virginia, June 12, 2015.

5-102 ESTCP Final Report, "Validation of the Low-Range Differential Pressure (LRDP) Leak Detection System for Small Leaks in Bulk Fuel Tanks," Prepared by Environmental Security Technology Certification Program, U. S. Department of Defense. (EPA-R09-UST-2015-0441-0344-LRDP-24.pdf)

5-103 Center for Chemical Process Safety of the American Institute of Chemical Engineers, "Guidelines for Process Equipment Reliability Data with Data Tables," New York, New York, 1989.

5-104 Blanton, C. H., and S. A. Eide, "Savannah River Site Generic Data Base Development (U)," Westinghouse Savannah River Company, WSRC-TR-93-262, June 30, 1993.

5-105 Pickard, Lowe & Garrick, Inc., "Database for Probabilistic Risk Assessment for Light Water Nuclear Power Plants," proprietary, PLG-0500.

5-106 Lees, F. P., and M. S. Mannan, Lees' Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control, Fourth Edition, Volumes 1–3, August 2012.

# 6. Event Sequence Analysis

## 6.1 Introduction

The event sequence analysis is often referred to as the "heart" of a QRVA. In the event sequence analysis, the initiating events and chains of potential conditional response events are defined to characterize the event sequences or scenarios of the QRVA. In general terms, an event sequence diagram (ESD) is developed to characterize general classes of event scenarios for each initiating event based on the anticipated response of the target facility to the initiating event. These responses generally include a combination of system (or hardware) based responses along with human responses; e.g., facility operator actions taken in response to the initiating event and associated system responses. The ESDs are then applied to develop more detailed event trees to characterize detailed logical scenarios suitable for event sequence quantification.

The hazard of interest for this project is fuel contained in the Red Hill Facility. The concern is that the fuel received, stored, and issued from Red Hill could be accidentally released from the RHBFSTs, or from its connecting fuel lines, and make its way to the aquifer below the facility used for the city and Pearl Harbor drinking water. The sequence models developed in this project consider the accidental release of fuel from the RHBFSTs and from the fuel lines under the different conditions of operation at Red Hill. The accidental release of fuel from areas often connected to, but located downgrade from the Harbor Tunnel, upper and Lower Access Tunnels or the RHBFSTs are not of interest because any potential fuel release from other areas is not at risk to the aquifer; e.g., releases from the UGPH or from the ship piers at Pearl Harbor, though these other areas do pose a potential source of fuel release to Pearl Harbor itself.

This section describes the accident sequence models for internal initiating events. These same models will form the basis for the accident sequence models for other hazard group; e.g., seismic events, floods, and fires.

## 6.2 Bases and Assumptions

The bases and assumptions for the development of the event sequence analysis are summarized below.

1. There are 18 RHBFSTs assumed operational, and RHBFSTs 1 and 19 are permanently out of service.

2. The smaller range of fuel leaks directly to rock is represented by a leak rate of 1.5 gpm. The large range of leak rates is assumed represented by an equivalent hole size of 0.5" in diameter.

3. For overfilling events, the challenge rate is once per year per RHBFST; i.e., the frequency of fuel receipts in which the RHBFST fuel level is being raised to a maximum level consistent with the annual leak tightness tests.

4. For overfilling events, the final stages of the filling process are assumed to take place using the cargo pumps to add fuel from source tanks down below the UGPH.

5. For overfilling events, if a hole above the maximum operating level occurs, it is assumed to be equivalent to a 0.5" hole and located at 212'.

6. For overfilling events, the level settings for RHBFST 15 are assumed representative of other RHBFSTs.

7. It is assumed that to end an overfilling, the RHBFST skin or ball valve must close; i.e., credit for ending it by tripping the cargo pumps is neglected.

8. Based on the initial amount of fuel purchased for filling, the maximum amount a RHBFST can be overfilled is 22,500 barrels; i.e., up to a fuel level of 230.2'.

9. Once a drop in RHBFST level is detected by AFHE indicating a need to empty the RHBFST, the average time to confirm the leak and plan the response, up until fuel is started to be moved, is a minimum of 6 hours. Delays of up to 2 weeks beyond this initiation time are also considered depending on the sequence conditions.

10. For overfilling events, the fill rate is assumed to be at 2,080 barrels per hour.

11. There are no loads of importance supplied by power from Panel 2 at Red Hill.

12. If power supplying the 480V normal bus at ADIT 1 is lost, operating cargo pumps are assumed to trip off.

13. The generator on the hill above ADIT 1 supplies backup power to the UGPH MOVs.

14. The ADIT 1 supply and exhaust fans are assumed required for extended operation of the cargo pumps.

15. At least one supply and exhaust fan is needed to provide room cooling for the normal and emergency buses at Red Hill as displayed in Table 6-7.

16. The LAT supply and exhaust fans at Elevator 72 are supplied by the Red Hill 480V bus via Panel L.

17. Upper access tunnel lighting, radios and cameras are supplied by Panel LA.

18. Red Hill instruments and indications require successful operation of the AFHE system.

19. The train charger is assumed not needed for response to any leakage event.

20. Loss of either pair of supply fans or exhaust fans at Red Hill is assumed to require personnel evacuation.

21. Once Red Hill staff detects the presence of substantial fuel vapor in the LAT, they would evacuate all the tunnels.

22. It is assumed that once initiated, fuel can be moved from a leaking RHBFST at an effective constant rate of 2,500 barrels per hour until fuel level reaches 7.5'.

23. Below 7.5', the fuel movement rate, if needed, is reduced to represent draining of the last 7.5' of fuel.

24. If there is initially insufficient ullage in which to move fuel to, a delay of 2 weeks is assumed required to provide the needed ullage. Leakages occurring during a RHBFST return to service, however, are assumed to always have sufficient ullage available, as are overfilling events which require much less ullage to uncover the hole.

25. During a liner leak to rock, for the RHBFSTs containing F76, it is assumed that there is insufficient ullage to empty either RHBFST; i.e., a 2-week delay is assumed before initiating any fuel movement.

26. For nozzle leaks, and for other fuel line tunnel leaks, two representative hole sizes are assumed; i.e., 0.5" and 6" in equivalent diameters.

27. For nozzle leaks, the holes are below the bottom of the RHBFST. The added head of fuel is accounted for in the computation of fuel releases by slightly increasing the hole size to account for the additional head.

28. For nozzle leaks, changes in fuel line pressure are not credited for detection of the leak.

29. For a fuel line leak to the LAT requiring evacuation, it is assumed that the act of evacuation alone would be sufficient for the control room staff to contact management for instructions; i.e., not requiring a manual gauge to confirm that a RHBFST leak has occurred.

30. If there is a nozzle leak during a fuel movement and the skin and ball valve of the affected RHBFST cannot be closed, no credit is taken for emptying the affected RHBFST. Also, no credit is assumed when the nozzle leak is the larger, 6", hole size.

31. For a 0.5" nozzle leak, a minimum added delay time of 24 hours is assumed before initiation of fuel movement from the affected RHBFST to account for the time delay caused by evacuation, even though remote manipulation of the valves needed to affect the transfer is also possible.

32. For postulated fuel line leaks within the tunnels, the assumed leak location is at the mid-point of the modeled fuel line sections; i.e., one location per section. The postulated Section E fuel line leaks are assumed to occur below the Zone 7 bulkhead rather than above it. Nozzle leaks associated with RHBFSTs 17, 18, or 20 are still modeled to release fuel above the Zone 7 bulkhead.

33. For postulated fuel line leaks within the tunnels, the maximum time assumed for detection is half the 8-hour shift inspection period, or 4 hours. The sump pumps may instead start much sooner than this maximum, and this cue for detection is credited.

34. Estimates of the time for fuel released from a fuel line in a tunnel to reach the downhill sump are reached assuming the tunnel widths are 12' for Sections A, B, and C, and 24' for Sections D and E. The tunnel slope is averaged over each fuel line section.

35. Leakage rates through each postulated hole are evaluated assuming orifice flow with a conservative discharge coefficient of 1.0.

36. For fuel line leaks occurring at the time of an inter-RHBFST fuel transfer, but in which both cannot be isolated (i.e., a very low frequency sequence), the full contents of the second RHBFST are assumed released even if fuel is removed from the first RHBFST.

37. For fuel line leaks in which a fuel movement is in progress, the initial leakage rate is evaluated assuming that the affected RHBFST is always initially at 212'.

38. Leakage rates are assumed constant at the initially evaluated leakage flow rate until emptied or isolated, whereas leakage rates for liner leaks to rock are evaluated as a function of time and the available head of fuel above the leak location.

## 6.3 QRVA Event Sequence Analysis General Methodology

Once accident-initiating events have been identified and grouped, it is necessary to determine the response of the facility to each group. Two distinct methods for evaluating facility response are described here. One uses a function event tree as an intermediate analytical step for sorting out the complex relationships between accident initiators and system responses. The other method employs a detailed event-sequence analysis to explicitly define the response of key facility systems.

Detailed information on facility functions, systems, and operational schemes is required to identify expected responses and define criteria for successfully meeting the identified challenges. The facility-response evaluation determines how realistic or conservative the study will be. If information from the safety analysis report is used, its conservative bias must be taken into account. It is important to apply the most realistic information available in terms of the pressure, temperature, flow rates, and timing characteristics associated with systems designed to respond to accident-initiating events. Such information can be derived from analyses of transients by the facility or vendor-supplied calculations that can be justified and referenced.

### 6.3.1 Event Sequence Diagram Development

Event sequence analysis is another method used to identify the complex relationships between accident-initiating events and detailed system responses. Event sequence diagrams are developed for each group of initiating events. The ESD is an analytical tool intended to facilitate the collection and display of information required for developing system event trees. Its objective is to illustrate all possible success paths from a particular accident-initiating event to a stable safe condition.

The ESDs tend to include a significant amount of design and operational information relative to the potential success paths. Their construction is an iterative process with

input from various QRVA team members, particularly those who have transient analysis, operational, and simulator experience.

One useful aspect of the ESD is its capability to document the assumptions used in an event-tree analysis. The ESD can be very detailed, explicitly showing all the sequence options considered by the analyst. When simplifying assumptions are made in the event trees to facilitate quantification and to render the logic more tractable, the ESD can be used to demonstrate why such assumptions are believed to be bounding (conservative) or probabilistically justified.

In accomplishing a safety function, the effectiveness of a particular success path noted on an ESD depends in general on what systems are operable in the facility and on whether or not the process variables are within the design range of the particular system or subsystem. The method of accomplishing a safety function depends on the state of the facility at the time of an event, as affected by the event, the operator, and system actions.

Figure 6-1 shows a portion of one type of ESD. Each block represents a system performing a mitigating action, as indicated by the description on the right. Each action is initiated by the signals shown in the circles coming into the block from the left. Manual actuation of the system is indicated by the "M" in the bottom of the action block. Blocks without an "M" indicate automatic actuation. All actions appear in approximate temporal order.

The line that branches off from the heavy line above each block in Figure 6-1 indicates an alternative success path given that the expected mitigating action has failed or has failed to be performed. As many possible alternative success paths as are available are shown to the right of each expected action. After the various alternatives (usually safety and non-safety actions within the normal design bases) are tried and none succeed, then an oval is used to indicate special conditions like "failure to scram" or "excessive cooldown". The systems required to mitigate these special conditions are shown on another page of the ESD, as indicated by the transfer symbol on the oval.

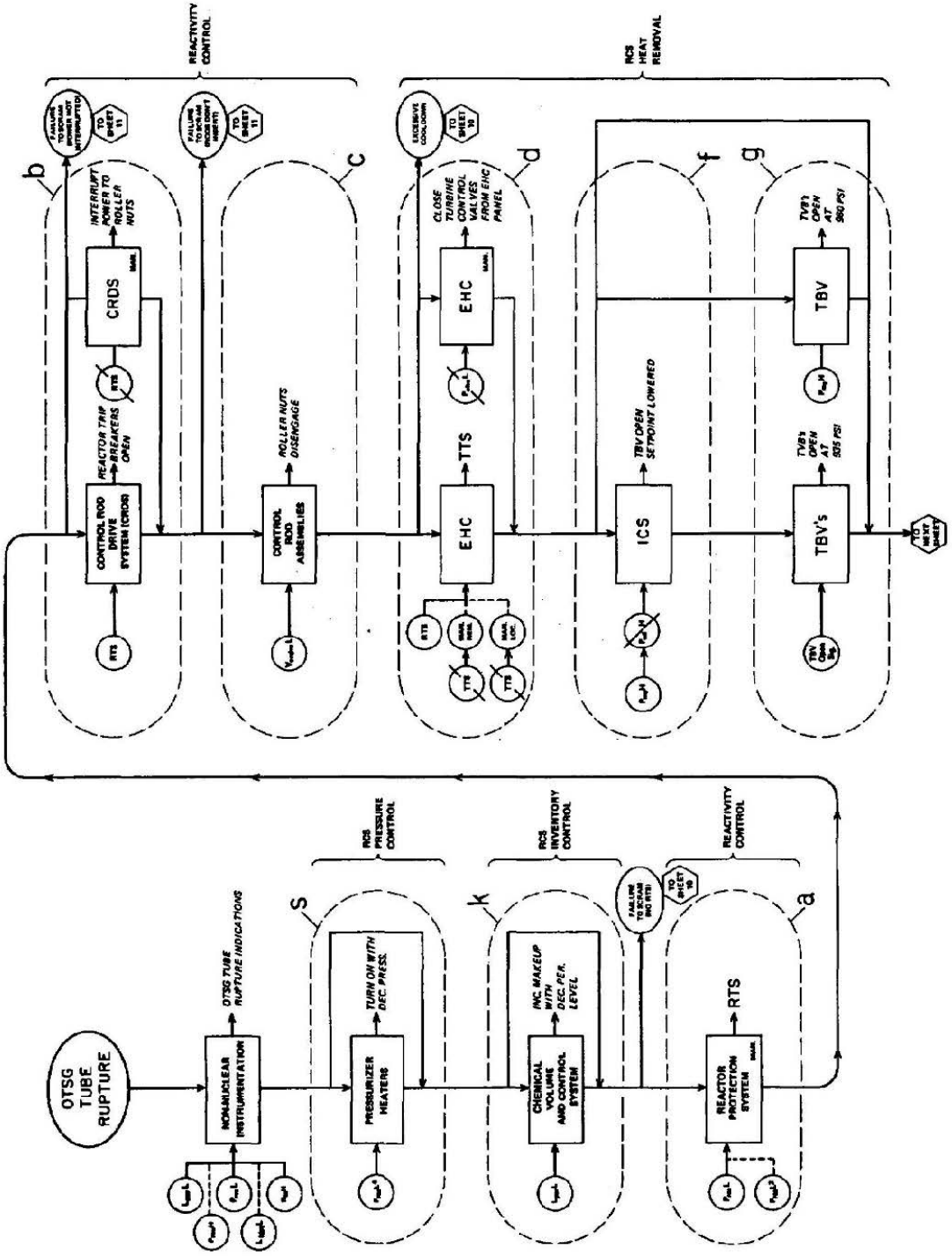



Figure 6-1. Excerpt from an Event-Sequence Diagram

In addition to documenting the agreement on the expected facility response to each initiating event, event-sequence analysis delineates the required operator/system interactions for the human-factors evaluation. The ESDs also help disseminate information to all project participants about how the facility has been assumed to respond to initiating events and helps in coordinating the development of accident sequences by documenting for the systems analyst which systems in the system event trees must be further analyzed.

### 6.3.2 Event Tree Development

The accident sequences associated with each initiating event can be fully delineated on the basis of a clear understanding and evaluation of the facility response to each type of initiating event. This delineation of sequences is accomplished by developing detailed system event trees. As described in this section, system event trees can be developed from either function event trees or event sequence diagrams, but the method used for accident-sequence quantification depends on the approach followed in developing the trees. Event trees developed from function event trees are quantified by the method of fault-tree linking, whereas event trees developed from sequence diagrams are quantified by using the method of event trees with boundary conditions. For the RHBFSF QRVA, the event sequences are quantified applying the method of event trees with boundary conditions.

Figure 6-2 is a symbolic representation of an event tree. Arrayed across the top are the various systems or safety functions. At the left, we enter the tree with the occurrence of an initiating event, and then ask, “Does A work, or not?” The tree branches at this point, with the upper branch representing “A works” and the lower branch representing “A fails”. Some event tree software packages (e.g., RISKMAN) permit multiple branches (i.e., three or more) under a single top event. This example illustrates the simplest case, where each branch is binary. At System B, there is another branching, and so on. Note that some systems of the facility may be bypassed; that is, not questioned, because of events that occurred previously in an event sequence.

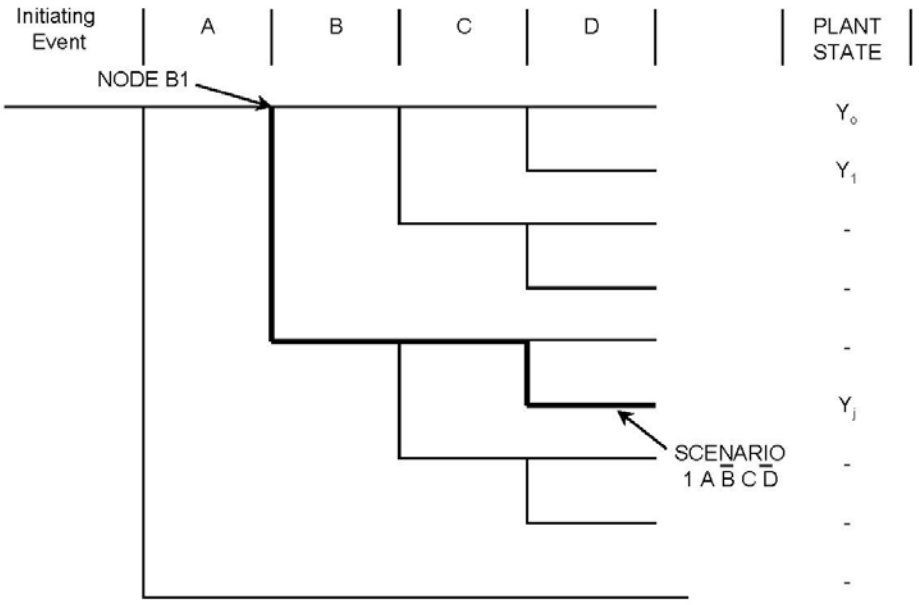



**Figure 6-2. Simplified Facility Event Tree**

In this way, each path through the tree represents a scenario—sequence of events beginning with the specified initiating event and leading to a damage state—represented by the symbol "Y". The various branch points arrayed across the top of the event tree (A, B, C, etc.) are referred to as top events.

A given system may be represented by several different top events. For example, Top Events A, B, and C could represent three different trains of a three-train auxiliary feedwater system. Alternatively, Top Events A and B could represent different functions performed by a single system; e.g., high-pressure injection and high-pressure recirculation cooling.

Each path through an event tree is characterized by the particular entry state or initiating event and by the failed or successful systems along that path. Thus, for example, in the simplified facility event tree shown in Figure 6-2, the scenario

$$S = IA\overline{B}C\overline{D}$$

(represented by the darkened line in the diagram) consists of initiating event or entry state "I", followed by the success of Top Events A and C, and the failure of Top Events B and D.

The frequency of this scenario may be written as

$$f(S) = f(I)f(A:I)f(\overline{B}:I,A)F(C:I,A,\overline{B})F(\overline{D}:I,A,\overline{B},C)$$

where the failure fractions (i.e., $f(\overline{B}:I,A)$ and $F(\overline{D}:I,A,\overline{B},C)$) are called split fractions. For example, $f(\overline{B}:I,A)$ represents the fraction of all sequences at Node B1 that take the lower

(i.e., failure) branch at this point. (The fraction of sequences at that node that result in success is simply equal, of course, to one minus the failure fraction. Thus, there is no need to define separate split fractions for success and failure).

Note that a split fraction can be viewed as a special case (or particular manifestation) of the top event to which it corresponds. Thus, $f(\overline{B}: I, A)$, which is the failure fraction of Top Event B when Top Event A succeeds, may take on a different value from $f(\overline{B}: I, \overline{A})$, the corresponding split fraction conditional on the failure of Top Event A. This might be the case, for example, if Top Event A represents a support system (e.g., electric power or service water) that is needed for the success of Top Event A.

To summarize, the basic building block in the event tree approach to risk analysis is the top event that represents a system, subsystem, or safety function. Each top event, in turn, is characterized by one or more split fractions, which defines the numerical values of the failure probability associated with that top event along different paths in the event tree; i.e., conditional on the success or failure of all previous top events.

Event tree analysis software codes, such as RISKMAN, process the event trees built from systems analyses, and calculate the frequency of sequences contributing to the various damage states.

### 6.3.3 Functional Event Tree Development

The use of function event trees to evaluate facility responses requires the development of an event tree that orders and depicts safety functions according to the mitigating requirements of each group of initiating events. The headings of the function event tree are statements of safety functions that can be translated in terms of the systems performing each function. Success criteria are then defined for each of these systems. This stepwise process provides the information needed for preparing the more detailed system event trees that delineate the system accident sequences.

Function event trees are developed for each group of initiators because each group generates a distinctly different facility response. The function event tree is not an end product, it is an intermediate step that provides a baseline of information and permits a stepwise approach to sorting out the complex relationships between potential initiating events and the response of mitigating features. It is the initial step in structuring facility responses to accident conditions in a temporal format. The top events of function event trees are eventually decomposed into statements of system operation or unavailability that can be quantitatively measured.

In constructing the event tree, the analyst considers the functions required to prevent loss of fuel inventory control, potential consequences, and the relationships between safety functions.

The function event tree serves as a guide for the development of system event trees. The determination of potential facility damage and/or consequences in the system trees must be consistent with the basic results of the function event trees.

Each safety function that is an event-tree heading is performed by a collection of systems. Some systems may perform more than one function or portions of several

functions, depending on facility design. It is necessary to determine which systems are required to successfully perform each safety function to establish the headings of the system event tree.

Some safety functions will be performed by different systems, depending on the accident. Information about the level of detail to which the systems are specified is fed iteratively back into the classification of accidents. For example, the control of fuel inventory may require only a few selected systems.

Definitions of joint operation will assist in eliminating meaningless sequences. Response-time definitions will help determine the order of the headings. The required complement of equipment for each system will reveal when failure in one mode of system operation will not induce a failure in a subsequent mode. This system-success information along with the functional relationships will determine which sequences are to be included in the system event tree.

#### *6.3.3.1 System and Train Level Event Tree Development (including event tree top event definition, ordering, split fraction definition, end state definition, binning, etc.)*

After extensive review by operational and administrative personnel, the actions noted on the ESDs are grouped to define event tree headings. The headings are selected for the following reasons:

1. To show what safety function or system failures will produce each facility damage state.

2. To display important dependences.

3. To group facility systems to facilitate the calculation of accident sequence frequencies.

In deciding how to group the ESD actions into event tree headings, the following guidelines are applied:

1. Use a minimum number of event tree headings consistent with the reasons for choosing the headings as described above.

2. If an event tree heading affects only one other heading, roll them together into a single heading.

3. Have only one failure effect come from each event tree heading.

4. If an event tree heading significantly affects the boundary conditions on two or more other headings, keep it separate.

Usually the event tree headings are single systems or parts of systems, either frontline or supporting, as this allows the effect of the failure of each system to be more clearly defined. Sometimes, in an effort to simplify the tree, the heading may be “too much” or “too little” of a safety function. The reason for including more than one system in a

heading is to minimize the number of event tree branch points from which both branches lead to the same facility damage state. This helps to minimize the number of branches in the event tree. Minimizing the number of branches generally clarifies the message transmitted by the event tree.

Since the ESD has been used to trace out each sequence on a system level before the development of the event tree, the event tree does not have to be used for this purpose. Most of the failures that are important to loss of fuel inventory control have already been identified on the ESD, and the important ones can be summarized on the event tree.

#### *6.3.3.2 Definition of System Success and Failure Criteria*

The definition of functional success in terms of systems will include primarily the engineered safety features of the facility. However, other systems may also provide necessary or backup mitigating actions.

Support systems, such as electric power, do not directly perform the required safety functions. However, they could significantly contribute to the unavailability of a system or group of systems that perform safety functions. Therefore, it is necessary to define the support systems for each frontline system and to include them in the system analysis.

Specific success criteria for each system that performs safety or support functions must be established. In addition to a performance definition (e.g., flow rate, response time, trip limits), these success criteria must be stated in discrete hardware terms, such as the number of required pumps, flow paths, instrument trains, or power buses. This hardware definition will support the fault-tree analysis of systems and the construction of the system event trees. The system-success criteria should also, as appropriate, address the joint operation of systems. For example, for some initiating events at a boiling water reactor (BWR), low-pressure makeup systems can be used only in conjunction with depressurization systems.

Definitions of joint operation will assist in eliminating meaningless sequences. Response-time definitions will help determine the order of the headings. The required complement of equipment for each system will reveal when failure in one mode of system operation will not induce a failure in a subsequent mode. This system-success information along with the functional relationships will determine which sequences are to be included in the system event tree.

Each heading in the system event trees must eventually be quantified. In many cases, detailed system models must be developed to determine the likelihood of system failure. To support the detailed system modeling, each event tree heading that is to be further developed must be translated from the system-success criteria previously developed (Section 3.4.3.1 of NUREG/CR-2300) to a statement defining the criteria for system failure.

The system models for event tree headings require exactly defined failure criteria, which are based on the success criteria defined for each event tree heading. In this context, failure and success criteria are not exact opposites of each other because previous failures in the accident sequence may dictate that either some part of the system is

already unavailable or that different system components must operate. Each system-failure criterion is defined as part of an event tree sequence, consisting of the previous successes or failures of other systems, that leads to the definition of boundary conditions on the system's operation. Sometimes these boundary conditions affect the fault tree top event and thus the fault tree logic. Therefore, different system-failure criteria may have to be identified for each event tree heading under each boundary condition on the system(s) in that heading.

The system-success criteria are based on a calculation of the facility response to postulated conditions.

Data are required to support the adoption of specific success or failure criteria. The best sources of such data are those analyses that have been done under realistic assumptions about system performance and are as close as possible to the accident sequence being considered. For some sequences, generally conservative success criteria are acceptable estimates; for others they can mislead by introducing physically unrealistic assumptions. Such unrealistic assumptions must be treated very carefully so that they do not eventually carry the whole sequence or impact a complete assessment in an unrealistic conservative direction.

Other information may also be used to help define supportable and realistic success and failure criteria. One source of such information is persons who have extensive experience in facility phenomenological analyses or who have operated facilities through numerous accident sequences. Data from this source must be carefully documented in order to ensure that the judgments are supportable. It is important to clearly understand the relationship of the systems denoted in the event tree headings and their support systems. Each frontline system should be reviewed in context with its identified failure criteria to determine the required support elements.

System event trees can generally accommodate the support system in two different ways. One way is to define event tree headings that are more composite in nature and to determine the impact of support-system failures through system modeling. The other way is to define more discrete event tree headings wherein the support systems are broken out and explicitly included in the event tree itself.

#### *6.3.3.3 Dynamic Human Action Addition to Event Trees*

An integral part of developing event trees is identifying and incorporating dynamic human actions into the trees. This is accomplished primarily via the procedures review conducted during the ESD development process. Dynamic human actions are those actions expected to be performed by procedure in response to a potential fuel release scenario. For facility operators, these actions are often identified as "immediate actions" in their emergency response procedures and training. Important dynamic human actions are included as top events in the event trees, as deemed appropriate by event sequence analysts working with human reliability analysts.

#### *6.3.3.4 Event Sequence Recovery Action Addition to Event Trees*

Closely related to the incorporation of dynamic human actions in the event trees is the incorporation of recovery human actions in the trees. Recovery actions are those

actions designed to recover functions that may have been lost during the event scenario. Recovery actions are not immediate actions documented in emergency response procedures, but they may be described elsewhere in these procedures. Recovery actions are generally implemented subsequent to any associated dynamic human actions. They generally occur after the facility has reached some point of stability (as assessed by the operators); after the initiating event has occurred; and after the facility immediate responses, both system automatic responses and dynamic human actions, have been completed.

#### *6.3.3.5 Event Tree Split Fraction Logic Rule Development*

Each branch point in an event tree defines a split fraction that will ultimately be quantified and applied in the quantification of event sequence frequencies.

When the method of event trees with boundary conditions is used, algebraic expressions are (usually) implicitly developed for each facility damage bin (FDB) by a stepwise process. This development process is implicit because, unlike in the fault-tree-linking method, no single Boolean expression at the component level is defined for each bin; it is merely implied. However, after an optional initial screening for dominant sequences, either method can be used to combine distributions in an identical way. The key differences between the methods lie in how the dominant sequences are defined and how the frequency for each facility-damage bin is determined. The main steps in this approach are outlined below, followed by a discussion of means to limit event tree size.

As described in Section 3.7.3.3 of NUREG/CR-2300, the method of event trees with boundary conditions uses more detailed event trees and therefore simpler fault trees than does the fault-tree-linking approach. In particular, the support systems found to be important are included explicitly as top events in the event trees. In this approach, then, "systems" or "top events" are narrowly defined. Thus, important dependences between top events are shown explicitly in the event tree rather than being contained in the fault trees underlying the top events. In this approach, separate fault trees or system models are, in effect, also written for each branch point of the event tree. These fault trees then explicitly recognize the states of the systems or top events upstream on the path leading to that branch point.[††] When such a fault tree is quantified, it yields the split fractions—that is, the frequencies of the events that make up the sequence—for that specific branch point. To be more specific, it yields the split fraction for that top event conditional upon the path through the event tree by which that top event is reached.

The first step is to develop event trees displaying all the significant intersystem dependences between the frontline systems whose performance is pertinent for the initiating event of interest. These result from common support systems and any other dependences (human error, environmental) judged to be important. The event trees include these support-system operability states as well as those of the frontline systems. Section 3.7.3 of NUREG/CR-2300 illustrates the event tree development. Note that the pertinent dependences between support systems are to be identified and displayed in the event tree. In addition, multiple branches (reflecting partial success) rather than just binary (success or fail) branches are used where this more appropriately describes

†† This recognition can also be thought of as boundary conditions on the system fault tree—hence the term "event trees with boundary conditions".

the support-system states and facilitates the quantification of the frontline system. For example, for the electric power heading of the event tree with, say, two buses supplying the safety systems, four branches would be included in the event tree to describe the availability of electric power. These branches would represent "both buses working", "Bus 1 working and Bus 2 failed", "Bus 1 failed and Bus 2 working", and "both buses failed".

When the event trees have been completed, the split fractions in the event trees are determined from logic models for the system or top event under the conditions represented by the particular branch point or node in question. The system logic models are usually in the form of fault trees, but they can be reliability block diagrams, GO models, subevent trees, failure modes and effects analysis models, or any other kind of model, all of these forms, if properly done, being logically equivalent.

Simple fault trees are then written to relate the state of the top event system to the states of its components. From the minimal cut sets of these trees, we can obtain the necessary condition for system failure in terms of sets of component failures. That is, the system does not fail unless at least one cut set of components fails.

The question then devolves upon what could cause the failure of one of these cut sets. The answers to this question are recorded and systematized through the use of a cause table (see Table 6-1 for an abbreviated example). In this table, all possible causes ("candidate" causes) are listed in the left column.

**Table 6-1. Example of Format for a Cause Table for Double Failures (buses available)**

| Cause | Failure Frequency | Effect | | | |
|---|---|---|---|---|---|
| | | Components | System | Other Systems | Initiating Events |
| Coincident Hardware Failures | $4.5 \times 10^{-6}$ | Mainly Pumps | Fails | No Effect | No Effect |
| Testing | $1.0 \times 10^{-10}$ | Pumps | No Effect | No Effect | No Effect |
| Maintenance and Hardware Failure | $2.0 \times 10^{-4}$ | Pumps or MV-8700A, B | Fails | No Effect | No Effect |
| Human Error and Hardware Failure | $8.2 \times 10^{-9}$ | MOV-8809A, B Closed Failure on Other Side | Fails | No Effect | No Effect |
| Other | $4.6 \times 10^{-5}$ | Valves or Pumps | Fails | No Effect | No Effect |
| Total | $3.0 \times 10^{-4}$ | | | | |

*Dominant contributor = maintenance combined with hardware failure.*

Each cause is then evaluated as part of the system analysis. The components that would fail from this cause are listed in Column 3. If those components constitute a cut set, thus failing the system, this is noted in Column 4. If a particular cause does result

in system failure, the frequency of that failure is recorded in Column 2. (More specifically, what is recorded here is the fraction of times in our thought experiment that the system fails at the branch point in question as a result of this particular cause.)

The sum of the entries in Column 2 (i.e., the sum of all frequencies of system-failure causes) is the split fraction for system failure at the branch point in question. The bottom of the cause table can be used to accommodate the contribution from "other" causes; i.e., from all causes not otherwise called out in the table. If such entries are used, the analyst should be careful to list all contributors to "other causes".

If the system should fail as a result of a particular cause, we then ask whether that same cause might also result in some other system failing or in an initiating event. If so, then it is a potential "common" cause and needs to be called out for special treatment in the analysis. Columns 5 and 6 in the cause table are used to call attention to such situations. Because split fractions are simply multiplied together, the identification of dependent failures in the cause table and subsequently in the event tree is critical and should be given a great deal of attention.

Some of the more advanced event tree software packages (e.g., RISKMAN) allow the user to enter the split fraction names and the logic defining the split fractions to be selected for a given sequence based on the status of events occurring earlier in the sequence or on the type of initiating event. This is also where the logic associating split fractions with branch names for top events with multiple branches is entered.

The following notation is used for split fraction logic rules:

| | |
|---|---|
| S | Success |
| F | Failure |
| B | Bypass |
| + | Or |
| * | And |
| - | Not |
| ( ) | Parentheses for Grouping of Expressions; Nesting Is Allowed |
| = | Equality of Top Event Branch State to F, S, B |
| INIT | Initiator |

The operator precedence is: ( ), -, *, +.

Certain rules apply in defining split fraction and binning logic, as follows:

For top events with multiple branches, you must define the split fraction to use with each branch by using the branch name in a logic rule, as shown above.

To use multistate top events in logic rules, specify the branch name, rather than "S" (for success) or "F" (for failure).

As a sequence is analyzed, if there are several rules that might describe the states of previous top events at that point (successful, failed, or bypassed), the split fraction for the first applicable rule in the list will be used.

Specifying the number 1 (i.e., the universal set) as logic for a split fraction defines it as the default value to be used for cases of that top event not covered by previous rules. This is useful because split fraction logic must cover all logical possibilities for each split fraction. If there is a tree sequence for which a split fraction is not defined, an error will be generated when the initiating event is quantified.

Split fraction logic may be dependent on top events in the current tree or in other trees as long as those top events precede that being considered when the trees are linked together for quantification.

Split fractions need not be defined in order as they appear across the tree; however, it is wise to group split fractions together for clarity of organization.

When the split fraction rules are complete, some types of errors will not be detected at this point, but will cause the quantification of the tree to fail. These include split fractions missing from the master frequency file, use of top events not defined in other trees, and cases in which split fraction logic is not defined for a sequence.

#### *6.3.3.6 Event Tree Binning Rule Development*

The consequences of accident sequences are then evaluated by the process described in Chapter 7 of NUREG/CR-2300. This process may or may not group the accident sequences into facility-damage bins. However, because of the similarities among certain accident sequences and the amount of work involved in their analysis, the accident sequences are usually so grouped. For our purposes, a FDB can contain one accident sequence (in which case the FDB and the accident sequence are synonymous) or many accident sequences if the results of the containment analysis so specify. Basically, the binning process provides some ability to combine and reduce the total number of sequences in quantification, but binning is not a requirement for quantification.

The accident sequences provided for analysis are the output of the system event trees. To reduce the number of sequences that must be analyzed, these sequences can be grouped into facility-damage states or bins. Alternatively, the selection of accident sequences for analysis can be based on their likelihoods. In the binning process, sequences are grouped according to accident characteristics that affect the response of the containment and the release of fuel into the environment. The development of bins and the development of the containment event tree are therefore very closely related. The representative sequences are then analyzed with computer codes, and the results (accident timing, flows, pressures, and rate of release from facility containment) are supplied to the fate and transport task. Conditions associated with the fuel release from facility containment are also provided to the fate and transport consequence analysts. Sensitivity studies are performed as required to quantify event tree branching

probabilities and to estimate the contribution of uncertainties in physical processes to the uncertainties in the total risk.

## 6.4 Initiating Events

The event sequence internal event, initiating events that are applicable to Red Hill and the connecting fuel lines within the Lower Access Tunnel and the Harbor Tunnel can be grouped into four categories. These broad initiating event categories are:

- Leaks Directly from a RHBFST through Its Liner below the Current Fuel Level and Eventually to the Surrounding Rock
- Leaks to Rock above the Nominal Fuel Level due to Overfilling a RHBFST
- Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST
- Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel which May Be Isolable

Chronic or undetected leaks, which may persist and release fuel over an extended period are considered separately. The chronic, rather than acute, nature of such releases are treated by methods other than those described here in Section 6.

The full list of initiating events considered for internal events is presented in Table 6-2. The list of initiating events is long because a separate initiating event is used for each operational RHBFST when it only affects the one RHBFST. There are 18 RHBFSTs assumed operational, and RHBFSTs 1 and 19 are permanently out of service.

## Table 6-2. List of Initiating Events Included in Model by Major Category

| IE Name | Initiator Description |
|---|---|
| 1. *Leaks Directly from a RHBFST through Its Liner and Eventually to the Surrounding Rock* | |
| LTK02 | 1.5gpm leak F24 to rock per calendar year for RHBFST 2 |
| LTK03 | 1.5gpm leak F24 to rock per calendar year for RHBFST 3 |
| LTK04 | 1.5gpm leak F24 to rock per calendar year for RHBFST 4 |
| LTK05 | 1.5gpm leak F24 to rock per calendar year for RHBFST 5 |
| LTK06 | 1.5gpm leak F24 to rock per calendar year for RHBFST 6 |
| LTK07 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 7 |
| LTK08 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 8 |
| LTK09 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 9 |
| LTK10 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 10 |
| LTK11 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 11 |
| LTK12 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 12 |
| LTK13 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 13 |
| LTK14 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 14 |
| LTK15 | 1.5gpm leak F76 to rock per calendar year for RHBFST 15 |
| LTK16 | 1.5gpm leak F76 to rock per calendar year for RHBFST 16 |
| LTK17 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 17 |
| LTK18 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 18 |
| LTK20 | 1.5gpm leak JP5 to rock per calendar year for RHBFST 20 |
| MTK02 | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 2 |
| MTK03 | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 3 |
| MTK04 | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 4 |
| MTK05 | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 5 |
| MTK06 | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 6 |
| MTK07 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 7 |
| MTK08 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 8 |
| MTK09 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 9 |
| MTK10 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 10 |
| MTK11 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 11 |
| MTK12 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 12 |

## Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)

| IE Name | Initiator Description |
|---|---|
| MTK13 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 13 |
| MTK14 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 14 |
| MTK15 | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 15 |
| MTK16 | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 16 |
| MTK17 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 17 |
| MTK18 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 18 |
| MTK20 | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 20 |
| LRTS02 | 1.5gpm leak to rock per year during a Return to Service TK 2 |
| LRTS03 | 1.5gpm leak to rock per year during a Return to Service TK 3 |
| LRTS04 | 1.5gpm leak to rock per year during a Return to Service TK 4 |
| LRTS05 | 1.5gpm leak to rock per year during a Return to Service TK 5 |
| LRTS06 | 1.5gpm leak to rock per year during a Return to Service TK 6 |
| LRTS07 | 1.5gpm leak to rock per year during a Return to Service TK 7 |
| LRTS08 | 1.5gpm leak to rock per year during a Return to Service TK 8 |
| LRTS09 | 1.5gpm leak to rock per year during a Return to Service TK 9 |
| LRTS10 | 1.5gpm leak to rock per year during a Return to Service TK 10 |
| LRTS11 | 1.5gpm leak to rock per year during a Return to Service TK 11 |
| LRTS12 | 1.5gpm leak to rock per year during a Return to Service TK 12 |
| LRTS13 | 1.5gpm leak to rock per year during a Return to Service TK 13 |
| LRTS14 | 1.5gpm leak to rock per year during a Return to Service TK 14 |
| LRTS15 | 1.5gpm leak to rock per year during a Return to Service TK 15 |
| LRTS16 | 1.5gpm leak to rock per year during a Return to Service TK 16 |
| LRTS17 | 1.5gpm leak to rock per year during a Return to Service TK 17 |
| LRTS18 | 1.5gpm leak to rock per year during a Return to Service TK 18 |
| LRTS20 | 1.5gpm leak to rock per year during a Return to Service TK 20 |
| MRTS02 | MEDIUM leak to rock per year during a Return to Service TK 2 |
| MRTS03 | MEDIUM leak to rock per year during a Return to Service TK 3 |
| MRTS04 | MEDIUM leak to rock per year during a Return to Service TK 4 |
| MRTS05 | MEDIUM leak to rock per year during a Return to Service TK 5 |
| MRTS06 | MEDIUM leak to rock per year during a Return to Service TK 6 |
| MRTS07 | MEDIUM leak to rock per year during a Return to Service TK 7 |

## Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)

| IE Name | Initiator Description |
|---|---|
| MRTS08 | MEDIUM leak to rock per year during a Return to Service TK 8 |
| MRTS09 | MEDIUM leak to rock per year during a Return to Service TK 9 |
| MRTS10 | MEDIUM leak to rock per year during a Return to Service TK 10 |
| MRTS11 | MEDIUM leak to rock per year during a Return to Service TK 11 |
| MRTS12 | MEDIUM leak to rock per year during a Return to Service TK 12 |
| MRTS13 | MEDIUM leak to rock per year during a Return to Service TK 13 |
| MRTS14 | MEDIUM leak to rock per year during a Return to Service TK 14 |
| MRTS15 | MEDIUM leak to rock per year during a Return to Service TK 15 |
| MRTS16 | MEDIUM leak to rock per year during a Return to Service TK 16 |
| MRTS17 | MEDIUM leak to rock per year during a Return to Service TK 17 |
| MRTS18 | MEDIUM leak to rock per year during a Return to Service TK 18 |
| MRTS20 | MEDIUM leak to rock per year during a Return to Service TK 20 |
| LDTK02 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 2 |
| LDTK03 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 3 |
| LDTK04 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 4 |
| LDTK05 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 5 |
| LDTK06 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 6 |
| LDTK07 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 7 |
| LDTK08 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 8 |
| LDTK09 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 9 |
| LDTK10 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 10 |
| LDTK11 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 11 |
| LDTK12 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 12 |
| LDTK13 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 13 |
| LDTK14 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 14 |
| LDTK15 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 15 |
| LDTK16 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 16 |
| LDTK17 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 17 |
| LDTK18 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 18 |
| LDTK20 | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 20 |

**Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)**

| IE Name | Initiator Description |
|---|---|
| 2. *Leaks to Rock above the Nominal Fuel Level due to Overfilling a RHBFST* | |
| OVFL02 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK02 |
| OVFL03 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK03 |
| OVFL04 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK04 |
| OVFL05 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK05 |
| OVFL06 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK06 |
| OVFL07 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK07 |
| OVFL08 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK07 |
| OVFL09 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK09 |
| OVFL10 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK10 |
| OVFL11 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK11 |
| OVFL12 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK12 |
| OVFL13 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK12 |
| OVFL14 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK14 |
| OVFL15 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK15 |
| OVFL16 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK16 |
| OVFL17 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK17 |
| OVFL18 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK18 |
| OVFL20 | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK20 |
| 3. *Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST* | |
| NSTK02 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 2 |
| NSTK03 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 3 |
| NSTK04 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 4 |
| NSTK05 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 5 |
| NSTK06 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 6 |
| NSTK07 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 7 |
| NSTK08 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 8 |

## Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)

| IE Name | Initiator Description |
|---|---|
| NSTK09 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 9 |
| NSTK10 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 10 |
| NSTK11 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 11 |
| NSTK12 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 12 |
| NSTK13 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 13 |
| NSTK14 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 14 |
| NSTK15 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 15 |
| NSTK16 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 16 |
| NSTK17 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 17 |
| NSTK18 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 18 |
| NSTK20 | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 20 |
| NLTK02 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 2 |
| NLTK03 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 3 |
| NLTK04 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 4 |
| NLTK05 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 5 |
| NLTK06 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 6 |
| NLTK07 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 7 |
| NLTK08 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 8 |
| NLTK09 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 9 |
| NLTK10 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 10 |
| NLTK11 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 11 |
| NLTK12 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 12 |

## Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)

| IE Name | Initiator Description |
|---|---|
| NLTK13 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 13 |
| NLTK14 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 14 |
| NLTK15 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 15 |
| NLTK16 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 16 |
| NLTK17 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 17 |
| NLTK18 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 18 |
| NLTK20 | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 20 |
| SF24IS | Maintenance error creates full diameter hole at Skin Valve 102E in F24 line while all F24 RHBFSTs are Idle |
| SF24MS | Maintenance error creates full diameter hole at Skin Valve 102E in F24 line while there is a fuel movement in line |
| SF76IS | Maintenance error creates full diameter hole at Skin Valve 115E in F76 line while all F76 RHBFSTs are Idle |
| SF76MS | Maintenance error creates full diameter hole at Skin Valve 115E in F76 line while there is a fuel movement in line |
| SJP5IS | Maintenance error creates full diameter hole at Skin Valve 108E in JP5 line while all JP5 RHBFSTs are Idle |
| SJP5MS | Maintenance error creates full diameter hole at Skin Valve 108E in JP5 line while there is a fuel movement in line |
| 4. *Other Leaks from the LAT Fuel Line Piping to the LAT which May Be Isolable* | |
| SF24AL | Blue F24 16" line, from Sectional Valve 160 at ADIT 2Y down to Sectional Valve 159 at PH59, Large leak, pipe rupture |
| SF24AS | Blue F24 16" line, from Sectional Valve 160 at ADIT 2Y down to Sectional Valve 159 at PH59, Small leak, 0.5" φ |
| SF24BL | Blue F24 16" line, from normally closed Sectional Valve 161 at ADIT 3Y down to Sectional Valve 160 at ADIT 2Y, Large leak, pipe rupture |
| SF24BS | Blue F24 16" line, from normally closed Sectional Valve 161 at ADIT 3Y down to Sectional Valve 160 at ADIT 2Y, Small leak, 0.5" φ |
| SF24CL | Blue F24 16" line, from Sectional Valve 162 below Tanks 1&2 to normally closed Sectional Valve 161 at ADIT 3Y, Large leak, pipe rupture |

## Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)

| IE Name | Initiator Description |
|---|---|
| SF24CS | Blue F24 16" line, from Sectional Valve 162 below Tanks 1&2 to normally closed Sectional Valve 161 at ADIT 3Y, Small leak, 0.5" φ |
| SF24DL | Blue F24 16" line from line blind above Tanks 15&16 down to Sectional Valve 162 below Tanks 1&2, Large leak, pipe rupture |
| SF24DS | Blue F24 16" line from line blind above Tanks 15&16 down to Sectional Valve 162 below Tanks 1&2, Small leak, 0.5" φ |
| SF76AL | Green F76 32" line from Sectional Valve 152 at ADIT 2Y to Sectional Valve 151 at PH59, Large leak, pipe rupture |
| SF76AS | Green F76 32" line from Sectional Valve 152 at ADIT 2Y to Sectional Valve 151 at PH59, Small leak, 0.5" φ |
| SF76BL | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y, Large leak, pipe rupture |
| SF76BS | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y, Small leak, 0.5" φ |
| SF76CL | Green F76 32" line from Sectional Valve 154 below Tanks 1&2 down to normally closed Sectional Valve 153 at ADIT 3Y, Large leak, pipe rupture |
| SF76CS | Green F76 32" line from Sectional Valve 154 below Tanks 1&2 down to normally closed Sectional Valve 153 at ADIT 3Y, Small leak, 0.5" φ |
| SF76DL | Green F76 32" line from Sectional Valve 164 below Tanks 11&12 down to Sectional Valve 154 below Tanks 1&2, Large leak, pipe rupture |
| SF76DS | Green F76 32" line from Sectional Valve 164 below Tanks 11&12 down to Sectional Valve 154 below Tanks 1&2, Small leak, 0.5" φ |
| SF76EL | Green F76 32" line from blind above Tanks 15&16 down to Sectional Valve 164 below Tanks 11&12, Large leak, pipe rupture |
| SF76ES | Green F76 32" line from blind above Tanks 15&16 down to Sectional Valve 164 below Tanks 11&12, Small leak, 0.5" φ |
| SJP5AL | Gold JP5 18" line from Sectional Valve 156 at ADIT 2Y down to Section Valve 155 at PH59, Large leak, pipe rupture |
| SJP5AS | Gold JP5 18" line from Sectional Valve 156 at ADIT 2Y down to Section Valve 155 at PH59, Small leak, 0.5" φ |
| SJP5BL | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y, Large leak, pipe rupture |
| SJP5BS | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y, Small leak, 0.5" φ |
| SJP5CL | Gold JP5 18" line from Sectional Valve 158 below Tanks 1&2 down to normally closed Sectional Valve 157 at ADIT 3Y, Large leak, pipe rupture |
| SJP5CS | Gold JP5 18" line from Sectional Valve 158 below Tanks 1&2 down to normally closed Sectional Valve 157 at ADIT 3Y, Small leak, 0.5" φ |

**Table 6-2. List of Initiating Events Included in Model by Major Category (Continued)**

| IE Name | Initiator Description |
|---|---|
| SJP5DL | Gold JP5 18" line from Sectional Valve 163 below Tanks 11&12 down to Sectional Valve 158 below Tanks 1&2, Large leak, pipe rupture |
| SJP5DS | Gold JP5 18" line from Sectional Valve 163 below Tanks 11&12 down to Sectional Valve 158 below Tanks 1&2, Small leak, 0.5" φ |
| SJP5EL | Gold JP5 18" line from blind above Tanks 19&20 down to Sectional Valve 163 below Tanks 11&12, Large leak, pipe rupture |
| SJP5ES | Gold JP5 18" line from blind above Tanks 19&20 down to Sectional Valve 163 below Tanks 11&12, Small leak, 0.5" φ |
| SF24I | Maintenance error creates full diameter hole at Ball Valve 102E in F24 line while all F24 RHBFSTs are idle |
| SF24M | Maintenance error creates full diameter hole at Ball Valve 102E in F24 line while there is a fuel movement in line |
| SF76I | Maintenance error creates full diameter hole at Ball Valve 115E in F76 line while all F76 RHBFSTs are idle |
| SF76M | Maintenance error creates full diameter hole at Ball Valve 115E in F76 line while there is a fuel movement in line |
| SJP5I | Maintenance error creates full diameter hole at Ball Valve 108E in JP5 line while all JP5 RHBFSTs are idle |
| SJP5M | Maintenance error creates full diameter hole at Ball Valve 108E in JP5 line while there is a fuel movement in line |

The first major category of initiating events is that for fuel leaks directly to rock. There are five subcategories within this category as described below.

The first subcategory involves smaller size leak rates, represented by a 1.5 gpm flow rate. This range of smaller leak rates is within the detection capability of the fuel level monitoring system AFHE. Assuming the affected RHBFST is filled to 212', and the hole is at the bottom of the tank, this flow rate corresponds to a flow area of .08" in equivalent diameter.

A second subcategory of initiating events involving leaks to rock are those involving flow rates greater than any that have been observed in the history of the Red Hill facility. A medium size hole of 0.5" in equivalent diameter is assigned as representative of this subcategory. It's believed very likely that any liner through holes larger corresponding to a leakage flow rate greater than 1.5 gpm would be detected fairly quickly and before the hole has a chance to grow much larger. However, through holes on the order of 0.5" have been observed during tank inspections, high in the upper dome of more than one RHBFST. These holes are located well above the nominal operating fuel levels. A hole of 0.5" in equivalent diameter is assigned as representative of these larger holes. For the random, internal hazards (i.e., excluding earthquake events) which are the subject of this study, no mechanism has been identified for suddenly creating still larger holes

below the operating fuel level. Therefore, larger sizes were not considered for direct leaks to rock in this study.

A third and fourth subcategory of leaks to rock were defined for times when a RHBFST is being returned to service following a period in which the RHBFST was emptied of fuel, inspected, and major work performed on the RHBFST liner. Historical experience indicates that the probability of detecting a hole in the liner during fuel refilling is much higher than what can be characterized as random with time. The same two equivalent leak sizes as defined above are also defined here for leaks to rock during a RHBFST RTS; i.e., 1.5 gpm, or 0.5" equivalent diameter hole. The 2014 incident involving RHBFST 5, occurred during fuel filling a return to service, and the leakage flow rate averaged less than 1.5 gpm. In the early years of facility operation, a RHBFST being returned to service was first leak tested by filling with water. However, for environmental reasons, this practice is no longer permitted.

A fifth subcategory for leaks to rock involves leakage from the pipes penetrating the lower dome of a RHBFST. These pipes emerge into the LAT from the bottom of lower dome of each RHBFST. This fifth subcategory represents fuel leakages from the pipes, which are imbedded in concrete of the lower dome. It is argued that very small pipe leaks, on the order of 1.5 gpm are effectively represented by those identified in the first subcategory. A larger leak rate equivalent to a 0.5" hole is assigned as representative of larger leaks. Again, larger leaks from pipes have been observed to occur in other applications, but such events are judged very unlikely for Red Hill where the pipes are protected by the concrete they are embedded in. These pipes have many years of service, have walls thicker than the tank liner, are pressure tested during periodic tank inspections, and following any maintenance on these sections of pipe. Holes growing in size from these lines should be detected before they grow to a 0.5" equivalent size.

The second major category of initiating events for internal events are those for fuel leaks resulting from a tank overfilling. These events could also leak directly to rock. The current maximum operating fuel level in the RHBFSTs is roughly 212'. Many RHBFSTs are kept at lower fuel levels, some much lower. The 212' is approximately the fuel level at which RHBFSTs are now tested for leak tightness annually. These 1-week tests allow more accurate measurements of the change in fuel levels under stabilized conditions. Each fuel issue or receipt is carefully planned at Red Hill with operational orders provided to control the fuel movement. The source tank must have adequate inventory to exceed the maximum operating fuel level before there is an increased probability of the fuel level exceeding an existing through hole in the liner. In accordance with the available experience at Red Hill, the possibility of a hole existing further up the RHBFST's upper dome above the maximum operating level is considered. There is only one subcategory applied to this initiating event category. The initiating event is assumed to be the probability of a challenge to raise the fuel level near the maximum operating fuel level, such as would be necessary for each RHBFST, each year in preparation for the annual leak tightness test.

The third category of internal event initiating events involves the leakage from fuel line piping connecting directly to a RHBFST in the LAT. These are the lines where the pipes penetrating the lower dome emerge into the LAT. If a pipe leaks between the RHBFST and its skin valve or leaks from the skin valve itself, it would not be isolable. Both relatively small flow rates corresponding to a 0.5" hole in the pipe or external leakage

from a skin valve, and larger flow rates corresponding to a 6" hole are represented in three subcategories. The third subcategory also involves large leaks that are not isolable caused by a maintenance error involving a skin valve.

The fourth and final category of internal event initiating events involves the leakage from other fuel line piping into the LAT or into the Harbor Tunnel. There are three subcategories considered. The first involves random leakage events at different locations along any of separate fuel lines for the three fuel types handled at Red Hill; i.e., currently F24, F76, and JP5 fuel types. For this category the individual initiating events are by fuel line section rather than by individual RHBFSTs. The initiating events in the first two subcategories are defined by fuel line type, leak flow area, and by fuel section location. The two leak flow areas represented are 0.5" for small, and 6" for large equivalent diameter holes. The fuel line sections are defined specifically for the QRVA. See Figure 6-3. There are five section locations defined. These correspond to the locations between sectional valves, which can be used to isolate different sections at RHBFSF. There is only one set of sectional valves within the tank gallery. The other sets, which define the boundaries of the fuel line sections, are located below the tank gallery.

A third subcategory of initiating events in the fuel line leaks to LAT category involves maintenance errors. This is the one failure cause envisioned for potentially creating a larger than 6" equivalent hole size. Three such initiating events are defined; i.e., one for each fuel line type. Although a very likely event, the potential opening of the wrong fuel line, one which is still filled with fuel, is considered.

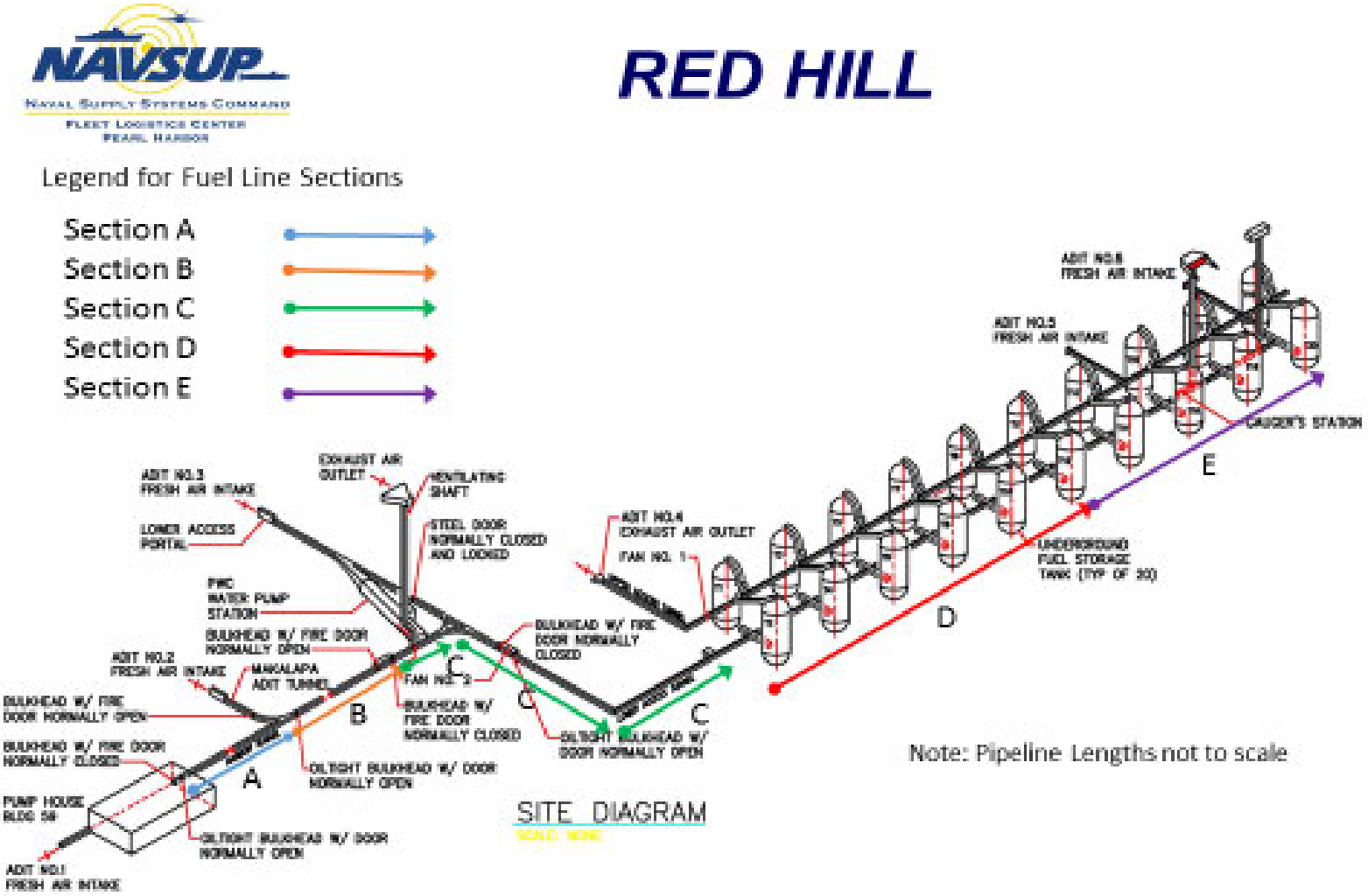



**Figure 6-3. Definition of QRVA Model Fuel Piping Sections**

Table 6-3 below summarizes information about hole sizes chosen as part of the selection of initiating events. Four types of initiating events resulting in leaks are included in the table.

**Table 6-3. Hole Sizes and Flow Rates for Types of Initiating Events**

| Leak Initiating Event Types | Ranges of Initial Hole Flow Rates (gpm) | | | | | |
|---|---|---|---|---|---|---|
| | Chronic | Observed | Postulated 0.5" Hole | | Postulated 6.0" Hole | |
| | | | Low | High | Low | High |
| RHBFST Leaks to Rock | <0.5 gph (~.006") | 1.5 (~.08") | 58 | 72 | NA | NA |
| Leak via Fuel Line to Tunnels with RHBFST Aligned | NA | NA | 73 | 93 | 10,500 | 13,400 |
| Leak via Fuel line to Tunnels without RHBFST Aligned | NA | NA | 10 | 56 | 1,400 | 7,800 |
| Leakage during RHBFST Overfill | NA | NA | 0 | 19 | NA | NA |

The selection of hole sizes and flow rates for the different initiating events is based in part on the available failure rate data. For the RHBFST liner, chronic leakage rates discussed in Section 5.4.6 are very small (i.e., less than 0.5 gph), with equivalent holes sizes of approximately .006" in diameter. For larger, detected and reported leakages through the RHBFST liner, the flow rates are still less than 2 gpm. A flow rate of 1.5 gpm was chosen to represent this type of initiating event. The hole size necessary to discharge 1.5 gpm varies with the hole location and fuel level. A minimum hole size of .08" in equivalent diameter is required when the RHBFST is at 212' and the hole is at the bottom of the tank.

Still larger leakage rates through a RHBFST liner have not been observed, but some larger holes have been identified when tank inspections are performed. Such holes are located above the normal fuel levels. An average of these detected, larger hole sizes (i.e., 0.5"), was chosen to represent the size of holes not yet experienced at RHBFSF. Flow rates through a 0.5" hole also vary by initial fuel level and hole location. With the postulated hole in the bottom of the RHBFST, typical low and high flow rates corresponding to fuel levels at 140' and 212' are listed in the Table 6-3. Much larger holes in the RHBFST liner are not expected from internal events considered in this Phase 1 study.

Generic data sources for external leakage from piping and piping components typically exclude leakage rates less than 1 gpm. That approach is also judged appropriate for the QRVA of the RHBFSF because such leakage rates are handled via the slop system during routine sample line activities. Generic data sources (see Section 5) for failure

rates of component external leakage start with flow ranges at the low end of between 1 and 50 gpm. Such flow rates correspond to about a 0.5" hole for RHBFSF fuel line piping in the tunnels. Table 6-3 shows ranges of flow rates assessed for leakage through 0.5" holes in fuel line piping for two conditions. One condition is for the case when a RHBFST is aligned to the fuel line at the time the leak occurs, and the other condition is for when no RHBFST is aligned so that the added head of the fuel is not applicable. The ranges of flow rates computed for such fuel line external leakage events are presented in Table 6-3. Most of the initial flow rates are greater than 50 gpm. The selection of an equivalent 0.5" diameter hole for RHBFSF may be conservative. The fuel line pressures at the RHBFSF are likely much lower than the generic systems from which the failure rates were derived; i.e., a 50 gpm flow rate in a 1,000 psi pipe would require a much smaller than 05" hole.

Leakages from RHBFST overfilling events, above the normal maximum fuel level of 212', are also postulated to occur through holes equivalent in size to a 0.5" diameter hole. Once the hole is covered with fuel, the release rate would vary as the tank continues filling, reaches its peak, and then is reduced after the filling process ends. Table 6-3 shows that the range of flow rates may vary from 0 to 19 gpm.

Larger holes in fuel line piping and components are certainly possible. However, generic data sources often define the larger ranges of leaks as simply greater than 50 gpm. A hole size of 6" equivalent diameter, is selected to represent the larger range of hole sizes. Such a hole would be consistent with a pipe puncture although no such holes have occurred at RHBFSF. Table 6-3 shows the low and high flow rates as a function of hole location in the fuel lines, and again with or without the liquid head of an aligned RHBFST undergoing a fuel movement. The initial flow rates through a 6" hole are seen to vary from a low of 1,400 gpm to a high of 13,400 gpm.

Table 6-4 shows the time in hours to drain the fuel level from a RHBFST starting from 212' to 50' through a postulated hole at the piping outlet into the LAT (i.e., a loss of about 226,000 barrels), as a function of hole size. These results were obtained using the time-dependent results of the RHBFST workbook model discussed in Section 6.7. For flow rates so far observed at the RHBFSF (i.e., less than 1.8 gpm), the time required is very long, indicating there is lots of time to mitigate the release. For a 0.5" hole, chosen to represent large liner leakage events that have not yet occurred at RHBFSF, the time to drain to 50' is still very long.

For 6" hole sizes, the time required to reach 50' shortens to just 21 hours. The initial flow rate through a 6" hole is more than 14,000 barrels per hour. This is more than double the typical fuel transfer rates typically achieved during fuel movements, indicating that even if a fuel movement was attempted, it would be only marginally successful. For still larger hole sizes, the times required are still shorter. Note that while a 32" diameter has been postulated in previous bounding studies for the RHBFSF, no pipe connecting to a RHBFST is currently larger than 20" in diameter. From the results presented in Table 6-4, it is seen that there is little point in postulating larger than 6" holes for analysis since the response to such events would be largely the same. Maintenance errors could potentially create larger hole sizes than 6". The potential for such errors are included in the study, but are simply evaluated as if they are also 6" holes; i.e., with no credit taken for actions to offload fuel from the affected RHBFST.

**Table 6-4. Time to Drain a RHBFST from 212' to 50' versus Hole Size**

| Hole Diameter | Hours to 50' | Initial Flow Rate in gpm | Initial Flow Rate in Barrels per Hour |
|---|---|---|---|
| .08" | 116,546 | 1.8 | 2.6 |
| .1" | 74,590 | 2.9 | 4.1 |
| 0.5" | 2,983 | 72 | 102 |
| 2" | 187 | 1,144 | 1,634 |
| 4" | 47 | 4,577 | 6,538 |
| 5" | 30 | 7,151 | 10,216 |
| 6" | 21 | 10,297 | 14,710 |
| 8" | 11.7 | 18,306 | 26,152 |
| 10" | 7.5 | 28,604 | 40,862 |
| 12" | 5.2 | 41,189 | 58,842 |
| 20" | 1.9 | 114,414 | 163,449 |
| 32" | 0.7 | 292,901 | 418,430 |

## 6.5 System Dependencies

One of the most important and detailed tasks in developing an integrated model for facility response to the identified initiating events is to explicitly identify the physical and functional interdependencies among the facility systems. A convenient method for displaying the plant interdependencies is through a set of tables that identify all possible system (and subsystem) interactions. Systems which support other systems are called support systems; e.g., electric power systems. Systems which directly perform the needed safety functions for a successful facility response are called frontline systems. Some support systems are often also supported by other support systems. The distinction between support and frontline systems is only for convenience in describing the dependencies. All systems use the same methods for quantifying their reliability and availability.

To develop these dependency tables, support system components are first grouped into common functional elements such as system trains, subsystems, or complete plant systems. This grouping must be done in a manner that the support-to-support and support-to-frontline system dependencies can be readily defined.

The table format provides system support functions listed vertically down the left side of the table. The supported systems are listed across the top. An “X” or a numbered note designator at an intersection in the table identifies a physical or functional dependency. Failure of the support system (or subsystem) affects the ability of the supported system to perform its required functions. Added text, or numbered notes can be used to explain a unique facility response or to clarify situations of partial dependence. An “X” indicates

complete dependence when failure of the support system (or subsystem) completely disables the supported system (or subsystem).

In general, train-wise dependencies are tracked in these dependency tables. This is especially necessary for the construction of event trees that model equipment groups of different trains in separate top events. In addition, the tables provide important information for the development of support system states and the assignment of split fractions in the quantification of event tree models. It is noted that, in most cases, only direct dependencies are included in the dependency tables. Secondary or cascaded dependencies are developed through the logic structure of the event sequence model event trees.

Once the functional dependencies between equipment of the facility are identified, then modeling of these systems can begin. Event tree top events are defined, which are associated with a particular function of the equipment included therein. Rather than identify a separate top event for each piece of equipment, the equipment are grouped by function. The equipment are also examined to see which depend on others and an ordering of the equipment is performed so that equipment in later top events only depend on the status of earlier top events representing equipment that supports them. For some pairs of equipment, there may be circular logic in which each depends on the other. In these cases the equipment represented by a first top event is chosen as initially supported and the circular logic is accounted for by failing both if the equipment represented by the second top event fails.

Table 6-5 illustrates the support-to-support system dependency table involving only the electric power systems located at the underground pump house and at ADIT 1 (ADIT being a horizontal passage leading into a mine for the purposes of access or drainage). The grouping of the table headings is, in some cases, at a more detailed level than the finally defined event tree top events. The event tree top events will be defined in detail later in Section 6.4 and Section 7. The dependencies that are presented in Table 6-5 are used to develop the support systems event tree logic structure and the boundary conditions for each underground pump house and ADIT 1 electric power system top event. The diagonal grey squares simply indicate that the column and row list the same system.

Table 6-6 illustrates the support-to-support system dependency table involving only the electric power systems located at NAVFAC water pump house and ADIT 2 and 3 electrical and mechanical systems. With the exception of sharing power from offsite, these systems are dependent on each other but do not depend on any of the electrical systems at the underground pump house or ADIT 1. The dependencies that are presented in Table 6-6 are used to develop the support systems event tree logic structure and the boundary conditions for each NAVFAC water pump house and ADIT 2 and 3 electrical systems. Only those systems which support the NAVFAC water pump house or other ADIT 2 and 3 electrical and mechanical systems are shown as rows in Table 6-6.

Table 6-7 illustrates the support-to-support system dependency table involving only the electric power systems which support other Red Hill electric power systems. Again, with the exception of sharing power from offsite, these systems are dependent on each other but do not depend on any of the electrical systems at the underground pump house or

ADIT 1, nor the electrical systems at the NAVFAC pump house and ADIT 2. The dependencies that are presented in Table 6-7 are used to develop the support systems event tree logic structure and the boundary conditions for each Red Hill electrical power systems.

Table 6-8 illustrates the support-to-support dependency table involving the electrical systems at the underground pump house and ADIT 1 and the AFHE system with the supporting control room and AFHE systems. The dependencies that are presented in Table 6-8 are used to develop the control room and AFHE frontline system, event tree logic structure and the boundary conditions for these systems.

Table 6-9 illustrates the support-to-frontline dependency table involving the electric power systems at the underground pump house, ADIT 1 systems, and the AFHE supporting systems with the frontline systems located at the underground pump house and lower Harbor Tunnel systems. The dependencies that are presented in Table 6-9 are used to develop the frontline systems at the underground pump house and lower harbor tunnel, event tree logic structure, and the boundary conditions for these systems.

Table 6-10 illustrates the support-to-frontline dependency table involving the Red Hill electric power systems and the AFHE supporting systems with the frontline Red Hill mechanical systems. The dependencies that are presented in Table 6-10 are used to develop the frontline mechanical systems at Red Hill, event tree logic structure, and the boundary conditions for these systems.

Table 6-11 illustrates the support-to-frontline dependency table involving the Red Hill electric power systems and the AFHE supporting systems with the Red Hill electric systems; i.e., lighting, radios, cameras, indications, and signals. The dependencies that are presented in Table 6-11 are used to develop the top events for the electrical systems at Red Hill, event tree logic structure, and the boundary conditions for these systems.

**Table 6-5. Support to Support Dependencies among Electric Power Systems at the Underground Pump House and ADIT 1**

| Supporting Systems | Top Events | Impacts on Other Systems | Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | 100 kw Generator at ADIT 1 Entrance, 8 Hour Fuel | 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | Generator on Hill at ADIT 1 | UGPH Emergency 480V Bus | UGPH Emergency 480V Bus Cooling Fans EF-6a/b/c/d, EF-8/9, SF-5A/B, SF-7 | 480V P100 | 480V P101 | 480V P102 | 480V P103 | 480V P104 | XFMR 480/ 208V, P105 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP causes loss of power to all cargo pumps via the 2.4 kV bus and causes their discharge valves to fail closed, fails the fresh water pumps at the NAVFAC Pump house, challenges all four Standby Generators to start (i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6) and challenge the UPS Backup power for AFHE, UPS for both control rooms, and the UPS for the oil seal door magnets. If the ADIT 3 generator also fails then all power to ADIT 3 and its associated tunnel systems is lost. | | X | Challenge to ADIT 1 Generators | X | | | | | | | | | |
| XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | BUN24 | Loss of the 11.5/2.4 kV transformer loses power to all cargo pumps and causes the discharge flow control valves to go closed | | | | | | | | | | | | | |
| 100 kw Generator at ADIT 1 Tunnel Entrance, 8 Hours Fuel | – | If power from offsite also fails, then the power supply to FORFAC is lost. | | | | | | | | | | | | | |
| 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | BUN48 | Loss of offsite power to the normal 480V bus trips the cargo pumps, causes their discharge valves to fail closed, challenges the two generators at ADIT 1 to start, and challenges the UPS Backup power for the AFHE system and the UPS for both of the control rooms. | | | If Offsite Power Lost, then Challenges ADIT 1 Generators | | | | | | | | | | |
| Generator on Hill at ADIT 1 | GEN1 | If offsite power at ADIT 1 also fails, then fails UGPH normal 480V bus which causes cargo pumps to trip and a loss of power to the UGPH pump discharge valves. | | | | X, if 480V Supply at ADIT 1 from Offsite Power also Fails (1) | | Failed if offsite power lost to ADIT 1 and UGPH | | | | | | | |

**Table 6-5. Support to Support Dependencies among Electric Power Systems at the Underground Pump House and ADIT 1 (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | 100 kw Generator at ADIT 1 Entrance, 8 Hour Fuel | 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | Generator on Hill at ADIT 1 | UGPH Emergency 480V Bus | UGPH Emergency 480V Bus Cooling Fans EF-6a/b/c/d, EF-8/9, SF-5A/B, SF-7 | 480V P100 | 480V P101 | 480V P102 | 480V P103 | 480V P104 | XFMR 480/ 208V, P105 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UGPH Emergency 480V Bus | BUE48 | Causes loss of power to panels P100 to P105, challenges UPS for AFHE and main control room and power for the lower Harbor Tunnel radios, lighting, and cameras; fails CR air cond. and lighting; fails UGPH valves and fans, and fails power to the train charger. | | | | | | | X | X | X | X | X | X | X |
| UGPH Emergency 480V Bus Cooling Fans | BUE48 | After a period of heating will cause failure of power at the UGPH emergency 480V bus. | | | | | | X (after a period of heating) | | X | X | X | X | X | X |
| 480V P100 | BUE48 | Fails UGPH valves. | | | | | | | | | | | | | |
| 480V P101 | BUE48 | Fails UGPH valves and the train's charger. | | | | | | | | | | | | | |
| 480V P102 | BUE48 | Fails control room power and AFHE air conditioning, and fails the fans that cool the 11.5/480V transformer room. | | | | | | X (after a period of heating) | | | | | | | |
| 480V P103 | BUE48 | Fails UGPH valves. | | | | | | | | | | | | | |
| 480V P104 | BUE48 | Fails ADIT 1 fans and outside sump pumps and fails Harbor Tunnel's five sump pumps. | | | | | | | | | | | | | |
| XFMR 480/ 208V, P105 | BUE48 | Fails lights for control room, UGPH, and lower harbor tunnel and challenges UPS for the AFHE and harbor tunnel radios. | | | | | | | | | | | | | |

(1) Assumed Dependency

**Table 6-6. Support to Support Dependencies among the NAVFAC Water Pump House and ADIT 2 and ADIT 3 Systems**

| Supporting Systems | Top Events | Impacts on Other Systems | ADIT 2 Sump Pump | 11.5 kV/480 XFMR at NAVFAC Pump House | Main Pump Panel and Water Main Pumps | 11.5 kV/480 XFMR at NAVFAC Pump House | ADIT 3 Generator for Fresh Water (blue shed), 8-Hour Capacity | NAVFAC Pump House Panels B, 480/208V XFMR, and A | ADIT 3 Lighting and Sump Pumps P1706, P1707 (to settling tank) and Ventilation at Water Pumping Station |
|---|---|---|---|---|---|---|---|---|---|
| Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP causes loss of power to all cargo pumps via the 2.4 kV bus and causes their discharge valves to fail closed, fails the fresh water pumps at the NAVFAC Pump house, challenges all four standby generators to start (i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6) If the ADIT 3 generator also fails then all power to ADIT 3 and its associated tunnel systems is lost. | X (1) | X | X | X | Challenge ADIT 3 Generator | X | X, if ADIT 3 Generator also Fails |
| 11.5 kV/2.4 kV XFMR and Main Pumps Panel (ADIT 3) | B3EA | Fails power to NAVFAC pump house main pumps panel. | | | X | | | | |
| 11.5 kV/480 XFMR at NAVFAC Pump House | B3EA | Challenges ADIT 3 generator to start, if also failed power is lost to Panels B and A at NAVFAC pump house. | X, if ADIT 3 Generator Fails (1) | | | | Challenges ADIT 3 Generator | Challenges ADIT 3 Generator | X, if ADIT 3 Generator Fails |
| ADIT 3 NAVFAC Diesel Generator for Fresh Water | GEN3 | If offsite power is also lost, fails ADIT 3 lighting and Sump Pumps P1706, P1707, and ventilation fans at water pumping station. | | | | | | X, if Offsite Power also Lost via 480V Bus | X, if Offsite Power also lost |
| NAVFAC Pump House Panels B, 480/208V XFMR, and A | B3EA | Fails ADIT 3 lighting and Sump Pumps P1706, P1707, and ventilation fans at water pumping station. | X (1) | | | | | | X |

*(1) Assumed dependency but the ADIT 2 sump pump is not credited in the QRVA.*

## Table 6-7. Support to Support Dependencies among the Supporting Electric Power Systems and Other Electric Power Systems at Red Hill

| Supporting Systems | Top Events | Impacts on Other Systems | 11.5 kV/ 480V XFMR T10 and RH Normal Panel (LAT electrical room) | RH ADIT 5 Generator (480V, own battery) Outside, 11 Hours Fuel at Full Capacity | 480V RH Emergency Bus | LAT Supply Fans SF-1A and 1B via Elev. 72 Air Intake, and Exhaust Fans | Circuit 6 XFMR 480V/ 120V T13 | Circuit 8 – to 480V Panel P1 in Elev. 72 Upper Access Room | XFMR T14 480/208V/ 120V, 208/120V Panel P2, | Circuit 10 480V/ 208V/ 120V XFMR 15 | Circuit 1 XFMR 11 480V/ 208V/ 120V | Next to Gauger Station 208/120V Panel L | ADIT 5 Gen Bldg. 208/120V Panel G | Circuit 7 480V Panel PA | 480V Panels PP1–PP8 | Upper Harbor Tunnel Panels LP13, LP14, LP15; Lighting/ Cameras/ Radios | LAT Lighting Panels LP16-1, 16-2, 17-1, 17-2, and LP18 | UAT 208V/ 120V Lighting Panels LP19, 20, 21, 22, 23 | ADIT 6 Tunnel, 208/ 120V Panel LB | Upper Tunnel 5Y, 208/ 120V Panel LC | Gauger Station 208/ 120V Panel A | LAT 208/ 120V Panel LA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP causes loss of power to all cargo pumps via the 2.4 kV bus and causes their discharge valves to fail closed, fails the fresh water pumps at the NAVFAC Pump House, Challenges All Four Standby Generators to start (i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6) and challenge the UPS backup power for AFHE, UPS for both control rooms, and the UPS for the oil seal door magnets. If the ADIT 3 Generator also fails then all power to ADIT 3 and its associated tunnel systems is lost. | X | Challenge ADIT 5 Generator | | | | | | | | | | | | | | | | | | |
| 11.5 kV/480V XFMR T10 & RH 480V Normal Panel (LAT electrical room) | BRN48 | Loss of offsite power, the transformer, or the normal panel challenges the ADIT 5 generator to start and the oil seal door UPS to remain energized. | | Challenge ADIT 5 Generator | Momentarily Lost until ADIT 5 Generator Starts | | | | | | | | | | | | | | | | | |
| RH ADIT 5, 275 kw Generator (480v, own battery) Outside, 11 hours fuel | GEN5 | If offsite power also lost, fails power to 480V RH emergency bus. | | | X, if Offsite Power also Lost | | | | | | | | | | | | | | | | | |
| 480V RH Emergency Panel | BRE48 | Fails power to lights, radios (transfer to UPS), and cameras in upper Harbor Tunnel and Lower Access Tunnel, and all Red Hill power; i.e., to MOVs (Including sectionals down to 3Y), fans, sump pumps, elevators, and AFHE indications and alarm inputs. | | | | X (T1-16) | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| LAT Supply Fans SF-1A & 1B via Elev. 72 Air Intake, and Exhaust Fans | EFAN | Failure of these supply fans in the LAT may lead to overheating of both the 480V Red Hill normal and emergency buses in the electrical room; loss of any pair of SF-1A/B, EF-2A/B, or 1-A/1-B may require evacuation. | X(1) | | X, (1) | | | | | | | | | | | | | | | | | |

## Table 6-7. Support to Support Dependencies among the Supporting Electric Power Systems and Other Electric Power Systems at Red Hill (Continued)

| Supporting Systems | Top Events | Impacts on Other Systems | 11.5 kV/ 480V XFMR T10 and RH Normal Panel (LAT electrical room) | RH ADIT 5 Generator (480V, own battery) Outside, 11 Hours Fuel at Full Capacity | 480V RH Emergency Bus | LAT Supply Fans SF-1A and 1B via Elev. 72 Air Intake, and Exhaust Fans | Circuit 6 XFMR 480V/ 120V T13 | Circuit 8 – to 480V Panel P1 in Elev. 72 Upper Access Room | XFMR T14 480/208V/ 120V, 208/120V Panel P2, | Circuit 10 480V/ 208V/ 120V XFMR 15 | Circuit 1 XFMR 11 480V/ 208V/ 120V | Next to Gauger Station 208/120V Panel L | ADIT 5 Gen Bldg. 208/120V Panel G | Circuit 7 480V Panel PA | 480V Panels PP1–PP8 | Upper Harbor Tunnel Panels LP13, LP14, LP15; Lighting/ Cameras/ Radios | LAT Lighting Panels LP16-1, 16-2, 17-1, 17-2, and LP18 | UAT 208V/ 120V Lighting Panels LP19, 20, 21, 22, 23 | ADIT 6 Tunnel, 208/ 120V Panel LB | Upper Tunnel 5Y, 208/ 120V Panel LC | Gauger Station 208/ 120V Panel A | LAT 208/ 120V Panel LA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Circuit 6 to XFMR 480V/120V T13 | BRE48 | Fails upper harbor tunnel and LAT Panels LP13, 14, 15, and Panels 16-1, 16-2, 17-1, 17-2, and LP18; upper harbor lights, cameras, and radios (transfer to UPS), Elevator 72 controller, UAT Fans F-7a through F-7h, and ADIT 4 exhaust Fans EF-1A/B. | | | | | | | | | | | | | | X | X | | | | | |
| Circuit 8 – to 480V Panel P1 in Elev. 72 upper access room | BRE48 | Fails UAT Fans PS-4 & PS-5 at Tanks 17-20 and ADIT6 exhaust fans | | | | | | | X | | | | | | | | | | | | | |
| XFMR T14 480/208V/ 120V, 208/120V – Panel P2 | BRE48 | No loads of importance are on Panel P2 (1) | | | | | | | | | | | | | | | | | | | | |
| Circuit 10 to 480V/208V/ 120V – XFMR T15 | BRE48 | Fails power to Elev. 72 controller, UAT Panels LP19, 20, 21, 22, & 23, UAT Panel LB and ADIT 6 Panel LC; Fails Upper access tunnel (UAT), ADIT 6, and 5Y for lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | | | | X | X | X | | |
| Circuit 1 to XFMR T11 480V/208V/ 120V | BRE48 | Fails gauger station Panel A (gauger station lighting) and Panel L. | | | | X | | | | | | X | | | | | | | | | X | |
| Next to Gauger Station 208/120V Panel L | BRE48 | Fails LAT supply fans at Elev. 72, LAT supply fans SF-1A & 1B, Panel LA, and ADIT 5 Panel G. | | Feeds Battery Charger for ADIT 5 Generator | | X | | | | | | | X | | | | | | | | | | X |
| In ADIT 5 Gen Bldg. 120V Panel G | BRE48 | Fails LAT Supply Fans SF-1A/B at Elev. 72; ADIT 5 generator building lighting, and battery charger for ADIT 5 generator. | | | | X | | | | | | | | | | | | | | | | |

*(1) Assumed Dependency*

**Table 6-8. Support to Frontline Dependencies among the Underground Pump House and ADIT 1 Electric Power and AFHE Systems Including the Control Rooms**

| Supporting Systems | Top Events | Impacts on Other Systems | Control Room Power, Lighting, and Air Cond. | Alternate Control Room power, Lighting and Air Cond. at Fuel Operations Bldg.(normal power and 8-hour UPS) | AFHE | AFHE, Condensing/ Fan CU-1, AC-1 | Emergency Stop Control Panel | Panic Button |
|---|---|---|---|---|---|---|---|---|
| Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP challenges all four standby generators to start (i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6) and challenge the UPS Backup power for AFHE and the UPS for both control rooms. | | Challenge to 6-Hour Alternate CR UPS (not on backup generator) | Challenge to UPS 4-Hour Batteries until Generator Starts and Loads on 480V Emergency Bus | | Pumps Stop on Loss of Motive Power | Pumps Stop on Loss of Motive Power |
| XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | BUN24 | Loss of the 11.5/2.4 kV transformer loses power to all cargo pumps and causes the discharge flow control valves to go closed. | | | | | Pumps Stop on Loss of Motive Power | Pumps Stop on Loss of Motive Power |
| 100 kw Generator at ADIT 1 Tunnel Entrance, 8 Hours Fuel | – | If power from offsite also fails, then the power supply to FORFAC is lost. | | | | | | |
| 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | BUN48 | Loss of offsite power to the normal 480V bus trips the cargo pumps, causes their discharge valves to fail closed, challenges the two generators at ADIT 1 to start, and challenges the UPS Backup power for the AFHE system and the UPS for both of the control rooms. | | Challenge to Alternate CR 6-Hour UPS (not on generator) | | | Fails safe, Trip Cargo Pumps (1) | Fails Safe, Trip Cargo Pumps (1) |
| Generator on Hill at ADIT 1 | GEN1 | If offsite power at ADIT 1 also fails, then fails UGPH normal 480V bus which causes cargo pumps to trip and a loss of power to the UGPH pump discharge valves. | | | | | | |
| UGPH Emergency 480V Bus | BUE48 | Causes loss of power to Panels P100 to P105, challenges UPS for AFHE and main control room and power for the lower Harbor Tunnel radios, lighting, and cameras; fails CR air cond. and lighting; fails UGPH valves and fans, and fails power to the train charger. | Fails CR Power, Air Con., and Lighting | | X, Challenge to UPS 4-Hour Batteries, then Is Lost Afterwards | X | | |
| UGPH Emergency 480V Bus Cooling Fans | BUE48 | After a period of heating will cause failure of power at the UGPH emergency 480V bus. | | | X (delayed loss after heating) | | | |
| 480V P100 | BUE48 | Fails UGPH valves. | | | | | | |
| 480V P101 | BUE48 | Fails UGPH valves and the train's charger. | | | | | | |
| 480V P102 | BUE48 | Fails control room power and AFHE air conditioning, and fails the fans that cool the 11.5/480V transformer room. | Fails CR Air Con. | | | X | | |

**Table 6-8. Support to Frontline Dependencies among the Underground Pump House and ADIT 1 Electric Power and AFHE Systems Including the Control Rooms (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | Control Room Power, Lighting, and Air Cond. | Alternate Control Room power, Lighting and Air Cond. at Fuel Operations Bldg.(normal power and 8-hour UPS) | AFHE | AFHE, Condensing/ Fan CU-1, AC-1 | Emergency Stop Control Panel | Panic Button |
|---|---|---|---|---|---|---|---|---|
| 480V P103 | BUE48 | Fails UGPH valves. | | | | | | |
| 480V P104 | BUE48 | Fails ADIT 1 fans and outside sump pumps and fails harbor tunnel's five sump pumps. | | | | | | |
| XFMR 480/208V, P105 | BUE48 | Fails lights for control room, UGPH, and lower harbor tunnel and challenges UPS for the AFHE and harbor tunnel radios. | Fails CR Lights, Rely on Flashlight | | AFHE UPS on battery until Generator Loads, Fails Backup Fujitsu to AFHE; if Panel Lost All of AFHE Is Eventually Lost | | | |
| AFHE, Condensing/ Fan CU-1, AC-1 | AFHR | Leads to overheating AFHE. | | | X (delayed loss after overheating) | | | |

*(1) Assumed Dependency*

**Table 6-9. Support to Frontline Dependencies among the Underground Pump House, ADIT 1 Electric Power Systems and the AFHE Systems with the Frontline Systems at the Underground Pump House and Lower Harbor Tunnel**

| Supporting Systems | Top Events | Impacts on Other Systems | ADIT 1 Supply Fans F5A/B, F8, F6a-d (3/4 exhaust fans NR) | UGPH MOVs | Cargo Pumps: F-76, 5 Pumps JP-5, 3 Pumps F-24, 3 Pumps (F-24 was JP-8) | UGPH Lighting (no emergency backup) | ADIT 1 outside Sump Pump E1234 | Surge Tank Tunnel Fan EF-8 | Harbor Tunnel's Five Sump Pumps outside UGPH | Lower Harbor Tunnel Radios | Lower Harbor Tunnel Lighting and Cameras | Charger for Train |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Loss of All Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP challenges all four standby generators to start; i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6. | | | X, Pumps Stop on Loss of Motive Power | | | | | | | |
| XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | BUN24 | Loss of the 11.5/2.4 kV transformer loses power to all cargo pumps and causes the discharge flow control valves to go closed. | | | X (discharge control valve(s) also close) | | | | | | | |
| 100 kw Generator at ADIT 1 Tunnel Entrance, 8 Hours Fuel | - | If power from offsite also fails, then the power supply to FORFAC is lost. | | | | | | | | | | |
| 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | BUN48 | Loss of offsite power to the normal 480V bus trips the cargo pumps, causes their discharge valves to fail closed, challenges the two generators at ADIT 1 to start, and challenges the UPS backup power for the AFHE system and the UPS for both of the control rooms. | | | Cargo Pumps Trip [(1)]; AFHE UPS Provides Backup Power to the Pump Control Valves | | | | | | | |
| Generator on Hill at ADIT 1 | GEN1 | If offsite power at ADIT 1 also fails, then fails UGPH normal 480V bus which causes cargo pumps to trip and a loss of power to the UGPH pump discharge valves. | | X, if 480V supply at ADIT 1 from Offsite Power also Fails [(1)] | | | | | | | | |

**Table 6-9. Support to Frontline Dependencies among the Underground Pump House, ADIT 1 Electric Power Systems and the AFHE Systems with the Frontline Systems at the Underground Pump House and Lower Harbor Tunnel (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | ADIT 1 Supply Fans F5A/B, F8, F6a-d (3/4 exhaust fans NR) | UGPH MOVs | Cargo Pumps: F-76, 5 Pumps JP-5, 3 Pumps F-24, 3 Pumps (F-24 was JP-8) | UGPH Lighting (no emergency backup) | ADIT 1 outside Sump Pump E1234 | Surge Tank Tunnel Fan EF-8 | Harbor Tunnel's Five Sump Pumps outside UGPH | Lower Harbor Tunnel Radios | Lower Harbor Tunnel Lighting and Cameras | Charger for Train |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UGPH Emergency 480V Bus | BUE48 | Causes loss of power to Panels P100 to P105, challenges UPS for AFHE and main control room and power for the lower Harbor Tunnel radios, lighting, and cameras; fails CR air cond. and lighting; fails UGPH valves and fans, and fails power to the train charger. | X | X, UGPH Valves and Train Charger | | X | X | X | X | Challenges UPS Batteries for Radios | X | X |
| UGPH Emergency 480V Bus Cooling Fans | BUE48 | After a period of heating will cause failure of power at the UGPH emergency 480V bus. | | | | | | | | | | |
| 480V P100 | BUE48 | Fails UGPH valves. | | X | | | | | | | | |
| 480V P101 | BUE48 | Fails UGPH valves and the train's charger. | | X | | | | | | | | X |
| 480V P102 | BUE48 | Fails control room power and AFHE air conditioning, and fails the fans that cool the 11.5/480V transformer room. | | | | | | X | | | | |
| 480V P103 | BUE48 | Fails UGPH valves. | | X | | | | | | | | |
| 480V P104 | BUE48 | Fails ADIT 1 Fans and outside sump pumps and fails Harbor Tunnel's five sump pumps. | X | | | | X | X | X | | | |
| XFMR 480/ 208V, P105 | BUE48 | Fails lights for control room, UGPH, and lower harbor tunnel and challenges UPS for the AFHE and harbor tunnel radios. | | | | X | | | | Challenges UPS Batteries for Radios | X | |
| AFHE | AFHE | If crashes: causes cargo pumps to trip, disables RHBFST level alarms, and disables LAT main sump pump status indication and RHBFST temperature, level, and other indications in LAT and UAT. | | | X (pumps trip); AFHE UPS Provides Backup Power to Pump Control Valves | | | | | | | |

**Table 6-9. Support to Frontline Dependencies among the Underground Pump House, ADIT 1 Electric Power Systems and the AFHE Systems with the Frontline Systems at the Underground Pump House and Lower Harbor Tunnel (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | ADIT 1 Supply Fans F5A/B, F8, F6a-d (3/4 exhaust fans NR) | UGPH MOVs | Cargo Pumps: F-76, 5 Pumps JP-5, 3 Pumps F-24, 3 Pumps (F-24 was JP-8) | UGPH Lighting (no emergency backup) | ADIT 1 outside Sump Pump E1234 | Surge Tank Tunnel Fan EF-8 | Harbor Tunnel's Five Sump Pumps outside UGPH | Lower Harbor Tunnel Radios | Lower Harbor Tunnel Lighting and Cameras | Charger for Train |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Emergency Stop Control Panel | N/A | Trips operating cargo pumps on selected fuel (product) line(s). | | | Running Cargo Pumps Tripped from Power Source | | | | | | | |
| Panic Button | OPAN | Trips all operating cargo pumps and signals all RHBFST skin valves to close. | | | Running Cargo Pumps Tripped from Power Source | | | | | | | |
| ADIT 1 Supply Fans F5A/B, F8, F6a-d (3/4 exhaust fans NR) | | | | X, (1) | X, (1) | | | | | | | |
| RH Tanks Mechanical High Float Level | | | | | Operating Cargo Pumps Not Tripped | | | | | | | |

*(1) Assumed Dependency*

## Table 6-10. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Frontline Mechanical Systems at Red Hill

| Supporting Systems | Top Events | Impacts on Other Systems | RH LAT Oil Tight Door | Personnel Elevator 72 and Controller | RH Sectional MOVs, down to ADIT 3Y | LAT MOVs near Tanks 1–16 and 17–20 | RH Main Sump Pumps (100A, 100B) and Sewer Pump | RH Zone 3 (UAT) Sump Pump, P-0123; Broken | RH Zone 7 (LAT) Sump Pump P0124 (directs to main sump) | Cargo Elevator 73 | Cargo Elevator 73 Sump Pump 5F-1 | RH Fans Tanks 1–16 Tank Fans, EF1A/B – ADIT 4 UAT, EF2A/B-3Y Exhaust Fans, EF4A/B Harbor Tunnel to 3Y Fans, F7a-F-7h UAT Gauging Fans | LAT Supply Fans SF-1A and 1B at Elev. 72 | RH Fans 17–20 Tank Vent PS1A/B – Elev. 73 UAT, PS2A/B – from Elev. 73, to LAT | RH Fans 17–20 Tank Vent PS-4 and 5 – UAT Fans, PE-1A,1B – Exhaust Fans through ADIT 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11.5 kV/480V XFMR T10 & RH 480V Normal Panel (LAT electrical room) | BRN48 | Loss of offsite power, the transformer, or the normal panel challenges the ADIT 5 generator to start and the oil seal door UPS to remain energized. | Needs UPS Power to Stay Open Fails; Has UGPH Pushbutton to Close | | | | | | | | | | | | |
| RH ADIT 5, 275 kw Generator (480V, own battery) outside, 11 Hours Fuel | GEN5 | If offsite power also lost, fails power to 480V RH emergency bus. | | | | | | | | X [2] | | | | | |
| 480V RH Emergency Panel | BRE48 | Fails power to lights, radios (transfer to UPS), and cameras in upper Harbor Tunnel and Lower Access Tunnel, and all Red Hill power; i.e., to MOVs (including sectionals down to 3Y), fans, sump pumps, elevators, and AFHE indications and alarm inputs. | | X | X | X | X | X [1] | X | X [2] | X | X | X [1] | X | X |
| LAT Supply Fans SF-1A & 1B via Elev. 72 Air Intake, and Exhaust Fans | EFAN | Failure of these supply fans in the LAT may lead to overheating of both the 480v Red Hill normal and emergency buses in the electrical room; loss of any pair of SF-1A/B, EF-2A/B, or 1-A/1-B may require evacuation. | | | | | | | | | | | | | |
| Circuit 6 to XFMR 480V/120V T13 | BRE48 | Fails upper harbor tunnel and LAT Panels LP13, 14, 15, and Panels 16-1, 16-2, 17-1, 17-2, and LP18; Upper harbor lights, cameras, and radios (transfer to UPS), Elevator 72 controller, UAT Fans F-7a through F-7h, and ADIT 4 Exhaust Fans EF-1A/B. | | | | | | | | | | | | | |
| Circuit 8 – to 480V Panel P1 in Elev. 72 upper access room | BRE48 | Fails UAT Fans PS-4 & PS-5 at Tanks 17-20 and ADIT 6 exhaust fans. | | | | | | | | | | | | | X |

**Table 6-10. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Frontline Mechanical Systems at Red Hill (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | RH LAT Oil Tight Door | Personnel Elevator 72 and Controller | RH Sectional MOVs, down to ADIT 3Y | LAT MOVs near Tanks 1–16 and 17–20 | RH Main Sump Pumps (100A, 100B) and Sewer Pump | RH Zone 3 (UAT) Sump Pump, P-0123; Broken | RH Zone 7 (LAT) Sump Pump P0124 (directs to main sump) | Cargo Elevator 73 | Cargo Elevator 73 Sump Pump 5F-1 | RH Fans Tanks 1–16 Tank Fans, EF1A/B – ADIT 4 UAT, EF2A/B-3Y Exhaust Fans, EF4A/B Harbor Tunnel to 3Y Fans, F7a-F-7h UAT Gauging Fans | LAT Supply Fans SF-1A and 1B at Elev. 72 | RH Fans 17–20 Tank Vent PS1A/B – Elev. 73 UAT, PS2A/B – from Elev. 73, to LAT | RH Fans 17–20 Tank Vent PS-4 and 5 – UAT Fans, PE-1A,1B – Exhaust Fans through ADIT 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| XFMR T14 480/208V/ 120V, 208/120V – Panel P2, | BRE48 | No loads of importance are on Panel P2. (1) | | | | | | | | | | | | | |
| Circuit 10 to 480V/208V/ 120V – XFMR T15 | BRE48 | Fails power to Elev. 72 controller, UAT Panels LP19, 20, 21, 22, and 23, UAT Panel LB and ADIT 6 Panel LC; Fails Upper access tunnel, ADIT 6, and 5Y for lighting, cameras, and radios (transfers to UPS). | | X | | | | | | | | | | | |
| Circuit 1 to XFMR T11 480V/208V/ 120V | BRE48 | Fails Gauger Station Panels A (gauger station lighting) and Panel L. | | | | | | | | | X | | X | | |
| Next to Gauger Station 208/120V Panel L | BRE48 | Fails LAT supply fans at Elev. 72, LAT supply fans SF-1A and 1B, panel LA, and ADIT 5 Panel G. | | | | | | | | | X | | X | | |
| In ADIT 5 Gen BLDG. 120V Panel G | BRE48 | Fails LAT supply fans SF-1A/B at Elev. 72; ADIT 5 generator building lighting, and battery charger for ADIT 5 generator. | | | | | | | | | | | | | |
| Circuit 7 to 480V Panel PA | BRE48 | Fails Cargo Elevator 73 sump pump, and LAT MOVs near RHBFSTs 17 through 20. | | | | X (T17-20) | | | | | | | | | |
| Circuit 7 to 480V LAT Panels PP1–PP8 | BRE48 | Fails MOVs near RHBFSTs 1 through 16. | | | | X (T1-16) | | | | | | | | | |
| Upper Harbor Tunnel panels LP13, LP14, LP15; Lighting/ Cameras/ Radios | LPRH | Fails upper harbor tunnel lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | |
| LAT Lighting Panels LP16-1, 16-2, 17-1, 17-2, and LP18 | LPRH | Fails Lower Access Tunnel lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | |

**Table 6-10. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Frontline Mechanical Systems at Red Hill (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | RH LAT Oil Tight Door | Personnel Elevator 72 and Controller | RH Sectional MOVs, down to ADIT 3Y | LAT MOVs near Tanks 1–16 and 17–20 | RH Main Sump Pumps (100A, 100B) and Sewer Pump | RH Zone 3 (UAT) Sump Pump, P-0123; Broken | RH Zone 7 (LAT) Sump Pump P0124 (directs to main sump) | Cargo Elevator 73 | Cargo Elevator 73 Sump Pump 5F-1 | RH Fans Tanks 1–16 Tank Fans, EF1A/B – ADIT 4 UAT, EF2A/B-3Y Exhaust Fans, EF4A/B Harbor Tunnel to 3Y Fans, F7a-F-7h UAT Gauging Fans | LAT Supply Fans SF-1A and 1B at Elev. 72 | RH Fans 17–20 Tank Vent PS1A/B – Elev. 73 UAT, PS2A/B – from Elev. 73, to LAT | RH Fans 17–20 Tank Vent PS-4 and 5 – UAT Fans, PE-1A,1B – Exhaust Fans through ADIT 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UAT 208V/120V Lighting Panels LP19, 20, 21, 22, 23 | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | |
| ADIT 6 Tunnel, 208/120V Panel LB | LPRH | Fails ADIT 6 lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | |
| Upper Tunnel 5Y, 208/120V Panel LC | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). | | | | | | | | | | | | | |
| Gauger Station 208/120V Panel A | LPRH | Fails gauger station lighting. | | | | | | | | | | | | | |
| LAT 208/ 120V Panel LA | LPRH | Upper access tunnel lighting. | | | | | | | | | | | | | |
| AFHE | AFHE | If crashes: causes cargo pumps to trip, disables RHBFST level alarms, and disables LAT main sump pump status indication and RHBFST temperature, level, and other indications in LAT and UAT. | | | | | AFHE Only Tracks Status | | | | | | | | |
| Panic Button | OPAN | Trips all operating cargo pumps and signals all RHBFST skin valves to close. | | | | Skin Valves Signaled to Close | | | | | | | | | |
| RH Tanks Mechanical High Float Level | SWITCH | Loss of actuation allows cargo pumps to continue running and skin valve of affected RHBFST to remain open. | | | | Skin Valve Remains Open | | | | | | | | | |

*(1) Assumed Dependency*

*(2) The Cargo Elevator 73 Is Powered from RH Emergency Bus, but also Has a Direct Feed from the ADIT 5 Generator*

**Table 6-11. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Systems Requiring Electrical Support at Red Hill**

| Supporting Systems | Top Events | Impacts on Other Systems | LAT and Upper 1/2 Harbor Tunnel Lighting/ Cameras/ Radio | Gauger Station Lighting | Upper Level Access Lighting, Cameras and Radios | ADIT 5Y Lighting, Cameras, and Radios | ADIT 6 Lighting, Cameras, and Radios | ADIT 5 Generator Bldg. Lighting | RH Instruments and Indications | RH Tanks Warning and Critical UFM Alarms | RH Tanks Mechanical High Float Level – Trip Pumps/Skin Valve Signals |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 480V RH Emergency Panel | BRE48 | Fails power to lights, radios (transfer to UPS), and cameras in upper Harbor Tunnel and Lower Access Tunnel, and all Red Hill power; i.e., to MOVs (Including sectionals down to 3Y), fans, sump pumps, elevators, and AFHE indications and alarm inputs. | X | X | X | X | X | X | X | X (impact of losing AFHE) | X (skin valve power) |
| Circuit 10 to 480V/208V/ 120V – XFMR T15 | BRE48 | Fails power to Elev. 72 controller, UAT Panels LP19, 20, 21, 22, and 23, UAT Panel LB and ADIT 6 Panel LC; Fails Upper access tunnel, ADIT 6, and 5Y for lighting, cameras, and radios (transfers to UPS). | | | X | | X | | | | |
| Circuit 1 to XFMR T11 480V/208V/ 120V | BRE48 | Fails Gauger Station Panel A (gauger station lighting) and Panel L. | | X | | | | | | | |
| Next to Gauger Station 208/ 120V Panel L | BRE48 | Fails LAT supply fans at Elev. 72, LAT Supply Fans SF-1A and 1B, Panel LA, and ADIT 5 Panel G. | | | X (1) | | | X | | | |
| In ADIT 5 Gen Bldg. 120V Panel G | BRE48 | Fails LAT Supply Fans SF-1A/B at Elev. 72; ADIT 5 generator building lighting, and battery charger for ADIT 5 generator. | | | | | | X | | | |
| Circuit 7 to 480V Panel PA | BRE48 | Fails Cargo Elevator 73 sump pump, and LAT MOVs near RHBFSTs 17 through 20. | | | | | | | | | |
| Circuit 7 to 480V LAT Panels PP1-PP8 | BRE48 | Fails MOVs near RHBFSTs 1 through 16. | | | | | | | | | |
| Upper Harbor Tunnel Panels LP13, LP14, LP15; Lighting/ Cameras/ Radios | LPRH | Fails upper harbor tunnel lighting, cameras, and radios (transfers to UPS). | | | X | | | | | | |

**Table 6-11. Support to Frontline Dependencies among the Red Hill Electric Power Systems and the AFHE Systems with the Systems Requiring Electrical Support at Red Hill (Continued)**

| Supporting Systems | Top Events | Impacts on Other Systems | LAT and Upper 1/2 Harbor Tunnel Lighting/ Cameras/ Radio | Gauger Station Lighting | Upper Level Access Lighting, Cameras and Radios | ADIT 5Y Lighting, Cameras, and Radios | ADIT 6 Lighting, Cameras, and Radios | ADIT 5 Generator Bldg. Lighting | RH Instruments and Indications | RH Tanks Warning and Critical UFM Alarms | RH Tanks Mechanical High Float Level – Trip Pumps/Skin Valve Signals |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LAT Lighting Panels LP16-1, 16-2, 17-1, 17-2, and LP18 | LPRH | Fails Lower Access Tunnel lighting, cameras, and radios (Transfers to UPS). | X | | | | | | | | |
| UAT 208V/120V Lighting Panels LP19, 20, 21, 22, 23 | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). | | X (1) | X | | | | | | |
| ADIT 6 Tunnel, 208/120V Panel LB | LPRH | Fails ADIT 6 lighting, cameras, and radios (transfers to UPS). | | | | | X | | | | |
| Upper Tunnel 5Y, 208/120V Panel LC | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). | | | X | X | | | | | |
| Gauger Station 208/ 120V Panel A | LPRH | Fails gauger station lighting. | | X | | | | | | | |
| LAT 208/ 120V Panel LA | LPRH | Upper access tunnel lighting. | | | X (1) | | | | | | |
| AFHE | AFHE | If crashes: causes cargo pumps to trip, disables RHBFST level alarms, and disables LAT main sump pump status indication and RHBFST temperature, level, and other indications in LAT and UAT. | | | | | | | X (1) | X | |

*(1) assumed dependency*

Table 6-12 summarizes the disposition of equipment identified in the system dependency tables that are represented in event tree top events in the event sequence models. Additional event tree top events are developed in the following sections since they may make use of different combinations of these sets of equipment; e.g., both Red Hill valves and Harbor Tunnel sectional valves are needed for different approaches to empty a RHBFST.

**Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees**

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| Loss of all Offsite Power; to Connections at ADIT 1 and near ADIT 3 | GRID | LOOP causes loss of power to all cargo pumps via the 2.4 kV bus and causes their discharge valves to fail closed, fails the fresh water pumps at the NAVFAC Pump house, challenges all 4 Standby Generators to start (i.e., two at ADIT 1, one at ADIT 3, and one at ADIT 6) and challenge the UPS Backup power for AFHE, UPS for both control rooms, and the UPS for the oil seal door magnets. If the ADIT 3 Generator also fails then all power to ADIT 3 and its associated tunnel systems is lost. |
| XFMR 11.5/2.4 kV and 2.4 kV Normal Bus at UGPH | BUN24 | Loss of the 11.5/2.4 kV transformer loses power to all cargo pumps and causes the discharge flow control valves to go closed. |
| 100 kw Generator at ADIT 1 Tunnel Entrance, 8 Hours Fuel | – | If power from offsite also fails, then the power supply to FORFAC is lost, but this is not modeled in the QRVA. |
| 11.5k to 480V Transformer at ADIT 1 and Normal 480V Bus | BUN48 | Loss of offsite power to the normal 480V bus trips the cargo pumps, causes their discharge valves to fail closed, challenges the two generators at ADIT 1 to start, and challenges the UPS Backup power for the AFHE system and the UPS for both of the control rooms. |
| Generator on Hill at ADIT 1 | GEN1 | If offsite power at ADIT 1 also fails, then fails UGPH normal 480V bus which causes cargo pumps to trip and a loss of power to the UGPH pump discharge valves. |
| UGPH Emergency 480V Bus | BUE48 | Causes loss of power to Panels P100 to P105, challenges UPS for AFHE and main control room and power for the lower Harbor Tunnel radios, lighting, and cameras; fails CR air cond. and lighting; fails UGPH valves and fans, and fails power to the train charger. |
| UGPH Emergency 480V Bus Cooling Fans EF-6a/b/c/d, EF-8/9, SF-5A/B, SF-7 | BUE48 | After a period of heating will cause failure of power at the UGPH emergency 480V bus. |

## Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| 480V P100 | BUE48 | Fails UGPH valves. |
| 480V P101 | BUE48 | Fails UGPH valves and the train's charger. |
| 480V P102 | BUE48 | Fails control room power and AFHE air conditioning, and fails the fans that cool the 11.5/480V transformer room. |
| 480V P103 | BUE48 | Fails UGPH valves. |
| 480V P104 | BUE48 | Fails ADIT 1 fans and outside sump pumps and fails Harbor Tunnel's five sump pumps. |
| XFMR 480/ 208V, P105 | BUE48 | Fails lights for control room, UGPH, and lower harbor tunnel and challenges UPS for the AFHE and harbor tunnel radios. |
| 11.5 kV/2.4 kV XFMR and main pumps panel (ADIT 3) | B3EA | Fails power to NAVFAC pump house main pumps panel. |
| Water Main Pumps | – | These pumps are not modeled in the QRVA. |
| 11.5 kV/480 XFMR at NAVFAC Pump House | B3EA | Challenges ADIT 3 generator to start, if also failed power is lost to Panels B and A at NAVFAC pump house. |
| ADIT 3 NAVFAC Diesel Generator for Fresh Water | GEN3 | If offsite power is also lost, fails ADIT 3 lighting and Sump Pumps P1706, P1707, and ventilation fans at water pumping station. |
| NAVFAC Pump House Panels B, 480/208V XFMR, and A | B3EA | Fails ADIT 3 lighting and Sump Pumps P1706, P1707, and ventilation fans at water pumping station. |
| ADIT 2 Sump Pump | - | This is a small capacity pump and so is not modeled. |
| ADIT 3 Lighting and Sump Pumps P1706, P1707 (to settling tank) and Ventilation at Water Pumping Station | - | Lighting and ventilation in the ADIT 3 tunnel and water pump house would facilitate Red Hill evacuation and later access by recovery personnel but each has a flash light for this purpose and so it is not modeled. |
| 11.5 kV/480V XFMR T10 & RH 480V Normal Panel (LAT electrical room) | BRN48 | Loss of offsite power, the transformer, or the normal panel challenges the ADIT 5 generator to start and the oil seal door UPS to remain energized. |
| RH ADIT 5, 275 kw generator (480V, own battery) Outside, 11 Hours Fuel | BRE48 | If offsite power also lost, fails power to 480V RH emergency bus. |

## Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| 480V RH Emergency Panel | BRE48 | Fails power to lights, radios (transfer to UPS), and cameras in upper Harbor Tunnel and Lower Access Tunnel, and all Red Hill power; i.e., to MOVs (Including sectionals down to 3Y), fans, sump pumps, elevators, and AFHE indications and alarm inputs. |
| LAT Supply Fans SF-1A & 1B via Elev. 72 Air Intake | EFAN | Failure of these supply fans in the LAT may lead to overheating of both the 480V Red Hill normal and emergency buses in the electrical room. |
| Circuit 6 to XFMR 480V/120V T13 | BRE48 | Fails upper harbor tunnel and LAT Panels LP13, 14, 15, and Panels 16-1, 16-2, 17-1, 17-2, and LP18; upper harbor lights, cameras, and radios (transfer to UPS), Elevator 72 controller, UAT Fans F-7a through F-7h, and ADIT 4 Exhaust Fans EF-1A/B. |
| Circuit 8 – to 480V Panel P1 in Elev. 72 Upper Access Room | BRE48 | Fails UAT Fans PS-4 and PS-5 at Tanks 17–20 and ADIT 6 exhaust fans. |
| XFMR T14 480/208V/120V, 208/120V – Panel P2 | – | No loads have been identified for this panel. |
| Circuit 10 to 480V/208V/120V – XFMR T15 | BRE48 | Fails power to Elev. 72 controller, UAT Panels LP19, 20, 21, 22, and 23, UAT Panel LB and ADIT 6 Panel LC; fails Upper Access Tunnel, ADIT 6, and 5Y for lighting, cameras, and radios (transfers to UPS) |
| Circuit 1 to XFMR T11 480V/208V/120V | BRE48 | Fails Gauger Station Panel A (Gauger station lighting) and Panel L. |
| Next to Gauger Station 208/120V Panel L | BRE48 | Fails LAT supply fans at Elev. 72, LAT Supply Fans SF-1A and 1B, Panel LA, and ADIT 5 Panel G. |
| In ADIT 5 Gen Bldg. 120V Panel G | BRE48 | Fails LAT Supply Fans SF-1A/B at Elev. 72; ADIT 5 generator building lighting, and battery charger for ADIT 5 generator. |
| Circuit 7 to 480V Panel PA | BRE48 | Fails Cargo Elevator 73 sump pump, and LAT MOVs near RHBFSTs 17 through 20. |
| Circuit 7 to 480V LAT Panels PP1-PP8 | BRE48 | Fails MOVs near RHBFSTs 1 through 16. |
| Upper Harbor Tunnel Panels LP13, LP14, LP15; Lighting/Cameras/Radios | LPRH | Fails upper harbor tunnel lighting, cameras, and radios (transfers to UPS). |
| LAT Lighting Panels LP16-1, 16-2, 17-1, 17-2, and LP18 | LPRH | Fails Lower Access Tunnel lighting, cameras, and radios (transfers to UPS). |

## Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| UAT 208V/120V Lighting Panels LP19, 20, 21, 22, 23 | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). |
| ADIT 6 Tunnel, 208/120V Panel LB | LPRH | Fails ADIT 6 lighting, cameras, and radios (transfers to UPS). |
| Upper Tunnel 5Y, 208/120V Panel LC | LPRH | Fails Upper Access Tunnel lighting, cameras, and radios (transfers to UPS). |
| Gauger Station 208/120V Panel A | LPRH | Fails gauger station lighting. |
| LAT 208/120V Panel LA | LPRH | Upper access tunnel lighting. |
| Control Room Power, Lighting, and Air Cond. | CRM | Lighting and air conditioning in the main control room would facilitate the operator's response. There is no backup electric power for CR lighting. However, loss of the same UGPH 480V emergency bus would also disable remote valve operation in the UGPH. |
| Alternate Control Room Power, Lighting and Air Cond. at Fuel Operations Bldg.(normal power and 8-hour UPS) | ACRM | Alternate control room power, lighting and air cond. at Fuel Operations Bldg. (normal power and 8-hour UPS). |
| AFHE | AFHE | If crashes: causes cargo pumps to trip, prevents panic button closure signals, disables RHBFST level alarms, prevents RHBFST mechanical float high level signals, and disables LAT main sump pump status indication and RHBFST indications in UAT. |
| AFHE, Condensing/ Fan CU-1, AC-1 | AFHR | Leads to overheating AFHE. |
| Emergency Stop Control Panel | OPAN | The operating cargo pumps fail safe (trip off) on loss of electric power. The operator action to use the emergency stop control panel bounds the probability of failure for the panel. |
| Panic Button | OPAN | Trips all operating cargo pumps and signals all RHBFST skin valves to close. |
| ADIT 1 Supply Fans F5A/B, F8, F6a-d (3/4 exhaust fans NR) | UFAN | Loss of the UGPH supply or exhaust fans may cause cargo pumps to overheat and MOVs in pump house to require manual operation. |
| UGPH MOVs and Lower Harbor Tunnel MOVs | TFAN | Loss of any pair of fans above the LAT Bulkhead PE-1A/B, PS-1A/1B, or PS-2A/2B (excluding PS-4/5 as only for UAT at RHBFST 20) may require evacuation. |

## Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| Cargo Pumps:<br>F-76, 5 Pumps<br>JP-5, 3 Pumps<br>F-24, 3 Pumps<br>F-24 Was JP-8 | CARGO | The operating cargo pumps fail safe (off) on loss of electric power. Failure of the cargo pumps to operate precludes transfer of fuel from a RHBFST to higher elevation RHBFST tanks. |
| UGPH Lighting (no emergency backup) | ULIT | Loss of lighting would make alignment of the cargo pumps and/or the UGPH valves for gravity feed more difficult. Failure of this top event is implicitly considered within the operator error rates assigned. |
| ADIT 1 outside Sump Pump E1234 | - | This sump pump not credited for RH leak mitigation. |
| Surge Tank Tunnel Fan EF-8 | - | This fan is not needed for RH leak mitigation. |
| Harbor Tunnel's Five Sump Pumps outside UGPH | USUMP | These sump pumps not needed for RH leak mitigation but useful for Harbor leak mitigation. |
| Lower Harbor Tunnel Radios | ULIT | Power for these radios as represented by this top event is implicitly considered within the operator error rates assigned. |
| Lower Harbor Tunnel Lighting & Cameras | ULIT | Power for this lighting and cameras as represented by this top event are implicitly considered within the operator error rates assigned. |
| Charger for Train | – | The train is assumed not needed for RH leak mitigation. Its charge lasts 1 week. |
| RH LAT New Oil Tight Door | DOOR | Failure to close would release leaked fuel from LAT to harbor tunnel. |
| Personnel Elevator 72 & Controller | EL72 | Failure of the personnel elevator extends the time for top gauger actions; e.g., top gauging. |
| RH Sectional MOVs, down to ADIT 3Y | RMOV | Inability of sectional valves to remotely close extends the time to isolate leaks to the LAT. |
| LAT MOVs near Tanks 1–16 & 17–20 | RMOV | Inability of skin and ball valves to remotely close extends the time to isolate leaks to the LAT. |
| RH Main Sump Pumps (100A, 100B) & Sewer Pump (frontline) | MSUMP | Failure of main sump pumps in LAT precludes transfer of leaked fuel to S311. |
| RH Zone 3 (UAT) Sump Pump, P-0123; Broken | – | Failure of Zone 3 sump pump in UAT extends time to transfer leaked fuel from UAT. Presently no leakage to the UAT is considered. |

## Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| RH Zone 7 (LAT) Sump Pump P0124 (directs to main sump) | – | Failure of Zone 7 sump pump in LAT may preclude or extend the time for fuel leaked to Zone 7 to arrive at the main sump below the tank gallery. This is not important since the fuel is confined above the bulkhead. |
| Cargo Elevator 73 | EL73 | Failure of the cargo elevator extends the time for top gauger actions; e.g., top gauging. |
| Cargo Elevator 73 Sump Pump 5F-1 | – | Failure of the tiny cargo elevator sump pump is not expected to affect the operator's responses |
| RH Fans Tanks 1–16 Tank Fans, F7a-F-7h UAT Gauging Fans EF1A/B – ADIT 4 UAT, EF2A/B – 3Y Exhaust Fans, EF4A/B Harbor Tunnel to 3Y Fans, SF-1A & 1B at Elev. 72 | EFAN | Failure of pairs of ventilation fans may require RH tunnel(s) evacuation and therefore delay operator response to local actions; UAT gauging fans may complicate but not significantly delay top gauging; such fans are usually started 2 hours prior to top gauging.<br>Failure of the LAT exhaust fans to ADIT 3 or the supply fans near Elevator 72 may lead to overheating of both the 480V Red Hill normal and emergency buses in the electrical rooms and require evacuation from the tunnels. |
| RH Fans 17–20 Tank Vent PS1A/B – Elev. 73 UAT, PS2A/B – from Elev. 73, to LAT | TFAN | Failure of either of these pairs of supply fans in the RHBFST 17–20 side may lead to overheating of Elevator 73 and require evacuation from Zone 7. |
| RH Fans 17–20 Tank Vent PS-4 & 5 – UAT Fans, PE-1A, 1B – Exhaust Fans through ADIT 6 | TFAN | Failure of the PE-1A/B pair of exhaust fans at ADIT 6 may lead to overheating of the RH emergency bus and require evacuation from the LAT. Failure of PS-4 and five are assumed to have no effect. |
| LAT and Upper 1/2 Harbor Tunnel Lighting/Cameras/Radio | LPRH | Power for these lighting, cameras, and radios as represented by this top event is implicitly considered within the operator error rates assigned. |
| Gauger Station Lighting | LPRH | Power for this lighting as represented by this top event is implicitly considered within the operator error rates assigned. |
| Upper Level Access Lighting, Cameras, and Radios | LPRH | Power for these lighting, cameras, and radios as represented by this top event is implicitly considered within the operator error rates assigned. |
| ADIT 5Y Lighting, Cameras, and Radios | LPRH | Power for these lighting, cameras, and radios as represented by this top event is implicitly considered within the operator error rates assigned. |

**Table 6-12. Disposition of Support and Frontline Equipment Modeled in the QRVA Event Trees (Continued)**

| Supporting and Frontline Systems | Top Events | Impacts on Other Systems |
|---|---|---|
| ADIT 6 Lighting, Camera, and Radios | LPRH | Power for these lighting, cameras, and radios as represented by this top event is implicitly considered within the operator error rates assigned. |
| ADIT 5 Generator Bldg. Lighting | LPRH | Power for this lighting as represented by this top event is implicitly considered within the operator error rates assigned. |
| RH Instruments and Indications | RHIN | Failure of power to all RH Instruments and indications needed to support operator responses and for inputs to AFHE alarms. |
| RH Tanks Warning and Critical UFM Alarms | RHIN | Failure of all Red Hill AFHE power causes failure of low level alarms. |
| RH Tanks Mechanical High Float Level – Trip Pumps/Skin Valve Signals | RHIN | Failure of the mechanical high float level cargo pump trip and skin valve closure signals due to loss of power. |

Before assembling these top events into event trees for sequence quantification, it is necessary to understand the sequence of mitigating actions that may lessen the impacts of the initial leakage as defined by the initiating events. Event sequence diagrams are used to document these sequences as described in the next section.

## 6.6 Event Sequence Diagrams

As described in Section 6.4, there are four main categories of initiating events. The following presents the event sequence diagrams for each of these major categories of initiating events. The subcategories within each of the major categories are also accounted for in these event sequence diagrams.

The event sequence diagrams depict both normal and off-normal events along the sequence response to an initiating event. Rectangular symbols depict stochastic events that may have yes or no outcomes. The ovals provide descriptive information about the sequence of events which come before it, and the hexagons are sequence end states. These end states are described in words rather than identifying specific amounts of fuel released. Above each of the rectangles is an event tree top event identifier, or multiple identifiers if they all are used to represent the event described. These top events are described in detail in Section 7, at which time it will be useful to refer back to these event sequence diagrams.

### 6.6.1 Event Sequence Diagrams for RHBFST Tank Leaks

The ESD for tank leaks directly to rock is presented in Figure 6-4. This ESD was developed based on the facility operational guidance provided by Red Hill standard operating procedures (SOP) and based on responses to questions posed to Red Hill operations staff.

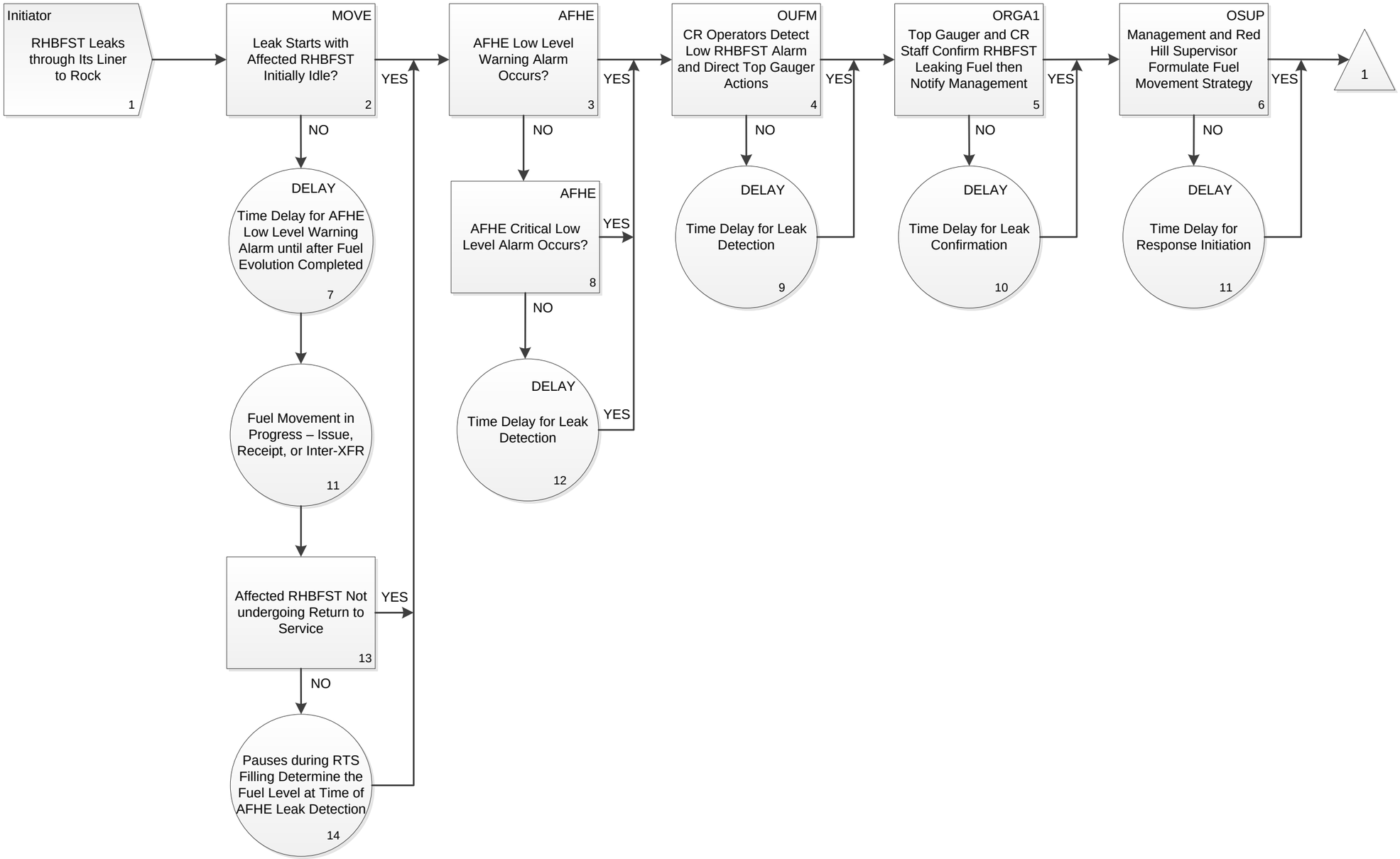



**Figure 6-4. Event Sequence Diagram for RHBFST Tank Leaks Directly to Rock (1 of 2)**

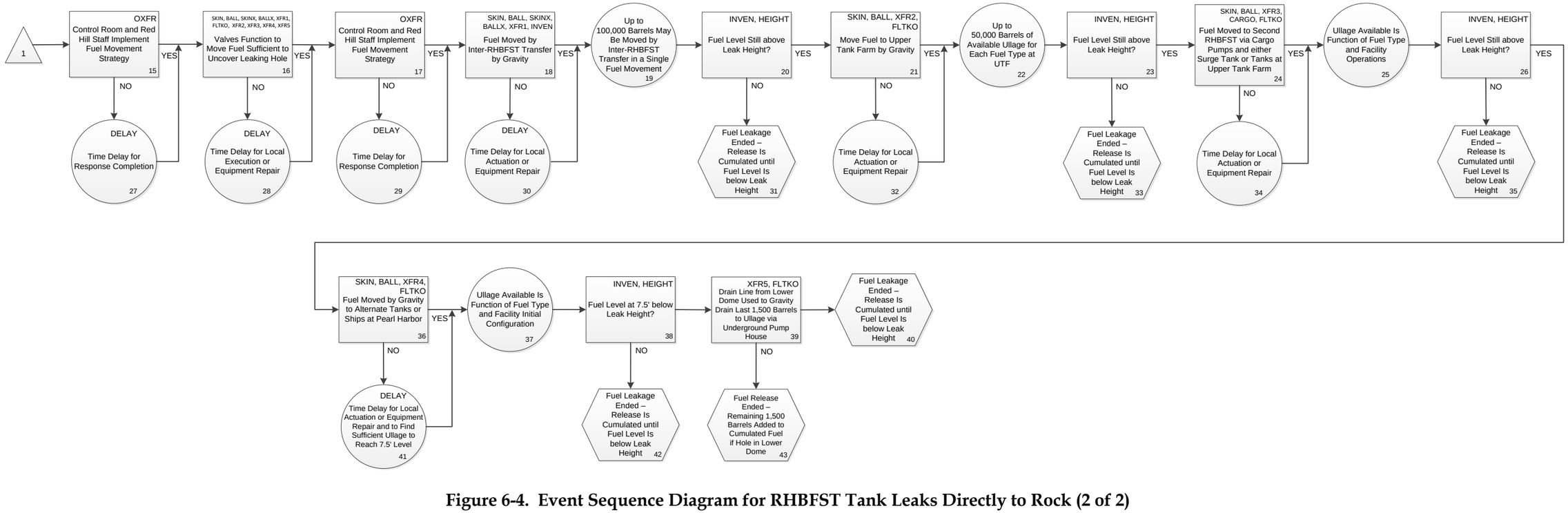



**Figure 6-4. Event Sequence Diagram for RHBFST Tank Leaks Directly to Rock (2 of 2)**

The ESD considers that the RHBFST now leaking may be initially idle at the time the leak starts, or that the RHBFST may instead be aligned for a fuel evolution (i.e., issue, receipt, or inter-tank transfer) at the time the leak starts. The ESD then indicates that if the RHBFST is not idle, then detection of the leak is delayed. This is because the AFHE system is not effective at detecting changes in level while fuel is being received or issued from the RHBFST. If the RHBFST is initially in a fuel movement, the leak event will go undetected until the fuel movement has ended, the RHBFST level has settled down (approximately 1 to 2 hours) and then sufficient leakage occurs so as to trigger the AFHE low level warning alarm.

During a RHBFST return to service, the filling process includes up to 10 pauses, each pause lasting 24 hours, as the fuel level increases to check for leaks; i.e., rather than filling the RHBFST from empty to full in one or two receipts. It is therefore possible to detect holes lower in the RHBFST during one of these 10 pauses prior to filling the RHBFST to the maximum operating level. In earlier years at Red Hill, records indicate that when a leak is detected and some fuel was removed, the operators would stop the emptying process before fully emptying the leaking RHBFST to check whether the level continues to drop. Such checks to see if the hole has been uncovered were made so as to locate the leak. This is no longer Red Hill operating practice. Even with the hole located, the RHBFST would still have to be emptied to fix the leak.

Of course, a large leakage flow rate could also be detected manually by the control room operators even right after the fuel movement is ended by observing changes in the AFHE level readings. However, to confirm that a leak is in progress, manual top gauge readings are taken and trended by operators. Given an AFHE low level or warning or critical alarm, the operators are tasked by procedures to confirm the readings of the AFHE by performing one or more top gauges manually. The operators are also tasked to perform a manual top gauge within 2 hours each time a fuel movement ends. If the AFHE system is working, both that system and confirmation by the top gauger at Red Hill that there is decreasing fuel level in the RHBFST is needed for further action to be taken.

Once a leak is confirmed, management and the Red Hill supervisor are notified of the situation. The Red Hill supervisor is then tasked with making a strategy for a response and to notify the Red Hill staff of his strategy. Typically, and for this ESD, the response involves a strategy for moving fuel from the leaking RHBFST. This mostly involves opening the skin and ball valves of the, then idle, RHBFST and directing the fuel to other tanks which have ullage; i.e., at Red Hill or down below. The Red Hill staff must then manually manipulate sufficient valves and possibly cargo pumps to implement the strategy. The idea is not to isolate the leak, but to move fuel from the leaking RHBFST before it has a chance to leak to rock. Delays at any step along the way can postpone the response, allowing additional fuel time to leak to rock. Once the leak and fuel movement draw down RHBFST fuel levels below the leaking hole, further leakage to rock ends.

The amount of fuel leaked out is then a function of many variables including: the leakage flow rate, the initial fuel level, the height of the hole through which the leak occurs, the time at which fuel is then being moved from the RHBFST, the rate it is emptied, and the time delays experienced during the response.

The last stochastic event in Sheet 1 of the ESD is actually a variety of actions and fuel movements that may be chosen or are necessary to effect the RHBFST being emptied. Additional detail expanding the logic of this one event is presented in Sheet 2 of the ESD.

The Sheet 2 ESD begins where the Red Hill staff is tasked to implement the supervisor's strategy to empty the RHBFST. Although the leaking RHBFST, depending on the level of the hole, may not have to be fully emptied to uncover the hole, the operational training is to empty the RHBFST in its entirety.

Five approaches may be involved in the strategy to empty a leaking RHBFST. As presented in Sheet 2 of the ESD, these are:

- XFR1 – Inter-RHBFST Transfer by Gravity
- XFR2 – Move Fuel to Upper Tank Farm by Gravity
- XFR3 – Cyclically Move Fuel to Another RHBFST Using the Cargo Pumps and Surge Tanks or via the UTF
- XFR4 – Move Fuel by Gravity to Alternate Tanks or Ships at Pearl Harbor
- XFR5 – Drain the Last 7.5' of Fuel from the Lower Dome Using the Fuel Lines to the UGPH

Not all of these approaches may be necessary to fully empty a RHBFST depending on the initial height of fuel. In the 2014 leak incident for RHBFST 5, the first three and fifth approaches were utilized. The fourth approach was not utilized. There are no procedural requirements of what order to implement these alternate approaches. It is likely, however, that Methods 1 and 2 would be given priority. Inter-RHBFST transfers by gravity or to ullage in the UTF, are not only a rapid way to move fuel, but also most effective when the leaking RHBFST is initially at its highest fuel level. Using the cargo pumps to move fuel to other RHBFSTs of the same fuel type allows one to take advantage of the ullage in those RHBFSTs.

The fifth approach involves draining the final 7.5' of fuel. The connecting pipe to the LAT which penetrates the lower dome also sticks open approximately 7.5' into a RHBFST. Therefore this pipe cannot be used to empty the bottom 7.5' of fuel. Instead a gravity drain is connected to the main fuel line to remove the last, approximately 1,500 barrels of fuel.

See Section 7 for a discussion of success criteria for each top event called out along the events in the ESD.

### 6.6.2 Event Sequence Diagrams for Leaks Resulting from Overfilling a RHBFST

The ESD for tank leaks resulting from overfilling a RHBFST and being released from a hole above the maximum operating level is presented in Figure 6-5. This ESD was developed based on the facility operational guidance provided by Red Hill standard operating procedures and based on responses to questions posed to Red Hill operations staff.

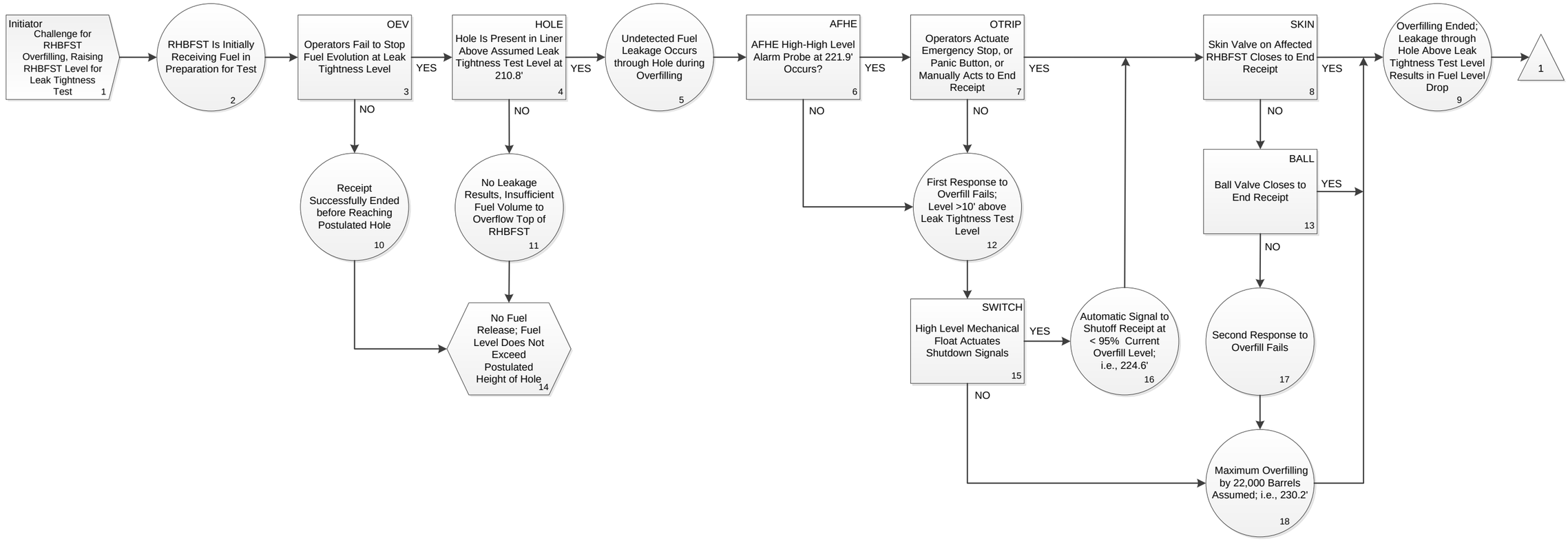



**Figure 6-5. Event Sequence Diagram for Leaks Resulting from Overfilling a RHBFST (1 of 2)**

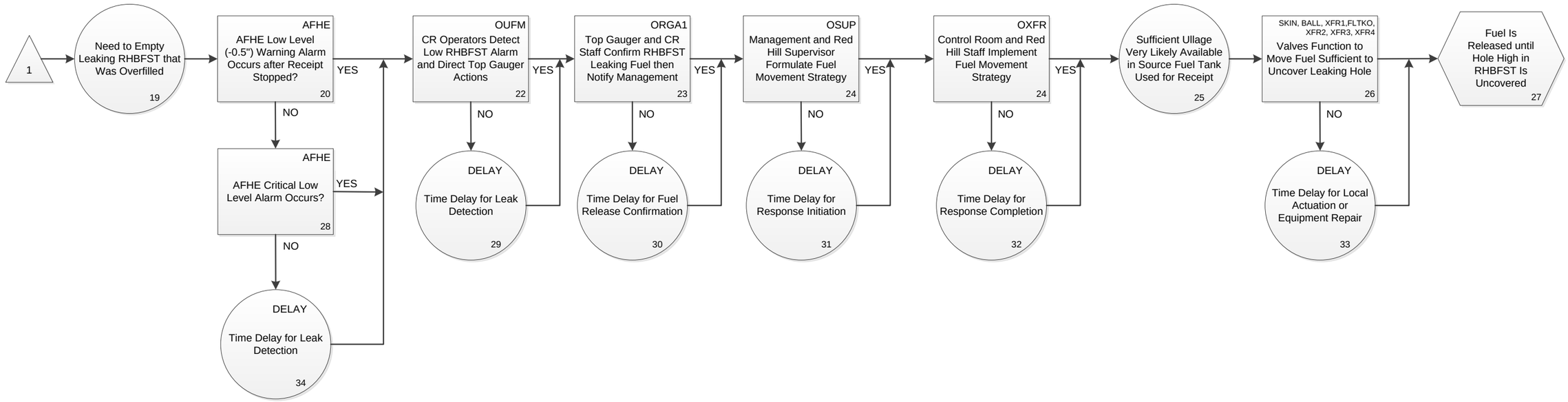



**Figure 6-5. Event Sequence Diagram for Leaks Resulting from Overfilling a RHBFST (2 of 2)**

Sheet 1 of the ESD begins assuming that a RHBFST is being raised to its maximum operating level in preparation for its annual leak tightness testing. Fuel is being received to raise the fuel level. It is assumed that the final stages of this receiving fuel is being performed using the cargo pumps to add fuel from down below the UGPH. The fuel movement planned to complete the RHBFST filling process may have been in error or the control room operators may have simply neglected to stop the fuel evolution as planned. This failure to halt the filling is unlikely because the source tank operator will also be monitoring the level draw down in his tank and alert the fuels department that too much fuel is being transferred.

Given the filling continues above the maximum operating level, the ESD questions whether there is a through hole in the RHBFST liner above the maximum operating level. If not, the sequence is ended with no release of fuel. There is also a large ventilation hole at the top of the upper dome in each RHBFST. However, overfilling by the amount of fuel needed to reach this level at the peak of the upper dome is judged not credible. It would require an extra 6,500 barrels to reach the upper dome opening, above the inventory needed to raise the level to 212' where the hole is postulated to be located. At roughly 2,500 barrels per hour this would mean the overfilling, above the planned stopping level, would have to last for more than 2 hours.

At a fuel level of 221.9', more than 10' above the planned fuel level to stop at (for RHBFST 15 settings used as representative values), a high-high level alarm probe would be sounded in the control room. The control room operators could use the emergency stop or panic buttons to trip the cargo pumps and close off the RHBFST being overfilled. If the overfilling continued, a high-high level alarm mechanical switch located inside the RHBFST would be actuated. This switch signals the RHBFST skin valve to close and the cargo pumps to be tripped, either of which terminates the receipt before the fuel level reaches 224.6'; i.e., at a fuel level still more than 15' below the top of the upper dome.

The ESD further questions whether the skin or ball valves close to terminate the overfilling. Tripping of the cargo pumps alone would end the receipt, but no credit is taken for this trip. This is conservative, but not overly so because the skin and ball valves are redundant and highly reliable.

Once the overfilling is ended, the ESD transfers to Sheet 2. The model postulates that the hole above the maximum operating level is just barely above it, at 212'. Therefore the fuel above 212' starts leaking while the overfilling continues during the time it takes to detect the later drop in fuel level after the overfilling ends, and then also during the time it takes to empty the RHBFST to a level below the postulated hole location.

Sheet 2 of the ESD considers the response of the AFHE low level warning alarm after tank settling and a decrease in level of 0.5". This would be the first automatic cue to the control room operators that there not only was an overfilling, but that as a result, leakage from the RHBFST was occurring. As with any fuel movement, after a 2-hour period of RHBFST settling, the top gauger would be tasked to top gauge the affected RHBFST even before the low level warning alarm. Once the leak is confirmed, the sequence of actions and events in the ESD is similar to that illustrated in Section 6.6.1 for direct leaks to rock.

Similar to the presentation in Section 6.6.1, once a leak is confirmed, management and the Red Hill supervisor are notified of the situation. The Red Hill supervisor is then tasked with making a strategy for a response and to notify the Red Hill staff of his strategy. Typically, and for this ESD, the response involves a strategy for moving fuel from the leaking RHBFST. This mostly involves opening the skin and ball valves of the, then idle, RHBFST and directing the fuel to other tanks which have ullage; i.e., at Red Hill or down below. The Red Hill staff must then manually manipulate sufficient valves and possibly cargo pumps to implement the strategy. The idea is not to isolate the leak, but to move fuel from the leaking RHBFST before it has a chance to leak to rock. Delays at any step along the way can postpone the response allowing additional fuel time to leak to rock. Once the leak and fuel movement draw down RHBFST fuel levels below the leaking hole, further leakage to rock ends.

One difference from the direct leaks to rock category of initiating events is that for RHBFST overfilling it is very likely that there is sufficient ullage for moving fuel to since a tank source was just used to fill the now overfilled RHBFST. Further, to stop the leak by uncovering the postulated hole requires only a small portion of the total RHBFST inventory to be offloaded.

The amount of fuel leaked out is then a function of many variables including: the leakage flow rate, the initial fuel level, the height of the hole through which the leak occurs, the time at which fuel is then being moved from the RHBFST, the rate it is emptied, and the time delays experienced during the response.

The last stochastic event in Sheet 1 of the ESD is actually a variety of actions and fuel movements that may be chosen or are necessary to effect the RHBFST being emptied. Additional details expanding the logic of this one event are presented in Sheet 2 of the ESD for direct leaks to rock and are presented in Section 6.6.1.

See Section 7 for a discussion of success criteria for each top event called out along the events in the ESD.

### 6.6.3 Event Sequence Diagrams for Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST

The ESD for unisolable leaks from the LAT fuel line piping connecting directly to a RHBFST is presented in Figure 6-6. Such leaks can also be thought of as nozzle leaks. Here the term nozzle refers to the short section of pipe exiting from the lower dome and ending at the RHBFST's skin valve. External leakage from the skin valve is also considered as contributing to the nozzle leak frequency since it too cannot be isolated by closing the skin valve. The ESD for nozzle leaks to the LAT was developed based on the facility operational guidance provided by Red Hill standard operating procedures and based on responses to questions posed to Red Hill operations staff.

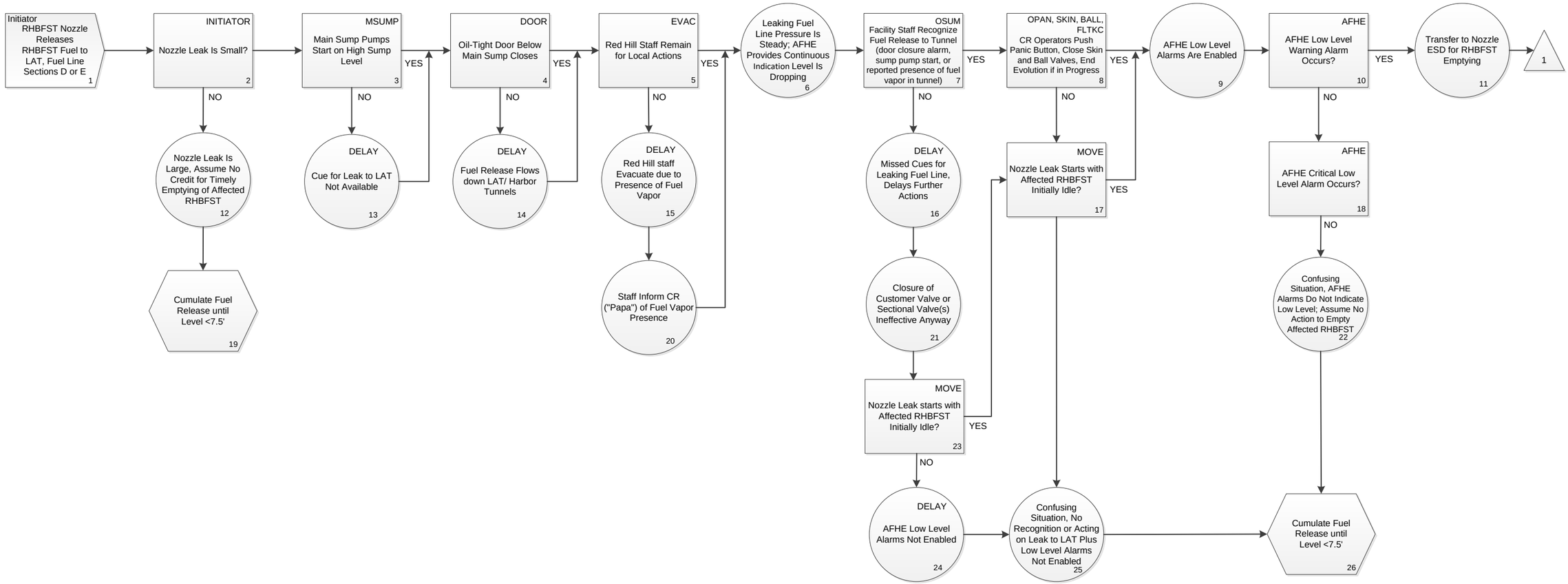



**Figure 6-6. Event Sequence Diagram for Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST (1 of 2)**

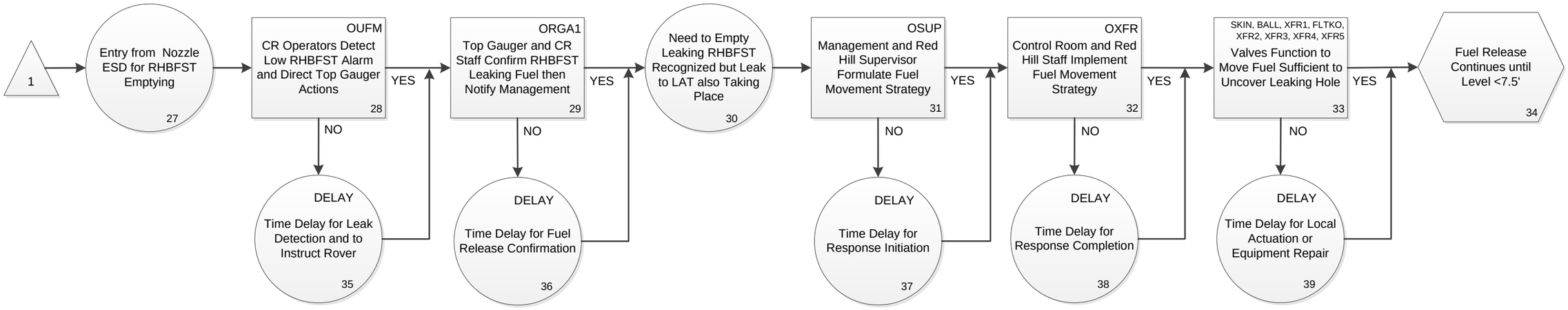



**Figure 6-6. Event Sequence Diagram for Unisolable Leaks from the LAT Fuel Line Piping Connecting Directly to a RHBFST (2 of 2)**

Sheet 1 of the ESD first questions whether the nozzle leak flow is small (equivalent to a 0.5" diameter hole) or is large (equivalent to a 6" diameter hole or larger). If the nozzle leak is large, no credit is given for mitigating the release of fuel from the affected RHBFST.

If the nozzle leak is small, the ESD considers credit for detecting the leakage within the LAT, ending any initially active fuel movement, detecting the subsequent drop in RHBFST level, and then emptying the affected RHBFST. The methods for detecting the leakage to the LAT include: detecting the start of the main sump pumps as fuel travels to and fills the sump to a high level, the closure of the new oil-tight door, and the detected presence of fuel vapor in the LAT by the staff present there. Once the staff in the LAT detects the fuel presence, it is assumed they would evacuate. After evacuation, or before if there is time, it is expected that the Red Hill staff evacuated would report back to the control room what had occurred.

Once leakage is detected and the control room operators are notified, the ESD questions whether they would actuate the panic button and close the affected ball valve. Only if the nozzle leak occurs with the affected RHBFST initially idle and the operators push the panic button on the affected RHBFST, is credit then taken for detecting the drop in RHBFST fuel level via the AFHE low level warning alarm. If the AFHE system does not operate, then no further actions are credited and the affected RHBFST will drain to the 7.5' when the leak stops.

Sheet 2 of the ESD considers the response of the AFHE low level warning alarm and a decrease in level of 0.5". With the Red Hill staff having evacuated from the LAT, and likely the UAT, the ability to confirm the low level AFHE alarm by top gauging may be problematical. Some delay time is expected, but the control room should be able to recognize both the fuel presence in the LAT and the dropping level in an initially idle RHBFST and conclude what needs to be done. They are, after some delay, expected to then notify management and the supervisor for instructions. The sequence of actions and events in the ESD is then similar to that illustrated in ESD of Section 6.6.1 for direct leaks to rock.

Similar to the presentation in Section 6.6.1, once a leak is confirmed, management and the Red Hill supervisor are notified of the situation. The Red Hill supervisor is then tasked with making a strategy for a response and to notify the Red Hill staff of his strategy. Typically, and for this ESD, the response involves a strategy for moving fuel from the leaking RHBFST. This mostly involves opening the skin and ball valves of the affected RHBFST and directing the fuel to other tanks which have ullage; i.e., at Red Hill or down below. The Red Hill staff must then manually manipulate sufficient valves and possibly cargo pumps to implement the strategy. The idea is to move fuel from the affected RHBFST before it releases large portions of its contents to the LAT. Delays at any step along the way can postpone the response allowing additional time for fuel to leak to rock. Once the leak and fuel movement draw down RHBFST fuel levels below 7.5', further leakage to the LAT ends.

One difference from the direct leaks to rock category of initiating events is that, for nozzle leaks, the same path using for moving fuel to empty the RHBFST is also known to be leaking or at least suspected to be leaking. A second difference, is that with the

LAT evacuated, all valve manipulations must be performed remotely, as is usual, but without local confirmation of their positions.

The amount of fuel leaked out is then a function of many variables, including the initial leakage flow rate, the initial fuel level, the time at which fuel is then being moved from the RHBFST, the rate it is emptied, and the time delays experienced during the response.

The last stochastic event in Sheet 1 of the ESD in Figure 6-6 is actually a variety of actions and fuel movements that may be chosen or are necessary to effect the RHBFST being emptied. Additional details expanding the logic of this one event are presented in Sheet 2 of the ESD for direct leaks to rock and are presented in Section 6.6.1.

See Section 7 for a discussion of success criteria for each top event called out along the events in the ESD.

### 6.6.4 Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel

The ESD for isolable leaks from fuel line piping to the LAT or Harbor Tunnel is presented in Figure 6-7. When describing them as isolable, it is meant that any initially aligned RHBFST can be isolated from the leak location by closing its skin or ball valve. It does not mean that the leakage of fuel from the fuel line will necessarily be ended immediately. In addition to any aligned RHBFST, there are also sectional valves and locations along each of the three main fuel lines, so a break along any fuel line can most likely be isolated from above. Closure of the sectional valve(s) upstream of the leak will limit the release of fuel by gravity. If a fuel receipt is in progress at the time the leak initiates with pumping from the UGPH, then leakage from below the hole would also be ended as soon as the operating cargo pumps are tripped.

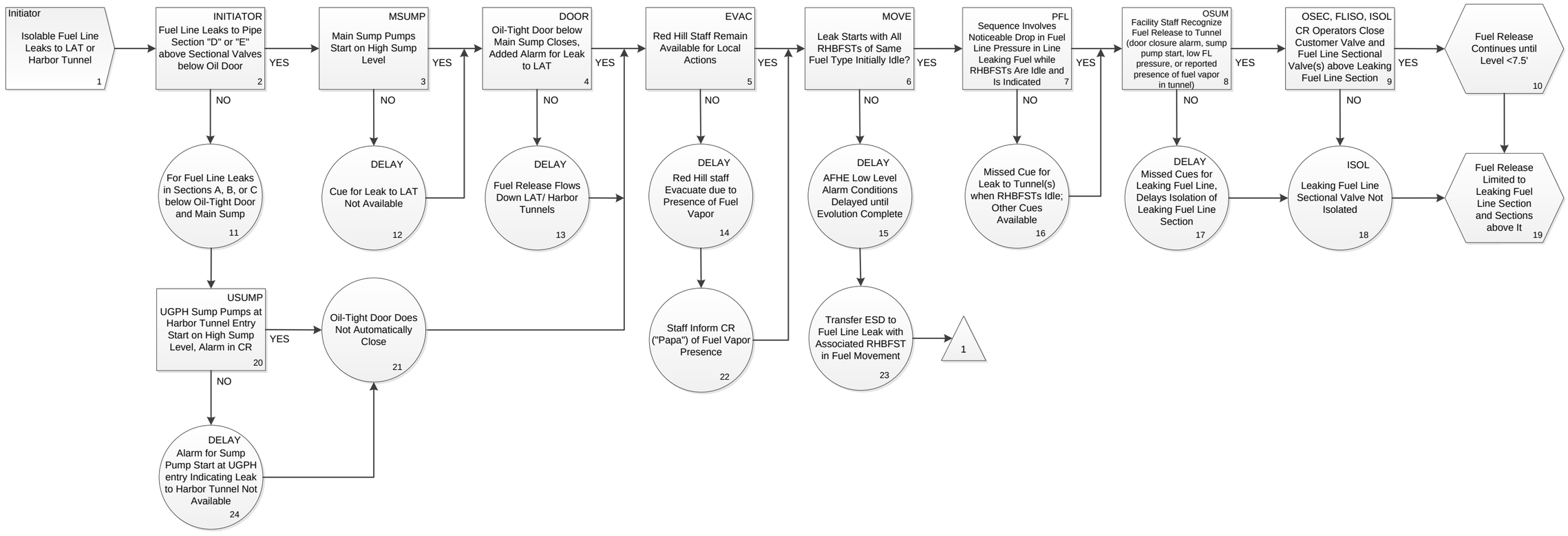



**Figure 6-7. Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel (1 of 3)**

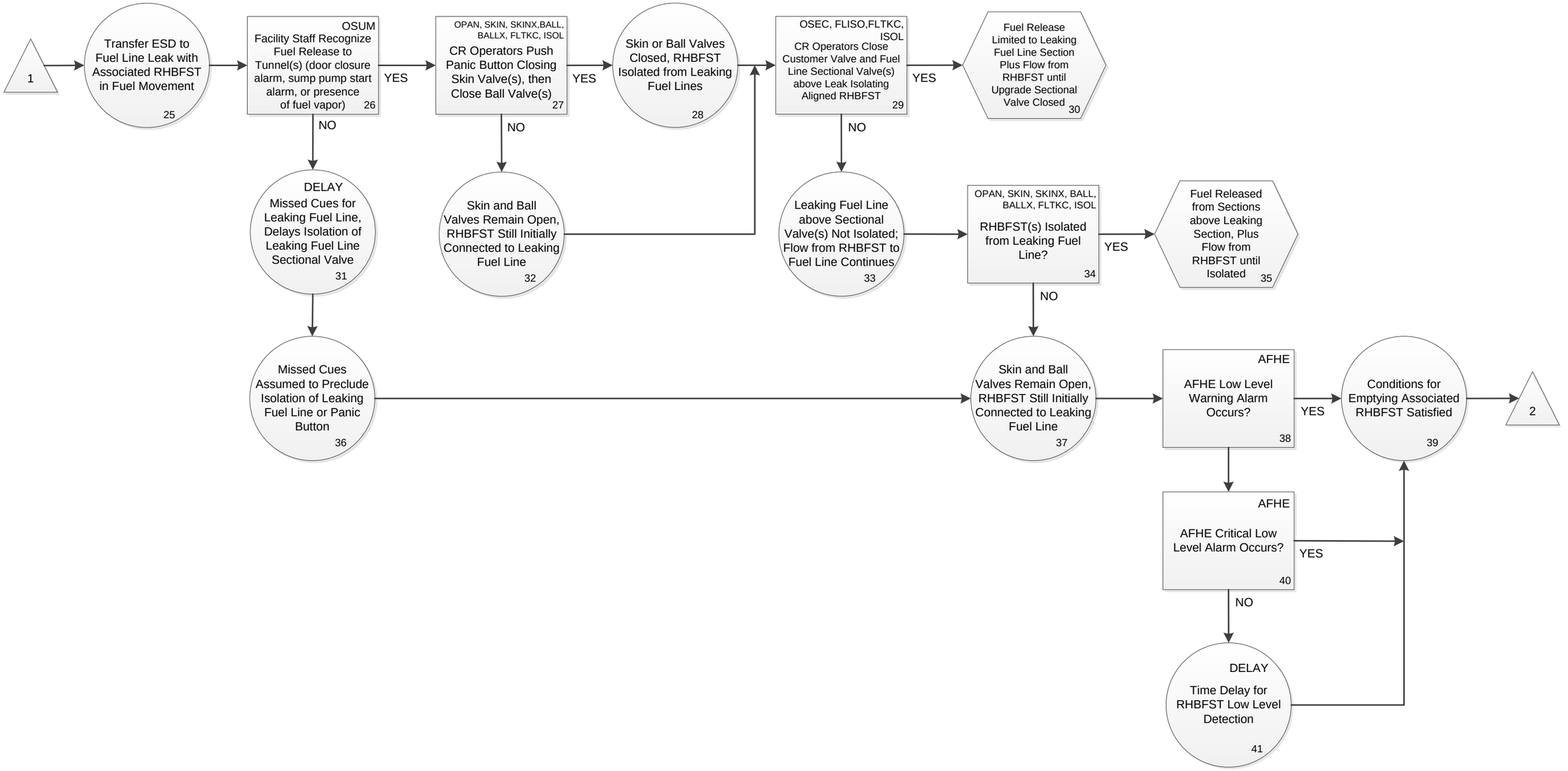



**Figure 6-7. Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel (2 of 3)**

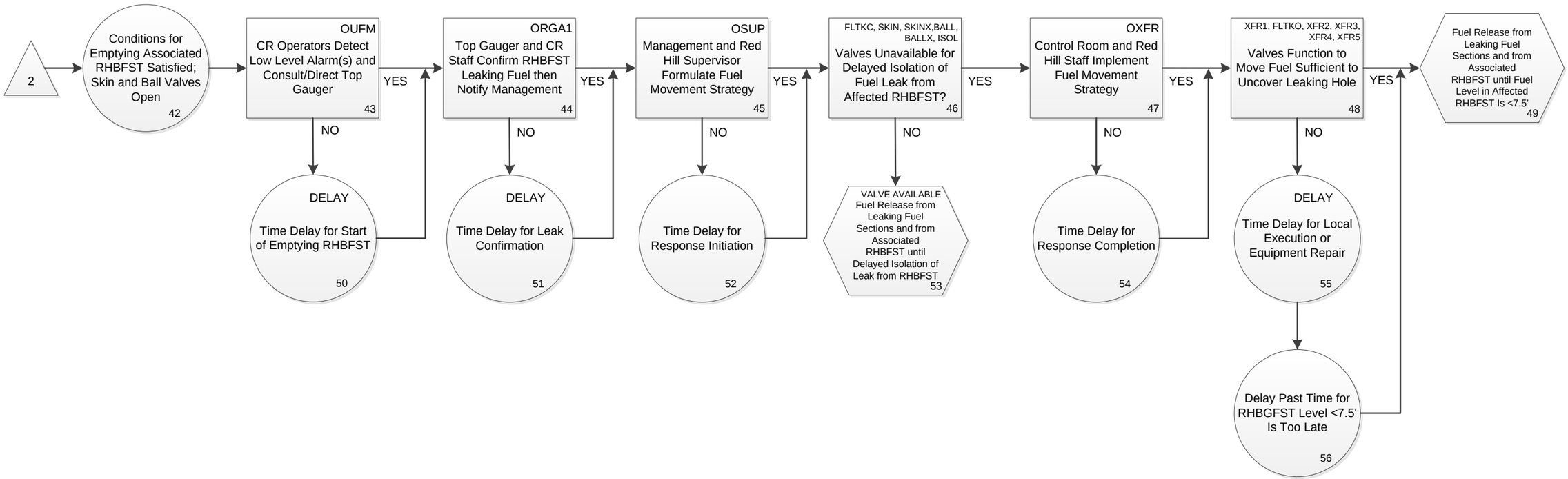



**Figure 6-7. Event Sequence Diagram for Isolable Leaks from Fuel Line Piping to the LAT or Harbor Tunnel (3 of 3)**

The ESD for isolable leaks to the LAT was developed based on the facility operational guidance provided by Red Hill standard operating procedures and based on responses to questions posed to Red Hill fuel operations staff.

Sheet 1 of the ESD first questions which section of the fuel lines the leak is located. If in Sections D or E (see Figure 6-3), the leak location is within the tank gallery and above the new oil tight door. Leaks located in Sections A, B, or C are below the new oil-tight door. The significance of the leak location is that it defines the cues available to the control room operators. In Sections D or E, the main sump pumps located below the tank gallery, but upstream of the oil tight door, should start on high sump level and the new oil tight door should close when its sump float senses the rise in fuel level.

For leaks in Sections A, B, or C, the new oil tight door would not close, at least initially, because the fuel released would instead flow downgrade. If the leak is located in Section C above the normally closed fan door, then a backup of released fuel above that door may occur that is sufficient to cause the new oil tight door to close. Even in this case, however, the new oil-tight door closure would have little impact on the fuel released from the hole location. Fuel released from a leak in Sections A, B, or C would flow downgrade and eventually end up in the large sump at the entry to the UGPH. There a high sump level alarm would notify the control room operators of the leak.

If a fuel line leak to the LAT or to the Harbor Tunnel occurs, the smell of fuel vapor is expected to be substantial and very noticeable, at least for leaks located in the tank gallery. Therefore, there is a good likelihood that any Red Hill staff located at Red Hill at the time of the leak would evacuate and notify the control room that a leak has occurred. Worker safety rules require the evacuation, which means the Red Hill staff would be unavailable initially to assist the control room team locally. Leaks to the Harbor Tunnel may not result in fuel vapors being detected at Red Hill. The ventilation flows are directed up the stack at 3Y and physically barred from entering the LAT by normally closed ventilation doors. However, some of the ventilation flow from Harbor Tunnel is directed in the UGPH and may be quickly detected by the staff present there or in the control room. Further, the LAT ventilation is also downgrade to the ventilation stack at 3Y; i.e., away from the tank gallery portion of the LAT.

The ESD also questions whether there is a fuel movement in progress at the time of the leak. If instead all RHBFSTs of the same fuel type are idle (i.e., not aligned, there skin and ball valves are already closed), then leakage from the fuel line piping alone is the only concern. For sequences with the RHBFSTs idle, leakage from the fuel line at any leak location would be indicated in the control room as a drop in fuel line pressure. Then there are two paths to follow. If the control room operators successfully close the upgrade sectional valve, then leakage will be limited to the leaking section plus what is leaked prior to the closure. If the control room operators do not close the sectional valve, then the fuel line inventory above the leak location would all be released.

For leak sequences which occur when a fuel movement is in progress (i.e., issue, receipt or inter-tank transfer) the ESD notes that the AFHE low level warning alarm would be disabled until the fuel movement is ended. The question concerning low fuel line pressure is bypassed because it would likely not be evident during a fuel movement. The ESD then transfers the logic flow to Sheet 2 for leak sequences starting when there is a fuel movement.

The need for the control room operators to recognize cues available and conclude there is a leak is then questioned. If not diagnosed initially, there could be a substantial delay time before action is taken, though eventually recognition of the leak is expected. The response should be to both push the panic button to end the fuel movement and close the aligned RHBFST's skin valve, follow that with closure of the ball valve, and to close the upgrade sectional valve on the leaking fuel. If the aligned RHBFST is isolated from the leaking fuel line, then the fuel release should be limited to the amount of fuel initially in the fuel line plus the amount leaked out prior to isolation. If the RHBFST is not isolated but the upgrade sectional valve is closed, the RHBFST may or may not be isolated from the hole in the leaking fuel line, depending on the segment leaking and the relative position of the RHBFST to the leak location and the upgrade sectional valve. For leaks in Sections A, B, or C, closure of the sectional valve alone would also isolate the aligned RHBFST from the fuel line leak location.

Without isolation of the initially aligned RHBFST, there would not be an AFHE low level warning alarm as a further cue to alert the operators to a fuel line leak. Additional time delay is expected, though eventually the AFHE should provide ample level indication that level in the RHBFST has fallen, indicating a leak is in progress.

Sheet 3 of the ESD considers the response to a low level indication in the still aligned RHBFST. With the Red Hill staff having evacuated from the LAT, and likely the UAT, the ability to confirm the low level AFHE alarm by top gauging may be problematical. Some delay time is expected, but the control room should be able to recognize both the fuel presence in the LAT and the dropping level in an initially aligned RHBFST and conclude that management and the Red Hill supervisor need to be contacted. They are, after some delay, expected to then notify management and the supervisor for instructions.

If the control room staff have not yet hit the panic button or otherwise signaled the aligned RHBFST's skin valve to close, it's expected that the supervisor would direct them to do so. The sequence of actions and events in the ESD is then similar to that illustrated in ESD of Section 6.6.1 for direct leaks to rock.

One difference from the direct leaks to rock category of initiating events is that for leaks from a fuel line into the LAT, the same path to be used for moving fuel to empty the RHBFST is also known to be leaking or at least suspected so. A second difference is that with the LAT evacuated, all valve manipulations must be performed remotely, as is usual, but without local confirmation of their positions. Further, the leak fall in RHBFST fuel level would continue until it is drained to the 7.5' and the remaining fuel would remain in the RHBFST.

The amount of fuel leaked out is then a function of many variables including: the initial leakage flow rate, the initial fuel level, the time at which fuel is then being moved from the RHBFST, the rate it is emptied, and the time delays experienced during the response.

The last stochastic event in Sheet 1 of the ESD in Figure 6-6 is actually a variety of actions and fuel movements that may be chosen or are necessary to effect the RHBFST being emptied. Additional details expanding the logic of this last stochastic event are presented in Sheet 2 of the ESD for direct leaks to rock; i.e., in Section 6.6.1.

See Section 7 for a discussion of success criteria for each top event called out along the events in the ESD.

## 6.7 Event Tree Models

Event trees are used to convert the ESDs into a form suitable for accident sequence frequency quantification. This section presents the event trees that are linked together to form an entire sequence path through the QRVA event sequence model. These event trees are developed using the information from the initiating event groupings, the system dependency tables, the ESDs, and Red Hill facility operating practices and training.

Figure 6-8 illustrates how the different event trees are linked together to form an entire accident sequence. The accident sequences start with an initiating event from one of the four categories of events. The individual initiating events are listed in Table 6-2.

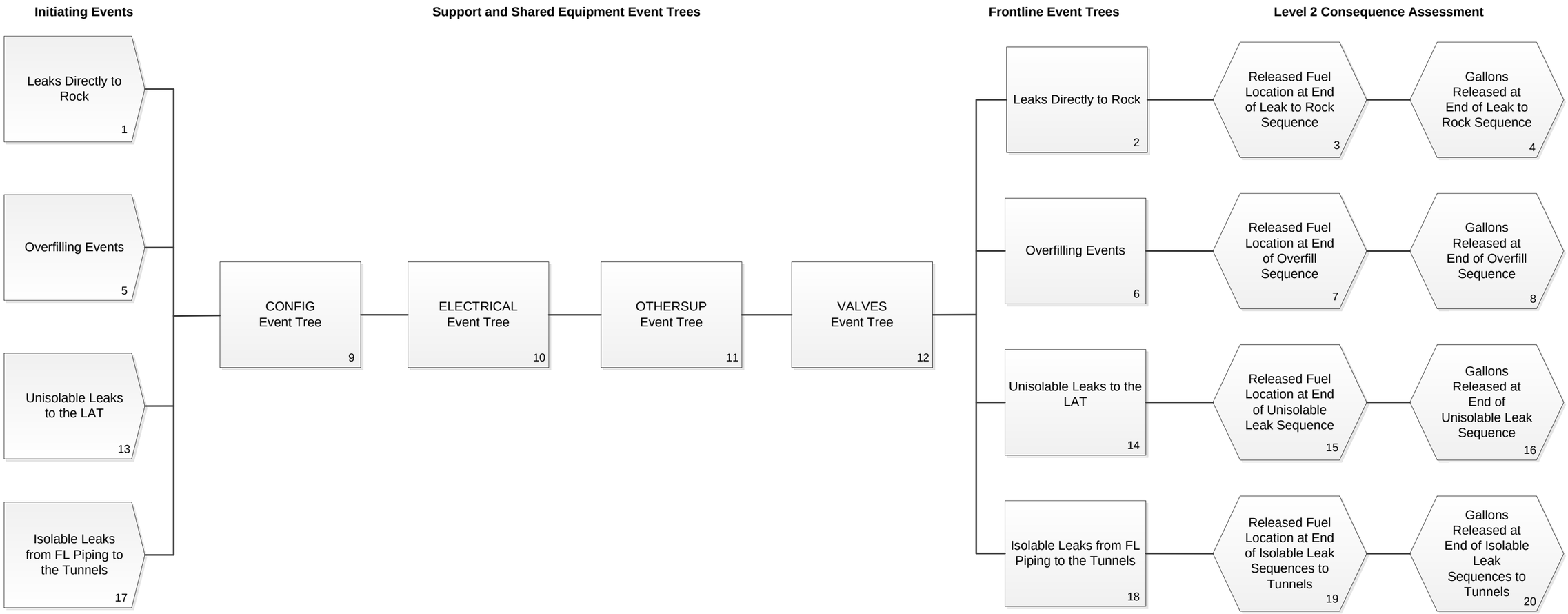



**Figure 6-8. Linking of Event Trees to Form an Entire Acute Sequence**

Then there are four event trees which are common to all of the QRVA accident sequences; i.e., CONFIG, ELECTRICAL, OTHERSUP, and VALVES. These common event trees represent the plant initial configuration at the time of the initiating event, the status of electrical systems which support equipment needed for accident detection and mitigation, other support systems which support accident detection and mitigation responses and often depend on electrical systems, and the status of key valves used for isolation and to direct fuel movements needed for accident mitigation. Equipment shared between different frontline system functions are included in these common event trees. These common event trees also contain top events which are simple switches that track the status of key sequence information (e.g., the fuel type involved) or impacts (e.g., whether evacuation from the tunnels is assumed) so as to make it easier to understand the detailed representations of each individual sequence.

Next, one of the four frontline event trees is linked at the end of the common event trees. The specific frontline tree used depends solely on the initiating event category which begins the accident sequence; i.e., a one-to-one correspondence. It is the frontline event trees which largely correspond to the stochastic events called out in the ESDs. Once the linked event trees are quantified, the frequency per calendar year of each path through the linked events is known.

In Figure 6-8, the Level 2 consequence assessment is also tracked for each individual sequence. For each sequence one of several scenarios is assigned indicating the ultimate location of released fuel for that sequence. These ultimate locations depend on the initial fuel release location, specifics about the sequence of events, and in some cases on the amount of fuel released. These ultimate fuel locations are tracked via the specific split fraction assigned to Top Event REL in each of the four frontline events. These fuel location scenarios are discussed further in Section 10.

Finally in Figure 6-8, the last set of boxes involves the assignment of end states to each accident sequence. The total gallons of fuel released from the initial leak location is chosen as the end state measure. These fuel released amounts are assigned as a single end state to each sequence. The logic used for assigning the end states is dependent on the specific sequence path. The computation of the gallons released and the logic used to assign the end states is documented in Section 6.8.

The event trees identified in Figure 6-8 are presented in the following subsections. Details about each top event are presented in Section 7.

### 6.7.1 Configuration Event Tree

The CONFIG event tree, as its name implies, describes the status of the different modes of operation of the Red Hill facility that may be on going at the time of an initiating event. The configuration tree also identifies the specific RHBFST that is associated with a specific leak location. In this approach, initiating events that have the same frequency for all RHBFSTs can be represented as one initiator but then duplicated for all RHBFSTs in service. Alternatively, an initiating event applicable to just one RHBFST can be accommodated by zeroing out the frequency of paths that would have involved other RHBFSTs. For the QRVA, when a class of fuel release is applicable to all RHBFSTs, a separate initiating event was defined for each RHBFST.

The status of the following top events in the configuration event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the configuration event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| LKLOC | Location of Leak within Facility |
| MOVE | Type of Fuel Movement Initially in Progress |
| TKID | RHBFST Associated with Leak |
| FUEL | Type of Leaking Fuel |
| TKXF | Source RHBFST Associated with Inter-Tank Transfer |
| TKLOC | LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT |
| HEIGHT | Height of Hole in RHBFST that is Leaking to Rock |
| SIZE | Size of Leak from RHBFST, or Fuel Line Piping |
| DIREC | Side of RHBFST that Leak Is On |
| INVEN | INVEN – Initial RHBFST Inventory Configuration. |

- LKLOC – Location of Leak within Facility (nine states)
- MOVE – Type of fuel movement initially in progress (four states)
- TKID – RHBFST Identifier Associated with the Leak (21 states)
- FUEL – Type of Leaking Fuel (four states)
- TKXF – Source RHBFST Associated with Inter-Tank Transfer (21 states)
- TKLOC – LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT (three states)
- HEIGHT – Height of Hole in RHBFST that Is Leaking (five states)
- SIZE – Size of Leak from RHBFST, or Fuel Line Piping (five states)
- DIREC – Side of RHBFST that Leak Is On (five states)
- INVEN – Initial RHBFST Inventory Configuration (11 states)

The CONFIG event tree is presented in Figure 6-9. The CONFIG event tree is a “branch everywhere” tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting

systems. Often top events have a state named NA, for use if a state of the top event does not apply for the sequence.

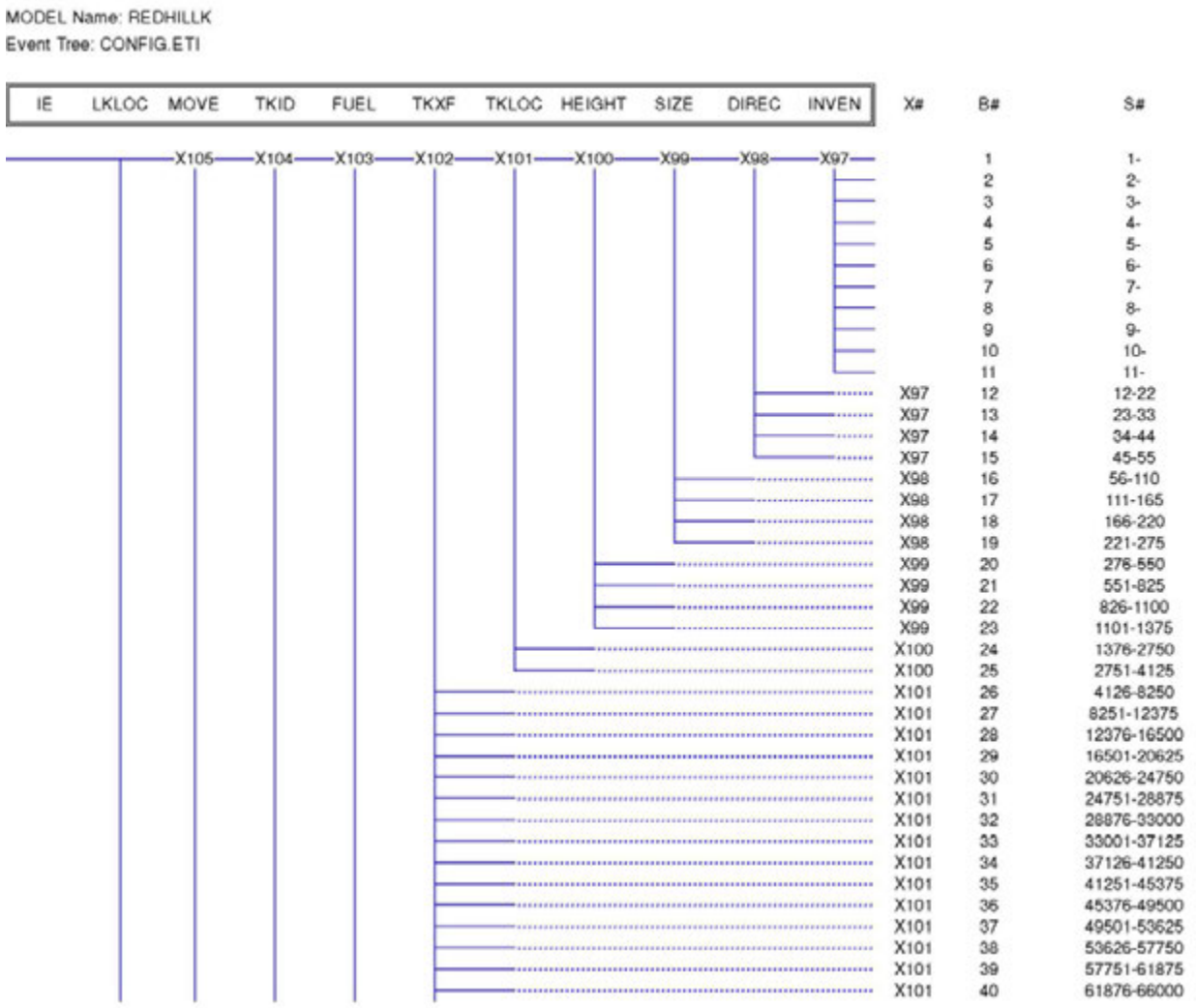



**Figure 6-9. CONFIG Event Tree Structure**

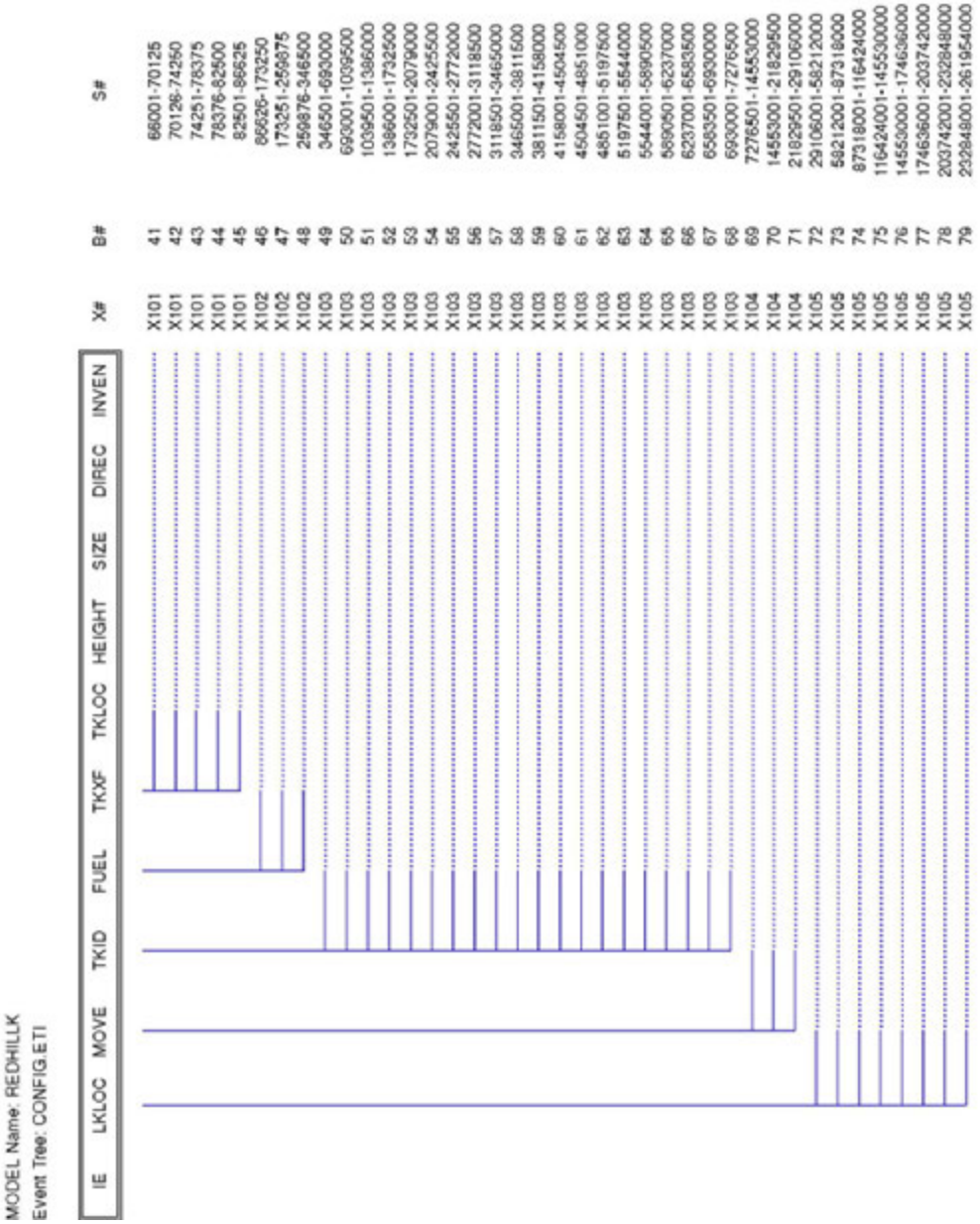



**Figure 6-9. CONFIG Event Tree Structure (Continued)**

### 6.7.2 ELECTRICAL Event Tree

The status of the following top events in the ELECTRICAL event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the ELECTRICAL event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| GRID | Offsite Grid |
| GRIDR | Recovery from Losses of Offsite Grid |
| BUN24 | UGPH 2.4kV Normal Bus |
| BUN48 | UGPH 480V Normal Bus |
| BUE48 | UGPH 480V Emergency Bus |
| GEN1 | Backup Generator at ADIT for UGPH 480V Emergency Bus |
| UFAN | ADIT 1 Supply and Exhaust Fans for UGPH cooling Cargo Pumps |
| B3EA | ADIT 3 208V Panel A |
| GEN3 | Backup Generator at ADIT 3 for 480V Panels B and A |
| BRN48 | Red Hill 480V Normal Bus |
| BRE48 | Red Hill 480V Emergency Bus |
| GEN5 | Backup Generator for Red Hill 480V Emergency Bus |
| LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras |
| AFHE | Automatic Fuel Handling Equipment |
| AFHR | AFHE Condensing and Fans for Heat Removal |
| EFAN | Fans for Tanks 1–16 in LAT & UAT Fail to Operate (also supply electrical room in LAT |
| TFAN | Fans for Tanks 17–20 LAT & UAT Fail to Operate (above bulkhead) |

The ELECTRICAL event tree is presented in Figure 6-10. The ELECTRICAL event tree is a “branch everywhere” tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. The only multi-state top event in this even tree is top event GRIDR, which has five states. GRIDR represents the different recovery times for random losses of offsite power; i.e., not induced by external events.

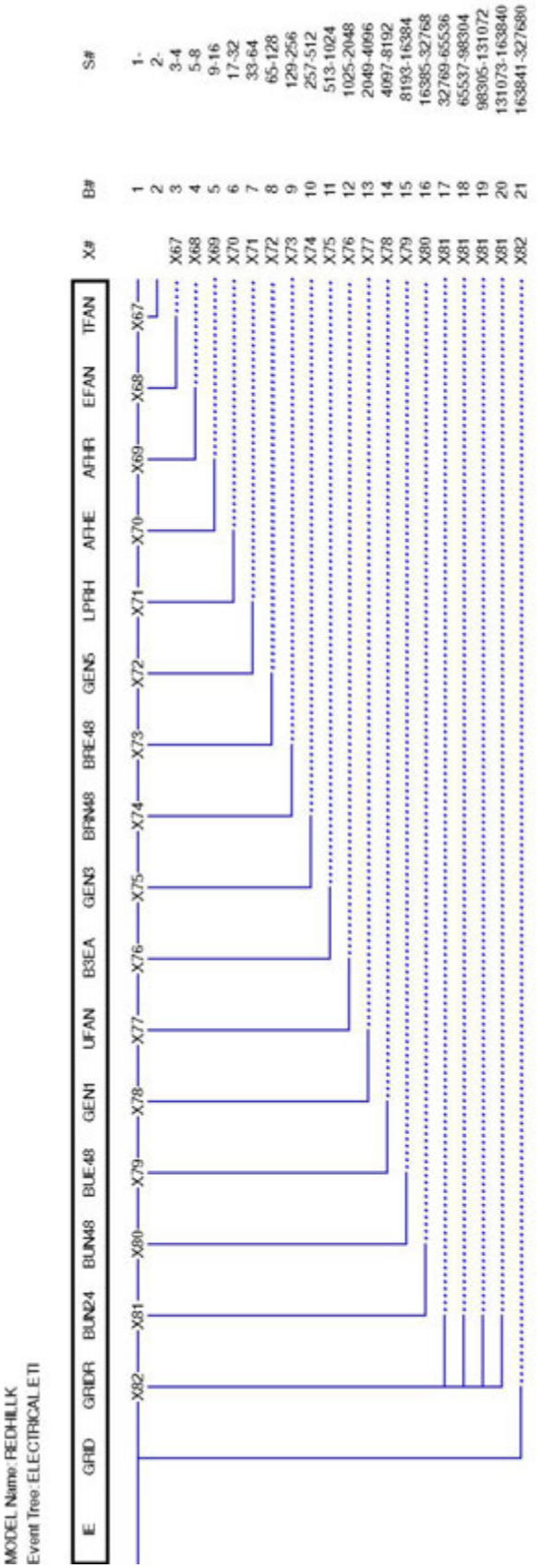



**Figure 6-10. ELECTRICAL Event Tree Structure**

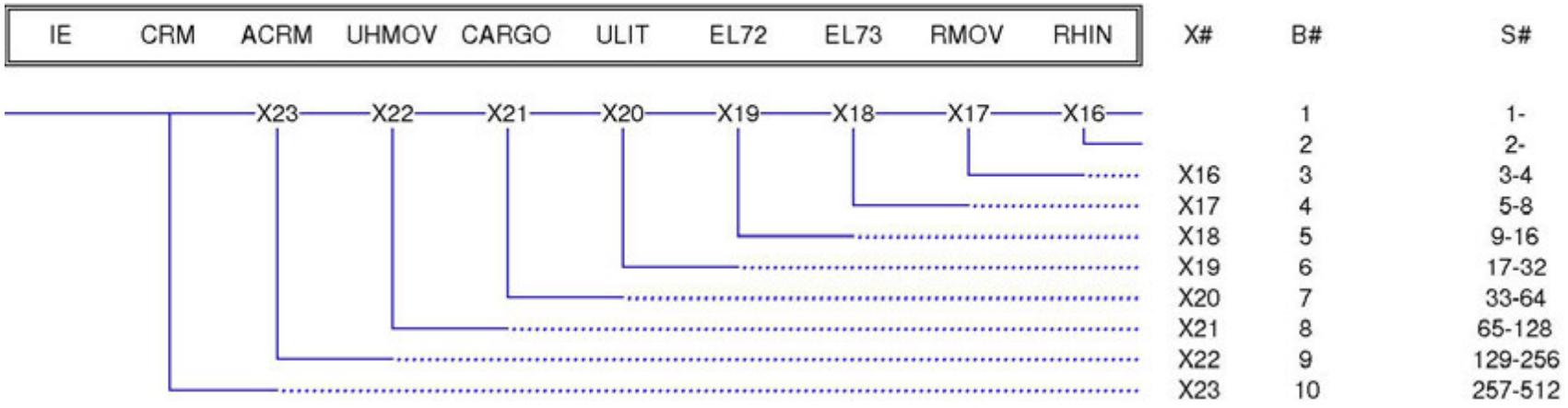
### 6.7.3 OTHERSUP Event Tree

The status of the following top events in the OTHERSUP event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the OTHERSUP event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| CRM | Control Room Electrical Power, Lighting, and Air Conditioning |
| ACRM | Alternate Control Room Electrical Power, Lighting, and Air Conditioning |
| UHMOV | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs |
| CARGO | Two or More Cargo Pumps Available to Move Leaking Fuel Type |
| ULIT | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting |
| EL72 | Personnel Elevator 72 & Controller |
| EL73 | Cargo Elevator 73 & Controller |
| RMOV | Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and all LAT MOVs |
| RHIN | Support for Red Hill Instruments, Indications, Level Alarms, and Signals |

The OTHERSUP event tree is presented in Figure 6-11. The OTHERSUP event tree is a “branch everywhere” tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. There are no multi-state top events in this event tree.

MODEL Name: REDHILLK
Event Tree: OTHERSUP.ETI




| X# | B# | S# |
|---|---|---|
| | 1 | 1- |
| | 2 | 2- |
| X16 | 3 | 3-4 |
| X17 | 4 | 5-8 |
| X18 | 5 | 9-16 |
| X19 | 6 | 17-32 |
| X20 | 7 | 33-64 |
| X21 | 8 | 65-128 |
| X22 | 9 | 129-256 |
| X23 | 10 | 257-512 |

**Figure 6-11. OTHERSUP Event Tree Structure**

### 6.7.4 VALVES Event Tree

The status of the following top events in the VALVES event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the VALVES event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| SKIN | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree |
| BALL | Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree |
| SKINX | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree |
| BALLX | BALLX - Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree |
| FLISO | FLISO – Successful Closure of the Upstream Sectional Valve |
| FLTKC | FLTKC – Successful Isolation of the Fuel Line Leak from All ALIGNED RHBFSTs |
| FLTKO | FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied |
| EVAC | Sequence Conditions Necessitate Initial Evacuation from RH |

The VALVES event tree is presented in Figure 6-12. The VALVES event tree is a "branch everywhere" tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. There are no multi-state top events in this event tree.

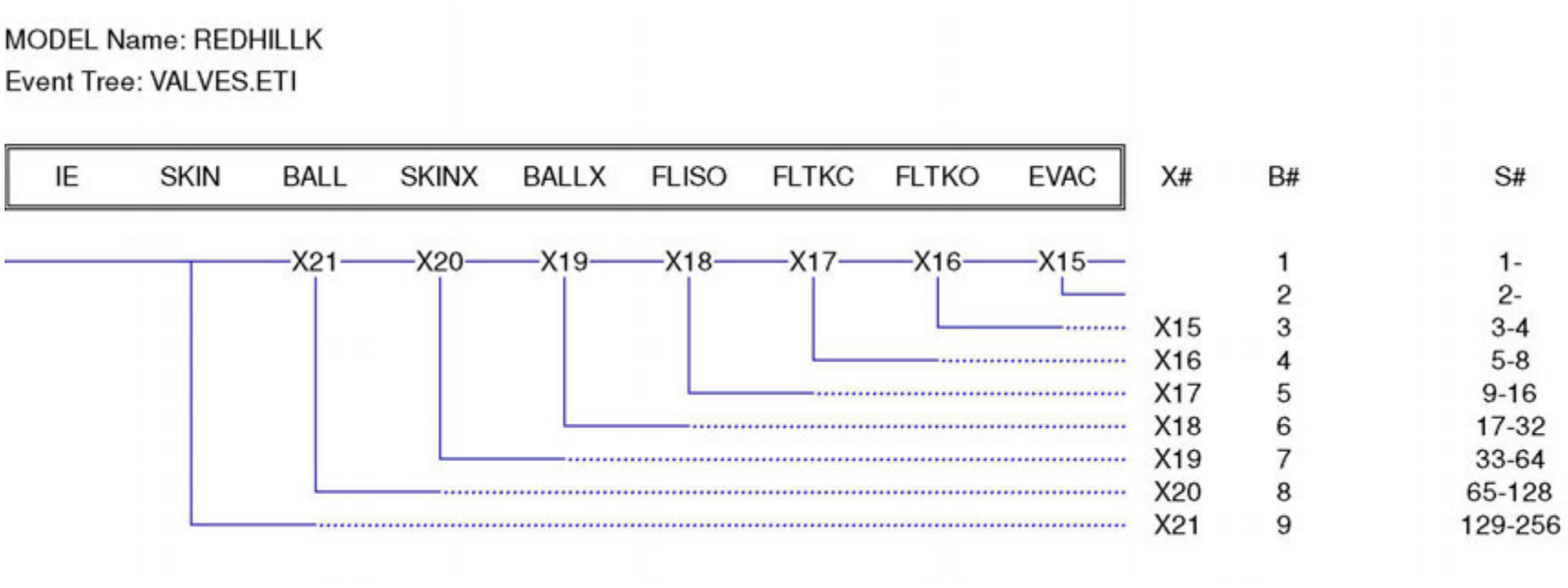



**Figure 6-12. VALVES Event Tree Structure**

### 6.7.5 Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock

The actions and equipment response events represented as top events in the TKLEAK event tree correspond to the associated event sequence diagram presented in Figure 6-4 of Section 6.6.1. One category of initiating events is a small leak through the RHBFST liner to the surrounding rock while the tank is idle; i.e., with its skin and ball valves closed. A leak of 1.5 gpm is first considered. Such a leak rate is at the upper end of the range of leak rates previously experienced at Red Hill. This flow rate is sufficient to drop the RHBFST level by 8/16" in about 27 hours. The AFHE system provides an automatic low level warning alarm when the RHBFST level drops by 8/16". A second low level critical alarm also sounds when the level change is greater than 12/16"; i.e., in about 41 hours for the postulated 1.5 gpm leak rate. For larger leaks, such as for a hole size equivalent to a 0.5" diameter hole at the bottom of a RHBFST fueled to its maximum operating level, the leakage rate would be large enough to reach these two alarm setpoints in just 0.6 hours and 0.85 hours, respectively.

If instead, the leaking RHBFST is undergoing a fuel movement at the time of the leak (see Top Event MOVE in the CONFIG event tree), the AFHE system (Top Event AFHE in the ELECTRICAL event tree) would not provide a low level warning or low level critical alarm while the fuel movement is in progress. Not until the fuel movement is over would such alarms be enabled. For a period of 2.5 hours after the fuel movement is over, the AFHE low level alarms are enabled but with alarm setpoints twice as high as the RHBFST idle setpoints. Temperature changes are one aspect of concern requiring a level settling period. After 2.5 hours, the dynamic setpoints are reset to static conditions. Therefore, the AFHE leakage detection time is lengthened for leaks initiated while a fuel movement is in progress. The durations of fuel movements (as tracked in Top Event DELAY) varies by the type of fuel movement (i.e., issuing, receiving, inter-tank transfers as tracked by Top Event MOVE in the CONFIG event tree) and by fuel type; i.e., F24, F76, or JP5 as tracked by Top Event FUE in the CONFIG event tree. Once the fuel movement is secured, the response to the leak is otherwise the same as for initially tank idle conditions.

In response to either of these two alarms, the control room operators are tasked by the UFM alarm response procedure to direct the top gauger to check that the skin and ball valves on the associated RHBFST are indeed fully shut and to manually gauge the RHBFST. There is no need to evacuate the LAT (unless ventilation also fails) since no fuel has been spilled to the LAT. The top gauger would perform these actions and report back to the control room. If the reduction in RHBFST level is confirmed then the control room operators would contact the Fuel Department Supervisor for further instructions. The supervisor would seek additional facility information and decide the best strategy to empty the leaking tank. There are different methods for moving fuel from a leaking RHBFST depending on the available ullage for the leaking fuel type. The supervisor would formulate a strategy which the entire Red Hill facility staff would then carry out as directed by the supervisor. The time to empty the leaking RHBFST depends on the specific strategies for moving fuel and the initial height of the leaking RHBFST. Until the RHBFST fuel level is lowered below the level of the leak, leakage would continue although at lower flow rates as the head from the fuel level is lowered.

The status of the following top events in the TKLEAK event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the TKLEAK

event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak |
| ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm |
| OSUP | Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST |
| OXFR | Control Room and Red Hill Staff Follow Strategy & Move Fuel from the Leaking RHBFST |
| XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST |
| XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor |
| XFR3 | Two-step Fuel Movement to Pump Fuel to Other RHBFSTs |
| XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor |
| XFR5 | Fuel Movement to Empty Bottom 7.5' of Lower Dome Using RHBFST Lower Drain Line |
| DELAY | Tank Empty Delay Time Based on Earlier Failures |
| REL | REL – Type of Fuel Release Scenario |

For modeling purposes, once initiated, a fuel movement rate of 2,500 barrels per hour is assumed. The fuel movement approaches represented by Top Events XFR1, XFR2, and XFR4 would likely be capable of moving fuel at a faster rate. The 2,500 barrels per hour is typical of a fuel movement rate for approach XFR3, which represents the pumping of fuel using cargo pumps to other RHBFSTs. Approach XFR3 offers the greatest flexibility as it takes advantage of the ullage in all other RHBFSTs of the same fuel type. During the 2014 RHBFST 5 leakage incident, the approaches represented by Top Events XFR1 and XFR3 were used sequentially. It is assumed that for the fuel movements needed to empty a RHBFST, the RHBFSTs receiving fuel would not be filled above the maximum normal operating level; i.e., approximately 212'. Depending on the effected fuel type and initial plant configuration, lower initial fuel levels are also possible.

The availability of places to move fuel to (i.e., ullage), is an important concern when emptying a RHBFST which may initially hold up to 300,000 barrels of fuel. Reviews of tank inventory data from early 2017 indicate that there is ample ullage for the F24 and JP5 fuel types. However, for F76 fuel, there are only two RHBFSTs which hold F76 and they are typically well over half full, so finding other ullage to completely empty an F76 RHBFST is necessary. Upper Tank Farm inventory data reviewed also indicates that there is likely to be a limit on the available ullage for each type of fuel there. Therefore, the QRVA model assumes that there would be a 2-week delay in finding sufficient ullage to empty one of the two RHBFSTs that hold F76. An exception to this assumption is for sequences involving a return to service. For leaks detected during a return to service, available ullage is assumed sufficient since the source tanks used for filling the affected

RHBFST should have available ullage to accept the same amount of F76 fuel they have just issued.

Top Event XFR5 represents the draining of the bottom 7.5' of the RHBFST's lower dome. The fuel line exit piping sticks up into the RHBFST approximately 7.5'. Therefore, the fuel below it may not be moved using any of the other approaches. Instead, a connection is made to the bottom of the RHBFST and the last 1,500 barrels of fuel are removed by gravity via the main fuel lines down to the UGPH. There it can be transported by trucks to Fuel Oil Reclamation Facility (FORFAC).

The TKLEAK event tree is presented in Figure 6-13. The TKLEAK event tree is a "branch everywhere" tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. The only multi-state top event in this event tree is for Top Event DELAY, representing alternate delay times for initiating the actions to move fuel from the leaking RHBFST.

MODEL Name: REDHILLK
Event Tree: TKLEAK.ETI

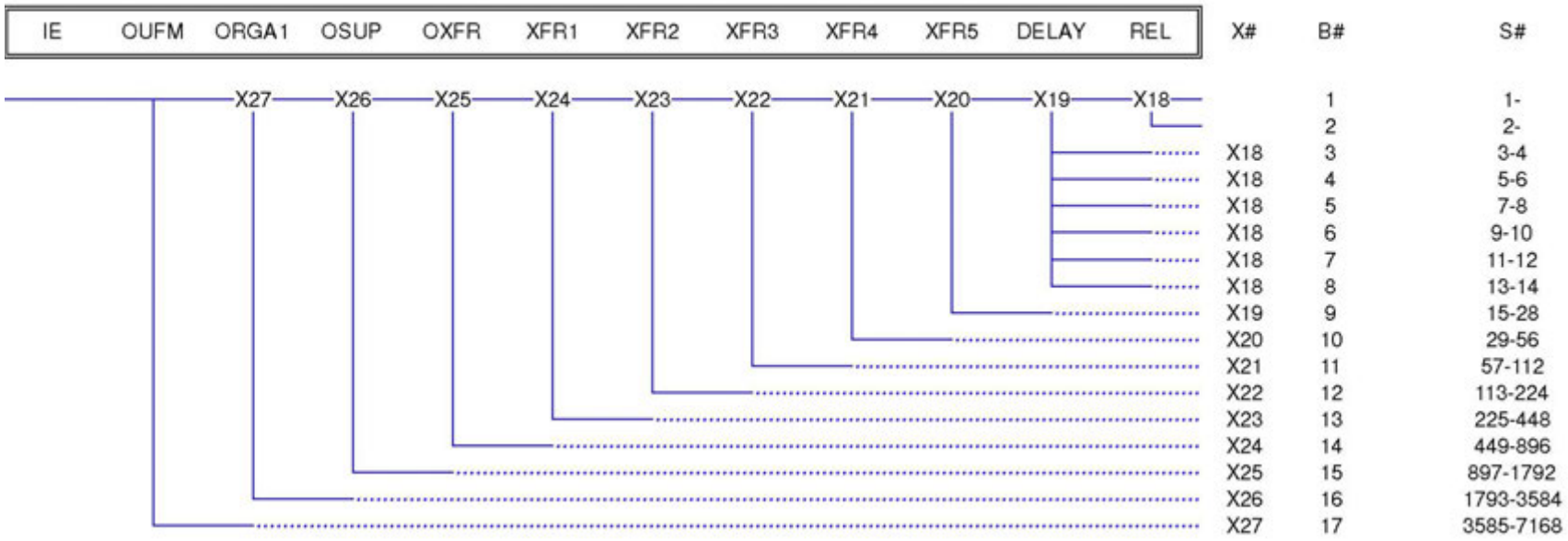



**Figure 6-13. TKLEAK Event Tree Structure; for Direct Leaks to Rock**

### 6.7.6 Frontline Event Tree 2 – OVERFILL Event Tree

The actions and equipment response events represented as top events in the OVERFILL event tree correspond to the associated event sequence diagram presented in Figure 6-5 of Section 6.6.2. One category of initiating events results from the refilling of a RHBFST to its maximum normal operating level; e.g., in preparation for an annual leak tightness level. Such a RHBFST refilling is assumed to occur once a year. The fuel movement planned to complete the RHBFST filling process may have been in error or the control room operators may have simply neglected to stop the fuel evolution as planned. This failure to halt the filling is unlikely because the source tank operator will also be monitoring the level draw down in his tank and alert the fuels department that too much fuel is being transferred. If filling is incorrectly allowed to continue, and fuel levels above the annual leak tightness level from prior years are reached, then fuel leakage could occur via a hole above that level. Holes occurring at the leak tightness level are not detected by those annual tests. Once overfilled, fuel leakage through the postulated hole could occur through the RHBFST liner to the surrounding rock.

Unlike direct leaks to rock (see Section 6.7.5), the OVERFILL initiators account for four periods of recovery:

1. At time zero when successful pre-evolution operator planning prevents the overfill, or there is no hole.

2. When the high-high level alarm probe cues the operators to halt the filling process by pushing the panic button.

3. When the mechanical float switch automatically trips the cargo pumps and sends a signal to close the RHBFST's skin valve.

4. When the fuel evolution finishes having added more fuel than is necessary and exhausts the source tank used for the filling.

An opening equivalent to a 0.5" diameter hole is assumed in the QRVA, and further, the undetected hole is conservatively assumed to be located just above 212', or approximately right above the annual leak tightness level. Fuel leakage then occurs as soon as this level is reached and the flow rate increases as the overfilling continues to raise in level. It is noted that for operational reasons, not all RHBFSTs are tested at approximately 212' every year; some are tested at lower fuel levels. However, over 2 or 3 years of tests, all RHBFST are tested at approximately 212'. RHBFST 15 was tested at 210.82' in 2015 and at 210.7' in 2013, before the annual test frequency was implemented.

Inter-tank transfer by gravity is assumed not used as the method to transfer fuel from the source tank for these events. The difference in base elevations of RHBFSTs holding F24 is at most 4'. For RHBFSTs holding F76, they are at the same base elevations. However, for RHBFSTs holding JP5, the maximum base elevation difference is 28'; e.g., between RHBFSTs 8 and 20. Therefore, the absolute maximum that such an inter-RHBFST transfer could overfill, assuming both the RHBFSTs are initially at 212' to begin with, is just 14'; i.e., to 226'. But such a fuel movement would not occur unless the

receiving RHBFST was less than 212'. Typically the initial fuel level in the receiving RHBFST would be much less than this and the amount of overfilling is limited.

Leakage flow rates through the previously undetected hole are determined by the extent of overfilling. Based on Red ill facility fuel movement data from early 2017, an average filling rate of 2,080 barrels per hour is assumed. Typically this filling rate would be decreased as the fuel evolution is about to end. An assumed fill rate of 2,080 barrels per hour is much larger than the leakage flow, for any amount of overfill. Therefore, the leakage could not be detected until the fuel movement to fill the RHBFST is eventually stopped. The cargo pumps are assumed being used to transfer fuel from tank sources below the UGPH (e.g., the upper tank farm) to the receiving RHBFST.

It is unlikely that such an overfilling would occur because there is careful planning before each fuel evolution is begun, and there are limits on the amount of fuel available at the source tank. In addition to the control room crew, staff is positioned at the source tank to ensure that more than the planned amount of fuel is not transferred.

A carefully defined high operating limit (HOL) for each RHBFST is set by adherence to API 653 criteria. For most RHBFSTs (i.e., RHBFSTs 5 through 20), this HOL is set at approximately 10' above the annual leak tightness level (i.e., 221.78' for RHBFST 15), though its height is not based on that test level. For the shorter RHBFSTs (RHBFSTs 2 through 4), the HOL is set about 2' above the annual leak tightness test level. The settings described in the following are specifically for RHBFST 15 and are assumed similar for all other tall RHBFSTs, which is most of them. A high-high level alarm probe is then set 2" higher than the HOL; i.e., at 221.94' for RHBFST 15). If level increases above the high-high level, an alarm is indicated in the control room. The AFHE high-high level alarm probe directly cues the operators to the overfilling condition, even though the operators previously failed to terminate the fuel movement manually as planned.

In response to the high-high level alarm probe, the control room operators would be tasked to push the panic button; i.e., Top Event OTRIP. For OTRIP, it is assumed that the probability for failure to act is the controlling probability but that the skin or ball valve must close to terminate the filling. Stopping the cargo pumps is also a way to end the receipt, but is not credited since it would not be effective if the filling was accomplished by an inter-RHBFST transfer.

A high-high level alarm mechanical float switch is set at about 1'10.5" above the high-high alarm level probe setting; i.e., 223.82'. This switch setting allows plenty of time for terminating the filling process before tank level can reach 95% of the current tank overfill level (i.e., at 224.58' less than the overfill level of 250.07' for RHBFST 15, or about 238' for the shorter RHBFSTs), even if filling was being carried out at the maximum rate (8,300 barrels per hour); i.e., the mechanical float switch settings is selected to terminate the filling before tank level reaches the 95% of the current overfill level, or at approximately 224'6".

The mechanical float switch not only detects the higher fuel level, but also automatically sends a signal to the affected RHBFST's skin valve to close and to the cargo pumps of that fuel type to trip. These signals are independent of the AFHE system. This automatic action takes just a few minutes to accomplish, but a delay period is used to

allow time for the operators to manually take action. Either closing the skin valve or tripping the cargo pumps, if they were being used, would halt the filling fuel evolution.

If the control room operators fail to respond to the AFHE high-high level alarm probe and the mechanical float actuation trip fail, then no additional credit for the operators revisiting these alarms is credited. In that case the leakage is governed by the filling ending when the available source of fuel is depleted. There is a limit on the amount of fuel that can be physically transferred from the source tank to the receiving RHBFST.

This is roughly the same as the excess 22,000 barrels assumed as limiting. This argument makes it hard to see how overfilling can be great enough to overflow the top of the dome at 250'. Only from a ship or refinery would there be enough fuel supply and those sources would be closely monitored to track the amounts supplied and paid for. Top Event XFR1 represents the method of fuel movement involving inter-RHBFST transfers by gravity. The method represented by XFR1 can be used to fill or empty, but due to minimal elevation differences, it is not a source that could lead to overfilling sufficiently to overflow the top of the tank dome.

A review of operating records indicates that typical receiving evolutions average about 44,500 barrels per receipt. It is conservatively assumed that half of this typical amount of fuel transferred if erroneously planned, may be in excess of the fuel volume needed to raise levels in the RHBFST to its annual leak tightness level of 212'. With this assumption, the maximum overfill is limited to 22,500 barrels that could conceivably be added above the annual leak tightness level, above which holes developed in the liner would not be detectable. This volume of fuel corresponds to an additional 16' of level in the RHBFST above the annual leak tightness test level; i.e., to 226.85'. This is also a way to estimate the receiving time of the period of overfilling from 212' to 226.85'; i.e., 22,500/2080 = 10.8 hours.

From 226.85' the initial leak rate through the hole is 18.93 gpm. The low level alarm (drop of 0.5") would be reached in about 2.4 hours and the critical low level alarm (drop of .75") in 3.5 hours. The dynamic low level alarm is set at a drop of 1" for the first 2.5 hours. The leak would not cause levels to drop 1" until 4.8 hours. Therefore, it is assumed that the dynamic low level alarm would be reset at 2.5 hours to the static alarm setpoint of 0.5" and require another 2.4 hours before there is another 0.5" drop actuating the static alarm; i.e., at a total of 4.92 hours from the time filling is ended. Assuming 6 hours from the time of the alarm to initiate an evolution to empty the RHBFST, this start of emptying would occur at 10.9 hours after the fill is ended. Similar but longer delay times would apply if the operators stop the leak at lower fuel levels.

Fuel leakage through the postulated hole would continue for as long as the RHBFST level is above the modeled location of the hole. The leakage rate increases as the overfilling progresses to the peak fuel level of 228'. Even if the mechanical float switch fails and the operators have not intervened by that time, it is assumed there is no more fuel to be transferred to the receiving tank. An overfilling by 22,500 barrels would take more than 10 hours from the time the fuel level reaches the annual leak tightness test level.

Once the filling (or receipt) is halted, the RHBFST level would drop due to the continued fuel leakage until the AFHE low level alarm is reached. The dynamic low level warning

alarm is set at a drop of 1" and is active for the first 2.5 hours after the receipt is terminated while the fuel settles out. After 2.5 hours, the low level warning alarm setpoint is reset to a level drop of 0.5". Given the AFHE low level alarm, the Red Hill Rover would be tasked to manually top gauge the affected RHBFST. The low level critical alarm would also provide an indication of the leak in progress.

Given an AFHE low level warning or critical alarm, the operators are tasked by procedures to confirm the readings of the AFHE by performing one or more top gauges manually. The operators are also tasked to perform a manual top gauge within 2 hours every time after a fuel movement ends. If the AFHE system is working, both that system and confirmation by the top gauger at Red Hill that there is decreasing fuel level in the RHBFST is needed to confirm the leak is in progress.

Once the leakage is confirmed, Red Hill staff would be tasked to drain fuel from the affected RHBFST to stop the leak. It is assumed that it would take 6 hours from the time of the low level warning alarm to initiate a new fuel evolution to move fuel from the affected RHBFST, thereby lowering the overfilled fuel level. Any of the first four fuel movement approaches described in the first frontline tree discussion (i.e., Section 6.7.5 Top Events XFR1, XFR2, XFR3, and XFR4) would also apply here for overfilling events. Again the fuel offloading rate is assumed to be 2,500 barrels per hour. A key difference is that the amount of fuel that must be moved from the RHBFST subjected to an overfilling with a leak, would be less since fuel level only needs to drop below the postulated hole location at roughly 212'. Calculations show that if no action was taken to empty the receiving RHBFST, the fuel above the 0.5" diameter hole would then all leak to rock over a period of 65 days.

The same approaches to move fuel would also apply if the overfilling is halted at much lower fuel levels. One key difference is that the undetected hole size is assumed to be larger, on the order of 0.5" in diameter as indicated is possible based on past RHBFST inspection records for levels of the RHBFST above the maximum fuel operating levels. A second key difference for this scenario, as compared to other RHBFST liner leaks to rock, is that the driving forces for leakage, and hence the leakage flow rate, would be lower; i.e., the postulated undetected hole is high in the RHBFST. For removal of fuel following an overfill event, it is assumed there is plenty of available ullage to offload the required inventory of fuel needed to uncover the hole and thereby stop the fuel leakage.

The frontline event tree top events for this class of initiating events are described below. They make up the frontline event tree OVERFILL. The availability and reliability of the AFHE system (Top Event AFHE) to provide the AFHE high-high level and low level alarms is already questioned in the ELECTRICAL event tree; i.e., as Top Event AFHE. Top Event SWITCH considers the mechanical float switch which operates automatically and independently from the AFHE system.

The status of the following top events in the OVERFILL event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the OVERFILL event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states they are also defined in Section 7.

| | |
|---|---|
| OEV | Operators Correctly Specify Fill Evolution and Stop Evolution when Planned at Maximum Operating Level |
| HOLE | Conditional Probability of Hole above Maximum Operating Level |
| OTRIP | After AFHE High Level Alarm, Operators Actuate an Emergency Stop of the Cargo Pumps or Press the Panic Button, then Direct the Rover to Locally Ensure the Skin Valve Closed and to Manually Gauge the Same Tank |
| SWITCH | High Level Mechanical FLOAT Switch Actuates Sending Signals to Deactivate All Facility Pumps, Actuate Timer for Valve Closures, and Signals Skin Valve on Affected Tank to Close |
| OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak |
| ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm |
| OSUP | Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST |
| OXFR | Control Room and Red Hill Staff Follow Strategy & Move Fuel from the Leaking RHBFST |
| XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST |
| XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor |
| XFR3 | Two-step Fuel Movement to Pump Fuel to Other RHBFSTs |
| XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor |
| XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line |
| DELAY | Tank Empty Delay Time Based on Earlier Failures |
| REL | REL – Type of Fuel Release Scenario |

The OVERFILL event tree is presented in Figure 6-14. The OVERFILL event tree is nearly a “branch everywhere” tree; that is, nearly every top event is questioned for all of the sequences in the event tree. The exceptions are for the success branches of both the first two top events, OEV and HOLE. The initiating event frequencies for overfills only represent a challenge to overfilling a RHBFST; i.e., the frequency of times per year when an individual RHBFST is having its fuel level raised to nearly the maximum operating level. If the control room operators successfully plan the evolution and stop the fuel movement at the applicable level (i.e., Top Event OEV=S) then no further event tree branching is required because there is no overfill. Similarly, given there is no pre-existing hole above the maximum operating level (i.e., HOLE=S) then there is no fuel release path for the fuel to leak to rock. So again, no further event tree branching is needed. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. The only multi-state top event in this event tree is for Top Event DELAY, representing alternate delay times modeled for initiating the actions to move fuel from the leaking RHBFST.

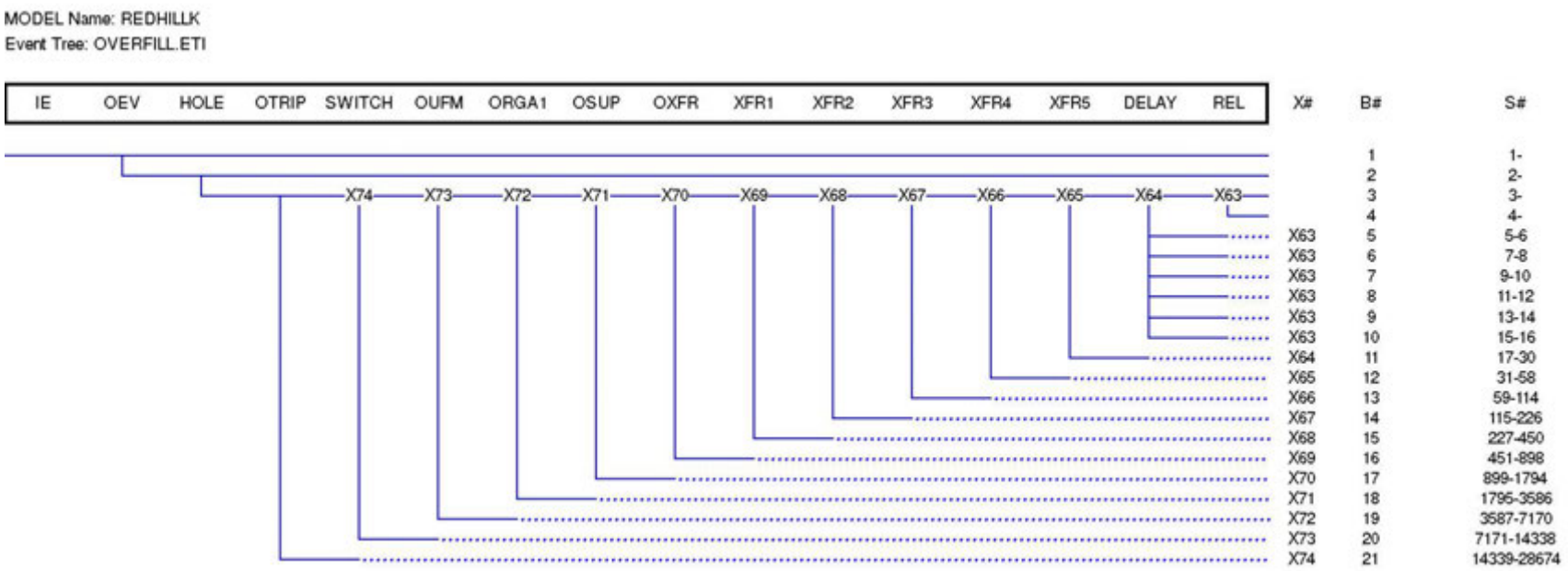



**Figure 6-14. OVERFILL Event Tree Structure; Overfills Resulting in Leaks to Rock**

### 6.7.7 Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT

The actions and equipment response events represented as top events in the NOZZLE event tree correspond to the associated event sequence diagram presented in Figure 6-6 of Section 6.6.3. One category of initiating events involves unisolable leaks to the LAT from the RHBFST nozzle or connecting skin valve. Such leaks cannot be isolated even though the RHBFST's ball valve may be closed. The leakage to the LAT will continue as long as there is fuel in the tank above the 7.5' level. Two hole sizes are postulated corresponding to the external leakage failure rate data for pipes and motor-operated valves. The flow areas for these two hole sizes are assumed equivalent to holes 0.5" and 6" in diameter. The 0.5" hole size represents all leak areas at or below 0.5". The 6" hole size represents all postulated leak sizes greater than 0.5" equivalent diameter holes. If the affected RHBFST has an initial fuel level of 212', these flow areas correspond to roughly 75 gpm and 10,800 gpm initial flow rates respectively. In these estimates, it is recognized that there is an additional 18' of head between the RHBFST bottom and the LAT tunnel floor. Measurements for the distance these pipe segments are below the tunnel roof were not available so the full 18' of added head was conservatively included when estimating these initial flow rates.

A hole size larger than 6" equivalent diameter was not postulated. The most likely cause of a large hole would be mechanical impact from construction work in the LAT, or earth movements which are to be considered separately in later phases of the QRVA. These valves are well separated from the main LAT along the cross-tie tunnels nearest the walls of the RHBFSTs. The fuel line valves and piping, that, if leaking, are unisolable, are located near the roof of the LAT. A 6" hole was postulated as possible (e.g., by an out of control forklift), but larger hole sizes were judged much less likely. Even so, a 6" hole size has such a large flow rate that with no action, an initially full RHBFST would be drained to the 7.5' level in just 28 hours. The 0.5" hole size could reduce level to the low level alarm setpoint in as little as 37 minutes. The 6" hole size would reach the low level alarm setpoint even more quickly, in about 15 seconds.

If instead, the leaking RHBFST is undergoing a fuel movement at the time of the leak (see Top Event MOVE in the CONFIG event tree, a much less likely condition than the RHBFST being idle), the AFHE system would not provide a low level warning, nor low level critical alarm. Not until the fuel movement is over would such alarms be enabled. However, such large flow rates to the LAT from any of RHBFSTs 2 to 16, would fill up the LAT main sump and cause one or both of the main sump pumps (P-0100A/B) to start. Though sump pump start or level is not alarmed in the control room, the sump pumps running are indicated there. It's expected that the control room operators would note the sump pump running indication in short order. LAT tunnel cameras also allow for remote, visual confirmation.

If the main sump pumps below the tank gallery operate to transfer released fuel to Tank S311 outside ADIT3, then the accumulation of fuel in the LAT would be delayed. Half the Tank S311 capacity may, on average, be available as ullage. This corresponds to about 20,000 gallons. At 75 gpm, either main sump pump could keep up the release, but the available ullage would be filled in an estimated 4.4 hours. For 6" hole scenarios, the release rate is much larger and the fuel accumulation would occur quickly (after the

new oil door closes) whether or not the sump pumps operate. If both sump pumps operated, the average ullage in Tank S311 could be filled in less than 45 minutes.

Changes in fuel line pressure are assumed not detectable for this category of unisolable leaks. If the tank is issuing or receiving the head from the RHBFST is still present. If the affected RHBFST is initially idle, the normally closed ball valve isolates the leak location from the fuel line sensed pressure locations.

There is no procedure directing them to do so, but once sump pumps running are indicated, the control room operators may try to isolate the fuel line sectional valves in the tank gallery. The isolation of the sectional valves is judged to have no significant effect on the fuel released from the affected RHBFST. If the decision is later to move fuel from the affected RHBFST, these sectional valves would likely have to be reopened to accomplish that.

For unisolated leaks from RHBFSTs 17, 18, and 20, the leaked fuel would instead first accumulate in the sump above the LAT bulkhead; i.e., in Zone 7. Sump Pump P-0124, would start automatically and this Zone 7 sump pump running would be indicated in the control room. The Zone 7 sump pump transfers fuel to the slop line which also ends up in the main sump below the tank gallery. With the Zone 7 sump pump running, even for the small unisolable leak postulated flow rate of 75 gpm, its capacity is too low to keep up with the fuel released, so fuel level would rise upgrade of the Zone 7 bulkhead. Eventually the spilled fuel level would increase to the known penetrations in the bulkhead above the man-door and additional flow to the tank gallery below would occur. LAT tunnel cameras also allow for remote, visual confirmation above the LAT bulkhead in Zone 7.

For such fuel release rates, the pungent smell of a substantial amount of released fuel would also be noted by the Red Hill Rover and others if present at Red Hill, and they would immediately evacuate Red Hill. Once the fuel movement is secured, either prematurely, or as planned, the response to the unisolable leak is the same as for initially tank idle conditions. The probability of a nozzle leak together with a concurrent fuel movement is very low, but still modeled.

The availability and reliability of the AFHE system to provide the low level warning and critical alarms is already questioned in the OTHERSUP event tree via Top Event AFHE. In response to either of the two AFHE low level alarms, the control room operators are tasked by the UFM alarm response procedure to direct the top gauger to check that the skin and ball valves on the associated RHBFST are indeed fully shut and to manually top gauge the affected RHBFST. For both the small and large unisolable leaks to the LAT as defined, the top gauger and others would likely instead evacuate Red Hill before performing these actions. The Red Hill Rover would be expected to contact the control room before or immediately after evacuation to notify them of the leaking fuel line, or at least of the pungent fuel odor. This notification is assumed sufficient for the control room operators to contact management and the Fuels Department Supervisor for further instructions.

The supervisor would seek additional facility information and decide the best strategy to respond to the situation, likely to begin emptying the leaking tank. There are different methods for moving fuel from a leaking RHBFST depending on the available ullage for

the leaking fuel type. The supervisor would formulate a strategy which the entire Red Hill facility staff would then carry out the strategy directed by the supervisor. The time to empty the leaking RHBFST depends on the specific strategies for moving fuel and the initial height of the leaking RHBFST. Until the RHBFST is emptied below 7.5', leakage would continue, although at lower flow rates as the available head from the fuel level is lowered. The outlet pipe rises inside the RHBFST to about 7.5' above the bottom of the tank. The fuel below this level could not drain out the unisolable leak hole location.

It is assumed that if the affected RHBFST is undergoing a fuel movement at the start of the leak and that the control room operators are unsuccessful at closing the affected RHBFST's skin valve or ball valve, then the conditions are confusing enough to preclude any strategy for emptying the affected RHBFST. The UFM procedures would not apply and the fuel line pressure indications may still read normal from the added RHBFST head. The fuel evolution may not be reset either, although the AFHE system should still indicate dropping fuel levels in the affected RHBFST even though the AFHE low level alarms are not enabled.

For the 0.5" unisolable leak category, a reduction in gallons leaked of as much as 97% can be achieved if fuel transfer to empty the affected RHBFST is started within 6 hours of the AFHE low level warning alarm. For the 6" unisolable leak category, the best that fuel release can be reduced is about 15%, and only if a fuel movement to empty the affected RHBFST is started with no unusual delay; i.e., within 6 hours after the low level warning alarm is received. Therefore, the QRVA assumes no credit emptying the affected RHBFST for the larger, 6" equivalent diameter, unisolable leaks. The only question then of interest for defining where the release fuel ends up, is whether the new oil-tight door closes.

The QRVA assumes that there is initially insufficient ullage to fully empty a RHBFST that holds F76. So for RHBFSTs 15 and 16, even for unisolable 0.5" equivalent diameter holes, a large amount of fuel would be released. An initial fuel movement to drain F76 by gravity to available ullage in tanks at the UTF could remove a portion of the fuel quickly, but this action is not credited in the QRVA.

The status of the following top events in the NOZZLE event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the NOZZLE event tree are summarized below and then described in more detail in Section 7 – Systems Analysis. If a top event has multiple states, they are also defined in Section 7.

| | |
|---|---|
| MSUMP | One of Two Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 |
| DOOR | Oil Tight Door below LAT Gallery Closes on High Float Level |
| OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak |
| OSUM | CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak |
| OPAN | CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button |

| | |
|---|---|
| ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm |
| OSUP | Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST |
| OXFR | Control Room and Red Hill Staff Follow Strategy & Move Fuel from the Leaking RHBFST |
| XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST |
| XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor |
| XFR3 | Two-step Fuel Movement to Pump Fuel to Other RHBFSTs |
| XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor |
| XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line |
| DELAY | Tank Empty Delay Time Based on Earlier Failures |
| REL | REL – Type of Fuel Release Scenario |

The NOZZLE event tree structure is presented in Figure 6-15. The NOZZLE event tree is a “branch everywhere” tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. The only multi-state top event in this event tree is for Top Event DELAY, which represents alternate delay times modeled for initiating the actions to move fuel from the leaking RHBFST.

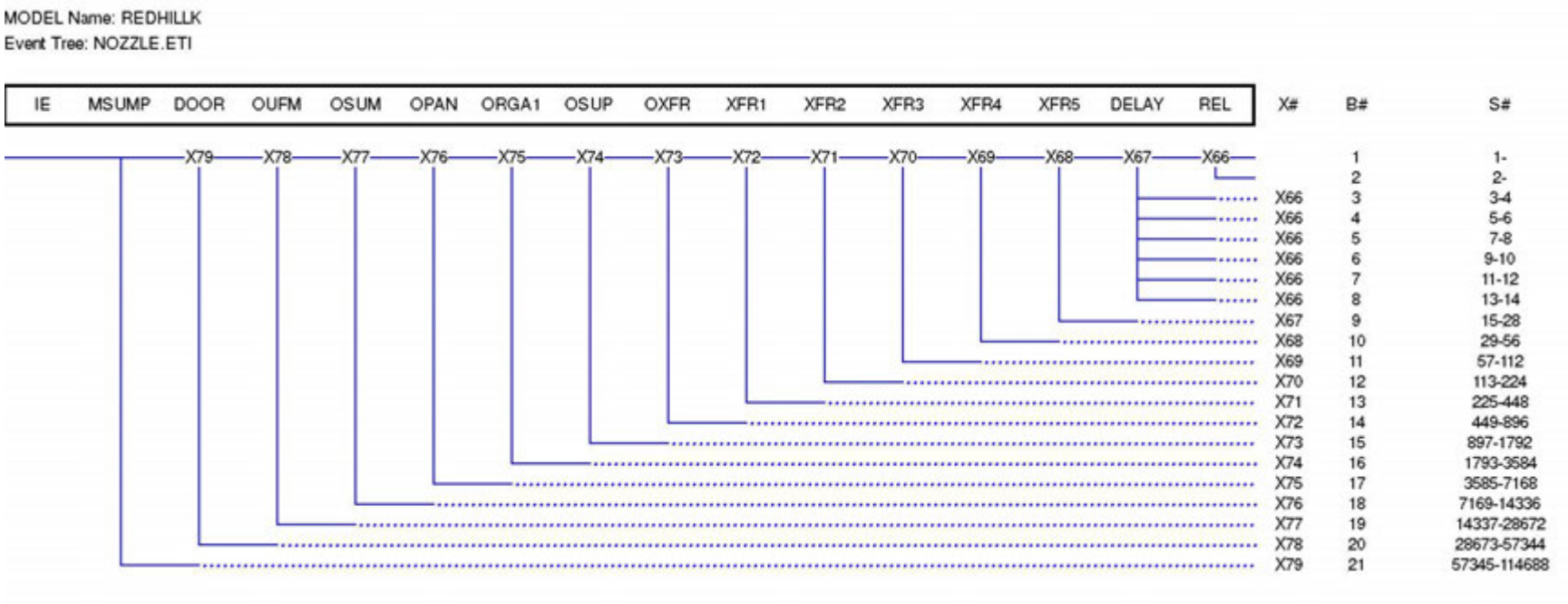



**Figure 6-15. NOZZLE Event Tree Structure; Unisolable Leaks from a RHBFST to the LAT**

### 6.7.8 Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel

The actions and equipment response events represented as top events in the TUNLEAK event tree correspond to the associated event sequence diagram presented in Figure 6-7 of Section 6.6.4. One category of initiating events involves isolable leaks from fuel lines to the LAT or to the Harbor Tunnel. When describing such leaks as isolable, it is also meant that any initially aligned RHBFST can be isolated from the fuel line leak location by closing its skin or ball valve. It does not mean that the fuel leakage from the fuel line will necessarily be ended immediately. In addition to the skin and ball valves of any aligned RHBFST, there are also sectional valves at various locations along each of the three main fuel lines. So a leak along any fuel line can most likely be isolated by closing the sectional valve above the leak location. Closure of the sectional valve upgrade of the leak will limit the release of fuel by gravity from the portions of the fuel line that are above the then closed sectional valve. If a fuel receipt with pumping from the UGPH is in progress at the time the leak initiates, then leakage of fuel below the hole would also be ended when the operating cargo pumps are tripped.

Two hole sizes are postulated for this category of leaks. The flow areas for these two hole sizes are assumed equivalent to holes 0.5" and 6" in diameter. The 0.5" hole size represents all leak areas at or below 0.5". The 6" hole size represents all postulated leak sizes greater than 0.5" equivalent diameter holes. If there is a RHBFST aligned for a fuel movement at the time the leak initiates, and the RHBFST fuel level is at 212', these flow areas correspond to roughly 75 gpm and 10,800 gpm initial flow rates, respectively. For sequence in which the RHBFSTs are idle, the flow rates are less and much more a function of the location of the leak and the head of the fuel in the line above the leak.

There are fuel leak initiating events postulated for each hole size (Top Event SIZE in CONFIG event tree), for each of five fuel line sections (Top Event LKLOC in CONFIG event tree), and for each of the three fuel line types (Top Event FUEL in CONFIG event tree). Figure 6-3 illustrates the different sections on a fuel line piping schematic as distinguished by the QRVA. If in Sections D or E, the leak location is within the tank gallery, and above the new oil tight door. Leaks located in Sections A, B, or C are below the new oil tight door. Sections A and B are in the Harbor Tunnel, while Sections C, D, and E are in the LAT.

For the QRVA model, the leak locations are assumed to be at the midpoint of each section. The choice of the mid-point means that not all fuel may be release from the leaking section, but it also means that there is more time to reach a downgrade sump than if the lowest point in the fuel line section were to be chosen. Because the tunnels grades are very slight, it can take a long time for fuel to flow the nearly 3 miles to the UGPH entry. However, each shift, the Harbor Tunnel is walked to check for such leaks and all other anomalies. The LAT is checked more frequently. Therefore, it is assumed that on average the released fuel would be detected after no longer than 4 hours. Calculations for shorter travel periods are based on the assumption that the entire tunnel floor is covered with the traveling fuel when computing the fuel tunnel velocity. No credit for the LAT drainage trough funneling the leakage to a narrower cross-section and hence speeding up the time to reach the sump. There is no drainage trough below the

main sump and new oil door. The slop line is routed through the drainage trough within the tank gallery portion of the LAT above the main sump.

One significance of the leak location is that it defines the cues that may be available to the control room operators. In Sections D or E, the main sump pumps (Top Event MSUMP in TUNLEAK event tree) located below the tank gallery but upstream of the oil tight door should start on high sump level, and the new oil tight door (Top Event DOOR in TUNLEAK event tree) should close when its sump float senses the rise in sump fuel level. Closure of the new oil door is alarmed in the control room indicating that appreciable liquid has accumulated.

For leaks in Sections A, B, or C, the new oil tight door would not close, at least initially, because the fuel released would instead flow downgrade. If the leak is located in Section C above the normally closed fan door, then a backup of released fuel above that door may occur that is sufficient to cause the new oil tight door to close. In this case, however, the new oil tight door closure would have little impact on the fuel released from the hole location. Fuel released from a leaks in Sections A, B, or C would flow downgrade and eventually end up in the large sump at the entry to the UGPH (Top Event USUMP in TUNLEAK event tree). There a high sump level alarm would notify the control room operators of the released fuel.

A hole size larger than 6" equivalent diameter was not postulated for isolable fuel line leaks. The most likely cause of a large hole would be mechanical impact from construction work in the LAT, or earth movements which are to be considered separately in later phases of the QRVA. The fuel lines are well protected from external impacts in the tunnels. The fuel line valves and piping in the tank gallery are located near the tunnel roof and so protected from most maintenance activity. The fuel lines in Sections A, B, and C are mounted along one side of the tunnels, but there is relatively little activity in these sections with the potential to cause a larger leak. A 6" hole was postulated as possible (e.g., by an out of control fork lift) but larger hole sizes were judged much less likely. The fuel lines in all five sections are readily accessible for inspection.

If all RHBFSTs of the same fuel type are idle (i.e., not aligned, with their skin and ball valves already closed), then leakage from the fuel line piping alone is the only concern. For sequences with the RHBFSTs idle, leakage from the fuel line, at any leak location, would be indicated in the control room as a drop in fuel line pressure (Top Event PFL in TUNLEAK event tree). If the control room operators successfully close the upgrade sectional valve, then leakage will be limited to the leaking section above the leak location, plus what is leaked prior to the closure. If the control room operators do not close the sectional valve, then the fuel line inventory above the leak location would all be released.

For leak sequences which occur when a fuel movement is in progress (i.e., Top Event MOVE in event tree for issue, receipt, or inter-tank transfer) the AFHE low level warning alarm (Top Event AFHE in ELECTRICAL event tree) would be disabled until the fuel movement is ended. Low fuel line pressure may also not be evident.

A fuel movement ongoing at the time the leak initiates, is a much less likely condition than that all RHBFSTs holding the same fuel type being idle. Not until the fuel

movement is over would the AFHE low level alarms be enabled. However, releases from either size leak to the LAT from any of RHBFSTs 2 to 16, would fill up the LAT main sump and cause one or both of the main sump pumps (P-0100A/B) to start (Top Event MSUMP in Event Tree TUNLEAK). Though sump pump start or level is not alarmed in the control room, the sump pumps running is indicated there. It's expected that the control room operators would note the sump pump running indication in short order. LAT tunnel cameras also allow for remote, visual confirmation of the leak and its location along the fuel lines.

If the main sump pumps below the tank gallery operate to transfer released fuel to Tank S311 outside ADIT3, then the accumulation of fuel in the LAT would be delayed. Half the Tank S311 capacity may, on average, be available as ullage. This corresponds to about 20,000 gallons. This is about the total volume of fuel in Section E of the F76 or JP5 lines. There are no F24 fuel lines in Section E. Section D has about 20,000 gallons of fuel in the JP5 or F24 lines. The F76 fuel has about twice that amount of Section D. This indicates that isolation of the upgrade sectional valve can often limit the total fuel released to what can be accommodated by the available ullage in Tank S311.

At 75 gpm, either main sump pump could keep up the release but the available ullage would be filled in an estimated 4.4 hours. For 6" hole fuel line leak scenarios, the fuel line release rate would be much higher. If both main sump pumps operated, the average ullage in Tank S311 could be filled in less than 45 minutes.

There is no procedure directing them to do so, but once sump pumps running are indicated, the control room operators may try to isolate the fuel line sectional valves in the tank gallery (Top Event OSEC in Event Tree TUNLEAK). The isolation of the sectional valves would limit the total amount of fuel released.

For isolated leaks from fuel line piping within Zone 7 (i.e., near RHBFSTs 17, 18, or 20) the leaked fuel would first accumulate in the Zone 7 sump above the LAT bulkhead. Sump Pump P-0124 would start automatically and the Zone 7 sump pump running would be indicated in the control room. The Zone 7 sump pump transfers fuel to the slop line which also ends up in the main sump below the tank gallery. With the Zone 7 sump pump running, even for the small unisolable leak postulated flow rate of 75 gpm, its capacity is too low to keep up with the fuel released and so fuel level would rise. However, there is not enough fuel in the fuel lines above the bulkhead as long as the RHBFSTs on the leaking line are initially idle. If a RHBFST was aligned to the leaking fuel line, then eventually the spilled fuel level would increase to the elevation of the known penetrations in the bulkhead above the man-door and additional flow to the tank gallery below would occur. LAT tunnel cameras also allow for remote, visual confirmation of any fuel lines leaking above the LAT bulkhead in Zone 7.

For such fuel release rates, the pungent smell of a substantial amount of released fuel would also be noted by the Red Hill Rover and others if present at Red Hill, and they would immediately evacuate Red Hill. This may be significant because it may take as much as 24 hours to obtain permission to re-enter Red Hill even if only to the UAT to perform a top gauge. With a substantial release to the LAT, it may not be accessible for much longer.

Once the fuel movement is secured, either prematurely, or as planned, the response to the isolable leak is the same as for initially tank idle conditions. The probability of a Section E fuel line leak in Zone 7 is slightly less than the Section E fuel line leaks in the upper half of the tank gallery but below the bulkhead. The QRVA therefore assumes that all fuel line leaks in Section E are located below the bulkhead; i.e., and not in Zone 7.

For leaks in Section A, B, or C, the new oil door would likely not close and the main sump would not fill with fuel. Instead, the released fuel would flow downgrade into the Harbor Tunnel. Eventually it would collect in the sump at the entry to the UGPH. Fuel vapor from fuel releases into the Harbor Tunnel would proceed mostly upgrade and out the ventilation exhaust stack below 3Y. However, a small portion (2,000 $ft^3$ out of 43,000 $ft^3$/min), would be exhausted downward into the UGPH and mix with 109,000 $ft^3$ per minute of air and then be exhausted via ADIT 1. Nevertheless, evacuation from Red Hill is assumed in such sequences.

The availability and reliability of the AFHE system to provide the low level warning and critical alarms is already questioned in the OTHERSUP event tree via Top Event AFHE. In response to either of the two AFHE low level alarms, the control room operators are tasked by the UFM alarm response procedure to direct the top gauger to check that the skin and ball valves on the associated RHBFST are indeed fully shut and to manually top gauge the affected RHBFST. For both the small and large unisolable leaks to the LAT as defined, the top gauger and others would likely instead evacuate Red Hill before performing these actions. The Red Hill rover would be expected to contact the control room before or immediately after evacuation to notify them of the leaking fuel line, or at least of the pungent released fuel odor. This notification is assumed sufficient for the control room operators to contact management and the Fuels Department supervisor for further instructions.

The supervisor would seek additional facility information and decide the best strategy to respond to the situation, likely to ensure that steps have been taken to isolate the leaking fuel line, and if an initially aligned RHBFST cannot be isolated, to direct that its fuel be moved to empty the RHBFST and thereby limit the release.

There are different methods for moving fuel from a leaking RHBFST depending on the available ullage for the leaking fuel type. The supervisor would formulate a strategy which the entire Red Hill facility staff would then carry out. The time to empty the leaking RHBFST depends on the specific strategies for moving fuel and the initial height of the leaking RHBFST. Until the RHBFST is emptied below 7.5', leakage would continue although at lower flow rates as the available head from the fuel level is lowered. The outlet pipe rises inside the RHBFST to about 7.5' above the bottom of the tank. The fuel below this level could not drain out the hole location even if it was not isolated.

The status of the following top events in the TUNLEAK event tree make up a portion of the full accident sequence through the linked event tree set. The top events in the TUNLEAK event tree are summarized below and then described in more detail in Section 7 – Systems Analysis.

| | |
|---|---|
| USUMP | One of Two Harbor Tunnel Sump Pumps at UGPH Entry Start and Transfer Leaked Fuel |
| MSUMP | One of Two Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 |
| DOOR | Oil Tight Door below LAT Gallery Closes on High Float Level |
| PFL | Fuel Line Pressure Drops due to Leak and Is Detected |
| OSUM | CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak |
| OPAN | CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button |
| OSEC | CR Operators REMOTE MANUALLY Close Sectional Valve(s) and Ball Valves as Applicable; Execution Only |
| OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak |
| ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm |
| OSUP | Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST |
| OXFR | Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST |
| ISOL | FL Leak Isolated from all RHBFSTs; by Upgrade Sectional, RHBFST Idle or Isolated – No Need to Empty |
| XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST |
| XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor |
| XFR3 | Two-Step Fuel Movement to Pump Fuel to Other RHBFSTs |
| XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor |
| XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line |
| DELAY | Tank Empty Delay Time Based on Earlier Failures |
| REL | REL – Type of Fuel Release Scenario |

The TUNLEAK event tree structure is presented in Figure 6-16. The TUNLEAK event tree is a “branch everywhere” tree; that is, every top event is questioned for all of the sequences in the event tree. The branches or nodes for some of the top events in certain sequences are guaranteed events (success or failure) due to the dependencies between the supporting systems. There are two multi-state top events in this event tree. Top Event ISOL is just two states but tracks the status of RHBFST isolation as YES or NO. Top Event DELAY is also multi-state. It represents alternate, sequence specific delay times modeled for initiating the actions to move fuel from a RHBFST that has not been isolated from the leaking fuel line.

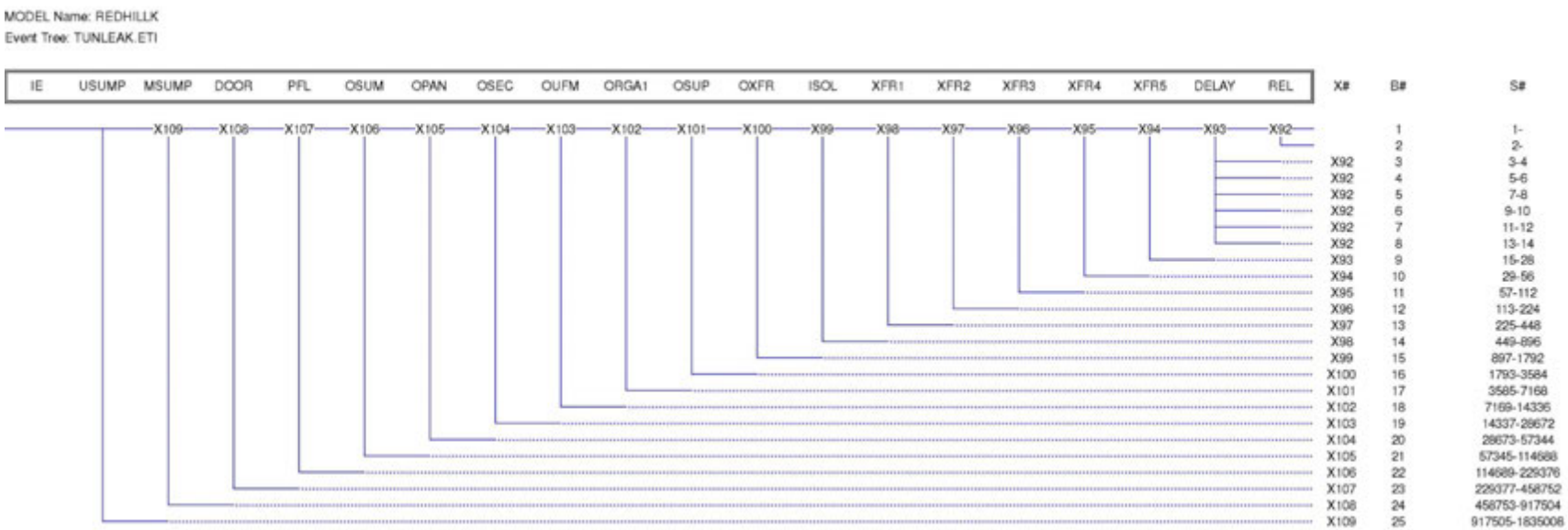



**Figure 6-16. TUNLEAK Event Tree Structure; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel**

## 6.8 Assessment of Acute Sequence End States – Gallons of Fuel Released

The top events and structures of the event tree models are described in Section 6.7. This section describes the development of end states which are assigned to each acute sequence path through the set of linked event trees. The end states are defined in terms of the amount of fuel released from its initial confinement; i.e., from the RHBFST, from a fuel line in the LAT or Harbor Tunnel, or from both. The amount of fuel released is tracked in 1,000s of gallons of fuel. Each end state is named with a three-letter code that identifies the frontline event tree to which it is used, followed by a number that identifies the amount of gallons of fuel released rounded to the nearest 1,000. So the end state names are of the form:

1. ROC10 – TKLEAK; Direct Leaks to Rock (10,000 gallons)

2. OFG118 – OVERFILL; Leaks to Rock above Maximum Operating Level (118,000 gallons)

3. NOZ10947 – NOZZLE, Unisolable Leaks from a RHBFST to the LAT (10,947,000 gallons)

4. TUN103 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel (103,000 gallons)

These end states do not track the ultimate location of fuel, but rather the amount of fuel that is released from the opening in the fuel confinement. The ultimate location(s) of the fuel released are instead described in Section 10 – Fuel Release Accident Sequence Analysis. In some sequences (e.g., if the new oil door closes), the released fuel may accumulate in the tank gallery portion of the LAT. In such sequences, much of the fuel initially in the associated RHBFST may not physically be released from the RHBFST for a long time, although an opening is available for release once space in the LAT is available. In the end states for such sequences, the fuel remaining in the RHBFST is still counted as “released”, or available for release.

In Section 6.8.1, the different analysis approaches used to estimate the amount of fuel released for different classes of sequences are described. In Section 6.8.2, the specific approaches applied to the four frontline event trees are then presented.

### 6.8.1 Approaches for Evaluating Gallons Released

There are a large number of accident sequences which are to be assigned end states tracking the amount of fuel released. The amounts of fuel released depend on the initial configuration of Red Hill, including whether a RHBFST is idle (i.e., isolated from the main fuel lines) or undergoing a fuel movement at the time the release is initiated. Also important in determining the amount of fuel released is the initial level of fuel in the associated RHBFST. Amounts released via the main fuel lines also depend on whether a RHBFST is undergoing a fuel movement, or if all RHBFSTs of the same fuel type are idle at the time the fuel line opening occurs. Small and large leak sizes are postulated for each leak location modeled. The most rapid releases modeled are from postulated

openings in the main fuel lines when a RHBFST of the same fuel type is aligned for a fuel movement.

Openings postulated in a fuel line can be partially isolated in that closure of the upgrade sectional valve can limit the amount of fuel released to that leaking section. Isolation of an initially aligned RHBFST (i.e., by closing its skin or ball valve) is much more important, since the fuel source of a RHBFST is much greater in volume. Credit for both types of isolations is taken for the classes of sequences for which end states are to be assigned. Failures to isolate are in lower frequency sequences. There is no credit given for delayed isolations from the postulated openings if the operators or equipment needed to perform the isolation are not initially available.

If the leak is directly from a RHBFST to rock, or if the initially aligned RHBFST cannot be isolated from the fuel line with the opening, then an alternative strategy can be effective. The strategy is to move fuel from the RHBFST that is leaking to other volumes of confinement; e.g., other RHBFSTs, tanks in the upper tank farm, etc. The amount of fuel released from such sequences is then dependent on the time at which emptying the RHBFST begins, the rate at which fuel is moved, and the leak flow rate through the postulated opening. Initial failures of the operators to initiate such fuel movements may be recovered, introducing a delay in the assumed time for actions to move fuel from the affected RHBFST. These factors are considered in the evaluation of fuel amounts released.

#### *6.8.1.1 Model of RHBFST Fuel Inventory Release*

An analyst's tool has been developed to facilitate the computation of fuel releases from a leaking RHBFST. This tool was initially developed for postulated liner through holes that directly leak to rock, but then also was applied to sequences involving fuel line openings in which the RHBFST was initially aligned and not isolated.

The analyst's tool is an Excel worksheet which represents the geometry of one RHBFST. The RHBFST cylinder and both upper and lower hemispherical domes are represented. The worksheet represents the dimensions for the larger of the two types of RHBFST; i.e., 250' tall consistent with the geometry of RHBFSTs 5 to 20. The smaller RHBFSTs (RHBFSTs 2, 3, and 4) are should behave similarly. The smaller RHBFST's shapes have similar geometries, except there is no extension, so that the cylinder portion is 12' shorter; i.e., total height is then 238'. Each circular cross-section vertical node represented in the model worksheet is 1/16" in height.

The RHBFST worksheet model does not use time-steps to solve for the amount of fuel released. Instead, given an initial fuel level, leakage rate, and fuel empty strategy, the worksheet evaluates the time for level to fall each 1/16" with the leakage and removal flow rates held constant during that time interval. The fuel released during the time it takes to fall each 1/16" is then summed until the postulated hole location height is uncovered. The sum is then the total amount of fuel released.

The inputs for the RHBFST worksheet model for specific sequences are as follows:

1. Initial Liquid Level in Feet (e.g., 212')
2. Equivalent Hole Diameter in Inches (e.g., 0.5")

3. Hole Location Measured from RHBFST Bottom in Feet (e.g., 0')
4. Time at which Fuel Emptying Begins in Hours (e.g., 6 hours from start of leakage)
5. Fuel Empty Rate in Barrels per Hour once Initiated (e.g., 2,500 barrels per hour)
6. Fuel Empty Rate for Lowest 7.5', below Outlet Pipe Riser (2,600 gallons per hour)

For the current assessment, the fuel empty rate is assumed to be constant at the input rate once the emptying is initiated. Below the 7.5' level, which is only applicable for leaks from the bottom of the RHBFST, a lower removal rate is assumed. This lower removal rate is consistent with the practice of draining the last 7.5' of fuel through a bottom drain in the lower dome and gravity flow via the main fuel line to the UGPH.

For fuel levels above 7.5', an empty rate of 2,500 barrels per hour is assumed for all sequences. This removal rate is consistent with the two-step approach that involves gravity feed from the affected RHBFST to either a surge tank at the UGPH, or to one of the tanks at the upper tank farm, and then use of the cargo pumps to transfer the fuel to a different RHBFST of the same fuel type with available ullage. This rate of fuel removal is significantly lower than could be achieved via inter-RHBFST transfers or by gravity feed to a tank at the upper tank farm by itself. The two-step approach, however, allows all available ullage in RHBFSTs to be taken advantage of. Inter-RHBFST gravity transfer to one other RHBFST alone or in combination with gravity feed to a tank at the upper tank farm is not sufficient to fully empty an initially full RHBFST; i.e., to completely empty a RHBFST initially at 212' (i.e., approximately 273,000 barrels) requires more ullage to move the fuel to. With the input assumptions listed above, the RHBFST worksheet model predicts 4.8 days to lower fuel to 7.5', and 5.7 days to fully empty the RHBFST. There is anecdotal evidence that the final 7.5' of fuel may be drained in as little as 6 hours once aligned.

The RHBFST worksheet model uses an orifice flow model to evaluate the leakage rate at each level. The volumetric flow rate, Q, is expressed as:

$$\mathrm{Q}\ (\mathrm{ft}^3/\mathrm{sec}) \ = \ \mathrm{C} * \mathrm{AREA} * (2 * \mathrm{g} * \mathrm{h})^{1/2}$$

Where:

C is the discharge coefficient (conservatively assumed to be 1.0 for all cases).

AREA is the flow area defined by the hole diameter.

g is the gravitational constant.

h is the head in feet computed as the distance between the current fuel level and the height of the hole.

In addition to an echo of the sequence case input, the RHBFST worksheet model outputs the following quantities in a convenient form:

**Table 6-13. Output Quantity**

| Output Quantity | Value |
|---|---|
| Leak Area in**2 | 230.39 |
| Initial Leak Rate GPM | 71.51 |
| Hours to UFM Warning 0.5" Drop | 0.607 |
| Hours to UFM Critical Alarm, 0.75" Drop | 0.878 |
| Days to Leak 27,000 Gallons | 0.262 |
| Days to 7.5 Ft. | 4.848 |
| Time to Hole Elev. in Days | 5.650 |
| Elev. at 4 Hours (ft.) | 211.69 |
| Elev. at 8 Hours (ft.) | 207.73 |
| Elev. at 2 Days (ft.) | 133.57 |
| Elev. at 4 Days (ft.) | 45.52 |
| Elev. at 10 Days (ft.) | N/A |
| Elev. at 30 Days (ft.) | N/A |
| Cumulative Gallons Leaked at Start of Fuel Transfer | 25,825 |
| Gallons Leaked at 4 Hours | 17,398 |
| Gallons Leaked at 8 Hours | 34,269 |
| Gallons Leaked at 2 Days | 187,911 |
| Gallons Leaked at 4 Days | 320,270 |
| Gallons Leaked at 10 Days | N/A |
| Gallons Leaked at 30 Days | N/A |
| Gallons Leaked at 7.5 Ft. | 348,536 |
| Total Gallons Leaked at Leak Elevation | 360,842 |
| Total Barrels Leaked out at Leak Elev. | 8,591 |
| Initial Barrels above Leak Elev. | 272,949 |

Some outputs are not valid for the sequence case specified. In the above sample, the hole elevation is reached in less than 6 days, so the outputs for 10 and 30 days are not computed.

### 6.8.1.2 Model for Fuel Line Leaks

Models for leaks from a fuel line section in the LAT or Harbor Tunnel are needed for sequences which initiate with hole from the fuel lines. The fuel line sections were defined as the pipe segments between sectional valves. See Figure 6-3 for an illustration. The sectional valves which define the boundaries of these sections are presented in Table 6-14. Estimates of the volumes of these fuel line sections, which are normally kept full, were developed. These are presented in Table 6-15. The differences in inventories between the different fuel line types are largely attributed to the different pipe diameters; e.g., the F76 main fuel line is 32" in diameter. It is important to point out, though, that the largest fuel line pipe connecting to a RHBFST has a diameter of just 20". Most of the RHBFSTs are tied into the main fuel lines only through a 12"-diameter cross-tie pipe. The fuel line section with the largest fuel volume is Section B, which runs most of the length of the Harbor Tunnel.

**Table 6-14. Sectional Valve IDs at bottom of each Fuel Line Section**

| Section ID | A | B | C | D | E |
|---|---|---|---|---|---|
| **Valve Location** | **UGPH** | **ADIT 2** | **ADIT 3** | **Below RHBFST 1 and 2** | **Below RHBFSTs 11 and 12** |
| **F76** | 151 | 152 | 153 | 154 | 164 |
| **JP5** | 155 | 156 | 157 | 158 | 163 |
| **F24** | 159 | 160 | 161 | 162 | N/A* |

** The F24 fuel line has no sectional valve at the mid-tank gallery.*

**Table 6-15. Fuel Inventories in Gallons by Fuel Line Section**

| Section IDs | F76 | JP5 | F24 |
|---|---|---|---|
| **A** | 50,508 | 15,338 | 12,118 |
| **B** | 464,670 | 141,111 | 111,482 |
| **C** | 92,934 | 28,222 | 22,296 |
| **D** | 42,090 | 17,087 | 20,070 |
| **E** | 25,111 | 21,479 | 0 |
| **D+E (above new oil door)** | 67,200 | 38,566 | 20,070 |
| **C+D+E (LAT total)** | 160,134 | 66,788 | 42,366 |
| **B+C+D+E** | 624,804 | 207,899 | 153,848 |
| **A+B (Harbor Tunnel)** | 515,177 | 156,449 | 123,599 |
| **A+B+C+D+E (all sections)** | **675,312** | **223,237** | **165,965** |

Much of the fuel line inventory is contained in Fuel Line Sections A and B, which are in the Harbor Tunnel; i.e., 70 to 76% depending on the fuel type. Since much of the Harbor Tunnel is below the elevation of the water aquifer, it's the smaller inventories in Sections C, D, and E, which are the greater risk. This is if the fuel line postulated to be leaking is not aligned for a fuel movement at the time the leak initiates. If instead the fuel line is aligned for a fuel movement, then the much larger inventory of the associated RHBFST is at risk of being leaked regardless of the leak location. Sequence classes that involve postulated leaks from the fuel lines must then consider:

1. The Fuel Type and Pipe Section where the Leak Occurs (defined by the initiating event)

2. The Size of the Hole Postulated (defined by the initiating event)

3. The Flow Rate through the Postulated Hole (defined by hole size and fuel line pressure at the leak location)

4. The Timing of Cues to Detect the Leak (defined by the hole flow rate and travel time down the LAT or Harbor Tunnel to the first available sump)

5. The Time of Successful Sectional Valve Closure Given Cues of a Leak (time of cue arrival plus 15 minutes)

6. The Time of RHBFST(s) Isolation from the Leaking Fuel Line if Aligned Initially (time of cue arrival plus 15 minutes)

7. Actions to Empty an Associated RHBFST(s) if Not Isolated (defined by frontline event tree sequence)

8. The Leakage of Fuel from the Initially Aligned RHBFST if Its Isolation Fails (defined by leakage flow rate and time required to first initiate and then empty the associated RHBFST)

Though less likely than for one RHBFST, it is possible that two RHBFSTs may be aligned to the same fuel line to complete an inter-RHBFST gravity transfer, at the time a leak occurs.

In the assessment of total release in gallons for fuel line leaks, some common assumptions are shared for the two applicable frontline event trees; i.e., TUNLEAK and NOZZLE event trees.

1. The leak location is assumed to be at the mid-point of the section length, for purposes of estimating travel time to downgrade sumps and to establish the amount of fuel located above the hole.

2. The fuel line pressure at the leak location driving the fuel flow rate is conservatively assumed to remain the same as at the initiation of the leak for all time.

3. The fuel line pressure at the hole location is determined by the initial elevation at the break location and the elevation of the highest point of the fuel line in the LAT if all RHBFSTs are initially idle for the same fuel type.

4. The fuel line pressure at the hole location is determined by the initial elevation at the break location and a RHBFST fuel level of 212' if the fuel aligned is initially aligned to a RHBFST.

5. If the RHBFST is initially aligned but then isolated, the fuel line pressure at the hole location reverts to the isolated case thereafter in the sequence.

#### *6.8.1.3 Gravity Flow of Released Fuel Downgrade in Tunnels (Manning flow)*

Reference 6-1 used an open channel flow model to describe the flow of fuel released into the LAT tunnel downgrade to lower parts of the LAT, the ADIT 3 tunnel, the ADIT 2 tunnel, and the Harbor Tunnel. See Section 4.4.3 of Reference 6-1 for a full discussion. In short, Manning's equation for open channel flow relates the velocity or volumetric flow rate of released fuel flowing down an inclined plane of specific slope, hydraulic radius, and a roughness coefficient associated with the material surface of the flow path.

In Reference 6-2, the formula in terms of volumetric flow is given by

$$\mathrm{Q} = 1.49 * \mathrm{A} * \mathrm{R}^{2/3} * \mathrm{S}^{1/2}/\mathrm{N}$$

Where:

1.49 is a conversion factor for English units.

A is the cross-sectional flow area.

R is the hydraulic radius.

S is the slope of the tunnel.

N is a coefficient related to absolute surface roughness.

This correlation and the previously used approach are adopted for this study to assess the velocities of released fuel down the tunnels and to thereby estimate the depths of such flows.

The roughness coefficient can be selected from text books. For this project, a Manning roughness factor of 0.012 for smooth or finished concrete is chosen for all locations in the LAT and Harbor Tunnel. The slope of each tunnel section is estimated as the drop in elevation divided by the linear feet along the tunnel between the two points. Estimates of these parameters were obtained using the same values as reported in Reference 6-1. Tunnel widths were not provided in Reference 6-1. Tunnel widths of 12' for Sections A, B, and C and 24' for Section D and E were assumed.

The hydraulic radius is defined as the ratio of the wetted cross-sectional flow area of the channel to the wetted perimeter of the flow cross-section. The wetted cross-sectional flow area is D*W, where D is the fluid depth and W is the channel, or in this case, tunnel width. The wetted perimeter of the tunnel flow is then 2*D+W (i.e., three sides of the flow) where the top surface of the flow is omitted since it is not in contact with the tunnel surface.

Manning's equation for open channel flow is indeterminate since the depth of the flowing fluid used in the hydraulic radius is not initially known. An iteration procedure was used in Reference 6-1 for each fluid flow segment of assumed constant slope and tunnel width. Solution closure was obtained by comparing the computed volume flow downgrade with the leakage flow estimate.

In this study, the number of cases selected for evaluation was more limited so that the iteration was performed by a series of initial guesses until solution closure was achieved.

For this study, use was made of an online Manning equation solver at www.lmnoeng.com courtesy of LMNO Engineering, Research, and Software, Ltd.

As an example, for Section D in the tank gallery, a 75 gpm leakage flow rate is estimated for a 0.5" fuel line hole with a RHBFST aligned. After some iterates, the height of the downgrade flowing fuel in the LAT is estimated to be .01' at an incline of .01442 ft./ft. The online Manning flow calculator shows that the fuel downgrade velocity is 0.69 feet per second and that the volumetric flow rate is 0.166 ft.$^3$ per second:

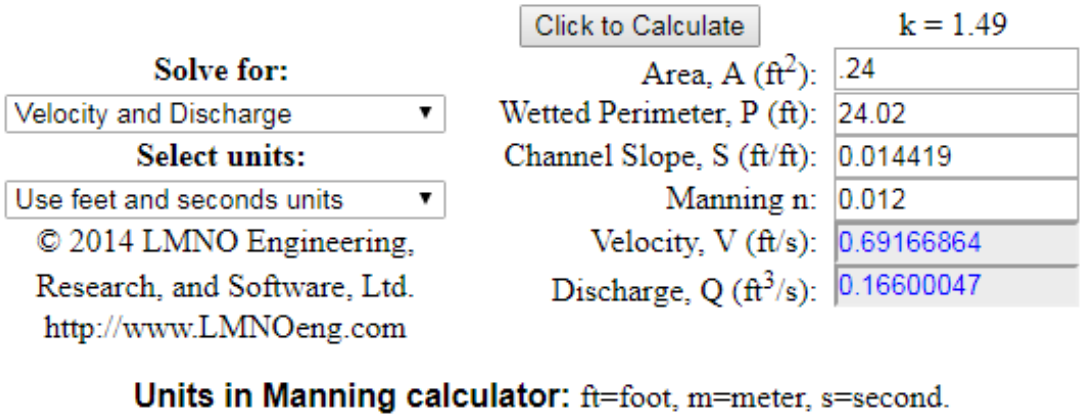



**Figure 6-17. Example Output from Online Manning Flow Calculator**

A downgrade fluid velocity of 0.69 ft./sec. is returned. The returned discharge rate, Q in ft.$^3$/sec., when divided by the number of ft.$^3$ per gallon (.133681) and multiplied by 60 to convert seconds to minutes, yields a flow rate of 74.5 gpm, slightly less than the leakage flow rate. This accuracy was judged acceptable for the purposes of this study. Assuming the leak is located at the top of Fuel Line Section D, and 1600' from the main sump just below the tank gallery, it would take 1600'/0.69 ft./sec., or about 39 minutes, to reach the main sump. Once a high sump level is reached, the sump pumps would actuate and this would be indicated in the control room. Such time delays until cues are present to alert the control room operators are considered in the delays until fuel line sectional valve closure and RHBFST isolation is attempted.

### 6.8.2 Gallons Released for Frontline Events Trees

This subsection describes the calculations of gallons released for the end states of each frontline event tree.

1. ROC10 – TKLEAK; Direct Leaks to Rock (10,000 gallons)

2. OFG118 – OVERFILL; Leaks to Rock above Maximum Operating Level (118,000 gallons)

3. NOZ10947 – NOZZLE, Unisolable Leaks from a RHBFST to the LAT (10,947,000 gallons)

4. TUN103 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel (103,000 gallons)

#### *6.8.2.1 Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock*

The TKLEAK event tree is used to represent the response to the five subcategories of initiating events that lead to fuel leakage to the rock surrounding the RHBFST. The general set of end states are assigned to the event tree and each sequence path is assigned to a single end state from that general set during sequence frequency quantification.

The gallons released are computed for each of the nine facility configuration states as represented by Top Event INVEN in the CONFIG event tree. These nine facility configurations distinguish the three different fuel types, the initial fuel level in the RHBFST when the leak occurs, and whether the RHBFST is undergoing a return to service when the leak is discovered. They are presented in Table 7-12 of Section 7.3.1.10. For each of the nine facility configurations possible, the calculation of gallons released also is evaluated separately for the size of the postulated leak (i.e., 1.5 gpm or 0.5" hole) and at what level in the RHBFST that the leak occurs. Four separate RHBFST levels are used to represent the different locations of the postulated hole. Leaks lower in the RHBFST release fuel at comparatively higher flow rates for the same hole size and require that more of the RHBFST fuel be emptied to uncover the hole location.

A total of 44 separate sequence conditions are evaluated using the RHBFST worksheet model described in Section 6.8.1.1. The 44 conditions are summarized in Table 6-16 along with the evaluated release of fuel, in gallons, to rock prior to uncovering the hole when the release stops. The input data assumed for the RHBFST worksheet model is the same as that listed in Section 6.8.1.1 with some variations.

## Table 6-16. Sequence Conditions Evaluated for Fuel Releases Leaks Directly to Rock

| Configuration ID | Leak gpm/Size | Initial Leak Rate gpm | Initial Fuel Level (ft.) | Leak Level (ft.) | Gallons Released (0 delay) | End State ID |
|---|---|---|---|---|---|---|
| F24A | 0.5" | 29.87 | 212 | 175 | 35,261 | ROC35 |
| F24A | 0.5" | 41.67 | 212 | 140 | 80,628 | ROC81 |
| F24A | 0.5" | 58.52 | 212 | 70 | 201,894 | ROC202 |
| F24A | 0.5" | 71.51 | 212 | 0 | 359,945 | ROC360 |
| F24B | 0.5" | 26.9 | 100 | 70 | 27,503 | ROC28 |
| F24B | 0.5" | 49.11 | 100 | 0 | 130,643 | ROC131 |
| F76C | 0.5" | 29.06 | 175 | 140 | 33,019 | ROC33 |
| F76C | 0.5" | 50.33 | 175 | 70 | 133,626 | ROC134 |
| F76C | 0.5" | 64.97 | 175 | 0 | 276,032 | ROC276 |
| JP5D | 0.5" | 29.87 | 212 | 175 | 35,261 | ROC35 |
| JP5D | 0.5" | 41.67 | 212 | 140 | 80,628 | ROC81 |
| JP5D | 0.5" | 58.52 | 212 | 70 | 201,894 | ROC202 |
| JP5D | 0.5" | 71.51 | 212 | 0 | 359,945 | ROC360 |
| JP5E | 0.5" | 18.38 | 14 | 0 | 22,893 | ROC23 |
| R100I | 0.5" | 26.9 | 100 | 70 | 27,503 | ROC28 |
| R100I | 0.5" | 49.11 | 100 | 0 | 130,643 | ROC131 |
| RF24F | 0.5" | 29.87 | 212 | 175 | 35,261 | ROC35 |
| RF24F | 0.5" | 41.67 | 212 | 140 | 80,628 | ROC81 |
| RF76G | 0.5" | 29.87 | 212 | 175 | 35,261 | ROC35 |
| RF76G | 0.5" | 41.67 | 212 | 140 | 80,628 | ROC81 |
| RJP5H | 0.5" | 29.87 | 212 | 175 | 35,261 | ROC35 |
| RJP5H | 0.5" | 41.67 | 212 | 140 | 80,628 | ROC81 |
| F24A | 1.5 gpm | 1.5 | 212 | 175 | 1,852 | ROC2 |
| F24A | 1.5 gpm | 1.5 | 212 | 140 | 3,035 | ROC3 |
| F24A | 1.5 gpm | 1.5 | 212 | 70 | 5,370 | ROC5 |
| F24A | 1.5 gpm | 1.5 | 212 | 0 | 8,038 | ROC8 |
| F24B | 1.5 gpm | 1.5 | 100 | 70 | 1,617 | ROC2 |
| F24B | 1.5 gpm | 1.5 | 100 | 0 | 4,414 | ROC4 |

**Table 6-16. Sequence Conditions Evaluated for Fuel Releases Leaks Directly to Rock (Continued)**

| Configuration ID | Leak gpm/Size | Initial Leak Rate gpm | Initial Fuel Level (ft.) | Leak Level (ft.) | Gallons Released (0 delay) | End State ID |
|---|---|---|---|---|---|---|
| F76C | 1.5 gpm | 1.5 | 175 | 140 | 1,794 | ROC2 |
| F76C | 1.5 gpm | 1.5 | 175 | 70 | 4,149 | ROC4 |
| F76C | 1.5 gpm | 1.5 | 175 | 0 | 6,797 | ROC7 |
| JP5D | 1.5 gpm | 1.5 | 212 | 175 | 1,852 | ROC2 |
| JP5D | 1.5 gpm | 1.5 | 212 | 140 | 3,035 | ROC3 |
| JP5D | 1.5 gpm | 1.5 | 212 | 70 | 5,370 | ROC5 |
| JP5D | 1.5 gpm | 1.5 | 212 | 0 | 8,038 | ROC8 |
| JP5E | 1.5 gpm | 1.5 | 14 | 0 | 2,352 | ROC2 |
| R100I | 1.5 gpm | 1.5 | 100 | 70 | 1,617 | ROC2 |
| R100I | 1.5 gpm | 1.5 | 100 | 0 | 4,455 | ROC4 |
| RF24F | 1.5 gpm | 1.5 | 212 | 175 | 1,852 | ROC2 |
| RF24F | 1.5 gpm | 1.5 | 212 | 140 | 3,034 | ROC3 |
| RF76G | 1.5 gpm | 1.5 | 212 | 175 | 1,852 | ROC2 |
| RF76G | 1.5 gpm | 1.5 | 212 | 140 | 3,034 | ROC3 |
| RJP5H | 1.5 gpm | 1.5 | 212 | 175 | 1,852 | ROC2 |
| RJP5H | 1.5 gpm | 1.5 | 212 | 140 | 3,034 | ROC3 |

For sequence conditions involving a 0.5” hole, the postulated hole is located at the specified RHBFST level. For the 1.5 gpm holes, the condition is modeled differently. The hole equivalent diameter in inches is chosen as a function of the hole location so that the same initial 1.5 gpm flow rate is achieved. Obviously, holes located higher in the RHBFST require larger hole sizes than those at the bottom of the RHBFST to achieve the same initial flow rate. The appropriate hole sizes were easily evaluated by trial and error using the RHBFST worksheet model. Recall that the RHBFST worksheet model computes the initial release flow rate in gpm as one of its outputs. A hole size of .075” in diameter would have an initial leak rate of 1.5 gpm is located at the bottom and with the RHBFST filled to 212’.

For the smaller, 1.5 gpm holes, there may be significant time between when the hole occurs and when the operators are alerted to the decrease in fuel level by the AFHE low level warning alarm; i.e., a fuel level drop of 8/16” triggers the alarm. This time until the warning alarm occurs is treated as an additional delay time prior to initiating fuel transfer from the leaking RHBFST. This time until the warning alarm occurs is added to an additional 6-hour delay between when the warning occurs and when the fuel is started to be moved. The 6 hours of delay is selected as a typical time that would be required for

the Red Hill staff to confirm, by manual top gauging, that a loss of fuel inventory is occurring; to notify management and the fuel department supervisor of the situation, the time needed to assess, plan, and decide what actions to take; plus the time to then set up a fuel evolution to begin emptying the leaking RHBFST. The RHBFST worksheet model uses the sum of the time to the low level alarm plus the 6 hours to represent the start of fuel being transferred from the leaking RHBFST.

The gallons of fuel released presented in Table 6-16 for each sequence condition, assume a realistic time that is needed to confirm the release, plan, and initiate the transfer of fuel from the leaking RHBFST after the AFHE low level warning is received. Additional delays in initiating the fuel transfer may also occur as detailed by the sequence of events along a specific path through the linked event trees. For example, it may take longer than anticipated to confirm that the affected RHBFST is indeed undergoing a loss of fuel inventory. Such a delay would be represented by an initial failure of Top Event ORGA1 in the TKLEAK event tree. If the affected RHBFST was undergoing a fuel evolution (i.e., receiving or issuing) at the time the hole occurs, then the time to the low level warning alarm would be delayed until after the fuel evolution was completed and the RHBFST fuel level drops further while in idle conditions. Use of these delay times for fuel evolutions helps to limit the number of sequence conditions evaluated using the RHBFST worksheet model. The extent of such delays depends on the duration of such fuel evolutions for different fuel types. More significant failures (e.g., loss of power at the Red Hill 480V emergency bus) could lead to longer delays, although local, manual manipulation of MOVs is still feasible without electrical power.

The total delay time beyond that typically expected under optimum conditions, is considered in the assessment of fuel released. The following discrete delay times were postulated:

1. 0 Hours
2. 4 Hours
3. 8 Hours
4. 12 Hours
5. 24 Hours
6. 72 Hours
7. 336 Hours (i.e., 2 weeks)

Separate fuel releases were evaluated for each of the 44 sequence conditions and 7 assumed delay times; i.e., delays beyond the typical 6-plus hours. Rather than exercise the RHBFST worksheet model for each sequence condition for these 7 delay times (308 cases), a simpler, conservative approach was taken. The initial fuel release rate was assumed to continue for the duration of the delay time, and this added release then added to the 0-hour delay time result. This approach is clearly conservative since the initial release rate would decrease as level in the affected RHBFST drops.

Table 6-17 presents the assumed impacts of individual top event failures on the start of fuel transfer from a leaking RHBFST as expressed by a time delay in the start of the fuel transfer. The top events are ordered by event trees which are linked together to assess leak directly to rock. Many of the early top events in the set have no impact on delay times because the top events are just switches. Multi-state top events may have

different time delay impacts depending on the specific top event state; e.g., Top Event GRIDR.

**Table 6-17. Time Delay Impacts of Top Event Failures**

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **CONFIG** | LKLOC | Location of Leak within Facility | N/A |
| **CONFIG** | MOVE | Type of Fuel Movement Initially in Progress | 24 Hours per Receipt<br>12 Hours per F24 or JP5 Issue<br>4 Hours per F76 Issue<br>24 Hours per XFER |
| **CONFIG** | TKID | RHBFST Associated with Leak | N/A |
| **CONFIG** | FUEL | Type of Leaking Fuel | N/A |
| **CONFIG** | TKXF | Source RHBFST Associated with Inter-Tank Transfer | N/A |
| **CONFIG** | TKLOC | LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT | N/A |
| **CONFIG** | HEIGHT | Height of Hole in RHBFST that Is Leaking to Rock | N/A |
| **CONFIG** | SIZE | Size of Leak from RHBFST, or Fuel Line Piping | N/A |
| **CONFIG** | DIREC | Side of RHBFST that Tank Leak Is On | N/A |
| **CONFIG** | INVEN | INVEN – Initial RHBFST Inventory Configuration | N/A |
| **ELECTRICAL** | GRID | Offsite Grid | See GRIDR |
| **ELECTRICAL** | GRIDR | Recovery from Losses of Offsite Grid | HR3 = 4 hours<br>HR6 = 8 hours<br>HR12 = 12 hours<br>HR24 = 24 hours |
| **ELECTRICAL** | BUN24 | UGPH 2.4 kV Normal Bus | 72 |
| **ELECTRICAL** | BUN48 | UGPH 480V Normal Bus | 72 |
| **ELECTRICAL** | BUE48 | UGPH 480V Emergency Bus | 72 |
| **ELECTRICAL** | GEN1 | Backup Generator at ADIT for UGPH 480V Emergency Bus | See GRIDR |
| **ELECTRICAL** | UFAN | ADIT 1 Supply and Exhaust Fans for UGPH Cooling Cargo Pumps | 72 |
| **ELECTRICAL** | B3EA | ADIT 3 208V Panel A | 72 |
| **ELECTRICAL** | GEN3 | Backup Generator at ADIT 3 for 480V Panels B and A | NA |

## Table 6-17. Time Delay Impacts of Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **ELECTRICAL** | BRN48 | Red Hill 480V Normal Bus | 72 |
| **ELECTRICAL** | BRE48 | Red Hill 480V Emergency Bus | 72 |
| **ELECTRICAL** | GEN5 | Red Hill 480V Emergency Bus | See GRIDR |
| **ELECTRICAL** | LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras | 8 |
| **ELECTRICAL** | AFHE | Automatic Fuel Handling Equipment | 12 |
| **ELECTRICAL** | AFHR | AFHE Condensing and Fans for Heat Removal | 72 |
| **ELECTRICAL** | EFAN | Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply electrical room in LAT) | 72 |
| **ELECTRICAL** | TFAN | Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead) | 72 |
| **OTHERSUP** | CRM | Control Room Electrical Power, Lighting, and Air Conditioning | 72 |
| **OTHERSUP** | ACRM | Alternate Control Room Electrical Power, Lighting, and Air Conditioning | NA |
| **OTHERSUP** | UHMOV | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs | NA |
| **OTHERSUP** | CARGO | Two or More Cargo Pumps Available to Move Leaking Fuel Type | 72 |
| **OTHERSUP** | ULIT | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting | NA |
| **OTHERSUP** | EL72 | Personnel Elevator 72 and Controller | 4 |
| **OTHERSUP** | EL73 | Cargo Elevator 73 | 4 |
| **OTHERSUP** | RMOV | Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and All LAT MOVs | N/A |
| **OTHERSUP** | RHIN | Support for Red Hill Instruments, Indications, Level Alarms, and Signals | N/A |

## Table 6-17. Time Delay Impacts of Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **VALVES** | SKIN | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| **VALVES** | BALL | Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| **VALVES** | SKINX | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| **VALVES** | BALLX | BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| **VALVES** | FLISO | FLISO – Successful Closure of the Upstream Sectional Valve | 72 |
| **VALVES** | FLTKC | FLTKC – Successful Isolation of the Fuel Line Leak from All RHBFSTs | 72 |
| **VALVES** | FLTKO | FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied | 72 |
| **VALVES** | EVAC | Sequence Conditions Necessitate Initial Evacuation from RH | 336 (combined with other top event failures) |
| **TKLEAK** | OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger | 8 |
| **TKLEAK** | ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm | 8 |
| **TKLEAK** | OSUP | Management and Red Hill Supervisor Formulate Response | 24 |
| **TKLEAK** | OXFR | Control Room and Red Hill Staff Move Fuel from the Leaking RHBFST | 24 |
| **TKLEAK** | XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST | 72 |

**Table 6-17. Time Delay Impacts of Top Event Failures (Continued)**

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **TKLEAK** | XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor | 72 |
| **TKLEAK** | XFR3 | Two-Step Fuel Movement to Pump Fuel to Other RHBFSTs | 72 |
| **TKLEAK** | XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor | 72 |
| **TKLEAK** | XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line | 72 |
| **TKLEAK** | DELAY | Tank Empty Delay Time Based on Earlier Failures | N/A |
| **TKLEAK** | REL | REL – Type of Fuel Release Scenario | N/A |

Some assumed time delays are function of multiple conditions including on the states of multiple top events along the sequence path. Table 6-18 summarizes the actual macro logic used for assigning the added delay times as a function of all top event success and failure states along a single sequence path. The status of each macro (e.g., TIM336HR, TIM72HR, etc.) represents the logical conditions in which a given delay time is assumed. In the event that multiple delay time macros are true in the same sequence, the longest delay time is used for assessing the amount of fuel released. The longest assumed time delay duration (TIM336HR) is used for sequence conditions in which there is insufficient ullage to empty the affected RHBFST below the hole location. In the event of insufficient ullage, a 2-week delay is assumed, to allow time for alternative ullage to be made available. In the RHBFST inventory data reviewed, the only concern with sufficient available ullage being available involved the two RHBFSTs which hold F76 fuel. These RHBFSTs were observed to have relatively high fuel levels throughout the period of time reviewed. There would be insufficient ullage to empty one of the RHBFSTs into the other, even allowing for the F76 ullage typically available at the upper tank farm.

## Table 6-18. Logic for Sequence Dependent Time Delays

| Macro ID | Macro Logic Rule |
|---|---|
| ULLAGEF | INVEN=F76C*(HEIGHT=LOW+HEIGHT=BOT)*-IERTS |
| XFRF24ASUC | INVEN=F24A*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S)+HEIGHT=MED*(XFR1=S+XFR2=S+XFR3=S)+HEIGHT=LOW*XFR3=S+HEIGHT=BOT*(XFR1=S*XFR2=S*XFR3=S*XFR5=S)) |
| XFRF24BSUC | INVEN=F24B*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW*(XFR2=S+XFR3=S)+HEIGHT=BOT*(XFR3=S*XFR5=S) ) |
| XFRF76CSUC | INVEN=F76C*(HEIGHT=HIGH+HEIGHT=MED*(XFR2=S+XFR3=S)) |
| XFRJP5DSUC | INVEN=JP5D*(HEIGHT=HIGH*(XFR1=S*XFR2=S+XFR3=S)+HEIGHT=MED*(XFR1=S+XFR3=S)+HEIGHT=LOW*XFR3=S +HEIGHT=BOT*XFR3=S*XFR5=S) |
| XFRJP5ESUC | INVEN=JP5E*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW+HEIGHT=BOT*XFR5=S*(XFR2=S+XFR3=S)) |
| XFRF24FSUC | INVEN=RF24F*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S+XFR4=S)+HEIGHT=MED*(XFR1=S*XFR2=S+XFR3=S+XFR4=S)+HEIGHT=LOW*(XFR3=S+XFR4=S)+HEIGHT=BOT*(XFR1=S*XFR2=S*XFR3=S+XFR4=S)*XFR5=S) |
| XFRF76GSUC | INVEN=RF76G*(HEIGHT=HIGH*(XFR2=S+XFR3=S+XFR4=S) +HEIGHT=MED*(XFR3=S+XFR4=S)+HEIGHT=LOW*XFR4=S+HEIGHT=BOT*XFR4=S*XFR5=S) |
| XFRJP5HSUC | INVEN=RJP5H*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S+XFR4=S) +HEIGHT=MED*(XFR1=S+XFR3=S+XFR4=S) +HEIGHT=LOW*(XFR3=S+XFR4=S)+HEIGHT=BOT*(XFR3=S+XFR4=S)*XFR5=S) |
| XFR100ISUC | INVEN=R100I*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW*(XFR2=S+XFR3=S+XFR4=S) +HEIGHT=BOT*(XFR3=S+XFR4=S)*XFR5=S) |
| XFRSUCCESS | XFRF24ASUC+XFRF24BSUC+XFRF76CSUC+XFRJP5DSUC+XFRJP5ESUC+XFRF24FSUC+XFRF76GSUC +XFRJP5HSUC+XFR100ISUC |
| JHEP24HR | OUFM=F*ORGA1=F+OUFM=F*OSUP=F+OUFM=F*OXFR=F+ORGA1=F*OSUP=F+ORGA1=F *OXFR=F+OSUP=F*OXFR=F |
| JHEP72HR | OUFM=F*ORGA1=F*OXFR=F+OUFM=F*OSUP=F*OXFR=F+ORGA1=F*OSUP=F*OXFR=F+OUFM=F* ORGA1=F*OSUP=F*OXFR=F |
| TIM336HR | ULLAGEF |
| TIM72HR | AFHR=F+B3EA=F+BALL=F+BALLX=F+BRE48=F+BRN48=F+BUE48=F+BUN48=F+BUN24=F +CARGO=F+CRM=F+EFAN=F+TFAN=F*IETKTOP4 +FLISO=F+FLTKC=F+FLTKO=F+SKIN=F+SKINX=F +UFAN=F+-XFRSUCCESS+JHEP72HR |
| TIM24HR | OSUP=F+OXFR=F+GRID=F*GRIDR=HR24+(MOVE=RECEV+MOVE=XFER)*-IERTS+JHEP24HR |

**Table 6-18. Logic for Sequence Dependent Time Delays (Continued)**

| Macro ID | Macro Logic Rule |
|---|---|
| TIM12HR | AFHE=F+GRID=F*GRIDR=HR12<br>+(FUEL=F24+FUEL=JP5)*MOVE=ISSUE |
| TIM8HR | LPRH=F+ORGA1=F+OUFM=F+GRID=F*GRIDR=HR6<br>+IERTS*MOVE=RECEV+ MOVE=XFER |
| TIM4HR | EL72=F+EL73=F+GRID=F*GRIDR=HR3 +OSUM=F<br>+FUEL=F76*MOVE=ISSUE |
| TIM8HR | LPRH=F+ORGA1=F+OUFM=F+GRID=F*GRIDR=HR6<br>+IERTS*MOVE=RECEV+ MOVE=XFER |
| TIM0HR | (-(TIM4HR+TIM8HR+TIM12HR+TIM24HR+TIM72HR+TIM336HR)) |

For the most part, time delay macros are made true by the state of a single top event along the sequence path. However, being more likely than multiple equipment failures, multiple operator action failures could appear in the same sequence; e.g., Macros JHEP24HR and JHEP72HR in Table 6-18. In these cases, the overall delay time was taken to be the sum of the individual action delays (i.e., as if the delays occurred in series), provided the actions failures were each related to the function of moving fuel from the affected RHBFST.

The macros which begin with the letters “XFR” deserve special mention. These macros are true if for the specific sequence facility configuration (e.g., F24A) as represented by Top Event INVEN, the combination of fuel transfer options available are sufficient to transfer enough fuel to uncover the hole for the hole height assumed. If not, an added 72-hour delay time is assumed to allow time for recovering the unavailable equipment.

#### *6.8.2.2 Frontline Event Tree 2 – OVERFILL; Leaks to Rock above Maximum Operating Level*

The OVERFILL event tree is used to represent the response to fuel leaks to rock from a RHBFST overfilling above the current, maximum operating fuel level of approximately 212’. The general set of end states are assigned to the event tree and each sequence path is assigned to a single end state from that general set during sequence frequency quantification.

The gallons released for overfill events are only computed for the configuration corresponding to the RHBFST filling. The RHBFST receiving rate is assumed to be 2,080 barrels per hour. Therefore, the number of sequence conditions requiring evaluation is much simpler than for the event tree representing tank leaks to rock discussed previously. A hole is postulated to occur above the 212’ level which would leak fuel to rock if an overfilling occurred. The hole size is assumed to be equivalent to a 0.5”-diameter hole, consistent with hole sizes observed in tank inspections for holes located high in a RHBFST. The hole is conservatively assumed to be just above the 212’ level as this maximizes the amount of fuel leakage that would occur.

If the operators successfully end the filling process as planned at 210.8', there is no release of fuel since there is no overfilling. If instead, the overfilling does occur, then the calculation of gallons released is evaluated separately for three conditions, as follows:

1. In response to a subsequent high-high level warning alarm, the operators terminate the filling process within 15 minutes with the peak level at 222.5'.

2. The mechanical float actuates shutdown of the filling process in time to limit the overfill level to 224.6'.

3. The overfilling ends when the source tank runs out of the available fuel to transfer, assumed to correspond to a RHBFST overfill level of 230.2'

Total fuel leakage for each of these three sequence conditions is made up of three time release phases.

1. During the continued overfilling above the hole while increasing level to the peak fuel level; i.e., a period of several hours.

2. During the time delay until the operators receive a low level warning alarm at a drop of 8/16" and then act to confirm the leak, develop an action plan, and then align valves to remove the excess fuel.

3. During the removal of fuel, once initiated, until sufficient fuel is removed so as to uncover the postulated hole at 212'.

The three conditions are summarized in Table 6-19 along with the evaluated release of fuel, in gallons, to rock prior to uncovering the hole when the release stops. The first time phase was computed by applying the RHBFST worksheet model in reverse; i.e., by assuming a fuel transfer out rate equal to the receiving rate (2,080 barrels per hour) and computing the fuel released during the time it takes to lower the level from the peak to the assumed location of the hole. The fuel released is equivalent to that which would be released during filling from the hole location to the peak fuel level. The second and third time phases are combined into one calculation since the RHBFST worksheet model can model the release of both the second and third time phases. The input data assumed for the RHBFST worksheet model is similar to that listed in Section 6.8.1.1 with some variations. The fuel transfer out rate is again assumed to be 2,500 barrels per hour. Notably, the initial fuel level was assumed to be the peak fuel level for the sequence condition, and the 0.5" equivalent diameter hole was always assumed at 212'.

## Table 6-19. Summary of Gallons Leaked from 0.5" Hole at 212' Assuming 6-Hour Delay after Low Level Warning Alarm Detected

| Maximum Tank Level (ft.) | Leak Rate at Peak Fuel Level (gpm) | Time to Low Level Warning Alarm (hours) | Time to Warning Alarm + 2.5 Hours | Total Time to Start of Fuel Transfer (with 6 hours) | Gallons Released during Overfilling above Hole | Gallons Released Starting from Peak Level | Total Fuel Released (gallons) | Sequence Condition Description |
|---|---|---|---|---|---|---|---|---|
| 222.5 | 15.87 | 2.33 | 4.83 | 10.83 | 8,194 | 13,491 | 21,685 | Given action to trip the cargo pumps and close the skin valve within 15 minutes after AFHE high-high level alarm probe. |
| 224.6 | 17.42 | 2.02 | 4.52 | 10.52 | 8,194 | 15,078 | 23,272 | Mechanical float system automatically ends filling by 95% (UST) of current RHBFST overfill level. |
| 230.2 | 20.95 | 1.40 | 3.90 | 9.90 | 8,194 | 19,026 | 27,220 | Maximum credible excess fuel added. |

Since there is no procedure for the actions to take when an overfilling event has ended, no action is credited until the AFHE low level warning alarm was sounded. Since a fuel movement will have just ended, the first 2.5 hours after the overfilling has ended, the AFHE warning alarm setpoints will be at their dynamic settings; i.e., requiring a level drop of 1" to sound the low level warning alarm. This change in level may not be reached within that 2.5 hours, after which the AFHE settings would be returned to static conditions; i.e., 8/16" change in level needed for the alarm to sound. It is conservatively modeled that the alarm settings would switch and the clock restart to signal the low level alarm. Adding to his delay in the start of fuel transfer is the 6-hour time needed to confirm the release, plan the action, and then perform the valve manipulation steps needed to begin the fuel removal from the overfilled RHBFST. This time until the warning alarm is treated as a delay time prior to initiating fuel transfer from the leaking RHBFST. The total time until fuel is actually moved is listed in Table 6-19 for each of the three sequence conditions along with the total gallons released from all three time phases.

Additional delays in initiating the fuel transfer may also occur as detailed by the sequence of events along a specific path through the linked event trees. For example, it may take longer than anticipated to confirm that the affected RHBFST is indeed undergoing a loss of fuel inventory. Such a delay would be represented by an initial failure of Top Event ORGA1 in the OVERFILL event tree. The extent of such delays depends on the duration of such fuel evolutions for different fuel types. More significant failures (e.g., loss of power at the Red Hill 480V emergency bus) could lead to longer delays, although local, manual manipulation of MOVs is still feasible without electrical power.

The total delay time beyond that typically expected under optimum conditions, is considered in the assessment of fuel released. The following discrete delay times were postulated:

1. 0 Hours
2. 4 Hours
3. 8 Hours
4. 12 Hours
5. 24 Hours
6. 72 Hours
7. 336 Hours (i.e., 2 weeks)

Separate fuel releases were evaluated for each of the three sequence conditions and for seven additional delay times (i.e., delays beyond the typical 6-plus hours). Rather than exercise the RHBFST worksheet model for each sequence condition for these seven delay times (21 cases), a simpler, conservative approach was taken. The initial fuel release rate was assumed to continue for the duration of the delay time, and this added release then added to the 0-hour delay time result. This approach is clearly conservative since the initial release rate would decrease as level in the affected RHBFST drops.

Table 6-20 presents the assumed impacts of individual top event failures on the start of fuel transfer from a leaking RHBFST as expressed by a time delay in the start of the fuel transfer. The top events are ordered by event trees which are linked together to assess

leak directly to rock. Many of the early top events in the set have no impact on delay times because the top events are just switches. Multi-state top events may have different time delay impacts depending on the specific top event state; e.g., Top Event GRIDR.

**Table 6-20. Time Delay Impacts for Top Event Failures**

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **CONFIG** | LKLOC | Location of Leak within Facility | N/A |
| **CONFIG** | MOVE | Type of Fuel Movement Initially in Progress | N/A |
| **CONFIG** | TKID | RHBFST Associated with Leak | N/A |
| **CONFIG** | FUEL | Type of Leaking Fuel | N/A |
| **CONFIG** | TKXF | Source RHBFST Associated with Inter-Tank Transfer | N/A |
| **CONFIG** | TKLOC | LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT | N/A |
| **CONFIG** | HEIGHT | Height of Hole in RHBFST that Is Leaking to Rock | N/A |
| **CONFIG** | SIZE | Size of Leak from RHBFST, or Fuel Line Piping | N/A |
| **CONFIG** | DIREC | Side of RHBFST that Tank Leak Is On | N/A |
| **CONFIG** | INVEN | INVEN – Initial RHBFST Inventory Configuration. | N/A |
| **ELECTRICAL** | GRID | Offsite Grid | See GRIDR |
| **ELECTRICAL** | GRIDR | Recovery from Losses of Offsite Grid | HR3 = 4 Hours<br>HR6 = 8 Hours<br>HR12 = 12 Hours<br>HR24 = 24 Hours |
| **ELECTRICAL** | BUN24 | UGPH 2.4 kV Normal Bus | 72 |
| **ELECTRICAL** | BUN48 | UGPH 480V Normal Bus | 72 |
| **ELECTRICAL** | BUE48 | UGPH 480V Emergency Bus | 72 |
| **ELECTRICAL** | GEN1 | Backup generator at ADIT for UGPH 480v Emergency Bus | See GRIDR |
| **ELECTRICAL** | UFAN | ADIT 1 Supply and Exhaust Fans for UGPH cooling Cargo Pumps | 72 |
| **ELECTRICAL** | B3EA | ADIT 3 208V Panel A | 72 |
| **ELECTRICAL** | GEN3 | Backup Generator at ADIT 3 for 480v Panels B and A. | N/A |
| **ELECTRICAL** | BRN48 | Red Hill 480V Normal Bus | 72 |
| **ELECTRICAL** | BRE48 | Red Hill 480V Emergency Bus | 72 |

## Table 6-20. Time Delay Impacts for Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **ELECTRICAL** | GEN5 | Red Hill 480V Emergency Bus | See GRIDR |
| **ELECTRICAL** | LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras | 8 |
| **ELECTRICAL** | AFHE | Automatic Fuel Handling Equipment | 12 |
| **ELECTRICAL** | AFHR | AFHE Condensing and Fans for Heat Removal | 72 |
| **ELECTRICAL** | EFAN | Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply electrical room in LAT) | 72 |
| **ELECTRICAL** | TFAN | Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead) | 72 |
| **OTHERSUP** | CRM | Control Room Electrical Power, Lighting, and Air Conditioning | 72 |
| **OTHERSUP** | ACRM | Alternate Control Room Electrical Power, Lighting, and Air Conditioning | N/A |
| **OTHERSUP** | UHMOV | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs | N/A |
| **OTHERSUP** | CARGO | Two or More Cargo Pumps Available to Move Leaking Fuel Type | N/A |
| **OTHERSUP** | ULIT | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting | N/A |
| **OTHERSUP** | EL72 | Personnel Elevator 72 and Controller | 4 |
| **OTHERSUP** | EL73 | Cargo Elevator 73 | 4 |
| **OTHERSUP** | RMOV | Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and All LAT MOVs | N/A |
| **OTHERSUP** | RHIN | Support for Red Hill Instruments, Indications, Level Alarms, and Signals | N/A |
| **VALVES** | SKIN | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| **VALVES** | BALL | Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| **VALVES** | SKINX | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| **VALVES** | BALLX | BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |

## Table 6-20. Time Delay Impacts for Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **VALVES** | FLISO | FLISO – Successful Closure of the Upstream Sectional Valve | 72 |
| **VALVES** | FLTKC | FLTKC – Successful Isolation of the Fuel Line Leak from All RHBFSTs | 72 |
| **VALVES** | FLTKO | FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied | 72 |
| **VALVES** | EVAC | Sequence Conditions Necessitate Initial Evacuation from RH | 336 |
| **OVERFILL** | OEV | Operators Correctly Specify Fill Evolution and Stop Evolution when Planned at Maximum Operating Level | N/A |
| **OVERFILL** | HOLE | Conditional Probability of Hole Above Maximum Operating Level | N/A |
| **OVERFILL** | OTRIP | After AFHE High Level Alarm, Operators Actuate an Emergency Stop of the Cargo Pumps or Press the Panic Button, then Direct the Rover to Locally Ensure the Skin Valve Is Closed and to Manually Gauge the Same Tank | N/A |
| **OVERFILL** | SWITCH | High Level Mechanical FLOAT Switch Actuates Sending Signals to Deactivate All Facility Pumps, Actuate Timer for Valve Closures, and Signals Skin Valve on Affected Tank to Close | N/A |
| **OVERFILL** | OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger | 8 |
| **OVERFILL** | ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm | 8 |
| **OVERFILL** | OSUP | Management and Red Hill Supervisor Formulate Response | 24 |
| **OVERFILL** | OXFR | Control Room and Red Hill Staff Move Fuel from the Leaking RHBFST | 24 |
| **OVERFILL** | XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST | 72 |
| **OVERFILL** | XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor | 72 |
| **OVERFILL** | XFR3 | Two-Step Fuel Movement to Pump Fuel to Other RHBFSTs | 72 |
| **OVERFILL** | XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor | 72 |

**Table 6-20. Time Delay Impacts for Top Event Failures (Continued)**

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| **OVERFILL** | XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line | N/A |
| **OVERFILL** | DELAY | Tank Empty Delay Time Based on Earlier Failures | N/A |
| **OVERFILL** | REL | REL – Type of Fuel Release Scenario | N/A |

Some assumed time delays are functions of multiple conditions including the states of multiple top events along the sequence path. Table 6-21 summarizes the actual macro logic used in the OVERFILL event tree for assigning the added delay times as a function of all top event success and failure states along a single sequence path. The status of each macro (e.g., TIM336HR, TIM72HR, etc.) represents the logical conditions in which a given delay time is assumed. In the event that multiple delay time macros are true in the same sequence, the longest delay time is used for assessing the amount of fuel released. The longest assumed time delay duration (TIM336HR) is used for sequence conditions in which there is insufficient ullage to empty the affected RHBFST below the hole location. It is assumed that there is always sufficient ullage following overfill events because the amount of fuel that must be removed to uncover the hole is limited and because the source tank should now have plenty of ullage. So the macro for insufficient ullage is never satisfied for OVERFILL events.

**Table 6-21. Overfill Logic for Sequence Dependent Time Delays**

| Macro ID | Macro Logic Rule |
|---|---|
| ULLAGEF | NEVER |
| XFR212JSUC | INVEN=IN212J*(XFR1=S+XFR2=S+XFR3=S+XFR4=S) |
| XFRSUCCESS | XFR212JSUC |
| JHEP24HR | OUFM=F*ORGA1=F+OUFM=F*OSUP=F+OUFM=F*OXFR=F+ORGA1=F*OSUP=F+ORGA1=F*OXFR=F+OSUP=F*OXFR=F |
| JHEP72HR | OUFM=F*ORGA1=F*OXFR=F+OUFM=F*OSUP=F*OXFR=F+ORGA1=F*OSUP=F*OXFR=F+OUFM=F*ORGA1=F*OSUP=F*OXFR=F |
| TIM336HR | ULLAGEF |
| TIM72HR | AFHR=F+B3EA=F+BRE48=F+BRN48=F+BUE48=F+BUN48=F+BUN24=F+CRM=F+EFAN=F+TFAN=F*IETKTOP4 +FLISO=F+FLTKC=F+FLTKO=F+SKIN=F+SKINX=F+BALL=F+BALLX=F+UFAN=F+-XFRSUCCESS+JHEP72HR |
| TIM24HR | OSUP=F+OXFR=F+GRID=F*(GRIDR=HR24)+JHEP24HR |
| TIM12HR | AFHE=F+GRID=F*(GRIDR=HR12) |
| TIM8HR | LPRH=F+ORGA1=F+OUFM=F+GRID=F*GRIDR=HR6 |
| TIM4HR | EL72=F+EL73=F+GRID=F*GRIDR=HR3 |
| TIM0HR | (-(TIM4HR+TIM8HR+TIM12HR+TIM24HR+TIM72HR+TIM336HR)) |

For the most part, time delay macros are made true by the state of a single top event along the sequence path. However, being more likely than multiple equipment failures, multiple operator action failures could appear in the same sequence; e.g., as represented by Macros JHEP24HR and JHEP72HR. In these cases, the overall delay time was taken to be the sum of the individual action delays (i.e., as if the delays occurred in series), provided the actions failures were each related to the function of moving fuel from the affected RHBFST.

The macros which begin with the letters “XFR” deserve special mention. These macros are true if the combination of fuel transfer options available are sufficient to transfer enough fuel to uncover the hole for the hole height postulated. If not, an added 72-hour delay time is assumed to allow time for recovering the unavailable equipment. For the OVERFILL sequences, the amount of fuel that must be transferred is limited so that any of XFR1, XFR2, XFR3, or XFR4 options alone is sufficient.

#### *6.8.2.3 Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT*

The NOZZLE event tree is used to represent the response to internal initiating events involving leakage from fuel line piping connecting directly to a RHBFST to the LAT. The general set of end states are assigned to the event tree and each sequence path is

assigned to a single end state during sequence frequency quantification from that general set.

The gallons released are computed for each of five facility configuration states as represented by Top Event INVEN in the CONFIG event tree. The other four facility configurations, considered for tank leaks, representing conditions during RHBFST returns to service are excluded from this assessment. These five facility configurations distinguish the three different fuel types and the initial fuel level in the RHBFST when the nozzle leak occurs.

Two nozzle hole sizes are modeled; i.e., with equivalent hole diameters of 0.5" and 6". Maintenance errors involving opening a fuel line at a skin valve could lead to larger release openings than the equivalent 6" holes assumed. However, such maintenance error events are lumped together with the random 6" events because, as is noted later, no credit is taken for transferring fuel from the affected RHBFST even for the smaller 6" hole sizes.

The hole location is always postulated to be below the bottom of the RHBFST consistent with being a nozzle leak. The RHBFST worksheet model does not represent hole locations lower than the bottom of the RHBFST. Therefore, slightly larger hole sizes were assumed whose initial fuel release flow rates match the flow rate that would be expected if an additional 18' of head from the bottom of the RHBFST lower dome to the floor of the LAT were to be accounted for. This assumption is likely conservative because the nozzle piping up to the skin valve is above the floor of the LAT.

For the 6" hole size, no credit is given for transferring fuel from the affected RHBFST. Instead, a 336-hour delay time is assumed, but with such a large delay, the RHBFST's contents are fully released long before that time. For the 0.5" hole size, credit is assumed for transferring fuel from the affected RHBFST, but this time with a minimum added delay time of 24 hours. Recall that with such a release of fuel to the LAT the initial response of workers present will be to evacuate the LAT. Remote actions by the control room staff are still possible.

Unlike for simple tank leaks directly to rock, for nozzle leaks, the possibility of two RHBFSTs undergoing an inter-RHBFST gravity transfer is also considered. The affected RHBFST cannot be isolated from the leak location, but the other RHBFST aligned for the transfer may still be isolated. If there is no inter-RHBFST gravity transfer in process or if the second RHBFST is isolated, then a macro, ONETKOPEN, is assigned to be true and the release is just from one RHBFST. However, if an inter-RHBFST gravity transfer was in progress at the time of the nozzle leaks and the second RHBFST is not isolated, then fuel release from both RHBFSTs may occur; i.e., when Macro BOTHTKOPEN is true. The RHBFST worksheet model does not represent flow from two RHBFSTs, so a simple approximation is made for these low frequency sequences. The total release from both RHBFSTs is assumed to equal the release from the affected RHBFST plus the amount of fuel released from a RHBFST which did not have fuel transferred from it. Effectively, this assumption means that for such sequences, no credit is given for transferring fuel from the second RHBFST which remains unisolated.

Therefore, a total of 20 separate sequence conditions are evaluated using the RHBFST worksheet model described in Section 6.8.1.1. The 20 conditions are summarized in Table 6-22 along with the evaluated release of fuel, in gallons, to the LAT which continues until level drops to the 7.5' level in the affected RHBFST at which time the fuel release stops. The input data provided to the RHBFST worksheet model is the same as that listed in Section 6.8.1.1 with the variations noted above. Again the RHBFST worksheet model was used summing the time to the low level alarm plus 6 hours to represent the start of fuel being transferred from the leaking RHBFST at a rate of 2,500 barrels per hour.

**Table 6-22. Summary of Gallons Released for Nozzle Leaks**

| Fuel Config. | Hole Size (inches) | Initial Fuel Level (ft.) | Initial Leak Rate (gpm) | Second Tank Isolated? | Fuel Released if No Fuel Transfer (gallons) | Fuel Release with Fuel Transfer, 0 Delay (gallons) |
|---|---|---|---|---|---|---|
| F24A | 0.5 | 212 | 74.69 | ONETKOPEN | 11,413,507 | 362,327 |
| F24B | 0.5 | 100 | 51.3 | ONETKOPEN | 4,833,304 | 123,587 |
| F76C | 0.5 | 176 | 68.05 | ONETKOPEN | 9,298,442 | 277,433 |
| JP5D | 0.5 | 212 | 74.69 | ONETKOPEN | 11,413,507 | 362,327 |
| JP5E | 0.5 | 14 | 19.19 | ONETKOPEN | 146,052 | 9,067 |
| F24A | 0.5 | 212 | 74.69 | BOTHTKOPEN | 22,827,014 | 11,775,834 |
| F24B | 0.5 | 100 | 51.3 | BOTHTKOPEN | 16,246,811 | 11,537,094 |
| F76C | 0.5 | 176 | 68.05 | BOTHTKOPEN | 18,596,883 | 9,575,875 |
| JP5D | 0.5 | 212 | 74.69 | BOTHTKOPEN | 22,827,014 | 11,775,834 |
| JP5E | 0.5 | 14 | 19.19 | BOTHTKOPEN | 11,559,559 | 11,422,574 |
| F24A | 6.1 | 212 | 10,748 | ONETKOPEN | 11,413,507 | 9,729,154 |
| F24B | 6.1 | 100 | 7,382 | ONETKOPEN | 4,833,304 | 4,168,069 |
| F76C | 6.1 | 176 | 9,793 | ONETKOPEN | 9,361,275 | 7,912,361 |
| JP5D | 6.1 | 212 | 10,748 | ONETKOPEN | 11,413,507 | 9,729,154 |
| JP5E | 6.1 | 14 | 2,762 | ONETKOPEN | 146,052 | 146,052 |
| F24A | 6.1 | 212 | 10,748 | BOTHTKOPEN | 22,827,014 | 21,142,661 |
| F24B | 6.1 | 100 | 7,382 | BOTHTKOPEN | 16,246,811 | 15,581,576 |
| F76C | 6.1 | 176 | 9,793 | BOTHTKOPEN | 18,722,550 | 17,273,636 |
| JP5D | 6.1 | 212 | 10,748 | BOTHTKOPEN | 22,827,014 | 21,142,661 |
| JP5E | 6.1 | 14 | 2,762 | BOTHTKOPEN | 11,559,559 | 11,559,559 |

Additional delays in initiating the fuel transfer may also occur as detailed by the sequence of events along a specific path through the linked event trees. For example, it may take longer than anticipated to confirm that the affected RHBFST is indeed undergoing a loss of fuel inventory. Such a delay would be represented by an initial failure of Top Event ORGA1 in the NOZZLE event tree. If the affected RHBFST was undergoing a fuel evolution (i.e., receiving or issuing) at the time the hole occurs, then the time to the low level warning alarm would be delayed until after the fuel evolution was completed and the RHBFST fuel level drops further while in idle conditions. Use of these delay times for fuel evolutions helps to limit the number of sequence conditions evaluated using the RHBFST worksheet model. The extent of such delays depends on the duration of such fuel evolutions for different fuel types. More significant failures (e.g., loss of power at the Red Hill 480V emergency bus) could lead to longer delays, although local, manual manipulation of MOVs is still feasible without electrical power.

The total delay time beyond that typically expected under optimum conditions, is considered in the assessment of fuel released. The following discrete delay times were postulated:

1. 0 Hours
2. 4 Hours
3. 8 Hours
4. 12 Hours
5. 24 Hours
6. 72 Hours
7. 336 Hours (i.e., 2 weeks)

Separate fuel releases were evaluated for each of the 20 sequence conditions and 7 modeled delay times (i.e., delays beyond the typical 6-plus hours). Rather than exercise the RHBFST worksheet model for each sequence condition for these 7 delay times (140 cases), a simpler, conservative approach was taken. The initial fuel release rate was assumed to continue for the duration of the delay time, and this added release then added to the 0-hour delay time result. This approach is clearly conservative since the initial release rate would decrease as level in the affected RHBFST drops. Checks are made to ensure that the total estimated release does not exceed the initial RHBFST inventory for its initial fuel level.

Table 6-23 presents the modeled impacts of individual top event failures on the start of fuel transfer from a leaking RHBFST as expressed by a time delay in the start of the fuel transfer. The top events are ordered by event trees which are linked together to assess leak directly to rock. Many of the early top events in the set have no impact on delay times because the top events are just switches. Multi-state top events may have different time delay impacts depending on the specific top event state; e.g., Top Event GRIDR.

## Table 6-23. Time Delay Impacts of Top Event Failures

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| CONFIG | LKLOC | Location of Leak within Facility | NA |
| CONFIG | MOVE | Type of Fuel Movement Initially in Progress | 24 Hours per Receipt<br>12 Hours per F24 or JP5 Issue<br>4 Hours per F76 Issue<br>24 Hours per XFER |
| CONFIG | TKID | RHBFST Associated with Leak | N/A |
| CONFIG | FUEL | Type of Leaking Fuel | N/A |
| CONFIG | TKXF | Source RHBFST Associated with Inter-Tank Transfer | N/A |
| CONFIG | TKLOC | LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT | N/A |
| CONFIG | HEIGHT | Height of Hole in RHBFST that is Leaking to Rock | N/A |
| CONFIG | SIZE | Size of Leak from RHBFST, or Fuel Line Piping | N/A |
| CONFIG | DIREC | Side of RHBFST that Tank Leak Is On | N/A |
| CONFIG | INVEN | INVEN – Initial RHBFST Inventory Configuration | N/A |
| ELECTRICAL | GRID | Offsite Grid | See GRIDR |
| ELECTRICAL | GRIDR | Recovery from Losses of Offsite Grid | HR3 = 4 Hours<br>HR6 = 8 Hours<br>HR12 = 12 Hours<br>HR24 = 24 Hours |
| ELECTRICAL | BUN24 | UGPH 2.4 kV Normal Bus | 72 |
| ELECTRICAL | BUN48 | UGPH 480V Normal Bus | 72 |
| ELECTRICAL | BUE48 | UGPH 480V Emergency Bus | 72 |
| ELECTRICAL | GEN1 | Backup Generator at ADIT for UGPH 480V Emergency Bus | See GRIDR |
| ELECTRICAL | UFAN | ADIT 1 Supply and Exhaust Fans for UGPH Cooling Cargo Pumps | 72 |
| ELECTRICAL | B3EA | ADIT 3 208V Panel A | 72 |
| ELECTRICAL | GEN3 | Backup Generator at ADIT 3 for 480v Panels B and A | NA |

## Table 6-23. Time Delay Impacts of Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| ELECTRICAL | BRN48 | Red Hill 480V Normal Bus | 72 |
| ELECTRICAL | BRE48 | Red Hill 480V Emergency Bus | 72 |
| ELECTRICAL | GEN5 | Red Hill 480V Emergency Bus | See GRIDR |
| ELECTRICAL | LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras | 8 |
| ELECTRICAL | AFHE | Automatic Fuel Handling Equipment | 12 |
| ELECTRICAL | AFHR | AFHE Condensing and Fans for Heat Removal | 72 |
| ELECTRICAL | EFAN | Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply Electrical room in LAT) | 72 |
| ELECTRICAL | TFAN | Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead) | 72 |
| OTHERSUP | CRM | Control Room Electrical Power, Lighting, and Air Conditioning | 72 |
| OTHERSUP | ACRM | Alternate Control Room Electrical Power, Lighting, and Air Conditioning | NA |
| OTHERSUP | UHMOV | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs | NA |
| OTHERSUP | CARGO | Two or More Cargo Pumps Available to Move Leaking Fuel Type | 72 |
| OTHERSUP | ULIT | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting | NA |
| OTHERSUP | EL72 | Personnel Elevator 72 and Controller | 4 |
| OTHERSUP | EL73 | Cargo Elevator 73 | 4 |
| OTHERSUP | RMOV | Electrical Power for Red Hill Sectional Valves down to ADIT 3Y and All LAT MOVs | NA |
| OTHERSUP | RHIN | Support for Red Hill Instruments, Indications, Level Alarms, and Signals | NA |

## Table 6-23. Time Delay Impacts of Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| VALVES | SKIN | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| VALVES | BALL | Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| VALVES | SKINX | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| VALVES | BALLX | BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| VALVES | FLISO | FLISO – Successful Closure of the Upstream Sectional Valve | N/A |
| VALVES | FLTKC | FLTKC – Successful Isolation of the Fuel Line Leak from All RHBFSTs | N/A |
| VALVES | FLTKO | FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied | N/A |
| VALVES | EVAC | Sequence Conditions Necessitate Initial Evacuation from RH | 336 (combined with other top event failures) |
| NOZZLE | MSUMP | One of Two Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 | N/A |
| NOZZLE | DOOR | Oil Tight Door below LAT Gallery Closes on High Float Level | N/A |
| NOZZLE | OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger | 8 |
| NOZZLE | OSUM | CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak | 4 |
| NOZZLE | OPAN | CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button | N/A |

**Table 6-23. Time Delay Impacts of Top Event Failures (Continued)**

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| NOZZLE | ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm | 8 |
| NOZZLE | OSUP | Management and Red Hill Supervisor Formulate Response | 24 |
| NOZZLE | OXFR | Control Room and Red Hill Staff Move Fuel from the Leaking RHBFST | 24 |
| NOZZLE | XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST | 72 |
| NOZZLE | XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor | 72 |
| NOZZLE | XFR3 | Two-Step Fuel Movement to Pump Fuel to Other RHBFSTs | 72 |
| NOZZLE | XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor | 72 |
| NOZZLE | XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line | 72 |
| NOZZLE | DELAY | Tank Empty Delay Time Based on Earlier Failures | N/A |
| NOZZLE | REL | REL – Type of Fuel Release Scenario | N/A |

Some assumed time delays are a function of multiple conditions, including on the states of multiple top events along the sequence path. Table 6-24 summarizes the actual macro logic used for assigning the added delay times as a function of all top event success and failure states along a single sequence path. The status of each macro (e.g., TIM336HR, TIM72HR, etc.) represents the logical conditions in which a given delay time is assumed. In the event that multiple delay time macros are true in the same sequence, the longest delay time is used for assessing the amount of fuel released. The longest assumed time delay duration (TIM336HR) is used for sequence conditions in which there is insufficient ullage to empty the affected RHBFST below the hole location. In the event of insufficient ullage, a two week delay is assumed, to allow time for alternative ullage to be made available. In the RHBFST inventory data reviewed, the only concern with sufficient available ullage being available involved the two RHBFSTs which hold F76 fuel. These RHBFSTs were observed to have relatively high fuel levels throughout the period of time reviewed. There would be insufficient ullage to empty one of the RHBFSTs into the other to a level down to 7.5', even allowing for the F76 ullage typically available elsewhere at the upper tank farm.

## Table 6-24. NOZZLE Logic for Sequence Dependent Time Delays

| Macro ID | Macro Logic Rule |
|---|---|
| ULLAGEF | INVEN=F76C*(HEIGHT=LOW+HEIGHT=BOT) |
| XFRF24ASUC | INVEN=F24A*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S)+HEIGHT=MED*(XFR1=S+XFR2=S+XFR3=S)+HEIGHT=LOW*XFR3=S+HEIGHT=BOT*(XFR1=S*XFR2=S*XFR3=S*XFR5=S)) |
| XFRF24BSUC | INVEN=F24B*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW*(XFR2=S+XFR3=S)+HEIGHT=BOT*(XFR3=S*XFR5=S) ) |
| XFRF76CSUC | INVEN=F76C*(HEIGHT=HIGH+HEIGHT=MED*(XFR2=S+XFR3=S)) |
| XFRJP5DSUC | INVEN=JP5D*(HEIGHT=HIGH*(XFR1=S*XFR2=S+XFR3=S)+HEIGHT=MED*(XFR1=S+XFR3=S)+HEIGHT=LOW*XFR3=S +HEIGHT=BOT*XFR3=S*XFR5=S) |
| XFRJP5ESUC | INVEN=JP5E*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW+HEIGHT=BOT*XFR5=S*(XFR2=S+XFR3=S)) |
| XFRF24FSUC | INVEN=RF24F*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S+XFR4=S)+HEIGHT=MED*(XFR1=S*XFR2=S+XFR3=S+XFR4=S)+HEIGHT=LOW*(XFR3=S+XFR4=S)+HEIGHT=BOT*(XFR1=S*XFR2=S*XFR3=S+XFR4=S)*XFR5=S) |
| XFRF76GSUC | INVEN=RF76G*(HEIGHT=HIGH*(XFR2=S+XFR3=S+XFR4=S)+HEIGHT=MED*(XFR3=S+XFR4=S)+HEIGHT=LOW*XFR4=S+HEIGHT=BOT*XFR4=S*XFR5=S) |
| XFRJP5HSUC | INVEN=RJP5H*(HEIGHT=HIGH*(XFR1=S+XFR2=S+XFR3=S+XFR4=S)+HEIGHT=MED*(XFR1=S+XFR3=S+XFR4=S)+HEIGHT=LOW*(XFR3=S+XFR4=S)+HEIGHT=BOT*(XFR3=S+XFR4=S)*XFR5=S) |
| XFR100ISUC | INVEN=R100I*(HEIGHT=HIGH+HEIGHT=MED+HEIGHT=LOW*(XFR2=S+XFR3=S+XFR4=S)+HEIGHT=BOT*(XFR3=S+XFR4=S)*XFR5=S) |
| XFRSUCCESS | XFRF24ASUC+XFRF24BSUC+XFRF76CSUC+XFRJP5DSUC+XFRJP5ESUC+XFRF24FSUC+XFRF76GSUC+XFRJP5HSUC+XFR100ISUC |
| BOTHTKOPEN | MOVE=XFER*-(SKINX=S*-FSUPSKINX*OPAN=S +BALLX=S*-FSUPBALLX*OPAN=S) |
| ONETKOPEN | (-BOTHTKOPEN) |
| JHEP24HR | OUFM=F*ORGA1=F+OUFM=F*OSUP=F+OUFM=F*OXFR=F+ORGA1=F*OSUP=F+ORGA1=F*OXFR=F+OSUP=F*OXFR=F |
| JHEP72HR | OUFM=F*ORGA1=F*OXFR=F+OUFM=F*OSUP=F*OXFR=F+ORGA1=F*OSUP=F*OXFR=F+OUFM=F*ORGA1=F*OSUP=F*OXFR=F |
| TIM336HR | ULLAGEF + EVAC=EVACU*(SKIN=F+ FSUPSKIN+ BALL=F+ FSUPBALL+ MOVE=XFER*(SKINX=F+FSUPSKINX+BALLX=F+FSUPBALLX) +FLTKO=F + -XFRSUCCESS)*IELKLAT+IENOZZLRUP+IENOZZLFUL |

**Table 6-24. NOZZLE Logic for Sequence Dependent Time Delays (Continued)**

| Macro ID | Macro Logic Rule |
|---|---|
| TIM72HR | AFHR=F+B3EA=F+BALL=F+BALLX=F+BRE48=F+BRN48=F+BUE48=F+BUN48=F+BUN24=F+CARGO=F+CRM=F+EFAN=F+TFAN=F*IETKTOP4+SKIN=F+SKINX=F+UFAN=F+(-XFRSUCCESS*-MOVE=IDLE)+JHEP72HR |
| TIM24HR | OSUP=F+OXFR=F+GRID=F*GRIDR=HR24 +(MOVE=RECEV+MOVE=XFER)*-IERTS +IENOZZLS3 +JHEP24HR |
| TIM12HR | AFHE=F+GRID=F*GRIDR=HR12 +MOVE=ISSUE*(FUEL=F24+FUEL=JP5) |
| TIM8HR | LPRH=F+ORGA1=F+OUFM=F+GRID=F*GRIDR=HR6+IERTS*MOVE=RECEV+ MOVE=XFER |
| TIM4HR | EL72=F+EL73=F+GRID=F*GRIDR=HR3 +OSUM=F+FUEL=F76*MOVE=ISSUE |
| TIM0HR | (-(TIM4HR+TIM8HR+TIM12HR+TIM24HR+TIM72HR+TIM336HR)) |

For the most part, time delay macros are made true by the state of a single top event along the sequence path. However, being more likely than multiple equipment failures, multiple operator action failures could appear in the same sequence; e.g., Macros JHEP24HR and JHEP72HR. In these cases, the overall delay time was taken to be the sum of the individual action delays (i.e., as if the delays occurred in series), provided the failure actions were each related to the function of moving fuel from the affected RHBFST.

The macros which begin with the letters “XFR” deserve special mention. These macros are true if for the specific sequence facility configuration (e.g., F24A) as represent by top event INVEN, the combination of fuel transfer options available are sufficient to transfer enough fuel to uncover the hole for the hole height location. If not, an added 72-hour delay time is assumed to allow time for recovering the unavailable equipment.

#### *6.8.2.4 Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel*

The TUNLEAK event tree is used to represent the response to the initiating events that involve leakage from other fuel line piping into the LAT or to the Harbor Tunnel. The general set of end states are assigned to the event tree and during sequence frequency quantification each sequence path is assigned to a single end state from that general set.

The evaluation of gallons released for each end state for the TUNLEAK event tree is the most complicated of the four frontline event trees. This is because not only are there three fuel line types, but each fuel may be released from the five different sections of piping; i.e., see Figure 6-3. These fuel line sections hold different volumes of fuel and are of different sizes. Moreover, the sections are of different lengths, inclines, and proximity to tunnel sumps whose pumps starting serve as a cue for subsequent operator

actions. Further, two different hole sizes are postulated; i.e., 0.5" and 6" equivalent diameter holes.

Here also the plant response to the initial pipe leak is more involved. The sequence of response events, can affect the amount of fuel released. The operators may close a sectional valve to limit gravity flow from upgrade fuel lines. Whether the facility is idle at the time of initial release, or undergoing a fuel movement can also affect the amount released. If a fuel movement is in progress, the operators may close the affected RHBFST's skin valve to isolate flow from it out the leaking fuel line. After isolation of the affected RHBFST, the fuel line pressure at the hole location driving the release would also be lower. The closure of a sectional valve may also isolate an initially aligned RHBFST from the hole depending on the hole location and fuel type. If an inter-RHBFST gravity transfer is in progress at the time the release initiates, then one or both RHBFSTs may remain aligned depending on the failure of the operators to end the fuel movement by closing the skin valve of both RHBFSTs.

Here the number of sequence conditions for evaluation numbered 168; i.e., 6 alternative sequence responses for each of 28 unique initiating events. For the 0-hour additional delay time, these sequence conditions were evaluated by a combination of simple volume balances and use of the RHBFST worksheet model (see Section 6.8.1.1) when transferring fuel from an unisolated RHBFST is applicable. For the low frequency sequence conditions involving two RHBFSTs remaining aligned; the release contribution from the second RHBFST was assumed the same as for the sequence condition with only one RHBFST case remaining aligned; i.e., effectively doubling the contribution.

The 168 sequence conditions are summarized in Table 6-25 along with the evaluated release of fuel, in gallons through the hole in the fuel line. If the fuel line is isolated from all RHBFSTs, the maximum amount released is the fuel line inventory above the modeled hole location. If an initially aligned RHBFST remains aligned, fuel release stops only when fuel level in the affected RHBFST drops below 7.5'. If a RHBFST is initially aligned but is isolated, the amount of fuel released may exceed the initial fuel inventory above the hole location because the aligned RHBFST refills the leaking fuel line until RHBFST isolation is affected. The input data used for the RHBFST worksheet model is the same as that listed in Section 6.8.1.1, with some variations. One key difference is that the initial fuel level in an initially aligned RHBFST was conservatively assumed to be 212'. This assumption reduces the number of sequence conditions and is conservative.

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| A | SF24AS | 0.5 | IDLE | 54.0 | Yes | Isolated | 159,907 | N/A | 8,273 |
| A | SF24AS | 0.5 | IDLE | 54.0 | No | Isolated | 159,907 | N/A | 159,907 |
| A | SF24AS | 0.5 | (ISSUE+RECEV+XFER) | 89.4 | Yes | Isolated | 159,907 | N/A | 9,099 |
| A | SF24AS | 0.5 | (ISSUE+RECEV+XFER) | 89.4 | No | Isolated | 159,907 | N/A | 162,947 |
| A | SF24AS | 0.5 | (ISSUE+RECEV+XFER) | 89.4 | N/A | 1 Not | 159,907 | 431,914 | 594,861 |
| A | SF24AS | 0.5 | XFER | 89.4 | N/A | 2 Not | 159,907 | 863,828 | 1,026,775 |
| B | SF24BS | 0.5 | IDLE | 41.7 | Yes | Isolated | 98,107 | N/A | 65,673 |
| B | SF24BS | 0.5 | IDLE | 41.7 | No | Isolated | 98,107 | N/A | 98,107 |
| B | SF24BS | 0.5 | (ISSUE+RECEV+XFER) | 82.5 | Yes | Isolated | 98,107 | N/A | 71,004 |
| B | SF24BS | 0.5 | (ISSUE+RECEV+XFER) | 82.5 | No | Isolated | 98,107 | N/A | 113,370 |
| B | SF24BS | 0.5 | (ISSUE+RECEV+XFER) | 82.5 | N/A | 1 Not | 98,107 | 403,010 | 516,380 |
| B | SF24BS | 0.5 | XFER | 82.5 | N/A | 2 Not | 98,107 | 806,020 | 919,390 |
| C | SF24CS | 0.5 | IDLE | 23.8 | Yes | Isolated | 31,218 | N/A | 17,108 |
| C | SF24CS | 0.5 | IDLE | 23.8 | No | Isolated | 31,218 | N/A | 31,218 |
| C | SF24CS | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | Yes | Isolated | 31,218 | N/A | 29,913 |
| C | SF24CS | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | No | Isolated | 31,218 | N/A | 49,983 |
| C | SF24CS | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | N/A | 1 Not | 31,218 | 367,975 | 417,958 |
| C | SF24CS | 0.5 | XFER | 75.1 | N/A | 2 Not | 31,218 | 735,950 | 785,933 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| D | SF24DS | 0.5 | IDLE | 16.7 | Yes | Isolated | 10,035 | N/A | 10,035 |
| D | SF24DS | 0.5 | IDLE | 16.7 | No | Isolated | 10,035 | N/A | 10,035 |
| D | SF24DS | 0.5 | (ISSUE+RECEV+XFER) | 73.1 | Yes | Isolated | 10,035 | N/A | 12,155 |
| D | SF24DS | 0.5 | (ISSUE+RECEV+XFER) | 73.1 | No | Isolated | 10,035 | N/A | 12,155 |
| D | SF24DS | 0.5 | (ISSUE+RECEV+XFER) | 73.1 | N/A | 1 Not | 10,035 | 354,213 | 356,345 |
| D | SF24DS | 0.5 | XFER | 73.1 | N/A | 2 Not | 10,035 | 708,426 | 720,581 |
| A | SJP5AS | 0.5 | IDLE | 55.8 | Yes | Isolated | 215,568 | N/A | 10,236 |
| A | SJP5AS | 0.5 | IDLE | 55.8 | No | Isolated | 215,568 | N/A | 215,568 |
| A | SJP5AS | 0.5 | (ISSUE+RECEV+XFER) | 93.1 | Yes | Isolated | 215,568 | N/A | 10,833 |
| A | SJP5AS | 0.5 | (ISSUE+RECEV+XFER) | 93.1 | No | Isolated | 215,568 | N/A | 218,732 |
| A | SJP5AS | 0.5 | (ISSUE+RECEV+XFER) | 93.1 | N/A | 1 Not | 215,568 | 446,817 | 665,549 |
| A | SJP5AS | 0.5 | XFER | 93.1 | N/A | 2 Not | 215,568 | 893,634 | 1,112,366 |
| B | SJP5BS | 0.5 | IDLE | 44.0 | Yes | Isolated | 137,343 | N/A | 81,416 |
| B | SJP5BS | 0.5 | IDLE | 44.0 | No | Isolated | 137,343 | N/A | 137,343 |
| B | SJP5BS | 0.5 | (ISSUE+RECEV+XFER) | 86.5 | Yes | Isolated | 137,343 | N/A | 86,385 |
| B | SJP5BS | 0.5 | (ISSUE+RECEV+XFER) | 86.5 | No | Isolated | 137,343 | N/A | 153,173 |
| B | SJP5BS | 0.5 | (ISSUE+RECEV+XFER) | 86.5 | N/A | 1 Not | 137,343 | 417,214 | 570,387 |
| B | SJP5BS | 0.5 | XFER | 86.5 | N/A | 2 Not | 137,343 | 834,428 | 987,601 |
| C | SJP5CS | 0.5 | IDLE | 27.6 | Yes | Isolated | 52,677 | N/A | 21,011 |
| C | SJP5CS | 0.5 | IDLE | 27.6 | No | Isolated | 52,677 | N/A | 52,677 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| C | SJP5CS | 0.5 | (ISSUE+RECEV+XFER) | 79.4 | Yes | Isolated | 52,677 | N/A | 33,969 |
| C | SJP5CS | 0.5 | (ISSUE+RECEV+XFER) | 79.4 | No | Isolated | 52,677 | N/A | 72,535 |
| C | SJP5CS | 0.5 | (ISSUE+RECEV+XFER) | 79.4 | N/A | 1 Not | 52,677 | 384,535 | 457,070 |
| C | SJP5CS | 0.5 | XFER | 79.4 | N/A | 2 Not | 52,677 | 769,070 | 841,605 |
| D | SJP5DS | 0.5 | IDLE | 23.8 | Yes | Isolated | 30,022 | N/A | 9,282 |
| D | SJP5DS | 0.5 | IDLE | 23.8 | No | Isolated | 30,022 | N/A | 30,022 |
| D | SJP5DS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | Yes | Isolated | 30,022 | N/A | 10,342 |
| D | SJP5DS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | No | Isolated | 30,022 | N/A | 31,821 |
| D | SJP5DS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | N/A | 1 Not | 30,022 | 354,213 | 377,514 |
| D | SJP5DS | 0.5 | XFER | 78.2 | N/A | 2 Not | 30,022 | 735,950 | 759,252 |
| E | SJP5ES | 0.5 | IDLE | 13.9 | Yes | Isolated | 10,739 | N/A | 10,739 |
| E | SJP5ES | 0.5 | IDLE | 13.9 | No | Isolated | 10,739 | N/A | 10,739 |
| E | SJP5ES | 0.5 | (ISSUE+RECEV+XFER) | 75.8 | Yes | Isolated | 10,739 | N/A | 14,605 |
| E | SJP5ES | 0.5 | (ISSUE+RECEV+XFER) | 75.8 | No | Isolated | 10,739 | N/A | 14,605 |
| E | SJP5ES | 0.5 | (ISSUE+RECEV+XFER) | 75.8 | N/A | 1 Not | 10,739 | 367,975 | 382,580 |
| E | SJP5ES | 0.5 | XFER | 75.8 | N/A | 2 Not | 10,739 | 735,950 | 750,555 |
| A | SF76AS | 0.5 | IDLE | 54.0 | Yes | Isolated | 650,058 | N/A | 27,361 |
| A | SF76AS | 0.5 | IDLE | 54.0 | No | Isolated | 650,058 | N/A | 650,058 |
| A | SF76AS | 0.5 | (ISSUE+RECEV+XFER) | 92.0 | Yes | Isolated | 650,058 | N/A | 28,382 |
| A | SF76AS | 0.5 | (ISSUE+RECEV+XFER) | 92.0 | No | Isolated | 650,058 | N/A | 653,186 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| A | SF76AS | 0.5 | (ISSUE+RECEV+XFER) | 92.0 | N/A | 1 Not | 650,058 | 443,762 | 1,096,948 |
| A | SF76AS | 0.5 | XFER | 92.0 | N/A | 2 Not | 650,058 | 887,524 | 1,540,710 |
| B | SF76BS | 0.5 | IDLE | 41.7 | Yes | Isolated | 392,469 | N/A | 242,099 |
| B | SF76BS | 0.5 | IDLE | 41.7 | No | Isolated | 392,469 | N/A | 392,469 |
| B | SF76BS | 0.5 | (ISSUE+RECEV+XFER) | 85.4 | Yes | Isolated | 392,469 | N/A | 247,958 |
| B | SF76BS | 0.5 | (ISSUE+RECEV+XFER) | 85.4 | No | Isolated | 392,469 | N/A | 408,092 |
| B | SF76BS | 0.5 | (ISSUE+RECEV+XFER) | 85.4 | N/A | 1 Not | 392,469 | 414,240 | 822,332 |
| B | SF76BS | 0.5 | XFER | 85.4 | N/A | 2 Not | 392,469 | 828,480 | 1,236,572 |
| C | SF76CS | 0.5 | IDLE | 23.8 | Yes | Isolated | 113,667 | N/A | 52,427 |
| C | SF76CS | 0.5 | IDLE | 23.8 | No | Isolated | 113,667 | N/A | 113,667 |
| C | SF76CS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | Yes | Isolated | 113,667 | N/A | 66,017 |
| C | SF76CS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | No | Isolated | 113,667 | N/A | 133,217 |
| C | SF76CS | 0.5 | (ISSUE+RECEV+XFER) | 78.2 | N/A | 1 Not | 113,667 | 378,786 | 512,003 |
| C | SF76CS | 0.5 | XFER | 78.2 | N/A | 2 Not | 113,667 | 757,572 | 890,789 |
| D | SF76DS | 0.5 | IDLE | 19.4 | Yes | Isolated | 46,156 | N/A | 21,684 |
| D | SF76DS | 0.5 | IDLE | 19.4 | No | Isolated | 46,156 | N/A | 46,156 |
| D | SF76DS | 0.5 | (ISSUE+RECEV+XFER) | 77.0 | Yes | Isolated | 46,156 | N/A | 22,815 |
| D | SF76DS | 0.5 | (ISSUE+RECEV+XFER) | 77.0 | No | Isolated | 46,156 | N/A | 47,926 |
| D | SF76DS | 0.5 | (ISSUE+RECEV+XFER) | 77.0 | N/A | 1 Not | 46,156 | 373,364 | 400,284 |
| D | SF76DS | 0.5 | XFER | 77.0 | N/A | 2 Not | 46,156 | 746,728 | 794,654 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| E | SF76ES | 0.5 | IDLE | 9.8 | Yes | Isolated | 12,555 | N/A | 12,555 |
| E | SF76ES | 0.5 | IDLE | 9.8 | No | Isolated | 12,555 | N/A | 12,555 |
| E | SF76ES | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | Yes | Isolated | 12,555 | N/A | 17,288 |
| E | SF76ES | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | No | Isolated | 12,555 | N/A | 17,288 |
| E | SF76ES | 0.5 | (ISSUE+RECEV+XFER) | 75.1 | N/A | 1 Not | 12,555 | 365,147 | 382,435 |
| E | SF76ES | 0.5 | XFER | 75.1 | N/A | 2 Not | 12,555 | 730,294 | 747,582 |
| A | SF24AL | 6 | IDLE | 7,781 | Yes | Isolated | 159,907 | N/A | 114,993 |
| A | SF24AL | 6 | IDLE | 7,781 | No | Isolated | 159,907 | N/A | 159,907 |
| A | SF24AL | 6 | (ISSUE+RECEV+XFER) | 12,867 | Yes | Isolated | 159,907 | N/A | 179,764 |
| A | SF24AL | 6 | (ISSUE+RECEV+XFER) | 12,867 | No | Isolated | 159,907 | N/A | 333,612 |
| A | SF24AL | 6 | (ISSUE+RECEV+XFER) | 12,867 | N/A | 1 Not | 159,907 | 9,880,724 | 10,214,336 |
| A | SF24AL | 6 | XFER | 12,867 | N/A | 2 Not | 159,907 | 19,761,448 | 20,095,060 |
| B | SF24BL | 6 | IDLE | 6,008 | Yes | Isolated | 98,107 | N/A | 98,107 |
| B | SF24BL | 6 | IDLE | 6,008 | No | Isolated | 98,107 | N/A | 98,107 |
| B | SF24BL | 6 | (ISSUE+RECEV+XFER) | 11,880 | Yes | Isolated | 98,107 | N/A | 471,541 |
| B | SF24BL | 6 | (ISSUE+RECEV+XFER) | 11,880 | No | Isolated | 98,107 | N/A | 513,907 |
| B | SF24BL | 6 | (ISSUE+RECEV+XFER) | 11,880 | N/A | 1 Not | 98,107 | 9,853,806 | 10,367,713 |
| B | SF24BL | 6 | XFER | 11,880 | N/A | 2 Not | 98,107 | 19,707,612 | 20,221,519 |
| C | SF24CL | 6 | IDLE | 3,433 | Yes | Isolated | 31,218 | N/A | 31,218 |
| C | SF24CL | 6 | IDLE | 3,433 | No | Isolated | 31,218 | N/A | 31,218 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| C | SF24CL | 6 | (ISSUE+RECEV+XFER) | 10,808 | Yes | Isolated | 31,218 | N/A | 681,244 |
| C | SF24CL | 6 | (ISSUE+RECEV+XFER) | 10,808 | No | Isolated | 31,218 | N/A | 701,314 |
| C | SF24CL | 6 | (ISSUE+RECEV+XFER) | 10,808 | N/A | 1 Not | 31,218 | 9,688,352 | 10,389,666 |
| C | SF24CL | 6 | XFER | 10,808 | N/A | 2 Not | 31,218 | 19,376,704 | 20,078,018 |
| D | (SF24DL+SF24I+ SF24M) | 6 | IDLE | 2,402 | Yes | Isolated | 10,035 | N/A | 10,035 |
| D | (SF24DL+SF24I+ SF24M) | 6 | IDLE | 2,402 | No | Isolated | 10,035 | N/A | 10,035 |
| D | (SF24DL+SF24I+ SF24M) | 6 | (ISSUE+RECEV+XFER) | 10,526 | Yes | Isolated | 10,035 | N/A | 146,873 |
| D | (SF24DL+SF24I+ SF24M) | 6 | (ISSUE+RECEV+XFER) | 10,526 | No | Isolated | 10,035 | N/A | 146,873 |
| D | (SF24DL+SF24I+ SF24M) | 6 | (ISSUE+RECEV+XFER) | 10,526 | N/A | 1 Not | 10,035 | 9,633,429 | 9,780,302 |
| D | (SF24DL+SF24I+ SF24M) | 6 | XFER | 10,526 | N/A | 2 Not | 10,035 | 19,266,858 | 19,413,731 |
| A | SJP5AL | 6 | IDLE | 8,034 | Yes | Isolated | 215,568 | N/A | 120,948 |
| A | SJP5AL | 6 | IDLE | 8,034 | No | Isolated | 215,568 | N/A | 215,568 |
| A | SJP5AL | 6 | (ISSUE+RECEV+XFER) | 13,401 | Yes | Isolated | 215,568 | N/A | 187,242 |
| A | SJP5AL | 6 | (ISSUE+RECEV+XFER) | 13,401 | No | Isolated | 215,568 | N/A | 395,141 |
| A | SJP5AL | 6 | (ISSUE+RECEV+XFER) | 13,401 | N/A | 1 Not | 215,568 | 10,056,460 | 10,451,601 |
| A | SJP5AL | 6 | XFER | 13,401 | N/A | 2 Not | 215,568 | 20,112,920 | 20,508,061 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| B | SJP5BL | 6 | IDLE | 6,333 | Yes | Isolated | 137,343 | N/A | 137,343 |
| B | SJP5BL | 6 | IDLE | 6,333 | No | Isolated | 137,343 | N/A | 137,343 |
| B | SJP5BL | 6 | (ISSUE+RECEV+XFER) | 12,456 | Yes | Isolated | 137,343 | N/A | 494,059 |
| B | SJP5BL | 6 | (ISSUE+RECEV+XFER) | 12,456 | No | Isolated | 137,343 | N/A | 560,847 |
| B | SJP5BL | 6 | (ISSUE+RECEV+XFER) | 12,456 | N/A | 1 Not | 137,343 | 9,933,083 | 10,493,930 |
| B | SJP5BL | 6 | XFER | 12,456 | N/A | 2 Not | 137,343 | 19,866,166 | 20,427,013 |
| C | SJP5CL | 6 | IDLE | 3,974 | Yes | Isolated | 52,677 | N/A | 52,677 |
| C | SJP5CL | 6 | IDLE | 3,974 | No | Isolated | 52,677 | N/A | 52,677 |
| C | SJP5CL | 6 | (ISSUE+RECEV+XFER) | 11,438 | Yes | Isolated | 52,677 | N/A | 711,829 |
| C | SJP5CL | 6 | (ISSUE+RECEV+XFER) | 11,438 | No | Isolated | 52,677 | N/A | 750,395 |
| C | SJP5CL | 6 | (ISSUE+RECEV+XFER) | 11,438 | N/A | 1 Not | 52,677 | 9,781,725 | 10,532,120 |
| C | SJP5CL | 6 | XFER | 11,438 | N/A | 2 Not | 52,677 | 19,563,450 | 20,313,845 |
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | IDLE | 3,431 | Yes | Isolated | 30,022 | N/A | 30,022 |
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | IDLE | 3,431 | No | Isolated | 30,022 | N/A | 30,022 |
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | (ISSUE+RECEV+XFER) | 11,261 | Yes | Isolated | 30,022 | N/A | 141,424 |
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | (ISSUE+RECEV+XFER) | 11,261 | No | Isolated | 30,022 | N/A | 162,902 |
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | (ISSUE+RECEV+XFER) | 11,261 | N/A | 1 Not | 30,022 | 9,755,969 | 9,918,871 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| D | (SJP5DL+SJP5I+ SJP5M) | 6 | XFER | 11,261 | N/A | 2 Not | 30,022 | 19,511,938 | 19,674,840 |
| E | SJP5EL | 6 | IDLE | 2,000 | Yes | Isolated | 10,739 | N/A | 10,739 |
| E | SJP5EL | 6 | IDLE | 2,000 | No | Isolated | 10,739 | N/A | 10,739 |
| E | SJP5EL | 6 | (ISSUE+RECEV+XFER) | 10,910 | Yes | Isolated | 10,739 | N/A | 142,750 |
| E | SJP5EL | 6 | (ISSUE+RECEV+XFER) | 10,910 | No | Isolated | 10,739 | N/A | 142,750 |
| E | SJP5EL | 6 | (ISSUE+RECEV+XFER) | 10,910 | N/A | 1 Not | 10,739 | 9,700,312 | 9,843,062 |
| E | SJP5EL | 6 | XFER | 10,910 | N/A | 2 Not | 10,739 | 19,400,624 | 19,543,374 |
| A | SF76AL | 6 | IDLE | 7,781 | Yes | Isolated | 650,058 | N/A | 135,744 |
| A | SF76AL | 6 | IDLE | 7,781 | No | Isolated | 650,058 | N/A | 650,058 |
| A | SF76AL | 6 | (ISSUE+RECEV+XFER) | 13,250 | Yes | Isolated | 650,058 | N/A | 202,804 |
| A | SF76AL | 6 | (ISSUE+RECEV+XFER) | 13,250 | No | Isolated | 650,058 | N/A | 827,608 |
| A | SF76AL | 6 | (ISSUE+RECEV+XFER) | 13,250 | N/A | 1 Not | 650,058 | 10,037,425 | 10,865,033 |
| A | SF76AL | 6 | XFER | 13,250 | N/A | 2 Not | 650,058 | 20,074,850 | 20,902,458 |
| B | SF76BL | 6 | IDLE | 6,008 | Yes | Isolated | 392,469 | N/A | 392,469 |
| B | SF76BL | 6 | IDLE | 6,008 | No | Isolated | 392,469 | N/A | 392,469 |
| B | SF76BL | 6 | (ISSUE+RECEV+XFER) | 12,294 | Yes | Isolated | 392,469 | N/A | 662,625 |
| B | SF76BL | 6 | (ISSUE+RECEV+XFER) | 12,294 | No | Isolated | 392,469 | N/A | 822,759 |
| B | SF76BL | 6 | (ISSUE+RECEV+XFER) | 12,294 | N/A | 1 Not | 392,469 | 9,912,317 | 10,735,076 |
| B | SF76BL | 6 | XFER | 12,294 | N/A | 2 Not | 392,469 | 19,824,634 | 20,647,393 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| C | SF76CL | 6 | IDLE | 3,433 | Yes | Isolated | 113,667 | N/A | 113,667 |
| C | SF76CL | 6 | IDLE | 3,433 | No | Isolated | 113,667 | N/A | 113,667 |
| C | SF76CL | 6 | (ISSUE+RECEV+XFER) | 11,262 | Yes | Isolated | 113,667 | N/A | 733,449 |
| C | SF76CL | 6 | (ISSUE+RECEV+XFER) | 11,262 | No | Isolated | 113,667 | N/A | 800,649 |
| C | SF76CL | 6 | (ISSUE+RECEV+XFER) | 11,262 | N/A | 1 Not | 113,667 | 9,758,863 | 10,559,512 |
| C | SF76CL | 6 | XFER | 11,262 | N/A | 2 Not | 113,667 | 19,517,726 | 19,631,454 |
| D | SF76DL | 6 | IDLE | 2,787 | Yes | Isolated | 46,156 | N/A | 46,156 |
| D | SF76DL | 6 | IDLE | 2,787 | No | Isolated | 46,156 | N/A | 46,156 |
| D | SF76DL | 6 | (ISSUE+RECEV+XFER) | 11,082 | Yes | Isolated | 46,156 | N/A | 151,812 |
| D | SF76DL | 6 | (ISSUE+RECEV+XFER) | 11,082 | No | Isolated | 46,156 | N/A | 176,923 |
| D | SF76DL | 6 | (ISSUE+RECEV+XFER) | 11,082 | N/A | 1 Not | 46,156 | 9,726,916 | 9,903,839 |
| D | SF76DL | 6 | XFER | 11,082 | N/A | 2 Not | 46,156 | 19,453,832 | 19,630,755 |
| E | (SF76EL+SF76I+ SF76M) | 6 | IDLE | 1,414 | Yes | Isolated | 12,555 | N/A | 12,555 |
| E | (SF76EL+SF76I+ SF76M) | 6 | IDLE | 1,414 | No | Isolated | 12,555 | N/A | 12,555 |
| E | (SF76EL+SF76I+ SF76M) | 6 | (ISSUE+RECEV+XFER) | 10,818 | Yes | Isolated | 12,555 | N/A | 200,789 |
| E | (SF76EL+SF76I+ SF76M) | 6 | (ISSUE+RECEV+XFER) | 10,818 | No | Isolated | 12,555 | N/A | 200,789 |

## Table 6-25. Summary of Gallons Released for TUNLEAK Event Tree (Continued)

| Fuel Line Section | Initiating Event(s) | Hole Size (inches) | Fuel Movement Status | Initial Release Rate (gpm) | Section Valve Isolated? | RHBFST Isolated; 1 or 2 Not Isolated? | Gallons in Fuel Line above Hole | Release from RHBFST if Not Isolated | Total Gallons Released |
|---|---|---|---|---|---|---|---|---|---|
| E | (SF76EL+SF76I+ SF76M) | 6 | (ISSUE+RECEV+XFER) | 10,818 | N/A | 1 Not | 12,555 | 9,682,337 | 9,883,126 |
| E | (SF76EL+SF76I+ SF76M) | 6 | XFER | 10,818 | N/A | 2 Not | 12,555 | 19,364,674 | 19,565,463 |

The gallons of fuel released presented in Table 6-25 for each sequence condition, assume a realistic time (i.e., about 6 hours) that is needed to confirm the release, plan, and initiate the transfer of fuel from the leaking RHBFST after the AFHE low level warning is received. Additional delays in initiating the fuel transfer may also occur as detailed by the sequence of events along a specific path through the linked event trees. For example, it may take longer than anticipated to confirm that the affected RHBFST is indeed undergoing a loss of fuel inventory. Such a delay would be represented by an initial failure of Top Event ORGA1 in the TKLEAK event tree. If the affected RHBFST was undergoing a fuel evolution (i.e., receiving or issuing) at the time the hole occurs, then the time to the low level warning alarm would be delayed until after the fuel evolution was completed and the RHBFST fuel level drops further while in idle conditions. Use of these delay times for fuel evolutions helps to limit the number of sequence conditions evaluated using the RHBFST worksheet model. The extent of such delays depends on the duration of such fuel evolutions for different fuel types. More significant failures (e.g., loss of power at the Red Hill 480V emergency bus) could lead to longer delays, although local, manual manipulation of MOVs is still feasible without electrical power.

The total delay time beyond that typically expected under optimum conditions, is considered in the assessment of fuel released. The following discrete delay times were postulated:

1. 0 Hours
2. 4 Hours
3. 8 Hours
4. 12 Hours
5. 24 Hours
6. 72 Hours
7. 336 Hours (i.e., 2 weeks)

Separate fuel releases were evaluated for each of the 168 initiating event and sequence response combinations and 7 modeled delay times; i.e., delays beyond the typical 6-plus hours. Rather than exercise the RHBFST worksheet model for each sequence condition when fuel transfer from an aligned RHBFST was applicable, a simpler, conservative approach was taken. The initial fuel release rate was assumed to continue for the duration of the delay time, and this added release then added to the 0-hour delay time fuel release result. This approach is clearly conservative since the initial release rate would decrease as level in the affected RHBFST drops.

Table 6-26 presents the assumed impacts of individual top event failures on the start of fuel transfer from a leaking RHBFST as expressed by a time delay in the start of the fuel transfer. The top events are ordered by event trees which are linked together to assess leak directly to rock. Many of the early top events in the set have no impact on delay times because the top events are just switches. Multi-state top events may have different time delay impacts depending on the specific top event state; e.g., Top Event GRIDR.

## Table 6-26. Time Delay Impacts of TUNLEAK Top Event Failures

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| CONFIG | LKLOC | Location of Leak within Facility | N/A |
| CONFIG | MOVE | Type of Fuel Movement Initially in Progress | 24 Hours per Receipt<br>12 Hours per F24 or JP5 Issue<br>4 Hours per F76 Issue<br>24 Hours per XFER |
| CONFIG | TKID | RHBFST Associated with Leak | N/A |
| CONFIG | FUEL | Type of Leaking Fuel | N/A |
| CONFIG | TKXF | Source RHBFST Associated with Inter-Tank Transfer | N/A |
| CONFIG | TKLOC | LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT | N/A |
| CONFIG | HEIGHT | Height of Hole in RHBFST that Is Leaking to Rock | N/A |
| CONFIG | SIZE | Size of Leak from RHBFST, or Fuel Line Piping | N/A |
| CONFIG | DIREC | Side of RHBFST that Tank Leak Is On | N/A |
| CONFIG | INVEN | INVEN – Initial RHBFST Inventory Configuration | N/A |
| ELECTRICAL | GRID | Offsite Grid | See GRIDR |
| ELECTRICAL | GRIDR | Recovery from Losses of Offsite Grid | HR3 = 4 Hours<br>HR6 = 8 Hours<br>HR12 = 12 Hours<br>HR24 = 24 Hours |
| ELECTRICAL | BUN24 | UGPH 2.4 kV Normal Bus | 72 |
| ELECTRICAL | BUN48 | UGPH 480V Normal Bus | 72 |
| ELECTRICAL | BUE48 | UGPH 480V Emergency Bus | 72 |
| ELECTRICAL | GEN1 | Backup Generator at ADIT for UGPH 480V Emergency Bus | See GRIDR |
| ELECTRICAL | UFAN | ADIT 1 Supply and Exhaust Fans for UGPH Cooling Cargo Pumps | 72 |
| ELECTRICAL | B3EA | ADIT 3 208V Panel A | 72 |
| ELECTRICAL | GEN3 | Backup Generator at ADIT 3 for 480V Panels B and A | NA |
| ELECTRICAL | BRN48 | Red Hill 480V Normal Bus | 72 |
| ELECTRICAL | BRE48 | Red Hill 480V Emergency Bus | 72 |

## Table 6-26. Time Delay Impacts of TUNLEAK Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| ELECTRICAL | GEN5 | Red Hill 480V Emergency Bus | See GRIDR |
| ELECTRICAL | LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras | 8 |
| ELECTRICAL | AFHE | Automatic Fuel Handling Equipment | 12 |
| ELECTRICAL | AFHR | AFHE Condensing and Fans for Heat Removal | 72 |
| ELECTRICAL | EFAN | Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply electrical room in LAT) | 72 |
| ELECTRICAL | TFAN | Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead) | 72 |
| OTHERSUP | CRM | Control Room Electrical Power, Lighting, and Air Conditioning | 72 |
| OTHERSUP | ACRM | Alternate Control Room Electrical Power, Lighting, and Air Conditioning | N/A |
| OTHERSUP | UHMOV | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs | N/A |
| OTHERSUP | CARGO | Two or More Cargo Pumps Available to Move Leaking Fuel Type | 72 |
| OTHERSUP | ULIT | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting | N/A |
| OTHERSUP | EL72 | Personnel Elevator 72 and Controller | 4 |
| OTHERSUP | EL73 | Cargo Elevator 73 | 4 |
| OTHERSUP | RMOV | Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and All LAT MOVs | N/A |
| OTHERSUP | RHIN | Support for Red Hill Instruments, Indications, Level Alarms, and Signals. | N/A |
| VALVES | SKIN | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| VALVES | BALL | Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree | 72 |
| VALVES | SKINX | Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |

## Table 6-26. Time Delay Impacts of TUNLEAK Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| VALVES | BALLX | BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree | 72 |
| VALVES | FLISO | FLISO – Successful Closure of the Upstream Sectional Valve | N/A |
| VALVES | FLTKC | FLTKC – Successful Isolation of the Fuel Line Leak from All RHBFSTs | N/A |
| VALVES | FLTKO | FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied | 336 |
| VALVES | EVAC | Sequence Conditions Necessitate Initial Evacuation from RH | 336 (combined with other top event failures) |
| TUNLEAK | USUMP | One of Two Harbor Tunnel Sump Pumps at UGPH Entry Start and Transfer Leaked Fuel | N/A |
| TUNLEAK | MSUMP | One of Two Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 | N/A |
| TUNLEAK | DOOR | Oil-Tight Door below LAT Gallery Closes on High Float Level | N/A |
| TUNLEAK | OPFL | Operators Recognize Drop in Fuel Line Pressure | N/A |
| TUNLEAK | OSUM | CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak | 4 |
| TUNLEAK | OPAN | CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button | N/A |
| TUNLEAK | OSEC | CR Operators REMOTE MANUALLY Close Sectional Valve(s) and Ball Valves as Applicable; Execution Only | N/A |
| TUNLEAK | OUFM | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger | 8 |
| TUNLEAK | ORGA1 | Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm | 8 |
| TUNLEAK | OSUP | Management and Red Hill Supervisor Formulate Response | 24 |
| TUNLEAK | OXFR | Control Room and Red Hill Staff Move Fuel from the Leaking RHBFST | 24 |

## Table 6-26. Time Delay Impacts of TUNLEAK Top Event Failures (Continued)

| Event Tree | TE | TE Description | Delay |
|---|---|---|---|
| TUNLEAK | XFR1 | Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST | 72 |
| TUNLEAK | XFR2 | Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor | 72 |
| TUNLEAK | XFR3 | Two-Step Fuel Movement to Pump Fuel to Other RHBFSTs | 72 |
| TUNLEAK | XFR4 | Gravity Feed to Ships or Other Tanks at Pearl Harbor | 72 |
| TUNLEAK | XFR5 | Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line | N/A |
| TUNLEAK | DELAY | Tank empty Delay Time Based on Earlier Failures | N/A |
| TUNLEAK | REL | REL – Type of Fuel Release Scenario | N/A |

Some assumed time delays are a function of multiple conditions including being dependent on the states of multiple top events along the sequence path. Table 6-27 summarizes the actual macro logic used for assigning the added delay times as a function of all top event success and failure states along a single sequence path. The status of each macro (e.g., TIM336HR, TIM72HR, etc.) represents the logical conditions in which a given delay time is assumed. In the event that multiple delay time macros are true in the same sequence, the longest delay time is used for assessing the amount of fuel released. The longest assumed time delay duration (TIM336HR) is used for sequence conditions in which there is insufficient ullage to empty the affected RHBFST below the hole location. In the event of insufficient ullage, a 2-week delay is assumed, to allow time for alternative ullage to be made available. In the RHBFST inventory data reviewed, the only concern with sufficient available ullage being available involved the two RHBFSTs which hold F76 fuel. These RHBFSTs were observed to have relatively high fuel levels throughout the period of time reviewed. There would be insufficient ullage to empty one of the RHBFSTs into the other, even allowing for the F76 ullage typically available at the upper tank farm.

## Table 6-27. TUNLEAK Logic for Sequence Dependent Time Delays

| Macro ID | Macro Logic Rule |
|---|---|
| ULLAGEF | INVEN=F76C*(HEIGHT=LOW+HEIGHT=BOT) |
| XFRF24ASUC | INVEN=F24A*(HEIGHT=NA+HEIGHT=BOT*(XFR1=S*XFR2=S*XFR3=S)) |
| XFRF24BSUC | INVEN=F24B*(HEIGHT=NA+HEIGHT=BOT*(XFR3=S) ) |
| XFRF76CSUC | INVEN=F76C*(HEIGHT=HIGH+HEIGHT=MED*(XFR2=S+XFR3=S)) |
| XFRJP5DSUC | INVEN=JP5D*(HEIGHT=NA+HEIGHT=BOT*XFR3=S) |
| XFRJP5ESUC | INVEN=JP5E*(HEIGHT=NA+HEIGHT=BOT)*(XFR2=S+XFR3=S) |
| XFRF24FSUC | INVEN=RF24F*((HEIGHT=NA+HEIGHT=BOT)*(XFR1=S*XFR2=S*XFR3=S+XFR4=S)) |
| XFRF76GSUC | INVEN=RF76G*((HEIGHT=NA+HEIGHT=BOT)*XFR4=S) |
| XFRJP5HSUC | INVEN=RJP5H*((HEIGHT=NA+HEIGHT=BOT)*(XFR3=S+XFR4=S)) |
| XFR100ISUC | INVEN=R100I*((HEIGHT=NA+HEIGHT=BOT)*(XFR3=S+XFR4=S)) |
| XFRSUCCESS | XFRF24ASUC+XFRF24BSUC+XFRF76CSUC+XFRJP5DSUC+XFRJP5ESUC+XFRF24FSUC+XFRF76GSUC+XFRJP5HSUC+XFR100ISUC |
| SKINCLOSE | (SKIN=S*-FSUPSKIN*OPAN=S) |
| SKINXCLOSE | SKINX=S*-FSUPSKINX*OPAN=S |
| BALLCLOSE | BALL=S*-FSUPBALL*OPAN=S |
| BALLXCLOSE | BALLX=S*-FSUPBALLX*OPAN=S |
| FLTKCLOSE | FLTKC=S*-FSUPFLTKC*(OPAN=S) *(LKLOC=SECA+LKLOC=SECB+LKLOC=SECC+LKLOC=SECD*(TKLOC=E*(FUEL=F76+FUEL=JP5))) |
| FLISOCLOSE | FLISO=S*-FSUPFLISO*OSEC=S |
| ONETKOPEN | ISOL=NO*MOVE=XFER*( (SKINCLOSE+BALLCLOSE)*-(SKINXCLOSE+BALLXCLOSE) +-(SKINCLOSE+BALLCLOSE)*(SKINXCLOSE+BALLXCLOSE) )+ ISOL=NO*(MOVE=RECEV+MOVE=ISSUE)*-(SKINCLOSE+BALLCLOSE) |
| BOTHTKOPEN | MOVE=XFER*ISOL=NO*( -(SKINCLOSE+BALLCLOSE)*-(SKINXCLOSE+BALLXCLOSE) ) |
| JHEP24HR | OUFM=F*ORGA1=F+OUFM=F*OSUP=F+OUFM=F*OXFR=F+ORGA1=F*OSUP=F+ORGA1=F*OXFR=F+OSUP=F*OXFR=F |
| JHEP72HR | OUFM=F*ORGA1=F*OXFR=F+OUFM=F*OSUP=F*OXFR=F+ORGA1=F*OSUP=F*OXFR=F+OUFM=F*ORGA1=F*OSUP=F*OXFR=F |
| TIM336HR | ULLAGEF*-TKID=NA*ISOL=NO + EVAC=EVACU*(SKIN=F+ FSUPSKIN+ BALL=F+ FSUPBALL+ MOVE=XFER*(SKINX=F+FSUPSKINX+BALLX=F+FSUPBALLX) +FLTKO=F + -XFRSUCCESS)*IELKLAT*ISOL=NO |

**Table 6-27. TUNLEAK Logic for Sequence Dependent Time Delays (Continued)**

| Macro ID | Macro Logic Rule |
|---|---|
| TIM72HR | (AFHR=F+B3EA=F+BALL=F+BALLX=F+BRE48=F+BRN48=F+BUE48=F+ BUN48=F+BUN24=F+CARGO=F+CRM=F+EFAN=F +TFAN=F*IETKTOP4+SKIN=F+SKINX=F+UFAN=F +(-XFRSUCCESS*-MOVE=IDLE*ISOL=NO))*-TKID=NA+JHEP72HR |
| TIM24HR | (OSUP=F+OXFR=F+GRID=F*(GRIDR=HR24)+(MOVE=RECEV+MOVE=XFER)*ISOL=NO*-IERTS)*-TKID=NA+JHEP24HR |
| TIM12HR | (AFHE=F+GRID=F*(GRIDR=HR12)+(FUEL=F24+FUEL=JP5)*MOVE=ISSUE*ISOL=NO)*-TKID=NA |
| TIM8HR | (LPRH=F+ORGA1=F+OUFM=F+GRID=F*GRIDR=HR6+IERTS*MOVE=RECEV*ISOL=NO+ MOVE=XFER*ISOL=NO)*-TKID=NA |
| TIM4HR | (EL72=F+EL73=F+GRID=F*GRIDR=HR3+OSUM=F+ FUEL=F76*MOVE=ISSUE*ISOL=NO)*-TKID=NA |
| TIM0HR | (-(TIM4HR+TIM8HR+TIM12HR+TIM24HR+TIM72HR+TIM336HR)) |

For the most part, time delay macros are made true by the failure state of a single top event along the sequence path. However, being more likely than multiple equipment failures, multiple operator action failures could appear in the same sequence; e.g., Macros JHEP24HR and JHEP72HR. In these cases, the overall delay time was taken to be the sum of the individual action delays (i.e., as if the delays occurred in series), provided the actions failures were each related to the function of moving fuel from the affected RHBFST.

The macros which begin with the letters “XFR” deserve special mention. These macros are true if for the specific sequence facility configuration (e.g., F24A) as represented by Top Event INVEN, the combination of fuel transfer options available are sufficient to transfer enough fuel to uncover the hole for the hole height location modeled. If not, an added 72-hour delay time is assumed to allow time for recovering the unavailable equipment.

## 6.9 Section 6 References

6-1 “Red Hill Complex Fire, Safety, Life Safety, and Environmental Risk Assessment/Analysis Volume I of II, Final Submittal,” prepared by WillBros Engineers, Inc., for Department of the Navy Pacific Division Naval Facilities Engineering Command, Pearl Harbor, Hawaii, August 1998.

6-2 Victor L. Streeter, “Fluid Mechanics,” Fifth Edition. McGraw Hill Company, 1973. Pages 278–281.

# 7. Systems Analysis

## 7.1 Introduction

The system analysis is designed to address the logic modeling required to adequately characterize and quantify the node probabilities (split fraction values) defined and applied in the event sequence analysis. In QRVA, this is typically accomplished via the application of fault tree analysis (FTA) or reliability equation development. The system analysis is often performed first in a general way to characterize each major system questioned in the event sequence analysis, but then is refined to focus specifically on performing the modeling required to accurately characterize and quantify the event sequence event tree split fractions.

## 7.2 QRVA System Analysis General Methodology

### 7.2.1 Systems Analysis

Systems analysis involves the construction of models for the facility systems covered in the risk assessment. The systems to be analyzed and their success criteria are identified in conjunction with event tree development in an iterative process. Assistance from phenomenological and fuel containment analyses may be needed to derive realistic system-success criteria. The system models generally consist of fault trees developed to a level of detail consistent with available information and data. Thus, there is some interface with the database-development subtask discussed later. In addition, human errors associated with the testing, maintenance, or operation of the systems are included in the system model, and thus system modeling interfaces directly with the analysis of human reliability and procedures. Common-cause contributors and potential systems interactions should also be included to ensure proper integration into the analysis.

#### *7.2.1.1 Specification of Analysis Ground Rules and Model Resolution*

Each system analysis will proceed according to certain ground rules or constraints. Some are imposed directly by the design or operational conditions attendant on the definition of the fault tree top event, others are imposed by the limitations of the analytical process itself. All analysis ground rules that have a bearing on the completed system model must be clearly understood, incorporated into the model, and appropriately documented.

In the performance of a risk assessment, the systems to be analyzed are essentially defined at two levels. The first level of definition is a functional one, it is directly related to the function the system must perform to successfully respond to an accident condition or a transient. This definition provides insight into the overall role of the system in relation to a particular accident sequence. The second level of definition is physical, it identifies the hardware required for the system to function. This hardware definition is normally included in the statement of the top event of the fault tree and describes the minimum acceptable state of system operability. This definition provides the analytical boundaries for the various system analyses. It is important to identify and fully document

the boundaries of each system. These boundaries may be different from the traditional system boundaries that are identified in information describing the system or the facility.

All support-system interfaces with the frontline system must be accounted for and included in the analysis. Certain system interfaces may be quite complex (i.e., instrumentation and control) and require a specific definition of the system boundaries considered in a particular analysis. Some components may be found to be within the boundaries of more than one system.

Experience has shown that the interfaces between a frontline system and its support systems may be most important to the system evaluation. In that regard a more formal search and documentation of all elements that depend on input from another source beyond the identified system boundary may be appropriate. The procedure used in the Interim Reliability Evaluation Program included a search for, and an evaluation of, potential support-system failures that could affect the operation of frontline systems. This search and evaluation procedure resembled a failure modes and effects analysis, which is more fully described in Section 3.6 of NUREG/CR-2300. An example of the format used is shown in Figure 7-1. The level of detail shown in the FMEA example may not be necessary for all evaluations. However, the concept is important in that all areas of interface and support required for system operation are thoroughly defined and evaluated.

Although the systems analyst must make every effort to obtain and fully use all available system information in the course of the system modeling, he will inevitably have to make a number of assumptions about the details of system operation, capacities, and credible failure mechanisms. The accuracy of all assumptions should be verified, and the supporting rationale should be documented. It is extremely important that all assumptions be fully described and documented. To preserve traceability, even the assumptions that are obvious to the analyst should be explicitly stated.

| Front-line system | | | Support system | | | Failure mode | Fault effect | Detection | Diagnostics | Comments |
|---|---|---|---|---|---|---|---|---|---|---|
| System | Div. | Comp. | System | Div. | Component | | | | | |
| AFWS | A | MDP-1A | AC power | A | Breaker A1131 | Fail open | Concurrent failure to start or run (CFSR) | At pump test | Pump operability only | Treat as part of local pump failure |
| | B | MDP-1B | AC power | B | Breaker A1132 | Fail open | | | | |
| AFWS | A | MDP-1A | AC power | A | Bus E11 | Low or zero voltage | CFSR | Prompt | Control room monitors ESG E/F 11 voltage, alarmed | Partial failure noted for future reference |
| | B | MDP-1B | AC power | B | Bus F12 | | Possible motor burnout | Prompt | | |
| AFWS | A | MDP-1A | HVAC | A | Rx cooler 3A | No heat removal | Pump-motor burnout in 3-10 continuous service hours (CSH) | Shift walk-around | No warning for local faults | AC and SWS support systems of HVAC monitored but not HX |
| | B | MDP-1B | HVAC | B | Rx cooler 3B | No heat removal | | | | |
| AFWS | A | MDP-1A | ESWS | A | Oil cooler S31 | Loss of service water | Pump burnout in 1-3 CSH | At pump test | Local lube-oil temperature gauge, none in control room | ESWS header and pumps monitored but not lube-oil coolers; local manual valve alignment checked in maintenance procedure xx but not in periodic walk-around |
| | B | MDP-1B | ESWS | B | Oil cooler S32 | | | | | |
| AFWS | A | MDP-1A | DC power | A | Bus A131 | Low or zero voltage | Precludes auto or manual start, no local effect on already running pump | Prompt | Control room monitors XXX dc bus voltage--many lamps out in control room | Effect of dc power loss on ac not evaluated here; local motor controller latches on, needs dc to trip or close |
| | B | MDP-1B | DC power | B | Bus B132 | | | | | |

**Figure 7-1. Example of Format for a System-Interaction FMEA**





ABS Consulting

### 7.2.1.2 System Dependency Matrix Development

Experience in QRVA has shown that, prior to detailed development of the event tree logic structure, it is prudent to develop a system dependency matrix (SDM). The SDM is simply a cross-reference table that relates frontline system functions to their required support functions. For example, for the RHBFSF, frontline systems may be considered to be those systems that are designed to store and transfer fuel; e.g., fuel tanks, fuel transfer piping, and associated fuel transfer pumps and valves. Support systems provide functions supporting operation of the frontline systems. Support systems often provide support functions for multiple frontline systems in the facility. For example, a specific electric power system may provide motive power for multiple frontline pumps and/or valves. In this case, the specified electric power system would be considered to be a support system for the frontline fuel transfer system. Other typical support systems are systems providing actuation and control power for controlling pumps, valves, or other components, systems providing cooling water to water-cooled components, systems providing cooling air to air-cooled components (including general heating, ventilation, and air conditioning [HVAC] systems), lubrication systems, compressed air for air-operated components, etc. Support systems include support functions not only for frontline system hardware but also for required or anticipated human actions. Therefore, a compartment or area lighting system and/or HVAC system could be an important support system in the context of a QRVA. The SDM provides a valuable tool in facilitating a thorough understanding of system interactions and dependencies for QRVA event sequence and systems analysts.

### 7.2.1.3 Boolean Logic Model (e.g., fault tree) Top Event Definition

Boolean logic models (in this case, fault trees) are applied to analyze and quantify the split fractions of the event trees developed during the event sequence analysis of the QRVA. The actual development of the system logic model commences after the analyst has gained a thorough understanding of the system under consideration, especially about its integration into the overall accident-sequence definition process. The analytical ground rules (i.e., interfaces, assumptions, etc.) described above will guide the detailed development of the fault-tree model.

The basic concepts of fault-tree construction and analysis are well documented and need not be treated here in detail. The Fault Tree Handbook (Reference 7-1) presents a comprehensive treatment of the subject. The remainder of this section describes the elements of a fault tree model and addresses factors that have been shown to be important to the modeling of facility systems.

The starting point of fault tree development is definition of the “top event”. The top events for the QRVA fault trees are generally defined via the event tree top events. As we develop fault trees in “failure space” rather than “success space”, a fault tree top event is generally stated to describe failure of the associated system success criteria. For example, if a pumping system “P” is designed to provide “X” gallons per minute of flow from Point A to Point B in the facility, and we determine that this flow is required to meet functionality requirements for the QRVA, then the associated fault tree top event might read as “Insufficient flow provided by System P”.

### 7.2.1.4 System Failure Modes and Effects Analysis

To clearly define the fundamental elements of the basic events to be applied in the QRVA Boolean logic models (e.g., fault trees), the systems analysts perform a failure modes and effects analysis of their assigned systems prior to detailed fault tree development. As the fault tree top events have been defined prior to the start of detailed fault tree analysis, the FMEA may be considered a focused FMEA, which centers on those failure modes that could contribute to top event failure. As FMEAs are inductive (bottom-up) logic analyses, they can be quite broad in scope and labor-intensive. Defining system top events prior to performing the FMEA supports the focusing process and helps to limit the effort required for the FMEA designed to support QRVA system modeling. Detailed fundamental guidance for performing FMEA can be found in MIL-STE-1629A (Reference 7-2).

### 7.2.1.5 Boolean Logic Model (e.g., fault tree) Development

In fault-tree analysis, an undesired state of a system is specified and the system is then analyzed in the context of its environment and operation to find all of the credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the top event.

The fault tree approach is a deductive process, whereby the top event is postulated and the possible means for that event to occur are systematically deduced.

A fault tree does not contain all possible component-failure modes or all possible fault events that could cause system failure. It is tailored to its top event, which corresponds to a specific system-failure mode and associated timing constraints. Hence, the fault tree includes only the fault events and logical interrelationships that contribute to the top event. Furthermore, the postulated fault events that appear on the fault tree may not be exhaustive. They can include only the events considered to be significant, as determined by the analyst. It should be noted that the choice of fault events for inclusion is not arbitrary, it is guided by detailed fault-tree procedures, information on system design and operation, operating histories, input from facility personnel, the level of detail at which basic data are available, and the experience of the analyst.

It should also be understood that the fault tree is not itself a quantitative model. Although it lends itself to quantification through the Boolean representation of its minimal cut sets, the fault tree itself is a qualitative characterization of system fault logic.

Figure 7-2 illustrates a typical fault tree. Figure 7-3 shows and explains commonly used fault-tree symbols. Primary or intermediate events (or combinations of the two) are inputs to logical operators referred to as “gates”. The two basic types of fault-tree logic gates are the OR gate and the AND gate. Together with the NOT operator (commonly shown as a dot above the gate), these gates can be used to define any other specialized fault tree gate.

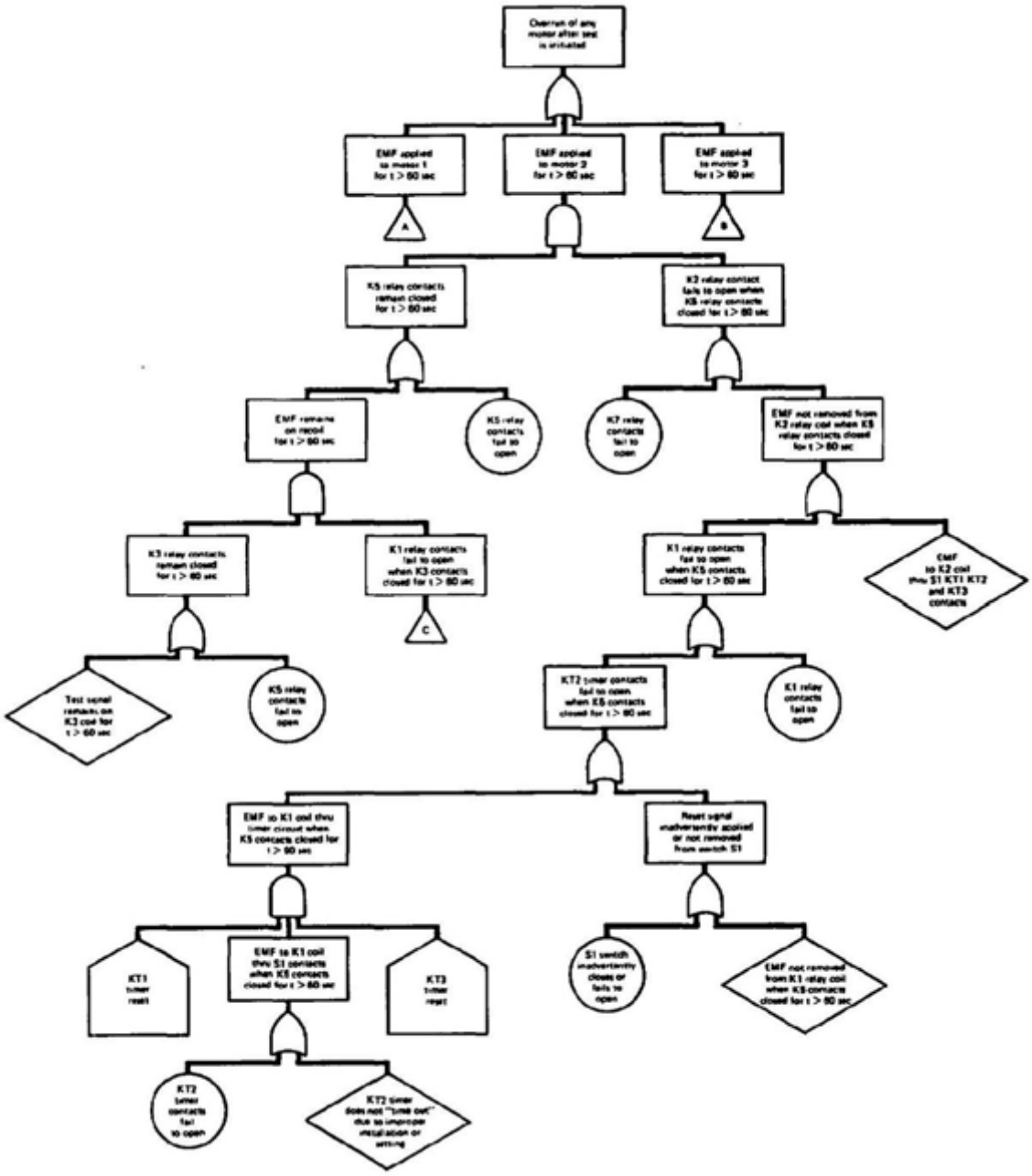
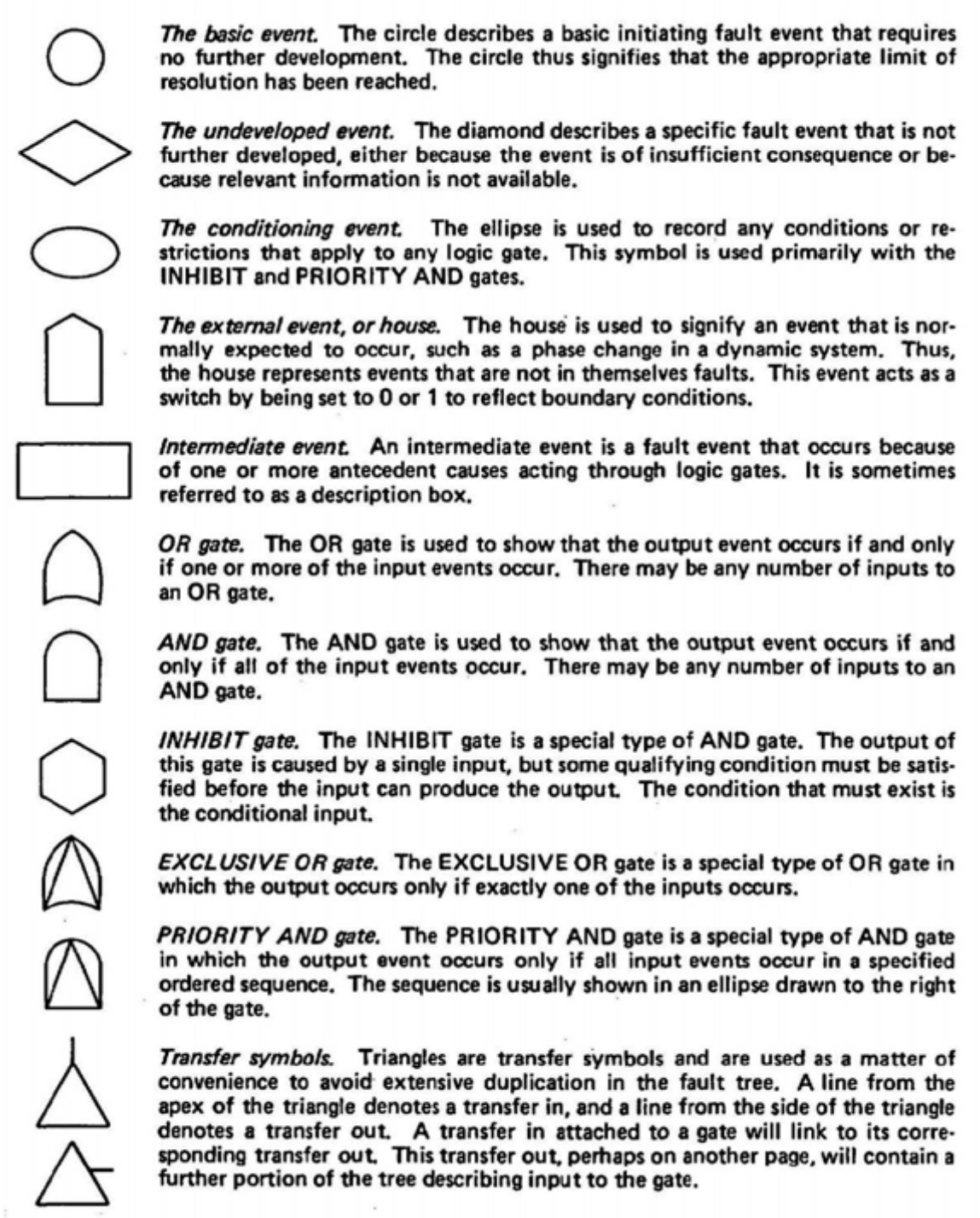


**Figure 7-2. Fault Tree for Overrun of Motor 2 (relay logic only)**



*The basic event.* The circle describes a basic initiating fault event that requires no further development. The circle thus signifies that the appropriate limit of resolution has been reached.

*The undeveloped event.* The diamond describes a specific fault event that is not further developed, either because the event is of insufficient consequence or because relevant information is not available.

*The conditioning event.* The ellipse is used to record any conditions or restrictions that apply to any logic gate. This symbol is used primarily with the INHIBIT and PRIORITY AND gates.

*The external event, or house.* The house is used to signify an event that is normally expected to occur, such as a phase change in a dynamic system. Thus, the house represents events that are not in themselves faults. This event acts as a switch by being set to 0 or 1 to reflect boundary conditions.

*Intermediate event.* An intermediate event is a fault event that occurs because of one or more antecedent causes acting through logic gates. It is sometimes referred to as a description box.

*OR gate.* The OR gate is used to show that the output event occurs if and only if one or more of the input events occur. There may be any number of inputs to an OR gate.

*AND gate.* The AND gate is used to show that the output event occurs if and only if all of the input events occur. There may be any number of inputs to an AND gate.

*INHIBIT gate.* The INHIBIT gate is a special type of AND gate. The output of this gate is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The condition that must exist is the conditional input.

*EXCLUSIVE OR gate.* The EXCLUSIVE OR gate is a special type of OR gate in which the output occurs only if exactly one of the inputs occurs.

*PRIORITY AND gate.* The PRIORITY AND gate is a special type of AND gate in which the output event occurs only if all input events occur in a specified ordered sequence. The sequence is usually shown in an ellipse drawn to the right of the gate.

*Transfer symbols.* Triangles are transfer symbols and are used as a matter of convenience to avoid extensive duplication in the fault tree. A line from the apex of the triangle denotes a transfer in, and a line from the side of the triangle denotes a transfer out. A transfer in attached to a gate will link to its corresponding transfer out. This transfer out, perhaps on another page, will contain a further portion of the tree describing input to the gate.

**Figure 7-3. Fault-Tree Symbols‡‡**

‡‡ A circle, diamond, ellipse, or "house", represents a primary event—that is, any event that is not developed further and does not have any inputs. The two basic types of fault-tree logic gates are the OR gate and the AND gate. Together with the NOT operator (commonly shown as a dot above the gate), these gates can be used to define any other specialized fault-tree gate.

In postulating a fault or failure for inclusion in a fault tree, it must be remembered that the proper definition of these events includes a specification not only of the undesirable component state but also the time it occurs. It is very important that the time be kept in mind in postulating the top event and incorporated into the analyst's thought processes when postulating all subsequent fault events. It is further useful to make a distinction between the specific term "failure" and the more general term "fault". This distinction can best be illustrated by example. If a relay closes properly when a voltage is passed across its terminals, the relay is in a state of success. If, however, the relay fails to close under these circumstances, it is in a state of failure. Another possibility is that the relay closes at the wrong time because of the improper functioning of some upstream component. This does not constitute a relay failure; however, the relay's closing at the wrong time may well cause the entire circuit to enter an unsatisfactory state. Such an occurrence is called a "fault". It can thus be said that, in general terms, all failures are faults, but not all faults are failures. Failures are basic abnormal occurrences, whereas faults can be described as "higher order" events.

Each fault event that appears in a fault tree contains a reference to the particular failure mode associated with that event. It is important to differentiate between the terms "failure mode", "failure mechanism", and "failure effect". When speaking of "failure effects", the only concern is with why the failure is of interest; that is, what are the effects of the failure, if any, on the system? In contrast, a "failure mode" specifies exactly which aspects of component failure are of concern. A "failure mechanism" is a statement of how a particular failure mode can occur. In this fashion, failure mechanisms produce failures modes, which in turn, result in certain failure effects on system operation. Each fault event should be carefully stated to ensure that it uniquely describes the condition of interest and that it is directly related to the numerical database.

#### *7.2.1.5.1 System Hardware Failure Mode Logic*

A key element of fault-tree analysis is the identification of hardware-related fault events that can contribute to the top event. To allow for a quantitative evaluation, the failure modes must be postulated in such a way that they are clearly defined and can be related to the numerical database. In postulating component-failure modes, care should be taken to ensure that they are realistic and consistent within the context of system operational requirements and environmental factors.

All component fault events can be described by one of three failure characteristics:

1. Failure on demand. Certain components are required to start, change state, or perform a particular function at a specific instant of time. Failure to respond as needed is referred to as failure on demand.

2. Standby failure. Some systems or components are normally in standby but are required to operate on demand. Failure could occur during this nonoperational period, preventing operation when required.

3. Operational failure. A given system or component may be normally operating or may start successfully but fail to continue to operate for the required period of time. This failure characteristic is referred to as an operational failure.

Depending on the specific context of the fault tree—for example, a specific mode of system operation—the analyst should evaluate each component in terms of the failure characteristics listed above. Chapter 5 of NUREG/CR-2300 provides additional information on the specification of failure modes for individual components and the associated numerical data.

#### *7.2.1.5.2 Incorporation of Maintenance and Testing*

In addition to the physical faults that can render a system unavailable, testing and maintenance activities can also make a significant contribution to unavailability. Unavailability due to testing or maintenance depends on the frequency and the duration of the test or maintenance act. Information on equipment unavailability due to testing can generally be obtained or derived from the technical specifications and maintenance records.

There are three general types of testing that should be considered for their potential impact on system unavailability:

1. System logic tests, which test the system control logic to ensure proper response to appropriate initiating signals.

2. System flow and operability tests, which verify the operability of such components as pumps and valves.

3. System tests that are performed after discovering the unavailability of a complementary safety system, generally referred to as tests after failure.

Testing schemes generally affect complete subsystems, and hence it is generally not necessary to consider each hardware element individually. Testing involving redundant portions of a system can be particularly important, and care should be taken that the constraints of the technical specifications are understood, evaluated, and properly accounted for in the fault tree. A complete understanding of the impact of all testing on system hardware and operational schemes is necessary for completeness and adds valuable insight into the overall operability of the system.

Maintenance activities can also make a significant contribution to system unavailability, and two types of maintenance need to be considered: scheduled and unscheduled. Scheduled, or preventive, maintenance actions are performed routinely. Information on the frequency or duration of each action can be obtained from maintenance procedures. Care should be exercised to ensure that outages associated with preventive maintenance are not already included in the time intervals assigned to testing and that the maintenance is not performed under conditions that would not contribute to system unavailability.

Unscheduled maintenance activities result when equipment failures occur and the failure is repaired or the equipment is replaced. Because these activities are not performed on a prescribed basis, the frequency and the mean duration time of the maintenance act must be determined from historical data. Chapter 5 of NUREG/CR-2300 provides information on the numerical database for maintenance activities.

#### 7.2.1.5.3 Incorporation of Human Error

The impact of facility operators on the outcome of potential accident sequences is one of the most important, as well as one of the most difficult, elements of system analysis. The potential for operator error is present in virtually every phase of system operation, testing, and maintenance. Furthermore, human error may affect the design, manufacture, and inspection of complex facilities and systems. However, certain types of human error are more amenable than others to exclusion in system modeling. For example, human errors associated with manufacturing are difficult to quantify, as are operator acts of commission because such a broad spectrum of actions would be candidates for evaluation.

The potential for human error must be considered during the detailed system analysis. Manual actions that can prevent or mitigate an accident sequence can be regarded in the same fashion as support systems like electric power or component cooling. In the context of system fault-tree analysis, human errors should be considered in terms of potential effects on individual components as well as potential effects on the operation of sub-systems or systems. Each individual component should be examined to determine the potential for a human error that might disable it.

The systems analyst must consider the potential for human error (and the possibility of human intervention to recover from a faulted condition) throughout all aspects of the analysis. The analysis of human errors cannot be considered a separate task; it is an integral part of the system analysis. The systems analyst should be as familiar with the operating, maintenance, and emergency procedures for the system under analysis as he is with the equipment hardware. However, in such analyses the detailed evaluation of a given human error may be performed separately by a specialist using the techniques discussed in Chapter 4 of NUREG/CR-2300. This specialist must be thoroughly informed of all boundary conditions that may affect this analysis and be familiar with the context in which the man-induced fault is being evaluated. Thus, the human-factors specialist must be regarded as an integral member of the analytical team.

In general, human errors may be presented on the fault trees as causes of component unavailability where the error contributes to the occurrence of the accident sequence being considered; e.g., failure to realign after testing. These errors can be defined by the system analysis in terms of the availability and content of procedures, environmental conditions, and other performance-shaping factors to permit a specialist in human reliability analysis to make an informed judgment. In contrast, human errors occurring during an accident cannot be properly evaluated on a system fault tree but must be considered as being dependent on the specific accident sequence and could be displayed on the event tree. Since human errors are accident- sequence dependent, the systems analyst must impart to the human-factors specialist a thorough understanding of the diagnostic information available to the facility staff, the procedures and precautions provided to the operator, the training of the operator in response to similar diagnostic patterns, as well as the stress, environmental, and other applicable performance-shaping factors.

To properly assess the likelihood of an accident sequence progressing to loss of fuel inventory control or releases of fuel from the facility, the potential for operator recovery from the sequence should be considered. Since the probability of a successful recovery

is strongly predicated on the specifics of the events that caused the accident sequence, the analysis of recovery depends not only on the sequence but also on its individual cut sets. Hence, it is not unusual for the analysis of recovery to be restricted to the dominant cut sets of the accident sequences that control the frequency of loss of fuel inventory control or of a specified release.

It is as important that the systems analyst thoroughly understand the assumptions and judgments used by the human-factors specialist in performing the human reliability analysis as it is that the specialist understand the specifics of the error being evaluated. The systems analyst must ascertain that the human reliability analysis was done in the context in which it is employed in the event trees or fault trees.

If potential human errors have been defined comprehensively, an initial screening may be required to identify the more important ones. This can be done during the initial quantification and requires the assignment of numerical values to each input fault event. Initial probabilities are assigned to human-error events in a conservative manner, and the system model is evaluated to determine significant contributors. The system models are reevaluated to determine the significance of human errors, and a detailed analysis can be performed for each minimal cut set where human error was found to be significant. This reevaluation is intended to provide a more realistic appraisal of the effects of human error.

#### *7.2.1.5.4 Incorporation of Dependent Events (e.g., common cause failure)*

The identification and the evaluation of dependent failures are both difficult and important. Because of this importance, the subject of dependent failures is discussed in several sections of the PRA procedure guide. Section 3.7 of NUREG/CR-2300 defines the various types of dependent failures and discusses the methods available for their evaluation. Chapters 10 and 11 of NUREG/CR-2300 provide guidance on the development of event-specific models for evaluating common-cause events like fires, floods, and earthquakes.

The question of evaluating dependent failures extends beyond methods for the development of system models. Therefore, Section 3.7 of NUREG/CR-2300 should be referred to for detailed information on this topic. However, it should be noted that the fault tree is the principal means of accounting for functional and shared-equipment dependences between components. A well-constructed fault tree can lead to the identification of fault events that affect or interact with other components in a system and sometimes with other interfacing systems. Evaluation of the minimal cut sets for each system can identify dependences and their impact on system unavailability. Each input event on the fault tree must be accurately and consistently named or coded to facilitate the evaluation.

## 7.3 QRVA Systems Analysis Assumptions

1. After recovery from loss of offsite power, it is assumed that once again power is supplied from offsite to ADIT 1 and ADIT 3, supplying the systems in the UGPH, the NAVFAC pump house, and to the RHBFSF.

2. As a modeling simplification, the failure of power at any one of the five panels (P100, P101, P102, P103, and P104) is conservatively assumed to have the same impact on the facility as failing power at the 480V UGPH emergency bus itself.

3. Both Supply Fans F5A and F5B and three of the four exhaust fans (F6a through F6d) are normally operating and assumed required for room ventilation to limit pump operating temperatures.

4. It is assumed that power Panel A and power Panel B will be available and powered either by the offsite power or the standby generator power.

5. As a modeling simplification, the failure of power at any one of the panels which supply motor-operated valves, ventilation fans, the two elevators, and selected Sump Pumps P1, P2, Panel L, Panel G, Panel PA, and Panels PP1 through PP8, or failure of Transformer T11, which supplies Panel L, is conservatively assumed to have the same impact on the facility as failing power at the 480V Red Hill emergency bus itself.

6. It is assumed that failure of power to any one of the following panels: LP13, P14, P15, LP16-1, LP16-2, LP17-1, LP17-2, LP18, LP19, LP20, LP21, LP22, LP23, LB, LC, Panel A, and Panel LA and the associated Step-Down Transformers T13 and T15 supplying these panels, is conservatively assumed to cause a loss of power for lighting, radios, and cameras for all of these areas. If power is lost from Red Hill 480V emergency bus (i.e., Top Event BRE48 fails), then all of these panels also lose power.

7. It is assumed that failure of the AFHE will disable the panic button, but would also cause any operating cargo pumps to trip.

8. It is assumed that the AFHE would fail after a period of operation without heat removal.

9. Failure of any of the fan pairs (Exhaust Fans PE-1A/1B and supply Fan Pairs PS-1A/1B and PS-2A/2B) is assumed to cause ventilation to be lost in both the LAT and the UAT below the bulkhead separating these areas from Tanks 17–20. Loss of any fan pair is also conservatively assumed to degrade air flow sufficiently to require Red Hill operating staff to evacuate the tunnels.

## 7.4 QRVA Systems Analysis Details

The systems analysis for the RHBFSF QRVA involves modeling top events as identified in each of the event trees. The organization of the event trees and the top events highly depend on the system dependencies which have been discussed in Section 6.5 of this report. This section includes the details for each top event model referenced by the following event trees (please see Section 6.7.1 to 6.7.8):

**Table 7-1. Event Tree Titles**

| Report Section | Event Tree Title |
|---|---|
| 6.7.1 | Configuration Event Tree |
| 6.7.2 | ELECTRICAL Event Tree |
| 6.7.3 | OTHERSUP Event Tree |
| 6.7.4 | VALVES Event Tree |
| 6.7.5 | Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock |
| 6.7.6 | Frontline Event Tree 2 – OVERFILL Event Tree |
| 6.7.7 | Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT |
| 6.7.8 | Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel |

### 7.4.1 The Top Events for the Configuration Event Tree

The top events of the configuration event tree are defined below:

**Table 7-2. Top Events Referenced by the Configuration Event Tree**

| Top Event | Description |
|---|---|
| LKLOC | Location of leak within the facility |
| MOVE | Type of fuel movement initially in progress |
| TKID | RHBFST associated with leak |
| FUEL | Type of leaking fuel |
| TKXF | Source RHBFST associated with inter-tank transfer |
| TKLOC | LAT location of associated RHBFST relative to fuel line leak to LAT |
| HEIGHT | Height of hole in RHBFST that is leaking to rock |
| SIZE | Size of leak from RHBFST or fuel line piping |
| DIREC | Side of RHBFST that leak is on |
| INVEN | Initial RHBFST inventory configuration |

#### *7.4.1.1 Top Event LKLOC — Location of Leak within Facility*

LKLOC is a multi-state top event used to model the location of a leak within the facility by providing a top event state for each location. The following Table 7-3 lists the states that represent a location within the RHBFSF.

**Table 7-3. LKLOC States Representing a Leak Location**

| State Name | State Description |
|---|---|
| ROCK | RHBFST to rock |
| SECA | Fuel line piping below ADIT2 |
| SECB | Fuel line piping ADIT2 to 3y |
| SECC | Fuel line piping 3y to oil door |
| SECD | Fuel line piping oil door to mid-tank gallery |
| SECE | Fuel line piping above highest sectional |
| NOZZL | RHBFST Nozzle to LAT |
| LOWDOM | RHBFST lower dome to rock |
| OVRFW | RHBFST overfill to rock |

### 7.4.1.2 Top Event MOVE — Type of Fuel Movement Initially in Progress

MOVE is a multi-state top event used to model the frequency of fuel movement for the three fuel types. The fuel movement frequency computation is further developed using a fault tree diagram which considers all fuel types and fuel movement states. Please see Figure C-13, MOVE Fault Tree Diagram.

**Table 7-4. MOVE States Representing Type of Fuel Movement**

| State Name | State Description |
|---|---|
| IDLE | No fuel movement |
| ISSUE | Tank issuing |
| RECEV | Tank receiving |
| XFER | Intra-tank transfer |

### 7.4.1.3 Top Event TKID — RHBFST Associated with Leak

TKID is a multi-state top event used to identify the RHBFST considered in the event tree sequence analysis.

**Table 7-5. TKID States Representing Each RHBFST**

| State Name | State Description |
|---|---|
| NA | No associated RH Tank |
| TK1 | RH Tank 1 |
| TK2 | RH Tank 2 |
| TK3 | RH Tank 3 |
| TK4 | RH Tank 4 |
| TK5 | RH Tank 5 |
| TK6 | RH Tank 6 |
| TK7 | RH Tank 7 |
| TK8 | RH Tank 8 |
| TK9 | RH Tank 9 |
| TK10 | RH Tank 10 |
| TK11 | RH Tank 11 |
| TK12 | RH Tank 12 |
| TK13 | RH Tank 13 |
| TK14 | RH Tank 14 |
| TK15 | RH Tank 15 |
| TK16 | RH Tank 16 |
| TK17 | RH Tank 17 |
| TK18 | RH Tank 18 |
| TK19 | RH Tank 19 |
| TK20 | RH Tank 20 |

#### 7.4.1.4 Top Event FUEL — Type of Leaking Fuel

FUEL is a multi-state top event used to identify the type of fuel considered in the event tree sequence analysis.

**Table 7-6. FUEL States Representing Type of Fuel**

| State Name | State Description |
|---|---|
| F76 | Diesel Marine |
| F24 | Jet Fuel 1 |
| JP5 | Jet Fuel 2 |
| PERM | NA Tank Out Of Service |

### 7.4.1.5 Top Event TKXF — Source RHBFST Associated with Inter-Tank Transfer

TKXF is a multi-state top event used to identify the RHBFST considered during an inter-tank transfer in the event tree sequence analysis.

**Table 7-7. TKXF States Representing Each RHBFST**

| State Name | State Description |
|---|---|
| NA | NO associated RH tank |
| TK1 | RH Tank 1 |
| TK2 | RH Tank 2 |
| TK3 | RH Tank 3 |
| TK4 | RH Tank 4 |
| TK5 | RH Tank 5 |
| TK6 | RH Tank 6 |
| TK7 | RH Tank 7 |
| TK8 | RH Tank 8 |
| TK9 | RH Tank 9 |
| TK10 | RH Tank 10 |
| TK11 | RH Tank 11 |
| TK12 | RH Tank 12 |
| TK13 | RH Tank 13 |
| TK14 | RH Tank 14 |
| TK15 | RH Tank 15 |
| TK16 | RH Tank 16 |
| TK17 | RH Tank 17 |
| TK18 | RH Tank 18 |
| TK19 | RH Tank 19 |
| TK20 | RH Tank 20 |

### 7.4.1.6 Top Event TKLOC — LAT Location of Associated RHBFST Relative to Fuel Line Leak to LAT

TKXF is a multi-state top event used to identify the location of RHBFST relative to the fuel line leak to the LAT.

**Table 7-8. TKLOC States Representing Each RHBFST Location Relative to the Fuel Line**

| State Name | State Description |
|---|---|
| NA | Not applicable, no FL leak to LAT |
| E | Tank above LAT sectional valve |
| D | Tank below LAT sectional valve or no valve |

### 7.4.1.7 Top Event HEIGHT — Height of Hole in RHBFST that is Leaking to Rock

HEIGHT is a multi-state top event used to identify the height of a hole in the RHBFST that is leaking to rock.

**Table 7-9. HEIGHT States Representing Height of a Hole**

| State Name | State Description |
|---|---|
| NA | Not a tank leak to rock |
| HIGH | Leak high in barrel, 175' |
| MEDIUM | Leak medium in barrel, 140' |
| LOW | Leak low in barrel, 70' |
| BOT | Leak in bottom of lower dome |

### 7.4.1.8 Top Event SIZE – Size of Leak from RHBFST or Fuel Line Piping

SIZE is a multi-state top event used to identify the size of a leak from RHBFST for fuel line piping.

**Table 7-10. SIZE States Representing Size of a Hole**

| State Name | State Description |
|---|---|
| S1 | 1.5 gpm |
| S2 | 50 gpm |
| S3 | 75 gpm |
| RUPT | 1000's gpm |
| FULLD | Fill pipe diameter |

### 7.4.1.9 Top Event DIREC — Side of RHBFST that Leak Is On

DIREC is a multi-state top event used to identify the side of RHBFST that the leak is on.

**Table 7-11. DIRC States Representing Direction of the Leak**

| State Name | State Description |
|---|---|
| NA | Not a RHBFST leak to rock |
| SE | Southeast |
| SW | Southwest |
| NW | Northwest |
| NE | Northeast |

### 7.4.1.10 Top Event INVEN — Initial RHBFST Inventory Configuration

INVEN is a multi-state top event used to determine the initial RHBFST fuel inventory.

**Table 7-12. INVEN States Representing Initial Fuel Inventory**

| State Name | State Description |
|---|---|
| NA | TKID=NA OR T1 +T19 |
| F24A | RHBFST AT 212 |
| F24B | RHBFST AT 100 |
| F76C | RHBFST AT 175 |
| JP5D | RHBFST AT 212 |
| JP5E | RHBFST AT 14 |
| RF24F | RTS RHBFST AT 212 |
| RF76G | RTS RHBFST AT 212 |
| RJP5H | RTS RHBFST AT 212 |
| R100I | RTS ALL FUELS AT 100' |
| IN212J | OVERFILL AT 212 |

### 7.4.2 The Top Events for the ELECTRICAL Event Tree

The top events of the Electrical event tree are defined below:

**Table 7-13. Top Events Referenced by ELECTRICAL Event Tree**

| | |
|---|---|
| GRID | Offsite Grid |
| GRIDR | Recovery from Losses of Offsite Grid |
| BUN24 | UGPH 2.4 kV Normal Bus |
| BUN48 | UGPH 480V Normal Bus |
| BUE48 | UGPH 480V Emergency Bus |
| GEN1 | Backup Generator at ADIT for UGPH 480V Emergency Bus |
| UFAN | ADIT 1 Supply and Exhaust Fans for UGPH Cooling Cargo Pumps |
| B3EA | ADIT 3 208V Panel A |
| GEN3 | Backup Generator at ADIT 3 for 480v Panels B and A |
| BRN48 | Red Hill 480V Normal Bus |
| BRE48 | Red Hill 480V Emergency Bus |
| GEN5 | Red Hill 480V Emergency Bus |
| LPRH | Red Hill Panels Supplying Lighting, Radios, and Cameras |
| AFHE | Automatic Fuel Handling Equipment |
| AFHR | AFHE Condensing and Fans for Heat Removal |
| EFAN | Fans for Tanks 1-16 in LAT & UAT Fail to operate (also Supply Electrical Room in LAT |
| TFAN | Fans for Tanks 17-20 in LAT & UAT Fail to Operate (above bulkhead) |

#### 7.4.2.1 Top Event GRID — Offsite Grid

This top event models the availability of offsite power supply to ADIT 1 and ADIT 3 supplying the systems in the underground pump house, the NAVFAC pump house, and to the RHBFSF following an initiating event. This event represents the equipment associated with the 11.5 kV transmission lines from Hawaii Electric Company (HECO) to the 11.5 kV transformers. This equipment is modeled by a single basic event and quantified using Red Hill specific line outage data. Success of this top event requires the offsite power supply from HECO to be available for 24 hours. Please see Figure C-14 for the GRID fault tree diagram.

#### 7.4.2.2 Top Event GRIDR – Recovery from Losses of Offsite Grid

This top event models the recovery duration from losses of offsite power. When recovered, offsite power is assumed to once again be supplied from offsite to ADIT 1 and ADIT 3 supplying the systems in the underground pump house, the NAVFAC pump house, and to the RHBFSF following an initiating event. The probabilities of recovery

durations are evaluated from the 30 recorded Red Hill specific offsite power losses in the last 30 years. The recovery duration profile is modeled using a multi-state top event. The top event GRIDR's five recovery states are defined as follows:

HR0 – Switch representing the status of power from offsite. If Top Event GRID is successful, this state has probability 0. If Top Event GRID is failed, this state has probability 1.0.

HR3 – Probability of recovering power from offsite within 3 hours of the initial loss; i.e., 0.83. If power from offsite was never lost (i.e., GRID was successful), then the probability of this state is 0.

HR6 - Probability of recovering power from offsite between 3 hours and 6 hours of the initial loss; i.e., 0.07. If power from offsite was never lost (i.e., GRID was successful), then the probability of this state is 0.

HR12 – Probability of recovering power from offsite between 6 hours and 12 hours of the initial loss; i.e., 0.09. If power from offsite was never lost (i.e., GRID was successful), then the probability of this state is 0.

HR24 – Probability of recovering power from offsite between 12 hours and 24 hours of the initial loss; i.e., 0.01. If power from offsite was never lost (i.e., GRID was successful), then the probability of this state is 0.

#### *7.4.2.3 Top Event BUN24 — UGPH 2.4 kV Normal Bus*

This top event models the availability of power from offsite to the UGPH 2.5 kV normal bus. The models include the 11.5 kV to 2.4 kV transformer. Success of this top event requires that the power supply from the offsite grid be available at the 2.4 kV normal bus for 24 hours. However, only the transformer and 2.4 kV normal bus are included in this top event. The recovery of offsite power is treated separately. Please see Figure C-15 for the BUN24 fault tree diagram.

#### *7.4.2.4 Top Event BUN48 — UGPH 480V Normal Bus*

This top event models the availability of power from offsite to the 480V normal bus for 24 hours. The top event model includes the 11.5 kV to 480V transformer supplying offsite power to the 480V Normal bus. If power is lost from offsite (i.e., GRID fails), 480V normal bus itself is de-energized; i.e., there is no backup power. The recovery of offsite power is treated separately. Please see Figure C-16 for the BUN48 fault tree diagram.

#### *7.4.2.5 Top Event BUE48 — UGPH 480V Emergency Bus*

This top event models the availability of power from offsite or from the standby generator at the ADIT 1 hillside to the 480V Emergency bus for 24 hours. The top event model includes the 11.5 kV to 480V transformer.

The UGPH 480V emergency bus supplies its own cooling fans and five other panels; i.e., 480V P100, P101, P102, P103, and P104. A 480V to 208V transformer is used to supply Panel P105 from the 480V UGPH emergency bus. A listing of all the loads

supplied by each of these panels is not available. However, it is known that Panel P102 supplies power to the transformer cooling fans, which if lost would lead to eventual overheating of the UGPH 480V transformer itself, which will deenergize the 480V emergency bus; i.e., have the same effect as failing the 480V bus itself. The most likely cause of losing power to the 480V emergency bus is the joint failure of power from both the offsite grid and the ADIT 1 generator. Therefore, as a modeling simplification, the failure of power at any one of these five panels is conservatively assumed to have the same impact on the facility as failing power at the 480V UGPH emergency bus itself.

If power is lost from offsite (i.e., Top Event GRID fails), but the 480V emergency bus itself is available, then backup power from the ADIT 1 hillside standby generator is credited to the 480V emergency bus until offsite power is recovered. The start and loading of the ADIT 1 hillside standby generator is automatic. This backup power source is treated separately in Top Event GEN1. Please see Figure C-17 for the BUE48 fault tree diagram.

### *7.4.2.6 GEN1 – Backup Generator at ADIT 1 for UGPH 480V Emergency Bus*

If power is lost from offsite (i.e., Top Event GRID fails), but the UGPH 480V emergency bus itself is available, then backup power from the ADIT 1 hillside standby generator is credited to the UGPH 480V emergency bus until offsite power is recovered. The start and loading of the ADIT 1 hillside standby generator is automatic. Please see Figure C-18 for the GEN1 fault tree diagram.

Four split fractions, GEN11, GEN12, GEN13 and GEN14, set the four house events EDGREQ3, EDGREQ6, EDGREQ12 and EDGREQ24, to specify the duration that the standby generator is required.

### *7.4.2.7 Top Event UFAN — ADIT 1 Supply and Exhaust Fans for UGPH*

This top event models the availability of the ventilation systems for the UGPH. This includes Supply Fans F5A and F5B, and Exhaust Fans F6a through F6d. These fans are supplied electric power from the UGPH 480V emergency bus. Both supply fans and three of the four exhaust fans are normally operating and assumed required for room ventilation to limit pump operating temperatures. These systems are required to permit long term operation of the cargo pumps for RHBFST receiving or for intra-tank fuel transfers via the surge tank. The mission time of these fans is assumed to be 24 hours. Please see Figure C-19 for the UFAN fault tree diagram.

Two split fractions, UFAN1 and UFAN2, control the inclusion/exclusion of Fail to Start (FTS) failure mode using house events listed in the following table (Table 7-14):

**Table 7-14. Fans Fail to Start House Events**

| Event Name | Event Description | Event Type |
|---|---|---|
| FTSEF6A | Fans Failure to Start | HOUSE Event |
| FTSEF6B | Fans Failure to Start | HOUSE Event |
| FTSEF6C | Fans Failure to Start | HOUSE Event |
| FTSEF6D | Fans Failure to Start | HOUSE Event |
| FTSSF5A | Fans Failure to Start | HOUSE Event |
| FTSSF5B | Fans Failure to Start | HOUSE Event |

UFAN1 split fraction excludes all Fans Failure to Start failure mode, and UFAN2 includes all Fans Failure to Start failure mode.

Given the functional redundancy of Fans F5A and F5B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode Fail to Run (FTR) and FTS.

Given the functional redundancy of Fans F6A, F6B, F6C and F6D, a third order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

The following figures shows the details of four common cause groups modeled to represent the dependent failures of UGPH ventilation system fans.

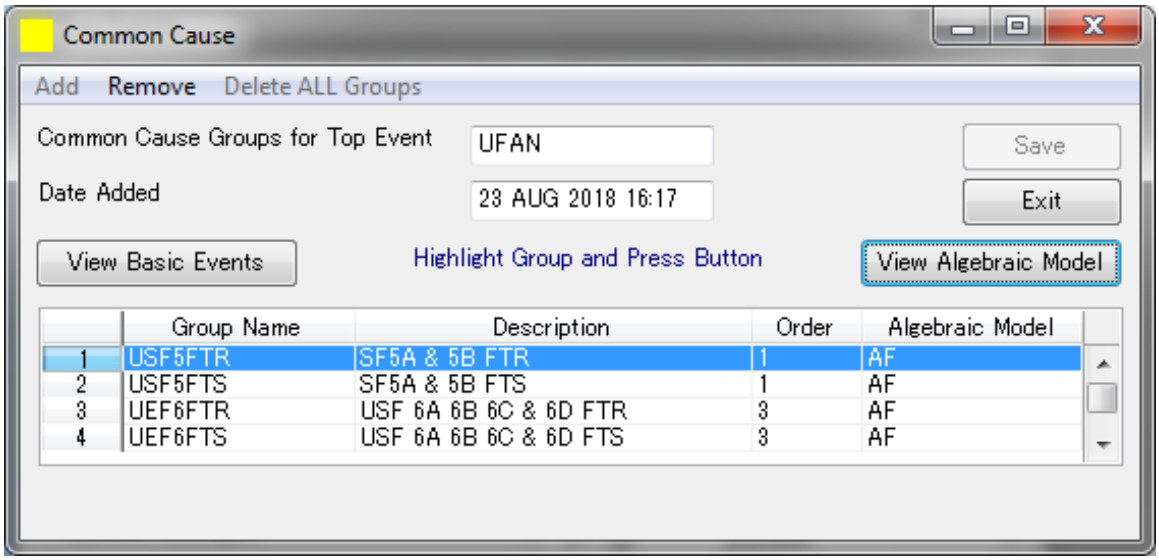



**Figure 7-4. UFAN Common Cause Groups**

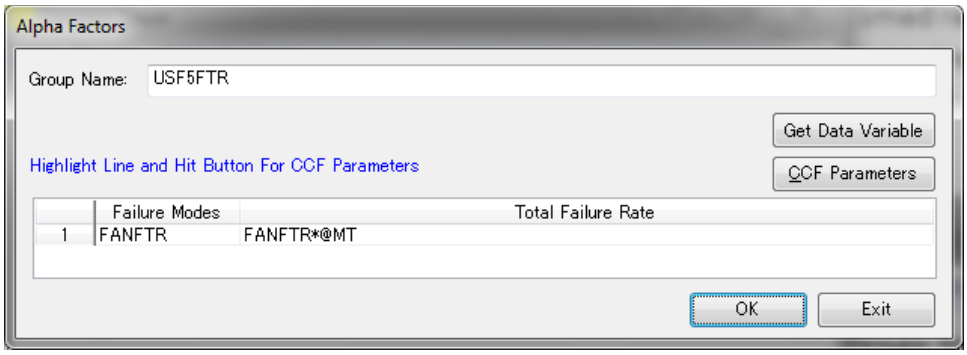



**Figure 7-5. UFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation**

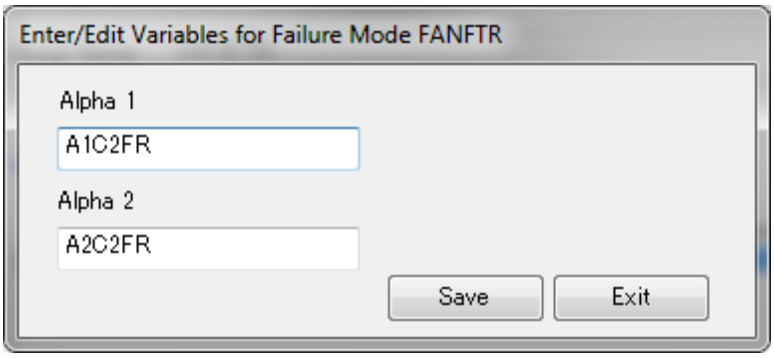



**Figure 7-6. UFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

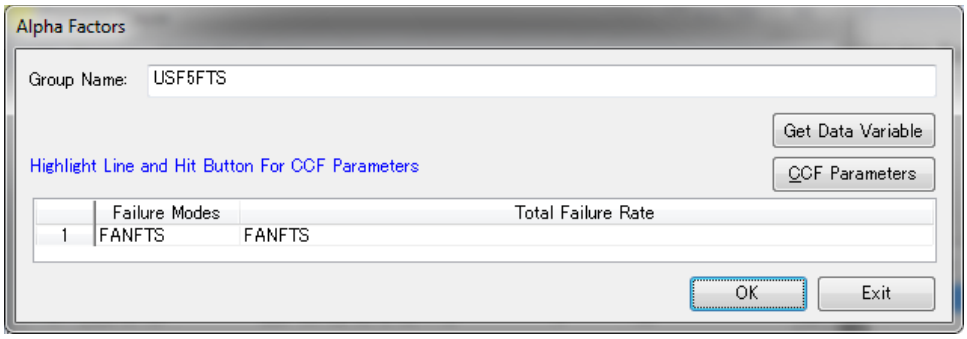



**Figure 7-7. UFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation**

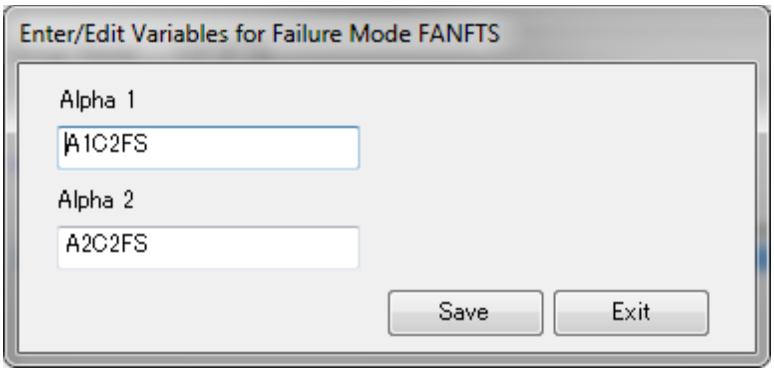



**Figure 7-8. UFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

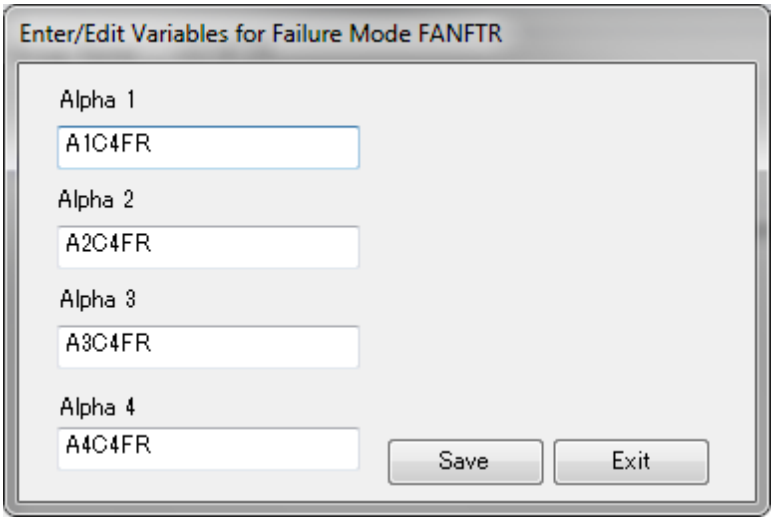



**Figure 7-9. UFAN 4th Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

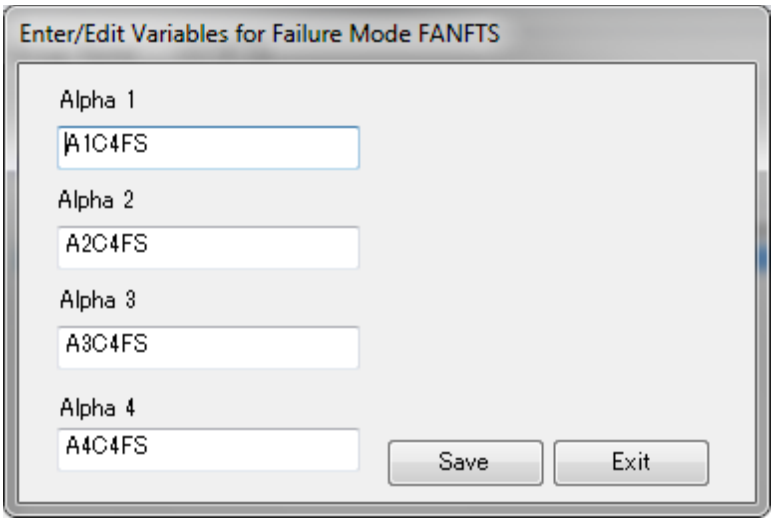



**Figure 7-10. UFAN 4th Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

To account for the unavailability of UGPH ventilation system fans due to maintenance, the maintenance unavailability for each fan was modeled as a maintenance alignment. Each alignment represents the fraction of time that a specific fan is out of service due to maintenance. The following figure shows the list of six maintenance alignments and one "NORMAL" alignment. The "Normal" alignment is the fraction of time that the fans are not in maintenance.

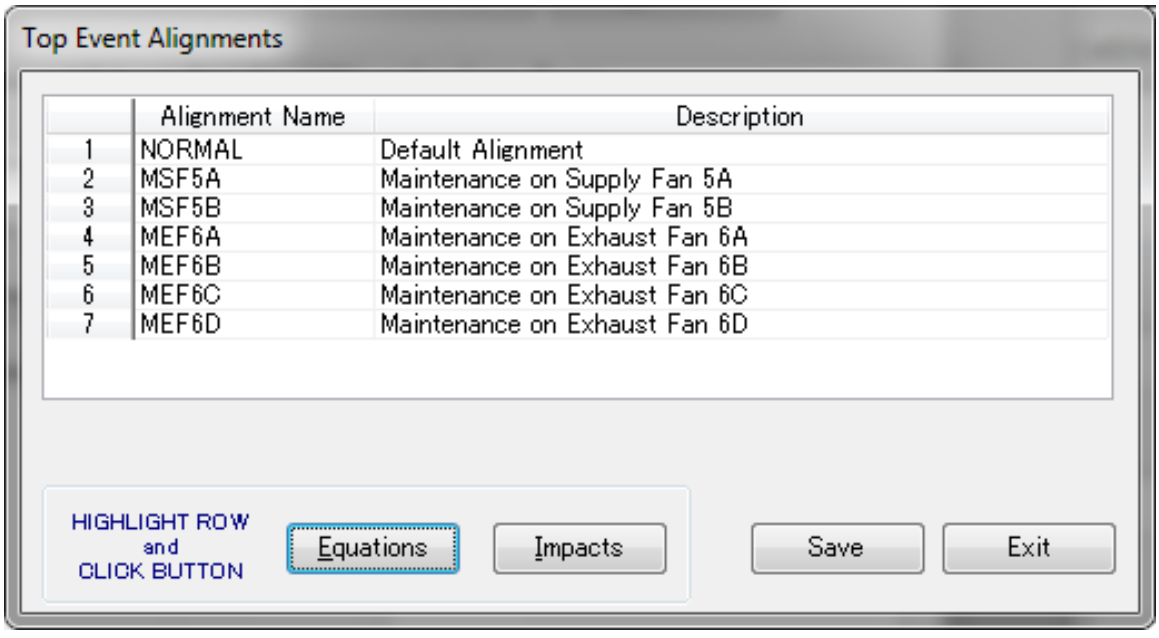



**Figure 7-11. UFAN Maintenance Alignments**

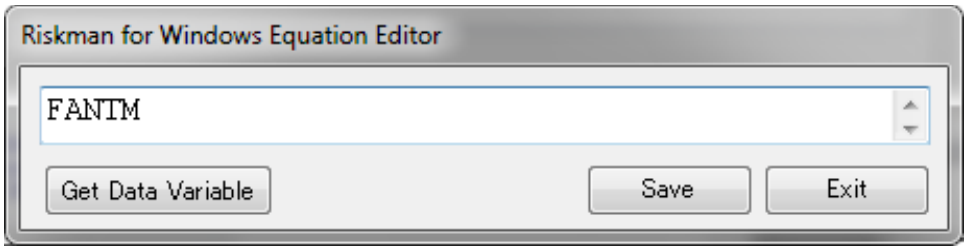



**Figure 7-12. UFAN Maintenance Alignment Equation**

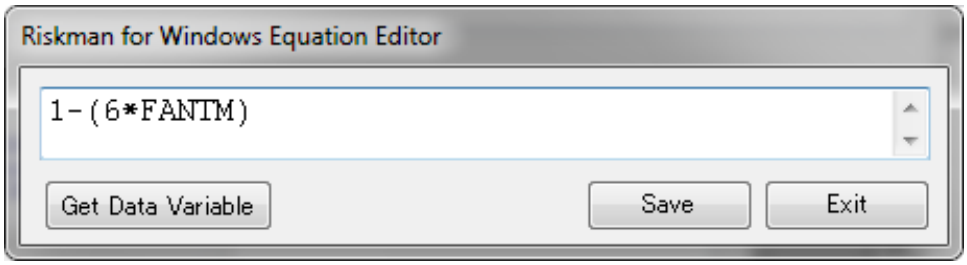



**Figure 7-13. UFAN Normal Alignment Equation**

### *7.4.2.8 Top Event B3EA — ADIT 3 208V Panel A*

This top event models the availability of power from offsite or from the standby generator at ADIT 3 to Panel A for 24 hours. Panel A supplies lighting to the ADIT 3 tunnel. The top event model includes the 11.5 kV to 480V transformer which normally brings power from offsite. To Power Panel A, Panel B must also be energized. Panel B provides power to the ventilation fans and the tunnel sump pump. These are assumed available if Top Event B3EA is successful. The water main pumps at ADIT 3 are supplied power from a 2.4 kV main pumps panel that is not backed up by the ADIT 3 generator. These main water pumps would be lost if power from offsite or the 11.5 kV to 2.4 kV transformer fails. However, these pumps perform no function to mitigate leaks at Red Hill and so are not modeled. Please see Figure C-20 for the B3EA fault tree diagram. The equation for the single basic event in this fault tree accounts for either transformers (11.5 kV to 480V, or 11.5 kV to 2.4 kV) failing or the two electrical panels, A and B, failing.

If power is lost from offsite (i.e., Top Event GRID fails), but the 480V Panel B itself is available, then backup power from the ADIT 3 standby generator is credited. Panel B supplies Panel A via a 480V to 208V/120V transformer. The start and loading of the ADIT 3 standby generator is automatic. This backup power is modeled separately in Top Event GEN3.

### *7.4.2.9 GEN3 – Backup Generator at ADIT 3 for 480V Panels B and A*

If power is lost from offsite (i.e., Top Event GRID fails), but Panels A and B are available, then backup power from the ADIT 3 standby generator is credited. The generator must operate until offsite power is recovered. The start and loading of the ADIT 3 standby generator is automatic. Please see Figure C-21 for the GEN3 fault tree diagram.

### 7.4.2.10 Top Event BRN48 — Red Hill 480V Normal Bus

This top event models the availability of power from offsite to the Red Hill 480V normal bus located in the LAT electrical room for 24 hours. The top event model includes the 11.5 kV to 480V transformer supplying offsite power to the Red Hill 480V Normal bus. If power is lost from offsite (i.e., GRID fails) this bus is de-energized; i.e., there is no backup power.

Loss of power to this bus does indirectly, however, challenge the ADIT 5 generator to start to supply the Red Hill 480V emergency bus. Other than the Red Hill 480V emergency bus, the only other significant load from the Red Hill 480V normal bus is power for the Red Hill LAT oil tight door. The uninterruptable power supply (UPS) for its magnets is then required to maintain the door open. Please see Figure C-22 for the BRN48 fault tree diagram.

Recovery of offsite power to the Red Hill 480V normal bus, given the hardware is available, is represented separately based on the status of electric power recovery Top Event GRIDR.

### 7.4.2.11 Top Event BRE48 — Red Hill 480V Emergency Bus

This top event models the availability of power from offsite to the Red Hill 480V emergency bus located in the LAT electrical room for 24 hours. The top event model includes the 11.5 kV to 480V transformer.

The Red Hill 480V emergency bus supplies its own cooling fans via Panel L and numerous other panels; i.e., Panels LP13, P14, P15, LP16-1, LP16-2, LP17-1, LP17-2, LP18, LP19, LP20, LP21, LP22, LP23, LB, LC, P1, P2, Panel A, Panel LA, Panel G, Panel PA, and Panels PP1 through PP8. Transformers T13, T14, and T15 are used to drop the voltage for some of these panels.

A listing of all the specific loads supplied by each of these panels is not available. However, what loads have been identified are most of these panels supply tunnel lighting, radios, and cameras. The panels which supply motor-operated valves, ventilation fans, the two elevators, and selected sump pumps are: P1, P2, Panel L, Panel G, Panel PA, and Panels PP1 through PP8. Therefore, as a modeling simplification, the failure of power at any one of these 13 panels, or failure of Transformer T11 which supplies Panel L, is conservatively assumed to have the same impact on the facility as failing power at the 480V Red Hill emergency bus itself. The remaining panels supplied by the 480V Red Hill emergency bus are instead modeled in Top Event LPRH.

The most likely cause of losing power to the 480V emergency bus is the joint failure of power from both the offsite grid and the ADIT 5 generator. If power is lost from offsite (i.e., Top Event GRID fails), the Red Hill 480V normal and emergency buses will de-energize, and the 275 kW standby generator at ADIT 5 will start and load the Red Hill emergency bus automatically via an automatic transfer switch. This standby generator is modeled in Top Event GEN5. Please see Figure C-23 for the BRE48 fault tree diagram.

### 7.4.2.12 GEN5 – Standby Generator at ADIT 5 for Red Hill 480V Emergency Bus

If power is lost from offsite (i.e., Top Event GRID fails), but the Red Hill 480V emergency bus is available, then backup power from the ADIT 5 standby generator is credited. The generator must operate until offsite power is recovered. The start and loading of the ADIT 5 standby generator is automatic. Please see Figure C-24for the GEN5 fault tree diagram.

### 7.4.2.13 Top Event LPRH – Red Hill Panels Supplying Lighting, Radios, and Cameras

This top event models the Red Hill panels supplied power from the Red Hill 480V emergency bus, but which only supply lighting, radios, and cameras in different Red Hill locations. The areas covered are the upper harbor tunnel, LAT, UAT, Gauger Station, and ADIT 6. Failure of power to any one of the following panels is conservatively assumed to cause a loss of power for lighting, radios, and cameras for all of these areas. If power is lost from Red Hill 480V emergency bus (i.e., Top Event BRE48 fails), then all of these panels also lose power.

The panels considered in this top event are: LP13, P14, P15, LP16-1, LP16-2, LP17-1, LP17-2, LP18, LP19, LP20, LP21, LP22, LP23, LB, LC, Panel A, and Panel LA. Associated Step-Down Transformers T13 and T15 supplying only these panels are also modeled in this top event. A mission time of 24 hours is assumed. Please see Figure C-25 for the LPRH fault tree diagram. The single basic event in this fault tree represents the 17 electrical panels combined.

### 7.4.2.14 Top Event AFHE — Automatic Fuel Handling Equipment

This top event models the availability of the AFHE system to provide indications, controls, and alarms to the control room operators for 24 hours. Failure of the AFHE is also assumed to disable the panic button but would also cause any operating cargo pumps to trip. The AFHE receives electric power from the UGPH 480V emergency bus; i.e., Top Event BUE48. Failure of the UGPH 480V emergency bus would challenge the AFHE's UPS to provide backup power. Power from the same bus supplies the backup power from Fujitsu so it would be lost as well. Without electric power, AFHE would be unavailable beyond 8 hours after which its UPS is discharged. Please see Figure C-26 for the AFHE fault tree diagram.

### 7.4.2.15 Top Event AFHR — AFHE Condensing and Fans for Heat Removal

This top event models the availability of the heat removal systems for the AFHE system. These systems are required to permit long term operation of the AFHE system to provide indications, controls, and alarms to the control room operators for 24 hours. After a period of operation without heat removal, the AFHE is assumed to fail. The impacted equipment are then the same as those specified for Top Event AFHE. The overheating of the AFHE occurs whether the system is supplied electric power from the UGPH 480V emergency bus (i.e., Top Event BUE48) or its UPS supply. Please see Figure C-27 for the AFHR fault tree diagram.

### 7.4.2.16 Top Event EFAN — Fans for Tanks 1–16 in LAT and UAT Fail to Operate (also supply electrical room in LAT)

This top event models the availability of Supply Fans SF-1A and SF-1B to provide room ventilation to the electrical room in the LAT for 24 hours. This top event also considers the exhaust fan pairs, 1-A/1-B and EF-2A/2B. Failure of any of the fan pairs is assumed to cause ventilation to be lost in both the LAT and the UAT below the bulkhead separating these areas from Tanks 17-20. Loss of any fan pair is also conservatively assumed to degrade air flow sufficiently to require Red Hill operating staff to evacuate the tunnels. This top event also considers if the Red Hill 480V normal and emergency buses are operating to supply the fans. The failure of electrical room ventilation may lead to excessive temperatures in that room, causing both the Red Hill normal and emergency buses to fail after a period of room heating caused by the loss of ventilation. Please see Figure C-28 for the EFAN fault tree diagram.

Given the functional redundancy of Exhaust Fans 1-A and 1-B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

Given the functional redundancy of Exhaust Fans 2-A and 2-B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

Given the functional redundancy of Supply Fans SF-1A and SF-1B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

The following figures shows the details of six common cause groups modeled to represent the dependent failures of the electrical room in the LAT ventilation system fans.

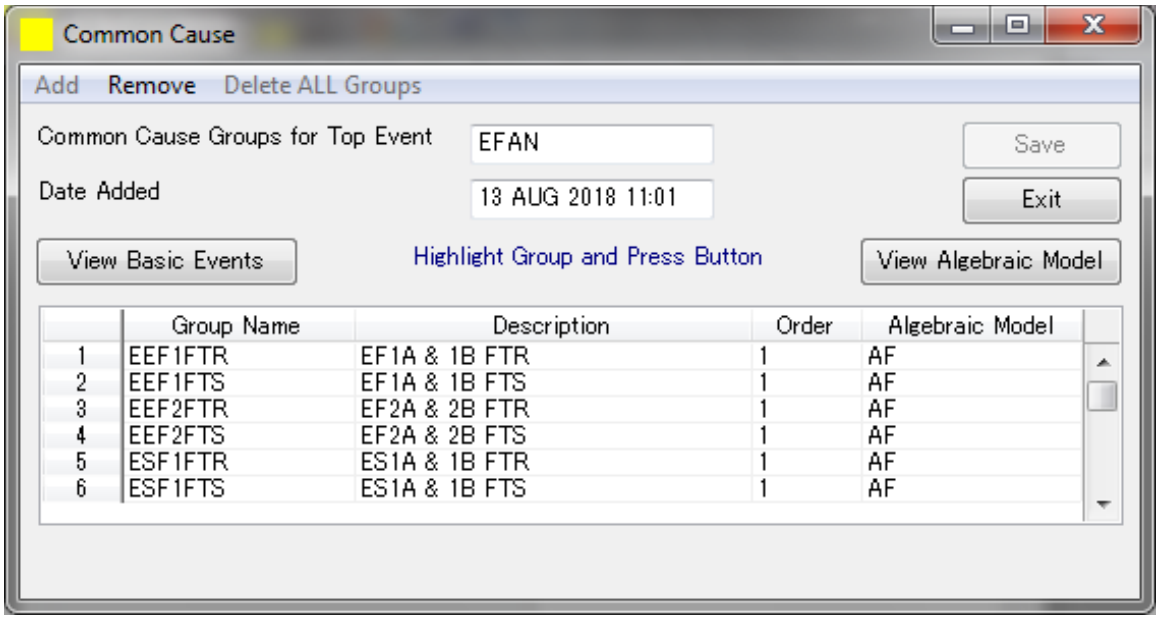



**Figure 7-14. EFAN Common Cause Groups**

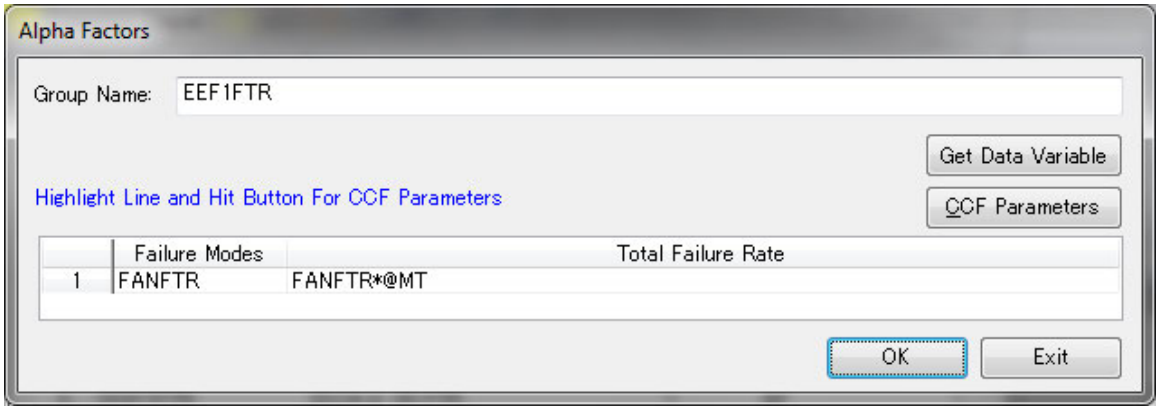



**Figure 7-15. EFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation**

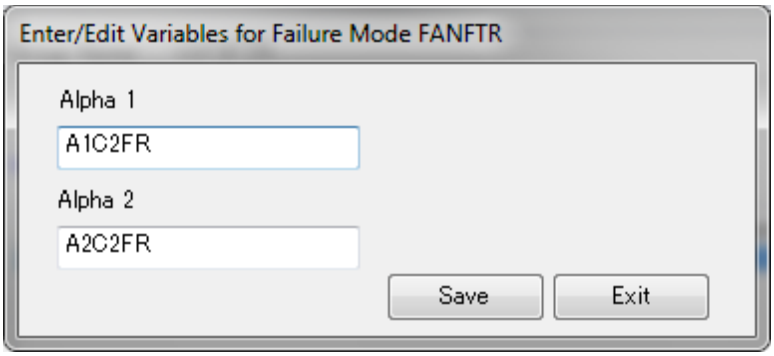



**Figure 7-16. EFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

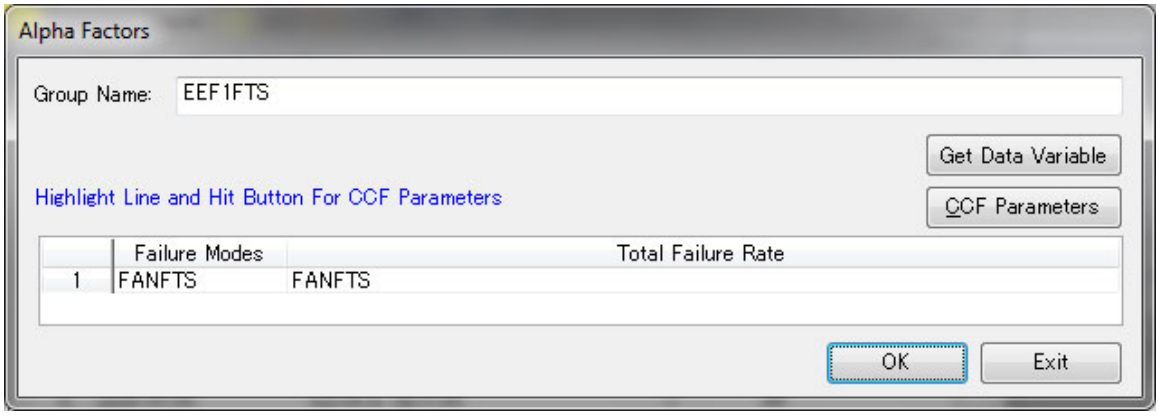



**Figure 7-17. EFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation**

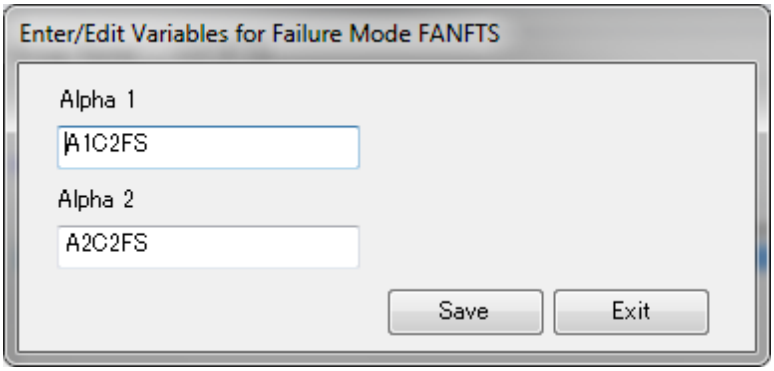



**Figure 7-18. EFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

To account for the unavailability of the electrical room in the LAT ventilation system fans due to maintenance, the maintenance unavailability for each fan was modeled as a maintenance alignment. Each alignment represents the fraction of time that a specific fan is out of service due to maintenance. The following figure shows the list of six

maintenance alignments and one “Normal” alignment. The “Normal” alignment is the fraction of time that the fans are not in maintenance.

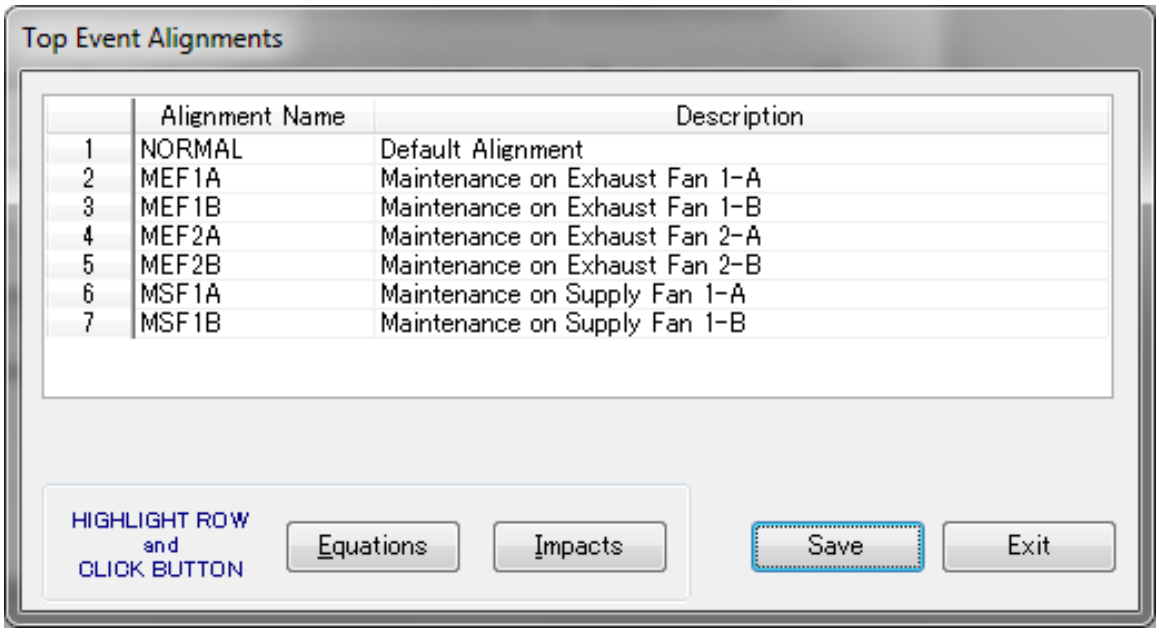



**Figure 7-19. EFAN Maintenance Alignments**

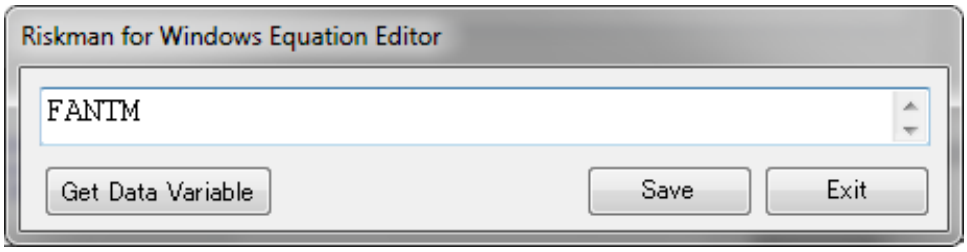



**Figure 7-20. EFAN Maintenance Alignment Equation**

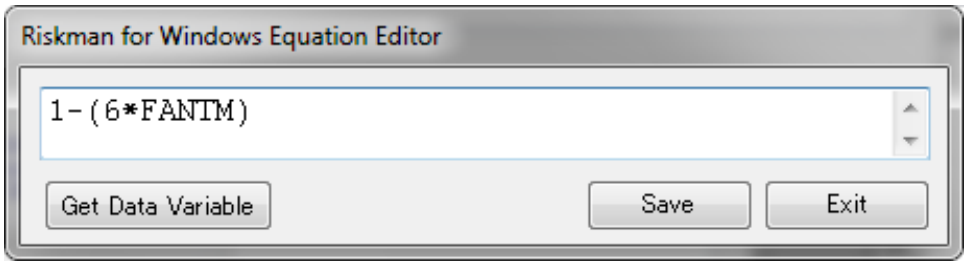



**Figure 7-21. EFAN Normal Alignment Equation**

### 7.4.2.17 Top Event TFAN — Fans for Tanks 17–20 LAT and UAT Fail to Operate (above bulkhead)

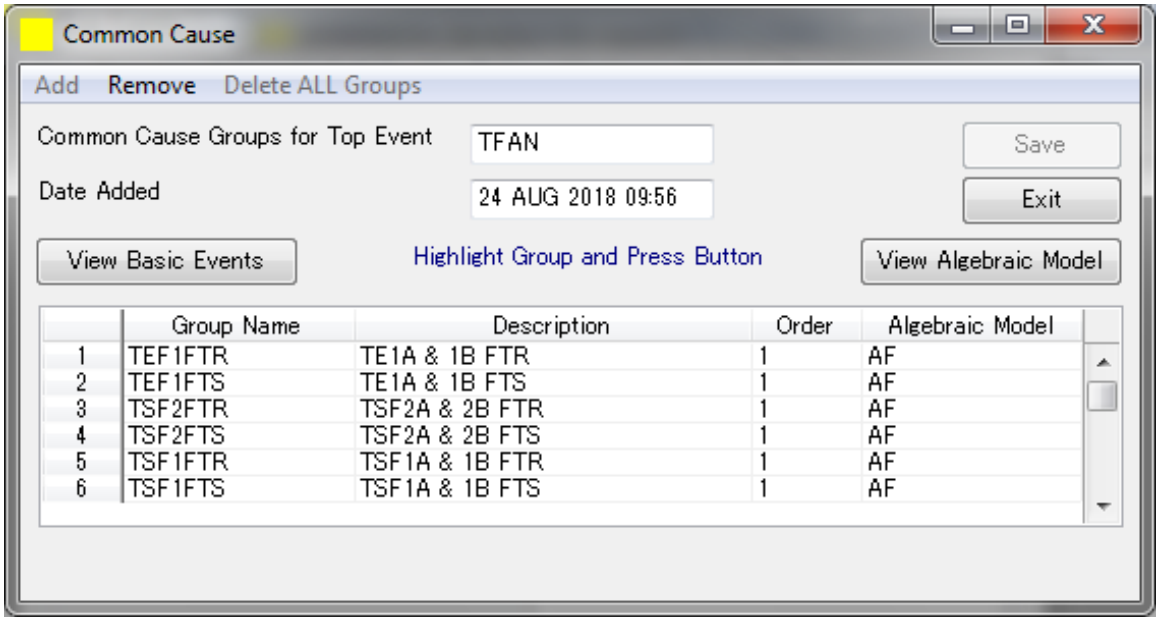
This top event models the availability of the ventilation system above the bulkhead separating RHBFSTs 1–16 from 17 through 20. This top event model considers the operation of Exhaust Fans PE-1A/1B and supply Fan Pairs PS-1A/1B and PS-2A/2B. Failure of any of the fan pairs is assumed to lose ventilation in both the LAT and the UAT above the bulkhead, separating these areas from Tanks 1–16. Loss of any fan pair is assumed to degrade air flow sufficiently to require Red Hill operating staff to evacuate the tunnels. This top event also considers if the Red Hill 480V normal and emergency buses are operating to supply the fans. Please see Figure C-29 for the TFAN fault tree diagram.

Given the functional redundancy of Exhaust Fans PE-1A/1B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

Given the functional redundancy of Supply Fans PS-1A/1B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

Given the functional redundancy of Supply Fans PS-2A/2B, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

The following figures shows the details of six common cause groups modeled to represent the dependent failures of the ventilation system fans above the bulkhead separating RHBFSTs 1–16 from 17 through 20.




| | Group Name | Description | Order | Algebraic Model |
|---|---|---|---|---|
| 1 | TEF1FTR | TE1A & 1B FTR | 1 | AF |
| 2 | TEF1FTS | TE1A & 1B FTS | 1 | AF |
| 3 | TSF2FTR | TSF2A & 2B FTR | 1 | AF |
| 4 | TSF2FTS | TSF2A & 2B FTS | 1 | AF |
| 5 | TSF1FTR | TSF1A & 1B FTR | 1 | AF |
| 6 | TSF1FTS | TSF1A & 1B FTS | 1 | AF |

**Figure 7-22. TFAN Common Cause Groups**

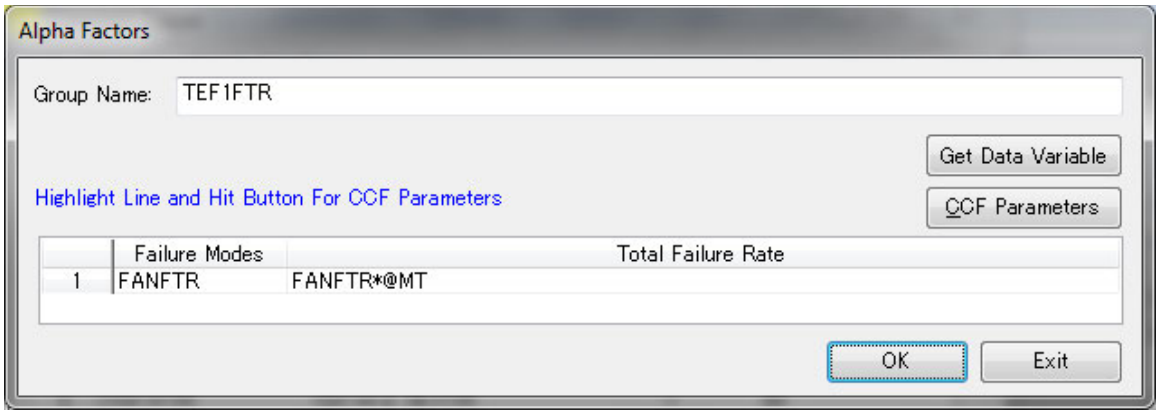



**Figure 7-23. TFAN Common Cause Fail to Run Failure Mode and Failure Rate Equation**

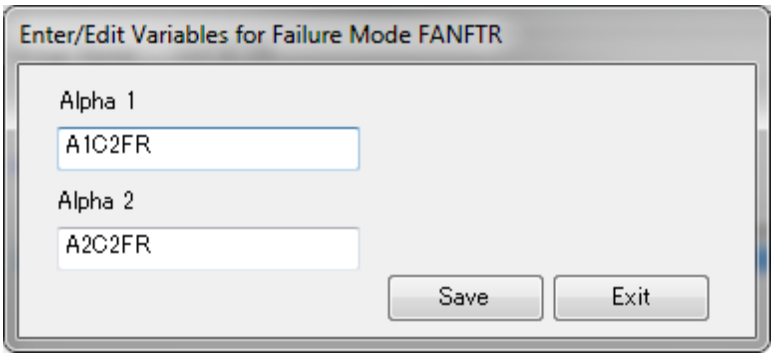



**Figure 7-24. TFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

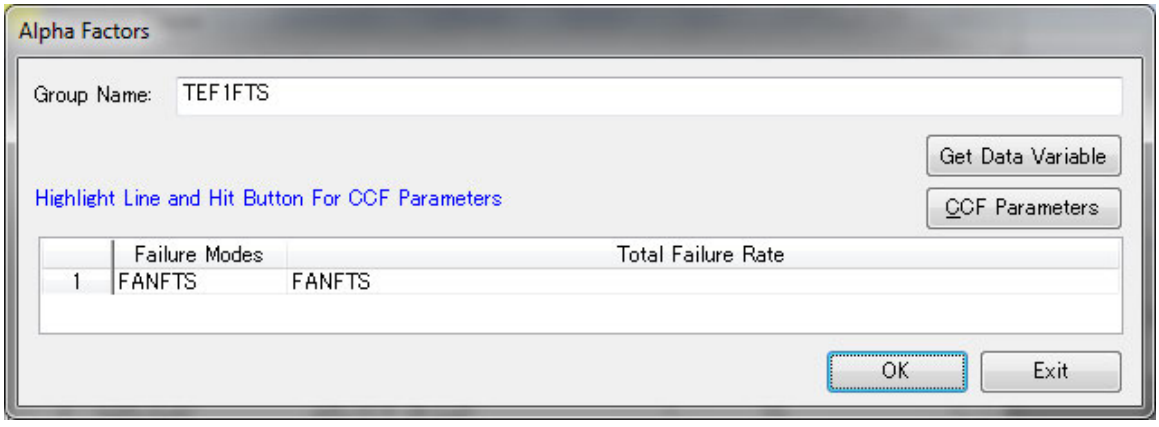



**Figure 7-25. TFAN Common Cause Fail to Start Failure Mode and Failure Rate Equation**

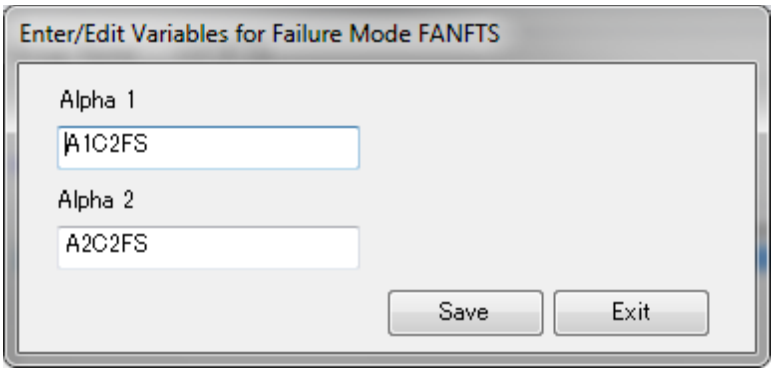



**Figure 7-26. TFAN 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

To account for the unavailability of the ventilation system above the bulkhead separating RHBFSTs 1–16 from 17 through 20 due to maintenance, the maintenance duration for each fan was modeled as a maintenance alignment. Each alignment represents the maintenance duration or the time that a specific fan is out of service. The following figure shows the list of six maintenance alignments and one "Normal" alignment. The "Normal" alignment is the duration of time that the fans are not in maintenance.

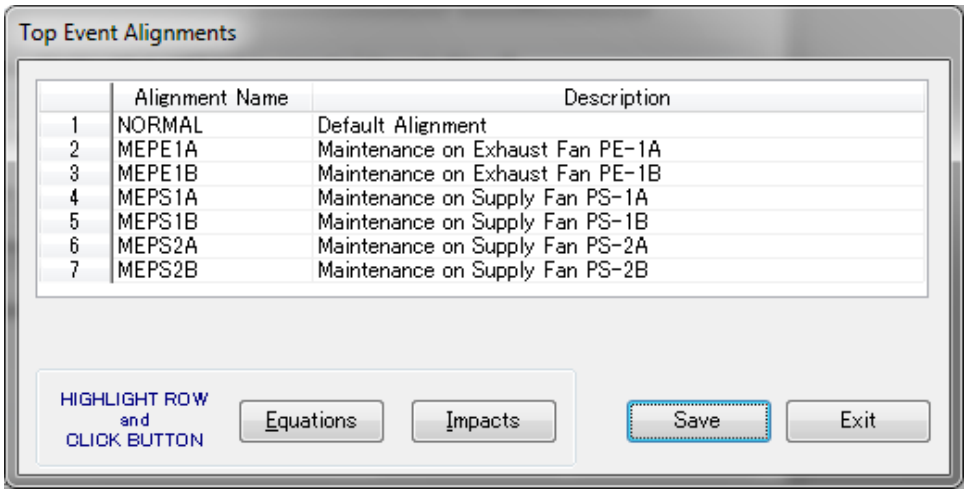



**Figure 7-27. TFAN Maintenance Alignments**

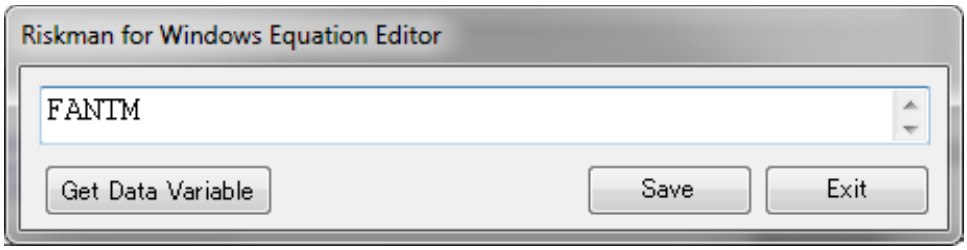



**Figure 7-28. TFAN Maintenance Alignment Equation**

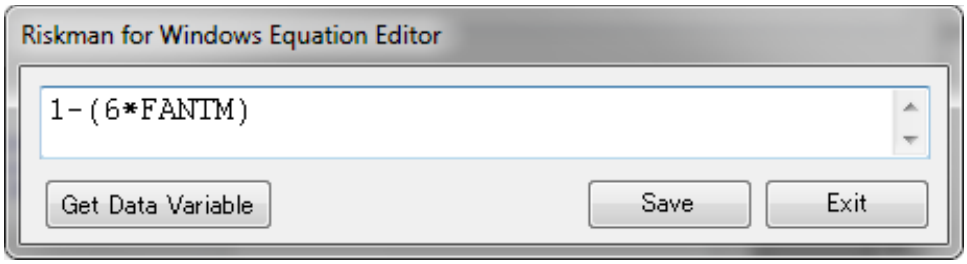



**Figure 7-29. TFAN Normal Alignment Equation**

### 7.4.3 The Top Events for the OTHERSUP Event Tree

The top events of the other supporting system event tree are defined below:

**Table 7-15. Top Events Referenced by OTHERSUP Event Tree**

| | |
|---|---|
| CRM | Control room electrical power, lighting, and air conditioning |
| ACRM | Alternate control room electrical power, lighting, and air conditioning |
| UHMOV | Electrical power to UGPH MOVs and Lower Harbor Tunnel MOVs |
| CARGO | Two or more cargo pumps available to move leaking fuel type |
| ULIT | Electrical power for UGPH lighting and Lower Harbor Tunnel lighting |
| EL72 | Personnel Elevator 72 & controller |
| EL73 | Cargo Elevator 73 & controller |
| RMOV | Electrical power for Red Hill sectional valves down to ADIT 3Y and all LAT MOVs |
| RHIN | Support for Red Hill instruments, indications, level alarms, and signals |

#### 7.4.3.1 Top Event CRM — Control Room Electrical Power, Lighting, and Air Conditioning

This top event models the availability of power to the control room for operator controls, lighting, and air conditioning following an initiating event. Success of this top event requires that power be available for 24 hours. Lighting and air conditioning in the main control room would facilitate the operator's actions in response to a leak. The source of power is from the UGPH 480V emergency bus; i.e., represented by Top Event BUE48. Loss of power challenges the control room UPS to maintain the control room controls. There is no backup electric power for CR Lighting.

#### *7.4.3.2 Top Event ACRM — Alternate Control Room Electrical Power, Lighting, and Air Conditioning*

This top event models the availability of power to the alternate control room in the Fuel Operations Building for operator controls, lighting, and air conditioning following an initiating event. Success of this top event requires that power be available for 24 hours. Lighting and air conditioning in the alternate control room would facilitate the operator's

actions in response to a leak. With the exception of cargo pump operation, the same controls are available in the main control room. The source of power is from the UGPH 480V normal bus; i.e., represented by Top Event BUN48. Its power source is not backed up by a standby generator. Loss of power challenges the alternate control room UPS to maintain the alternate control room controls. There is no backup electric power for alternate control room lighting.

#### *7.4.3.3 Top Event UHMOV – Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs*

This top event tracks the status of electrical power to the motor-operated valves in the UGPH and in the Lower Harbor Tunnel following an initiating event. Without electrical power to remotely operate these valves, it would take much longer to manually, and locally manipulate any of these valves. Success of this top event requires that power be available for 24 hours. The source of power is from the UGPH 480V emergency bus; i.e., represented by Top Event BUE48. Its power source is backed up by a standby generator. This top event is simply a switch to track the status of power to these valves.

#### *7.4.3.4 Top Event CARGO – Two or More Cargo Pumps Available to Move Leaking Fuel Type*

This top event models the 11 cargo pumps in the UGPH (i.e., 5 for F-76, 3 for JP-5, and 3 for F-24 fuel pumps) following an initiating event. Availability of these pumps is essential to transfer fuel to or from the RHBFSTs. Pumps for each fuel type have been modeled as a separate sub-tree. Please see Figure C-30 for the CARGO fault tree diagram for more details.

F76CPUMPS models the pumps and valves required to transfer F76 fuel type. Success of this sub-tree requires two out of five pumps (0201, 0202, 0203, 0204 and 0205) and associated valves to function. Due to the functional redundancy of Pumps 0201 through to 0205 a fourth order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

JP5CPUMPS models the pumps and valves required to transfer JP5 fuel type. Success of this sub-tree requires two out of three pumps (0206, 0207 and 0208) and associated valves to function. Due to the functional redundancy of Pumps 0206 through to 0208 a second order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

F24CPUMPS models the pumps and valves required to transfer F24 fuel type. Success of this sub-tree requires two out of three pumps (0209, 0210 and 0211) and associated valves to function. Due to the functional redundancy of Pumps 0209 through to 0211 a second order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

The following figures show the details of six common cause groups modeled to represent the dependent failures of the cargo pumps.

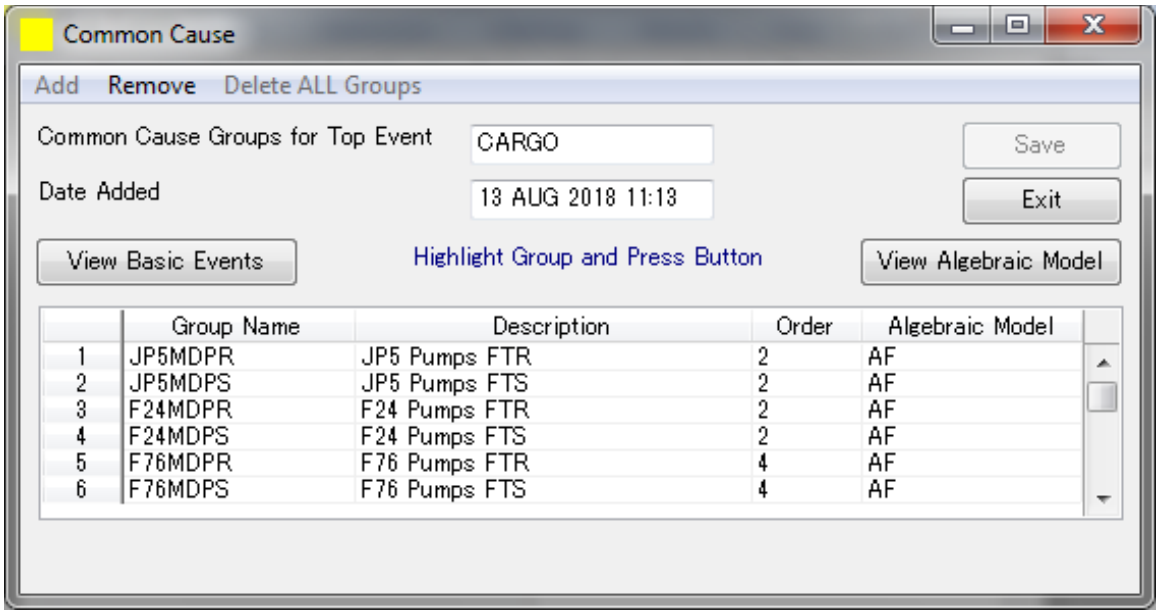



**Figure 7-30. CARGO Pumps Common Cause Groups**

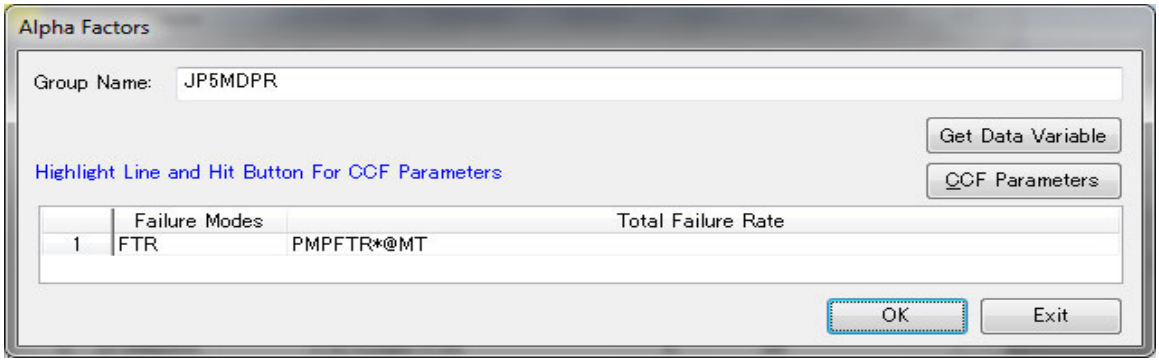



**Figure 7-31. CARGO Pumps Common Cause Fail to Run Failure Mode and Failure Rate Equation**

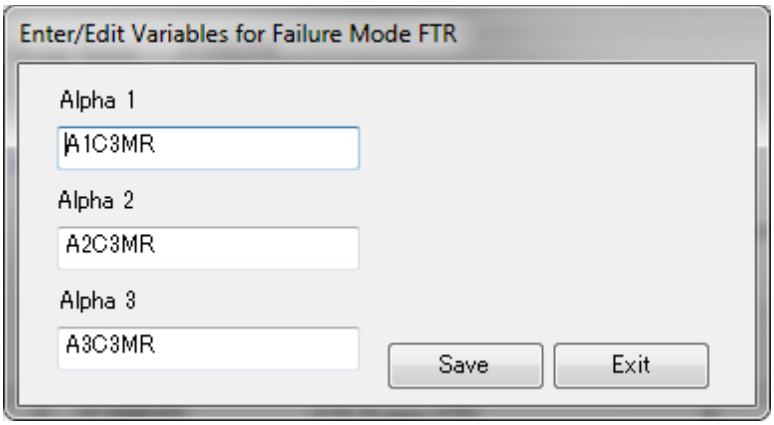



**Figure 7-32. CARGO Pumps 2nd Order Alpha Factor Common Cause Parameters for Pumps Fail to Run Failure Mode**

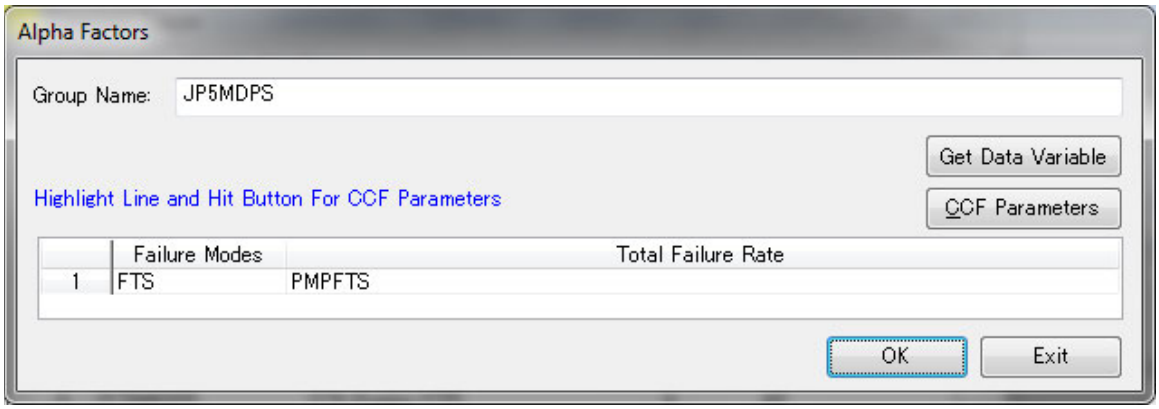



**Figure 7-33. CARGO Pumps Common Cause Fail to Start Failure Mode and Failure Rate Equation**

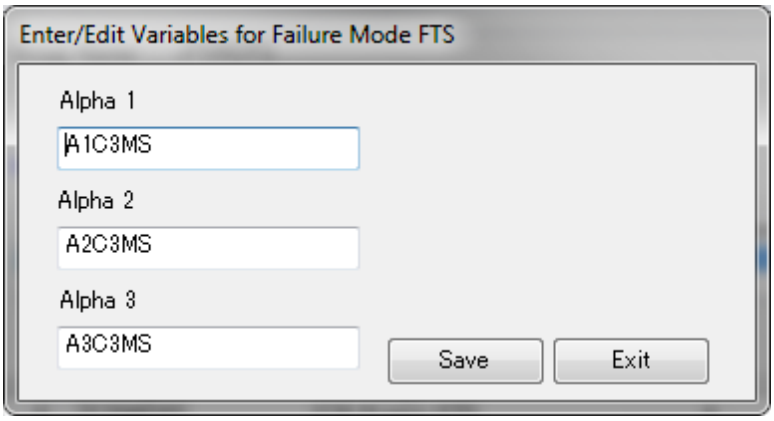



**Figure 7-34. CARGO Pumps 2nd Order Alpha Factor Common Cause Parameters for Pumps Fail to Start Failure Mode**

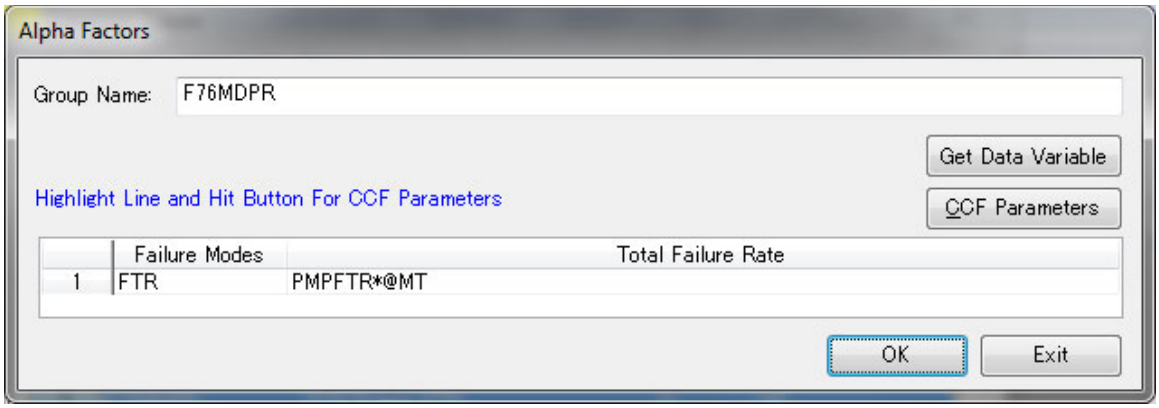



**Figure 7-35. CARGO Pumps Common Cause Fail to Run Failure Mode and Failure Rate Equation**

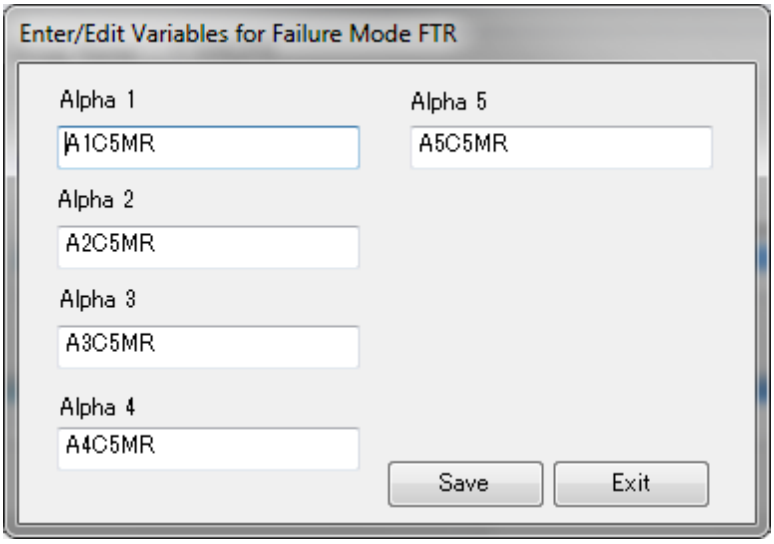



**Figure 7-36. CARGO Pumps 4th Order Alpha Factor Common Cause Parameters for Pumps Fail to Run Failure Mode**

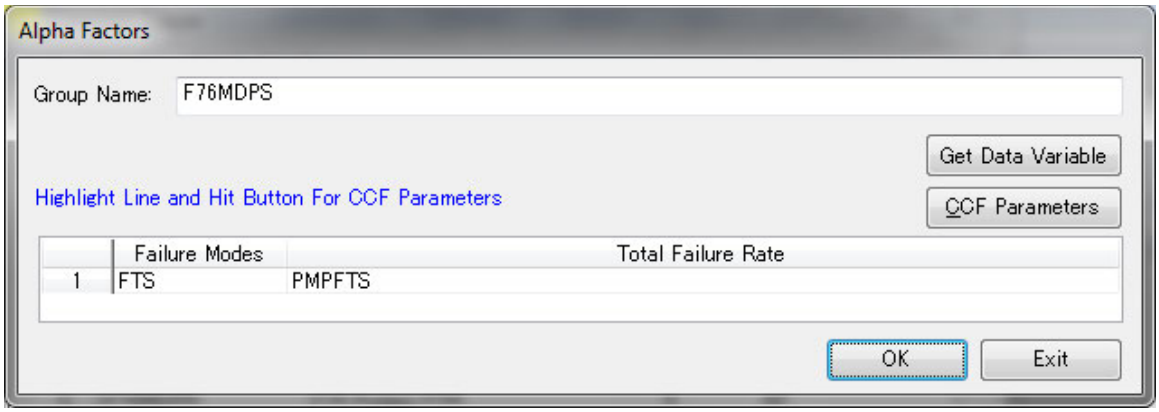



**Figure 7-37. CARGO Pumps Common Cause Fail to Start Failure Mode and Failure Rate Equation**

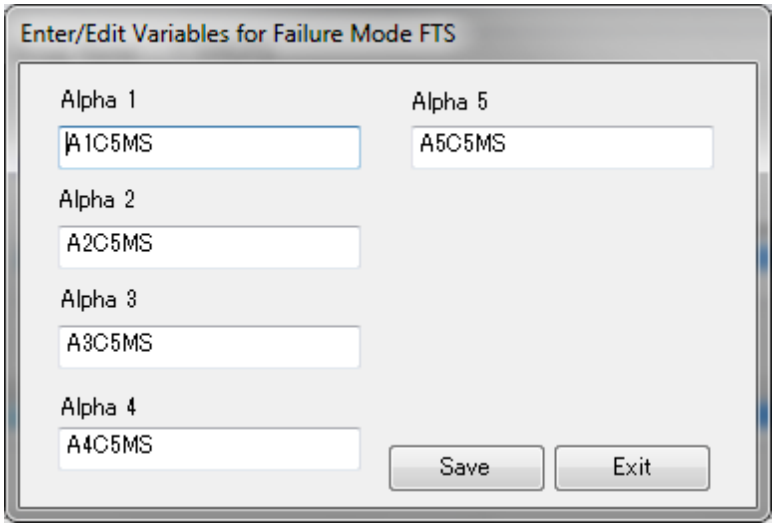



**Figure 7-38. CARGO Pumps 4th Order Alpha Factor Common Cause Parameters for Pumps Fail to Start Failure Mode**

### *7.4.3.5 Top Event ULIT – Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting*

This top event tracks the status of electrical power to the lights throughout the UGPH following an initiating event. Without lighting the staff's efforts to respond to a fuel leak would be hampered. Success of this top event requires that power be available for 24 hours. The source of power for the lights is from the UGPH 480V normal bus; i.e., represented by Top Event BUN48. Its power source is not backed up by a standby generator. This top event is simply a switch to track the status of UGPH lighting. The Lower Harbor Tunnel lighting has the same electrical power dependency.

### 7.4.3.6 Top Event EL72 – Personnel Elevator 72 and Controller

This top event tracks the availability of the personnel service elevator at Red Hill (i.e., Elevator 72) following an initiating event. Elevator 72 is located just above Tanks 15 and 16, and just below the bulkhead separating these tanks from Tanks 17 and 18. Without this elevator, the top gauger would most likely open the bulkhead to the upper LAT and take the cargo elevator (73) to the UAT for top gauging. Success of this top event requires that power be available for 24 hours. The source of power for personnel Elevator 72 is from the Red Hill 480V emergency bus; i.e., represented by Top Event BRE48. Its power source is backed up by a standby generator. This top event not only tracks the availability of electric power, but also considers random failures of the elevator to operate, including periods of time when the elevator is out of service for maintenance. The cargo elevator, 73, has the same electric power dependency, but is tracked separately because the random failures are not shared.

Please see Figure C-42, EL72 Fault Tree Diagram, for more details.

### 7.4.3.7 Top Event EL73 – Cargo Elevator 73

This top event tracks the availability of the cargo elevator at Red Hill (i.e., Elevator 73) following an initiating event. Elevator 73 is located just above Tanks 17 and 18 and below Tanks 19 and 20. Without this elevator, the top gauger would most likely open the bulkhead to the LAT and take the personnel elevator, 72, to the UAT for top gauging. Success of this top event requires that power be available for 24 hours. The source of power for Cargo Elevator 73 is from the Red Hill 480V emergency bus; i.e., represented by Top Event BRE48. Its power source is backed up by a standby generator. This top event not only tracks the availability of electric power, but also considers random failures of the elevator to operate, including periods of time when the elevator is out of service for maintenance. The personnel elevator, 72, has the same electric power dependency, but is tracked separately because the random failures of each elevator are not shared.

Please see Figure C-43, EL73 Fault Tree Diagram, for more details.

### 7.4.3.8 Top Event RMOV – Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and All LAT MOVs

This top event tracks the status of electrical power to the key MOVs at Red Hill; i.e., the sectional valves in the LAT down to ADIT 3Y and the skin and ball valves at each RHBFST following an initiating event. Without electrical power, remote operation of these valves would be prevented. Instead, local manual action would be necessary to complete the required valve manipulations and this would delay the completion times. Success of this top event requires that power be available for 24 hours. The source of power for these valves is all from the Red Hill 480V emergency bus; i.e., represented by Top Event BRE48. Its power source is backed up by a standby generator. This top event is simply a switch to track the status of electrical power to the valves. The sectional valves below 3Y are all powered from the UGPH 480V emergency bus, as tracked by earlier Top Event UHMOV.

#### 7.4.3.9 *Top Event RHIN – Support for Red Hill Instruments, Indications, Level Alarms, and Signals*

This top event tracks the status of electrical power and the AFHE system needed to support Red Hill instruments, indications, RHBFST level alarms, and signals. The only Red Hill actuation signal modeled is that of a mechanical float in each RHBFST. On detection of high level, an automatic signal is sent to trip the cargo pumps and to close the associated RHBFST skin valve in order to stop the detected overfilling. Other sensed conditions also are passed through the AFHE system to alert the control room operators. Success of this top event requires that power be available for 24 hours. The source of power for these devices is all from the Red Hill 480V emergency bus; i.e., represented by Top Event BRE48. Its power source is backed up by a standby generator. This top event is simply a switch to track the status of support to these devices.

### 7.4.4 The Top Events for the VALVES Event Tree

The top events of the Valves event tree are defined below:

**Table 7-16. Top Events Referenced by VALVES Event Tree**

| | |
|---|---|
| SKIN | Successful operation of the skin valve of the RHBFST identified in Top Event TKID of the configuration event tree |
| BALL | Successful operation of the ball valve of the RHBFST identified in Top Event TKID of the configuration event tree |
| SKINX | Successful operation of the skin valve of the RHBFST identified in Top Event TKXF of the configuration event tree |
| BALLX | BALLX - Successful operation of the ball valve of the RHBFST identified in Top Event TKXF of the configuration event tree |
| FLISO | FLISO – Successful closure of the upstream sectional valve |
| FLTKC | FLTKC – Successful isolation of the fuel line leak from all aligned RHBFSTs |
| FLTKO | FLTKO – Successful opening of the fuel line from a RHBFST that is to be emptied |
| EVAC | Sequence conditions necessitate initial evacuation from Red Hill |

#### 7.4.4.1 *Top Event SKIN – Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree*

The SKIN top event models the 20 skin valve failures on an individual basis based on the RHBFST identification. Please see Figure C-44, SKIN Fault Tree Diagram, for more details.

#### 7.4.4.2 Top Event BALL – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKID of the Configuration Event Tree

The BALL top event models the 20 ball valve failures on an individual basis based on the RHBFST identification. Please see Figure C-45, BALL Fault Tree Diagram, for more details.

#### 7.4.4.3 Top Event SKINX – Successful Operation of the Skin Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree

The SKINX top event models the 20 skin valve failures which may XFR fuel from associated RHBFST on an individual basis based on the RHBFST identification. Please see Figure C-46, SKINX Fault Tree Diagram, for more details.

#### 7.4.4.4 Top Even BALLX – Successful Operation of the Ball Valve of the RHBFST Identified in Top Event TKXF of the Configuration Event Tree

The BALLX top event models the 20 ball valve failures which may XFR fuel from associated RHBFST on an individual basis based on the RHBFST identification. Please see Figure C-47, BALLX Fault Tree Diagram, for more details.

#### 7.4.4.5 Top Event FLISO – Successful Closure of the Upstream Sectional Valve

The FLISO top event models successful closure or the sectional valve upstream of a pipe segment. Please see Figure C-48, FLISO Fault Tree Diagram, for more details.

#### 7.4.4.6 Top Event FLTKC – Successful Isolation of the Fuel Line Leak from All ALIGNED RHBFSTs

The FLTKC top event is a switch to identify the status of successful isolation of the fuel line leak from all aligned RHBFST. The following table lists the possible values for the switch.

**Table 7-17. FLTKC Switch Value**

| SF Name | Description |
|---|---|
| FLTKCY | Switch to indicate skin and ball valves not available |
| FLTKCS | Switch to track skin and ball valves are available to open |
| FLTKCN | RHBFST cannot be isolated from nozzle leaks |
| FLTKC9 | DEFAULT |

#### 7.4.4.7 Top Event FLTKO – Successful Opening of the Fuel Line from a RHBFST that Is to Be Emptied

The FLTKO top event models the number of sectional valves that are to be opened in order to empty a RHBFST. Please see Figure C-49, FLTKO Fault Tree Diagram, for more details.

#### 7.4.4.8 Top Event EVAC – Sequence Conditions Necessitate Initial Evacuation from Red Hill

The EVAC top event is a simple switch to identify if the facility is to be evacuated or not. The following table lists the possible values for the switch.

**Table 7-18. EVAC Switch Value**

| State Name | Description |
|---|---|
| EVACU | Evacuation required and assumed |
| REMAIN | Staff remain in Red Hill tunnels |

### 7.4.5 The Top Events for the Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock

The top events of the Frontline Event Tree 1 – TKLEAK; Direct Leaks to Rock event tree are defined below:

| | |
|---|---|
| OUFM | CR operators detect low RHBFST alarm and direct top gauger to confirm leak. |
| ORGA1 | Top gauger checks and confirms RHBFST that has a low level alarm. |
| OSUP | Management and Red Hill Supervisor formulate a strategy to empty RHBFST. |
| OXFR | Control room and Red Hill staff follow the strategy and move fuel from the leaking RHBFST. |
| XFR1 | Inter-tank transfer by gravity to move fuel from leaking RHBFST. |
| XFR2 | Issue fuel by gravity to tanks at the upper tank farm located at Pearl Harbor. |
| XFR3 | Two-step fuel movement to pump fuel to other RHBFSTs. |
| XFR4 | Gravity feed to ships or other tanks at Pearl Harbor. |
| XFR5 | Fuel movement to empty bottom 7.5’ of lower dome using RHBFST lower drain line. |
| DELAY | Tank empty delay time based on earlier failures. |
| REL | Type of fuel release scenario. |

#### 7.4.5.1 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak

The OUFM top event models the detection of an alarm given potential leak events. Please see Figure C-50, OUFM Fault Tree Diagram, for more details.

#### 7.4.5.2 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm

The ORGA1 top event models the checking and confirmation of a low level alarm given potential leak events. Please see Figure C-51, ORGA1 Fault Tree Diagram, for more details.

#### 7.4.5.3 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST

The OSUP top event models the success or failure of strategy to empty RHBFST given potential leak events. Please see Figure C-52, OSUP Fault Tree Diagram, for more details.

#### 7.4.5.4 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST

The OXFR top event models the success or failure of implementing the management strategy to empty RHBFST given potential leak events. Please see Figure C-53, OXFR Fault Tree Diagram, for more details.

#### 7.4.5.5 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST

The XFR1 top event models the availability of skin and ball valves required to perform an inter-tank gravity transfer to move fuel from a leaking RHBFST. Please see Figure C-54, XFR1 Fault Tree Diagram, for more details.

#### 7.4.5.6 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor

The XFR2 top event models the availability of skin and ball valves required to perform a gravity transfer to move fuel from a leaking RHBFST to the tank farm at Pearl Harbor. Please see Figure C-55, XFR2 Fault Tree Diagram, for more details.

#### 7.4.5.7 Top Event XFR3 – Two-step Fuel Movement to Pump Fuel to Other RHBFSTs

The XFR3 top event models the availability of skin, ball valves and pumps required to perform a two-step fuel movement to pump fuel from a leaking RHBFST to another RHBFST. Please see Figure C-56, XFR3 Fault Tree Diagram, for more details.

### 7.4.5.8 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor

The XFR4 top event models the availability of skin and ball valves required to gravity feed fuel from a leaking RHBFST to ships or other tanks at Pearl Harbor. Please see Figure C-57, XFR4 Fault Tree Diagram, for more details.

### 7.4.5.9 Top Event XFR5 – Fuel Movement to Empty Bottom 7.5′ of Lower Dome Using RHBFST Lower Drain Line

The XFR5 top event models the availability of hardware required for draining the bottom 7.5' of lower dome using RHBFST lower drain. Please see Figure C-58, XFR5 Fault Tree Diagram, for more details.

### 7.4.5.10 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures

The DELAY top event is a simple switch to identify delay in response time. The following table lists the possible values for the switch.

**Table 7-19. DELAY Switch Value**

| State Name | Description |
|---|---|
| NONE | No Delay |
| HR4 | 4 Hours |
| HR8 | 8 Hours |
| HR12 | 12 Hours |
| HR24 | 24 Hours |
| HR72 | 72 Hours |
| HR336 | 2 Weeks |

### 7.4.5.11 Top Event REL – Type of Fuel Release Scenario

The REL top event is a switch to identify type of fuel release scenario. The following table lists the possible values for the switch.

**Table 7-20. REL Switch Value**

| SF Name | Description |
|---|---|
| RE0 | No release. |
| RELA | Release directly to rock from a RHBFST. |
| RELB | Limited release to Zone 7 with RHBFST Idle; limited transfer to tank gallery; new oil door closes. |
| RELC | Large accumulation in Zone 7 with RHBFSTs not Idle or nozzle leak; release through ADIT 6; new oil door closes. |
| RELD | Accumulation in Zone 7; RHBFST not idle or nozzle leak; and new oil door closes. No release through ADIT 6. |
| RELE | Accumulation in tank gallery Sections D or E with RHBFST not idle or nozzle leak; LAT fills; new oil door closes. |
| RELF | Limited release to tank gallery Sections D or E with RHBFST idle or successfully isolated from leak; new oil door closes. |
| RELG | Limited release from Section C fuel line below new oil door; RHBFSTs idle; collects at ADIT 2 and UGPH entry. |
| RELH | Large accumulation from Section C below new oil door with RHBFSTs not idle; collects at UGPH until entry doors fail; large release via ADIT 1. |
| RELI | Limited release from fuel line Sections A or B leak below new oil door; RHBFSTs idle; collects at UGPH entry and ADIT 2 with no door overpressure failures. |
| RELJ | Large release from Section A or B fuel lines below new oil door; RHBFSTs not idle; accumulation at UGPH fails doors; large release through ADIT 1. |
| RELK | Accumulation in Zone 7 with RHBFSTs not idle or nozzle leak; large release through ADIT 6; new oil door fails to close; eventual overpressure of UGPH doors. |
| RELL | Accumulation in Zone 7; RHBFST not idle nor nozzle leak; no release through ADIT 6; new oil door fails to close; eventual overpressure of UGPH doors. |
| RELM | Large release to tank gallery Sections D or E with RHBFST not idle or nozzle leak; new oil door fails to close; eventual overpressure of UGPH doors. |
| RELN | Release from fuel line only to tank gallery Sections D or E with RHBFST idle; new oil door fails to close; collects at UGPH entry doors which remain intact. |

### 7.4.6 The Top Events for the Frontline Event Tree 2 – OVERFILL Event Tree

The top events of the Frontline Event Tree 2 – OVERFILL event tree are defined below:

**Table 7-21. Top Events Referenced by Frontline Event Tree 2 – OVERFIL Event Tree**

| | |
|---|---|
| OEV | Operators correctly specify fill evolution and stop evolution when planned at maximum operating level. |
| HOLE | Conditional probability of hole above maximum operating level. |
| OTRIP | After AFHE high level alarm, operators actuate an emergency stop of the cargo pumps or press the panic button, then direct the rover to locally ensure the skin valve closed and to manually gauge the same tank. |
| SWITCH | High level mechanical FLOAT switch actuates sending signals to deactivate all facility pumps, actuate timer for valve closures, and signals skin valve on affected tank to close. |
| OUFM | CR operators detect low RHBFST alarm and direct top gauger to confirm leak. |
| ORGA1 | Top gauger checks and confirms RHBFST that has a low level alarm. |
| OSUP | Management and Red Hill supervisor formulate strategy to empty RHBFST. |
| OXFR | Control room and Red Hill staff follow strategy and move fuel from the leaking RHBFST. |
| XFR1 | Inter-tank transfer by gravity to move fuel from leaking RHBFST. |
| XFR2 | Issue fuel by gravity to tanks at the upper tank farm located at Pearl Harbor. |
| XFR3 | Two-step fuel movement to pump fuel to other RHBFSTs. |
| XFR4 | Gravity feed to ships or other tanks at Pearl Harbor. |
| XFR5 | Fuel movement to empty lower dome using RHBFST lower drain line. |
| DELAY | Tank empty delay time based on earlier failures. |
| REL | Type of fuel release scenario. |

#### *7.4.6.1 Top Event OEV – Operators Correctly Specify Fill Evolution and Stop Evolution when Planned at Maximum Operating Level*

The OEV top event models the failure of the operator to correctly specify evolution and stop evolution when planned. Please see Figure C-59, OEV Fault Tree Diagram, for more details.

#### *7.4.6.2 Top Event HOLE – Conditional Probability of Hole above Maximum Operating Level*

The HOLE top event models the probability of a hole above the maximum operating fuel level. The derivation of the conditional probability of a hole above the maximum operating level is discussed in detail in Section 5.4.3.6. Please see Figure C-60, HOLE Fault Tree Diagram, for more details.

#### 7.4.6.3 Top Event OTRIP – After AFHE High Level Alarm, Operators Actuate an Emergency Stop of the Cargo Pumps or Press the Panic Button, then Direct the Rover to Locally Ensure the Skin Valve Closed and to Manually Gauge the Same Tank

The OTRIP top event models the failure of the operator to stop overfill after receiving the high level alarm. Please see Figure C-61, OTRIP Fault Tree Diagram, for more details.

#### 7.4.6.4 Top Event SWITCH – High Level Mechanical FLOAT Switch Actuates Sending Signals to Deactivate All Facility Pumps, Actuate Timer for Valve Closures, and Signals Skin Valve on Affected Tank to Close

The SWITCH top event is a simple switch to identify sending the high level mechanical float switch signal to deactivate all facility pumps, actuate timer for valve closures, and signals skin valve on affected tank to close. The following table lists the possible values for the switch.

**Table 7-22. SWITCH Switch Value**

| State Name | Description |
|---|---|
| SWITCH1 | MECHANICAL FLOAT SWITCH OPERATES ON HIGH LEVEL |
| SWITCHF | SUPPORT TO MECHANICAL FLOAT SWITCH FAILS |
| SWITCHS | SUCCESSFUL END OF OVERFILL FLOW GUARANTEED |

#### 7.4.6.5 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak

Please see the earlier description of the OUFM top event in Section 7.4.5.1.

#### 7.4.6.6 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm

Please see the earlier description of the ORGA1 top event in Section 7.4.5.2.

#### 7.4.6.7 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST

Please see the earlier description of the OSUP top event in Section 7.4.5.3.

#### 7.4.6.8 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST

Please see the earlier description of the OXFR top event in Section 7.4.5.3.

#### 7.4.6.9 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST

Please see the earlier description of the XFR1 top event in Section7.4.5.5.

#### 7.4.6.10 Top Event XFR2 – Issue Fuel by gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor

Please see the earlier description of the XFR2 top event in Section 7.4.5.6.

#### 7.4.6.11 Top Event XFR3 – Two-step Fuel Movement to Pump Fuel to Other RHBFSTs

Please see the earlier description of the XFR3 top event in Section 7.4.5.7.

#### 7.4.6.12 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor

Please see the earlier description of the XFR4 top event in Section 7.4.5.8.

#### 7.4.6.13 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line

Please see the earlier description of the XFR5 top event in Section 7.4.5.9.

#### 7.4.6.14 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures

Please see the earlier description of the DELAY top event in Section 7.4.5.10.

#### 7.4.6.15 Top Event REL – Type of Fuel Release Scenario

Please see the earlier description of the REL top event in Section 7.4.5.11.

### 7.4.7 The Top Events for the Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT

The top events of the Frontline Event Tree 3 – NOZZLE; Unisolable Leaks from a RHBFST to the LAT event tree are defined below:

**Table 7-23. Top Events Referenced by Frontline Event Tree 3 – NOZZLE Event Tree**

| | |
|---|---|
| MSUMP | 1 of 2 main sump pumps below tank gallery start and transfer leaked fuel from LAT to S311. |
| DOOR | Oil tight door below LAT gallery closes on high float level. |
| OUFM | CR operators detect low RHBFST alarm and direct top gauger to confirm leak. |
| OSUM | CR or RH rover (from gauger station) recognizes sump pump start and identifies the leak. |
| OPAN | CR operators actuate cargo pump trip and valve closures using panic button. |
| ORGA1 | Top gauger checks and confirms RHBFST that has a low level alarm. |
| OSUP | Management and Red Hill supervisor formulate strategy to empty RHBFST. |
| OXFR | Control room and Red Hill staff follow strategy and move fuel from the leaking RHBFST. |
| XFR1 | Inter-tank transfer by gravity to move fuel from leaking RHBFST. |
| XFR2 | Issue fuel by gravity to tanks at the upper tank farm located at Pearl Harbor. |
| XFR3 | Two-step fuel movement to pump fuel to other RHBFSTs. |
| XFR4 | Gravity feed to ships or other tanks at Pearl Harbor. |
| XFR5 | Fuel movement to empty lower dome using RHBFST lower drain line. |
| DELAY | Tank empty delay time based on earlier failures. |
| REL | Type of fuel release scenario. |

#### *7.4.7.1 Top Event MSUMP – 1 of 2 Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311*

The MSUMP top event models the failure of the main sump pumps, strainer and float actuation switch. Please see Figure C-62, MSUMP Fault Tree Diagram, for more details.

Given the functional redundancy of the main Sump Pumps 1 and 2, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode FTR and FTS.

The following figures shows the details of four common cause groups modeled to represent the dependent failures of sump pumps.

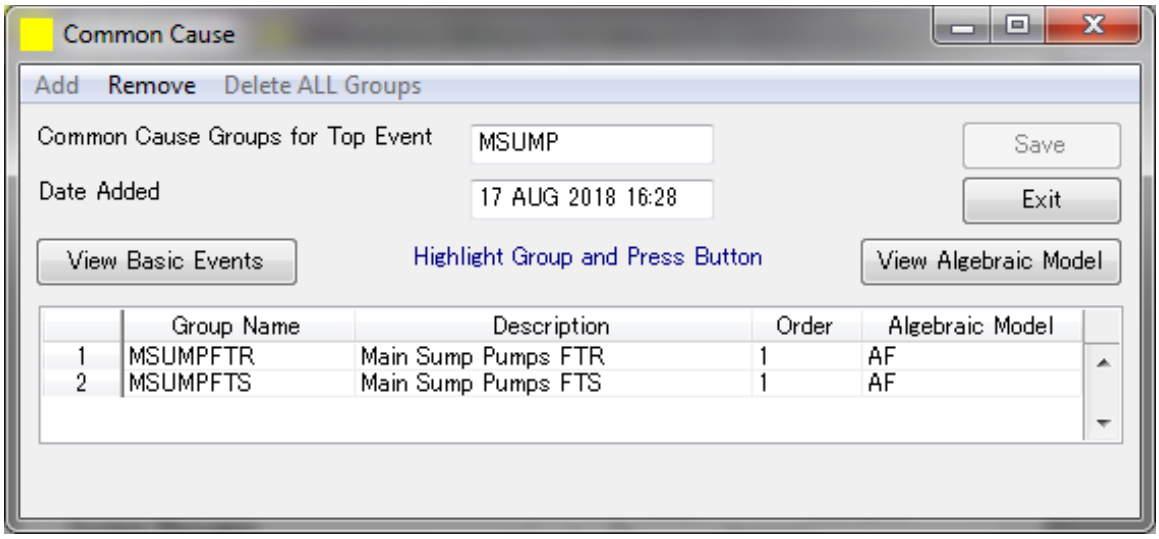



**Figure 7-39. MSUMP Common Cause Groups**

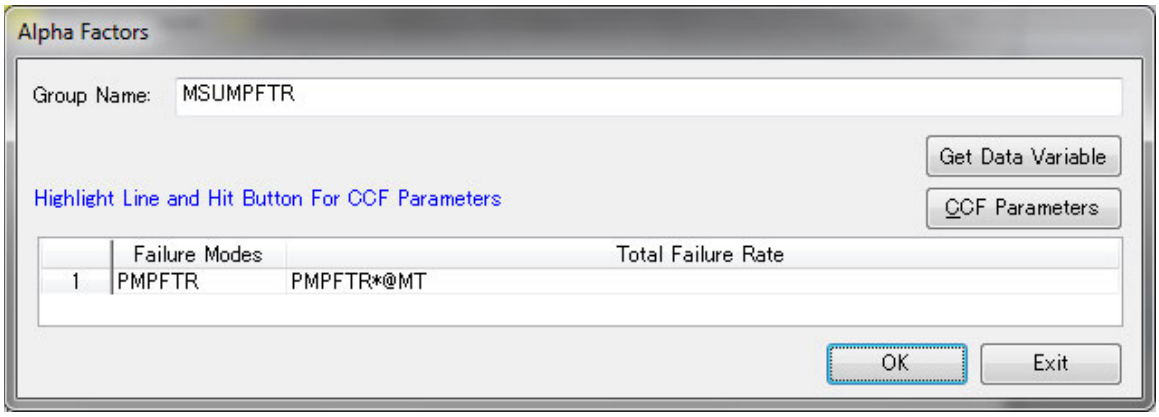



**Figure 7-40. MSUMP Common Cause Fail to Run Failure Mode and Failure Rate Equation**

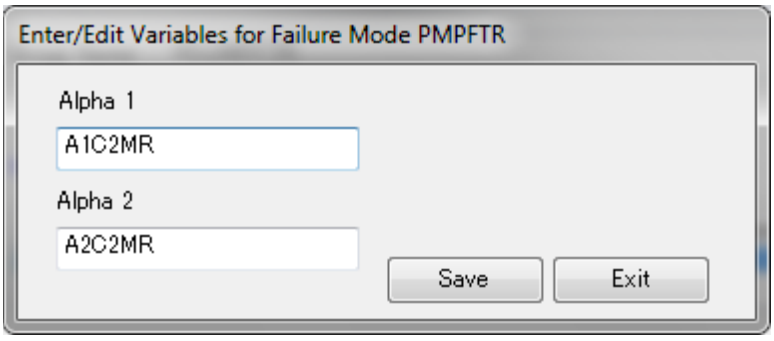



**Figure 7-41. MSUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

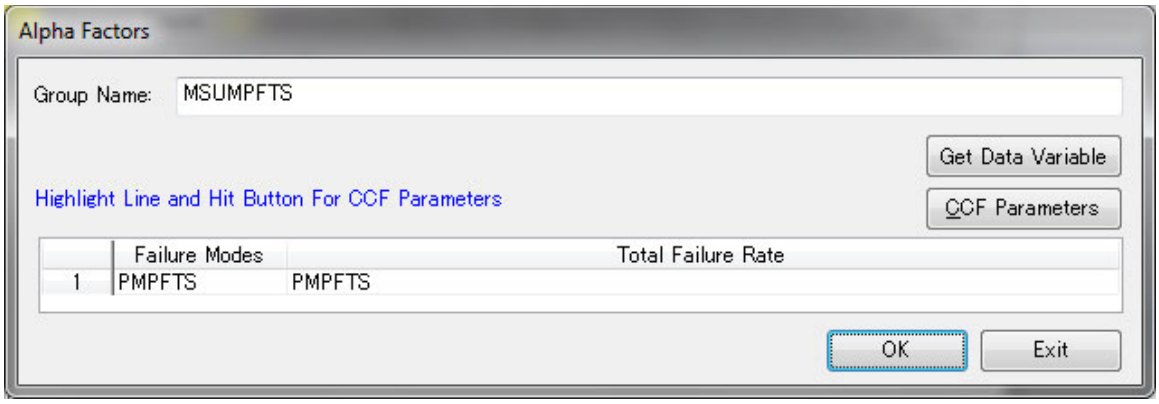



**Figure 7-42. MSUMP Common Cause Fail to Start Failure Mode and Failure Rate Equation**

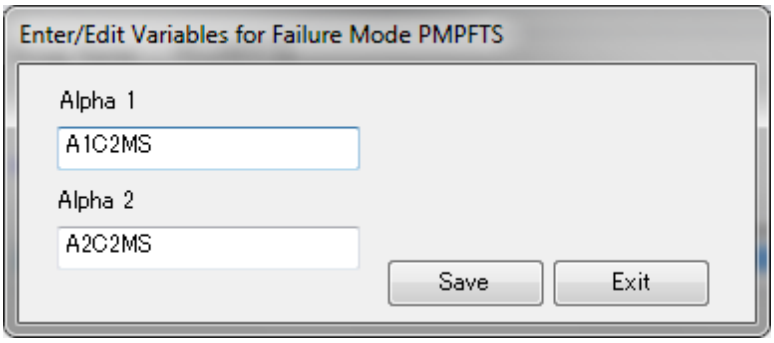



**Figure 7-43. MSUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

### *7.4.7.2 Top Event DOOR – Oil-Tight Door below LAT Gallery Closes on High Float Level*

The DOOR top event models the failure of the oil-tight door below LAT gallery to close. Please see Figure C-63, DOOR Fault Tree Diagram, for more details.

### *7.4.7.3 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak*

Please see the earlier description of the OUFM top event in Section 7.4.5.1.

### *7.4.7.4 Top Event OSUM – CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak*

The OSUM top event models the probability of the control room and Red Hill staff identifying leaks to the tunnel and its location. Please see Figure C-64, OSUM Fault Tree Diagram, for more details.

#### 7.4.7.5 Top Event OPAN – CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button

The OPAN top event models the probability of the operators to activate cargo pump trip and valve closures using the panic button. Please see Figure C-65, OPAN Fault Tree Diagram, for more details.

#### 7.4.7.6 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFSTs that Have a Low Level Alarm

Please see the earlier description of the ORGA1 top event in Section 7.4.5.2.

#### 7.4.7.7 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to empty RHBFST

Please see the earlier description of the OSUP top event in Section 7.4.5.3.

#### 7.4.7.8 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST

Please see the earlier description of the OXFR top event in Section 7.4.5.4.

#### 7.4.7.9 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST

Please see the earlier description of the XFR1 top event in Section 7.4.5.5.

#### 7.4.7.10 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor

Please see the earlier description of the XFR2 top event in Section 7.4.5.6.

#### 7.4.7.11 Top Event XFR3 – Two-Step Fuel Movement to Pump Fuel to other RHBFSTs

Please see the earlier description of the XFR3 top event in Section 7.4.5.7.

#### 7.4.7.12 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor

Please see the earlier description of the XFR4 top event in Section 7.4.5.8.

#### 7.4.7.13 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line

Please see the earlier description of the XFR5 top event in Section 7.4.5.9.

#### *7.4.7.14 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures*

Please see the earlier description of the DELAY top event in Section 7.4.5.10.

#### *7.4.7.15 Top Event REL - Type of Fuel Release Scenario*

Please see the earlier description of the REL top event in Section 7.4.5.11.

### 7.4.8 The Top Events for the Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel

The top events of the Frontline Event Tree 4 – TUNLEAK; Isolable Leaks from Fuel Lines to the LAT or Harbor Tunnel event tree are defined below:

**Table 7-24. Top Events Referenced by Frontline Event Tree 4 – TUNLEAK Event Tree**

| | |
|---|---|
| USUMP | 1 of 2 Harbor Tunnel sump pumps at UGPH entry start and transfer leaked fuel. |
| MSUMP | 1 of 2 main sump pumps below tank gallery start and transfer leaked fuel from LAT to S311. |
| DOOR | Oil tight door below LAT gallery closes on high float level. |
| PFL | Fuel line pressure drops due to leak and is detected. |
| OSUM | CR or RH rover (from gauger station) recognizes sump pump start and identifies the leak. |
| OPAN | CR operators actuate cargo pump trip and valve closures using panic button. |
| OSEC | CR operators REMOTE MANUALLY close sectional valve(s) and ball valves as applicable; execution only. |
| OUFM | CR operators detect low RHBFST alarm and direct top gauger to confirm leak. |
| ORGA1 | Top gauger checks and confirms RHBFST that has a low level alarm. |
| OSUP | Management and Red Hill supervisor formulate strategy to empty RHBFST. |
| OXFR | Control room and Red Hill staff follow strategy and move fuel from the leaking RHBFST. |
| ISOL | FL leak isolated from all RHBFSTs; by upgrade sectional, RHBFST idle or isolated - no need to empty. |
| XFR1 | Inter-tank transfer by gravity to move fuel from leaking RHBFST. |
| XFR2 | Issue fuel by gravity to tanks at the upper tank farm located at Pearl Harbor. |
| XFR3 | Two-step fuel movement to pump fuel to other RHBFSTs. |
| XFR4 | Gravity feed to ships or other tanks at Pearl Harbor. |
| XFR5 | Fuel movement to empty lower dome using RHBFST lower drain line. |
| DELAY | Tank empty delay time based on earlier failures. |
| REL | Type of fuel release scenario. |

### 7.4.8.1 Top Event USUMP – 1 of 2 Harbor Tunnel Sump Pumps at UGPH Entry Start and Transfer Leaked Fuel

The USUMP top event models the failure of the Harbor Tunnel sump pumps at UGPH, strainer and float actuation switch. Please see Figure C-66, USUMP Fault Tree Diagram, for more details.

Given the functional redundancy of the UGPH Sump Pumps 1 and 2, a first order Alpha Factor common cause group was created to account for the dependent failures for each failure mode, FTR and FTS.

The following figures show the details of four common cause groups modeled to represent the dependent failures of sump pumps.

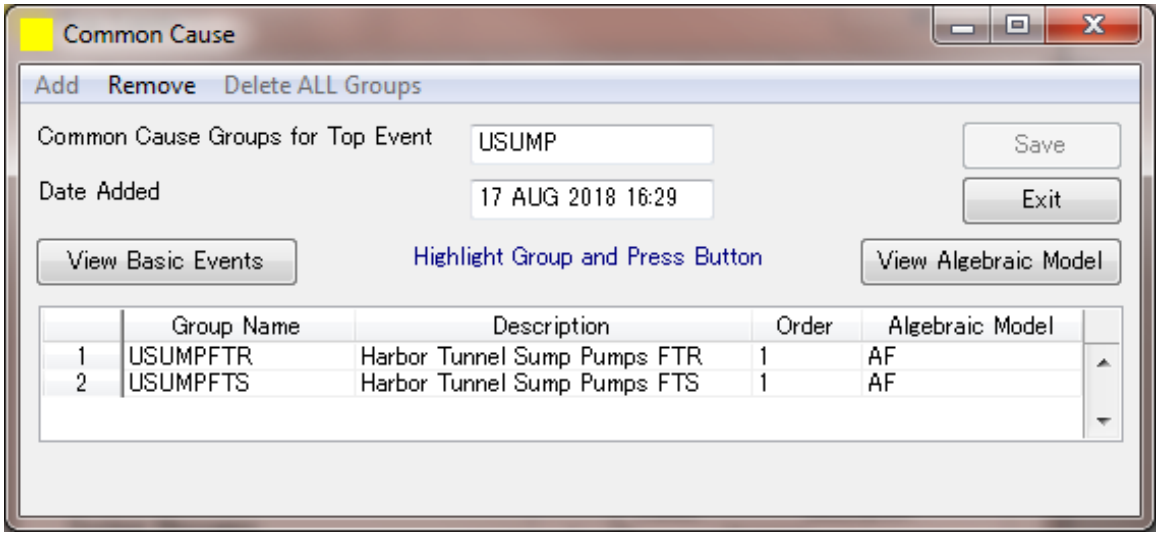



**Figure 7-44. USUMP Common Cause Groups**

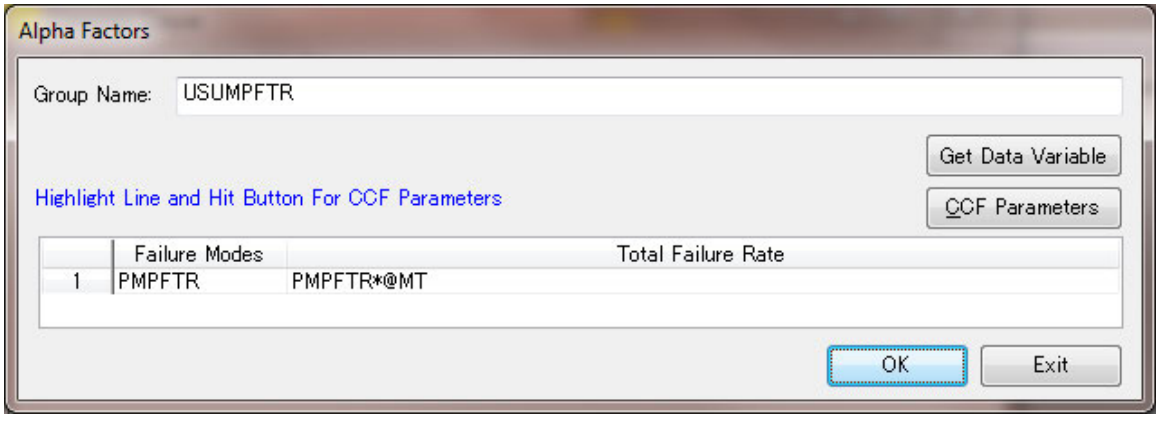



**Figure 7-45. USUMP Common Cause Fail to Run Failure Mode and Failure Rate Equation**

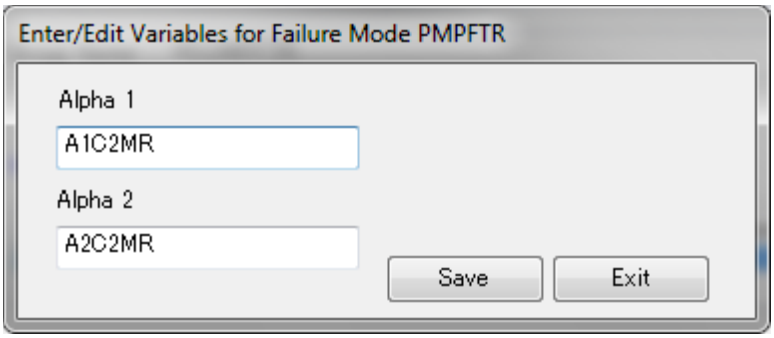



**Figure 7-46. USUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Run Failure Mode**

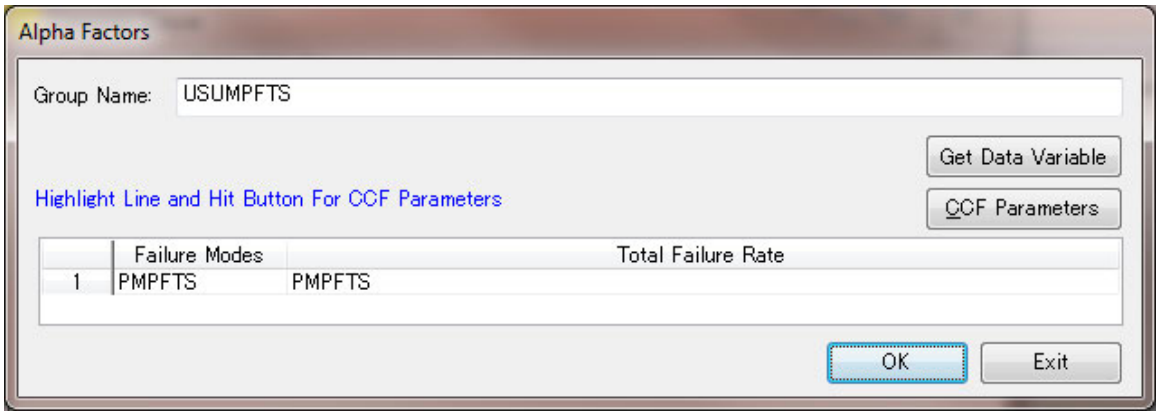



**Figure 7-47. USUMP Common Cause Fail to Start Failure Mode and Failure Rate Equation**

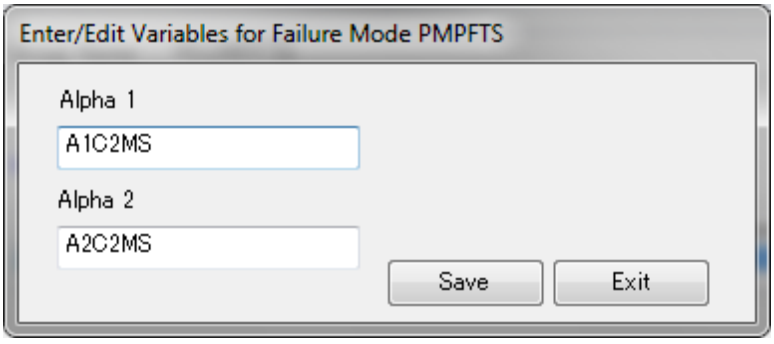



**Figure 7-48. USUMP 1st Order Alpha Factor Common Cause Parameters for Fan Fail to Start Failure Mode**

### *7.4.8.2 Top Event MSUMP – 1 of 2 Main Sump Pumps below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311*

Please see the earlier description of the MSUMP top event in Section 7.4.7.1.

### 7.4.8.3 Top Event DOOR – Oil-Tight Door below LAT Gallery Closes on High Float Level Top Event

Please see the earlier description of the DOOR top event in Section 7.4.7.2.

### 7.4.8.4 Top Event PFL – Fuel Line Pressure Drops due to Leak and Is Detected

The PFL top event models the probability of fuel line pressure dropping to a noticeable level and it is indicated during a leak to the tunnel. Please see Figure C-67, PFL Fault Tree Diagram, for more details.

### 7.4.8.5 Top Event OSUM – CR or RH Rover (from gauger station) Recognizes Sump Pump Start and Identifies the Leak

Please see the earlier description of the OSUM top event in Section 7.4.7.4.

### 7.4.8.6 Top Event OPAN – CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button

Please see the earlier description of the OPAN top event in Section 7.4.7.5.

### 7.4.8.7 Top Event OSEC – CR Operators REMOTE MANUALLY Close Sectional Valve(s) and Ball Valves as Applicable; Execution Only

The OSEC top event models the probability of failure to close sectional valves remotely or manually during fuel movement or idle phases while a hole/leak has been detected by the control room or the RH rover. Please see Figure C-68, OSEC Fault Tree Diagram, for more details.

### 7.4.8.8 Top Event OUFM – CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to Confirm Leak

Please see the earlier description of the OUFM top event in Section 7.4.5.1.

### 7.4.8.9 Top Event ORGA1 – Top Gauger Checks and Confirms RHBFST that Has a Low Level Alarm

Please see the earlier description of the ORGA1 top event in Section 7.4.5.2.

### 7.4.8.10 Top Event OSUP – Management and Red Hill Supervisor Formulate Strategy to Empty RHBFST

Please see the earlier description of the OSUP top event in Section 7.4.5.3.

### 7.4.8.11 Top Event OXFR – Control Room and Red Hill Staff Follow Strategy and Move Fuel from the Leaking RHBFST

Please see the earlier description of the OXFR top event in Section 7.4.5.4.

### 7.4.8.12 Top Event ISOL – FL Leak Isolated from All RHBFSTs; by Upgrade Sectional, RHBFST Idle or Isolated – No Need to Empty

The ISOL top event is a simple switch to identify the status of successful isolation of the fuel line leak from all RHBFST by using the upgrade sectional valve. The following table lists the possible values for the switch.

**Table 7-25. FLTKC Switch Value**

| SF Name | Description |
|---|---|
| ISOLY | FL leak isolated by sectional, tank idle, or skin or ball valves closed - switch |
| ISOLN | FL leak not isolated by sectional, tank idle, or skin or ball valves being closed - switch |
| ISOLS | Sequence not on this path |

### 7.4.8.13 Top Event XFR1 – Inter-Tank Transfer by Gravity to Move Fuel from Leaking RHBFST

Please see the earlier description of the XFR1 top event in Section 7.4.5.5.

### 7.4.8.14 Top Event XFR2 – Issue Fuel by Gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor

Please see the earlier description of the XFR2 top event in Section 7.4.5.6.

### 7.4.8.15 Top Event XFR3 – Two-Step Fuel Movement to Pump Fuel to other RHBFSTs

Please see the earlier description of the XFR3 top event in Section 7.4.5.7.

### 7.4.8.16 Top Event XFR4 – Gravity Feed to Ships or Other Tanks at Pearl Harbor

Please see the earlier description of the XFR4 top event in Section 7.4.5.8.

### 7.4.8.17 Top Event XFR5 – Fuel Movement to Empty Lower Dome Using RHBFST Lower Drain Line

Please see the earlier description of the XFR5 top event in Section 7.4.5.9.

### 7.4.8.18 Top Event DELAY – Tank Empty Delay Time Based on Earlier Failures

Please see the earlier description of the DELAY top event in Section 7.4.5.10.

### *7.4.8.19 Top Event REL – Type of Fuel Release Scenario*

Please see the earlier description of the REL top event in Section 7.4.5.11.

## 7.5 Section 7 References

7-1 Fault Tree Handbook, NUREG-0492, 1981.

7-2 Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, 1980.

# 8. Human Reliability Analysis

## 8.1 Introduction

Human reliability analysis performed in the context of QRVA is effectively a special focused area of data analysis designed to characterize and evaluate HFEs required to accurately complete the event sequence analysis and system analysis. For example, some of the event tree top events in the QRVA may be dedicated to addressing questions about the success or failure of expected or anticipated human actions that are prescribed by facility normal and emergency operating procedures. Similarly, systems analysts may identify human actions required for accurate Boolean logic model development or FTA in the systems analysis. HRA is primarily focused on evaluating these human actions and the associated HFEs to develop representative HEP values for incorporation into the QRVA.

## 8.2 QRVA Human Reliability Analysis General Methodology

Human reliability analysis is a method by which human reliability is estimated. In carrying out an HRA, it is necessary to identify those human actions that can have an effect on system reliability or availability. The most common application of HRA is the evaluation of human acts required in a system context. The consideration of extraneous actions is also important. The person in a system may not only fail to do what he is supposed to do, or fail to do it correctly, but he may also do something extraneous that could degrade the system. The latter is the weak link in HRA. It is not possible to anticipate all undesirable extraneous human actions. The best anyone can do is to identify those actions having the greatest potential for degrading system reliability and availability. The assignment of probability estimates to extraneous actions is difficult and uncertain. Often the best one can do is to estimate very broad ranges of probabilities of human errors that one believes include the true probability. Fortunately, the probabilities of extraneous actions are usually very low.

A method commonly used in solving practical human reliability problems is known as THERP—Technique for Human Error Rate Prediction (see Reference 8-1). Other common HRA methods include those described in References 8-2 through 8-6.

### 8.2.1 Human Failure Event Definition and Evaluation

Human actions and their associated human failure events modeled in QRVAs are generally initially identified during the ESD development process through review of facility procedures. However, applying guidance provided in References 8-1 through 8-6, event sequence analysts, systems analysts, and human reliability analysts work

together as a team to refine the definition of HFEs to be evaluated in the QRVA. There are three general types of HFEs evaluated in QRVAs, as follows:

- Type A HFEs – those HFEs associated with human errors that occur prior to the occurrence of an initiating event, but which impact the availability of functions or actions that contribute to event sequence frequency evaluation. These are often referred to as "pre-initiator HFEs".

- Type B HFEs – those HFEs that create or directly participate in creating an initiating event in the QRVA. These are "initiator HFEs". These HFEs are often inherently included in the evaluation of initiating events to be included in the QRVA.

- Type C HFEs – those HFEs that occur after the occurrence of an initiating event, which contribute to event sequence frequency evaluation. These are "post-initiator HFEs". As described previously herein, there are two general types of post-initiator HFEs as follows:

    - Dynamic HFEs – failures of human actions that are anticipated to occur as part of the early facility response to the initiating event. These actions are often associated with emergency response procedure "immediate actions". These are actions that facility operators are anticipated to know well via their training and qualification program.

    - Recovery HFEs – failures of human actions associated with recovering lost or failed functions deemed necessary or desirable to respond to or mitigate the consequences of event scenarios. These are actions to repair or restore functionality that may have originally been expected to be available for event sequence response. Recovery HFEs generally occur later in time than do dynamic HFEs.

#### *8.2.1.1 Operations, Maintenance, Testing, and Emergency Procedures Review*

To identify, define, and evaluate HFEs for the QRVA, the HRA analysts must review facility operations, maintenance, testing, and emergency response procedures. Depending upon the nature of the facility being analyzed and how it is managed, the HRA analysts may also need to review facility administrative procedures. Review of facility maintenance and testing procedures is important in identifying and evaluating Type A HFEs whereas review of facility operations and emergency response procedures is important in identifying and evaluating Type C HFEs.

#### 8.2.1.2 Operator Interviews and Scenario Walk-Throughs

Determination of human error probability values for specific HFEs involves a detailed evaluation of human action performance shaping factors (PSF) directly associated with modeled event sequences in accordance with guidance provided in HRA references, such as References 8-1 through 8-6. To rigorously evaluate these PSFs, it is critical the HRA analysts conduct interviews with facility operating shift crews. During these interviews, the HRA analysts describe the scenarios associated with identified HFEs, then perform talk-throughs and walk-throughs of these scenarios with the facility operating crews. Experience has shown that application of operator interview questionnaires or checklists is critical for successful HFE HEP evaluation. An example of a generic questionnaire for Type A pre-initiator HFEs is shown in Figure 8-1.

Similarly, an example of a generic questionnaire for Type C post-initiator HFEs is shown in Figure 8-2.

| Facility QRVA HRA Pre-Initiator HFE Operator Interview Questionnaire |
|---|
| **Date:** **Interviewer(s):** |
| **Human Action Designator:** |
| Description of Action: |
| 1. What Human Actions are related to this maintenance/calibration task? |
| |
| 2. How often is this task performed? |
| |
| 3. How often is this item tested? |
| |
| 4. What procedures are available for completing this task? |
| |
| 5. What are the steps involved in this procedure? |
| |
| 6. Are the steps written or oral? Are they general/narrative or detailed/step-by-step? |
| |
| 7. What is the stress level for each step of the procedure (low, moderate, high)? |
| |
| 8. Possible errors…<br>Display – similar to others? digital or analog?<br>Controls – similar to others? two position or multi position controller? breaker?<br>Valves – similar to others? position indication?<br>Recovery of checker errors – written materials? position indication? checkers? |
| |
| 9. Is the equipment configuration good or poor? |
| |
| 10. Is the I&C layout good or poor? |
| |
| 11. Is the quality of the written procedures good or poor? |
| |
| 12. Is the quality of administrative control good or poor? |
| |

**Figure 8-1. Type A Pre-Initiator HFE Questionnaire**

| Facility QRVA HRA Pre-Initiator HFE Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Human Action Designator:** | |
| Description of Action: | |
| 13. What checks are performed after completing the task to verify that it has been left in its intended state? | |
| | |
| 14. Can you identify any other pre-initiator human actions that might have an impact on the operators/technicians' ability to perform this action properly. If so, what are they (please list them)? | |
| | |
| 15. For each, how would you describe the level of interdependence: complete, high, moderate, low, zero (or no dependence)? | |
| | |

**Figure 8-1. Type A Pre-Initiator HFE Questionnaire (Continued)**

| Facility QRVA HRA Post-Initiator Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Interviewee(s):** | |
| **Human Action Designator:** | |
| Description of Action: | |
| 1. **What procedure(s) are used** to address this situation? | |
| | |
| 2. Do the operators receive training on this type of scenario? If so, **what type of training** (classroom, simulator, other)? If training is received, **how often** is it conducted? What is your experience specifically to this evolution or set of initial conditions? | |
| | |
| 3. What **cues and indications** are available for this condition in the facility? Where can they be observed by operators? | |
| | |
| 4. **How much time is needed** for the operator to see the cue and then diagnose the cue? | |
| | |
| 5. What is the degree of **clarity of the cues and indications** (very good, average, poor)? | |
| | |
| 6. Please generally **describe how you would anticipate this scenario playing out over time.** | |
| | |
| 7. Type of Response: (**Skill, Rule or Knowledge-based?**) | |
| | |
| 8. **Confirm** that failure to conduct the modeled step would lead to **failure of the top event.** | |
| | |
| 9. Is there a "point of no return" after which this action would be ineffective or have a negative impact on facility safety (e.g., is there a point of irreversible damage)? **How much time do you perceive having to perform this action before this point of no return** (low, best estimate, high)? What's the basis for this perception or knowledge? | |
| | |

**Figure 8-2. Type C Post-Initiator HFE Questionnaire**

| Facility QRVA HRA Post-Initiator Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Interviewee(s):** | |
| **Human Action Designator:** | |
| Description of Action: | |
| 10. After deciding to perform this action, **how much time** (low, best estimate, high) **would it take the crew to perform all parts of the action** (i.e., what is the actual required manipulation or execution time)? Note that this is different from the "point of no return" time. | |
| Low – [X] seconds/minutes/hours<br>Best estimate – [X] seconds/minutes/hours<br>High – [X] seconds/minutes/hours | |
| 11. **What facility equipment** and/or man-machine interfaces **are required to perform this action? Where are they located in the facility?** [Execution Performance Shaping Factors (PSFs) – Equipment Accessibility – Location(s)?] | |
| | |
| 12. How would you describe the **complexity of diagnosing the need for this action** (complex, simple)? | |
| | |
| 13. How would you describe the **complexity of performing this action** after it is diagnosed (complex, simple)? | |
| | |
| 14. Are the **cues/indications** required for diagnosing this action all located **in the control room?** Are the indications required for diagnosis available on the **front panels of the main control room**, or does the operator have to leave the main control area to read these indications? | |
| | |
| 15. Are the **indications** available **accurate** (consider facility local sensing environment)? | |
| | |
| 16. Has the crew received **training** in interpreting or obtaining the required information under conditions similar to those prevailing in **this scenario**? | |
| | |
| 17. Recovery – Which, if any, of the following recovery factors apply: **Self Review, Extra Crew, STA Review, Shift Change, ERF Review**? | |
| | |

**Figure 8-2. Type C Post-Initiator HFE Questionnaire (Continued)**

| Facility QRVA HRA Post-Initiator Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Interviewee(s):** | |
| **Human Action Designator:** | |
| Description of Action: | |
| 18. Do the cues/indications for this human action occur at a time of **high workload** or distraction? | |
| | |
| 19. Does this action require a one-time **check** of a parameter **or** does it require **monitor**ing of a parameter until a specified level or value is reached or achieved? | |
| | |
| 20. Is the critical value of the parameter/indication signaled by an **annunciator** (alarm)? | |
| | |
| 21. Is the layout, demarcation, and labeling of the control boards such that it is **easy to locate** the required indicator(s)? | |
| | |
| 22. Does the required **indicator have human engineering deficiencies** that are conducive to errors in reading the display? | |
| | |
| 23. Are cue states or **parameter values as stated in the procedure**? The "no" response is to be applied if an indicator is not obviously failed but would not give the value stated in the procedure. | |
| | |
| 24. Is the relevant instruction a **separate, stand-alone, numbered step** or is it "hidden" in some way that makes it easy to overlook, e.g., one of several statements in a paragraph, in a note or caution, or on the back of a page? | |
| | |
| 25. At the time of this human action, is the procedure reader using more than one text procedure? | |
| | |

**Figure 8-2. Type C Post-Initiator HFE Questionnaire (Continued)**

| Facility QRVA HRA Post-Initiator Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Interviewee(s):** | |
| **Human Action Designator:** | |
| Description of Action: | |
| 26. Is the step governing this human action in some way **more conspicuous** than surrounding steps? For example, steps proceeded by note or cautions, and steps that are formatted to emphasize logic terms are more eye-catching than simple action steps, and are less likely to be overlooked simply because they look different than surrounding steps. However, this effect is diluted if there are several such steps in view at one time. | |
| | |
| 27. Does the step include **unfamiliar nomenclature** or an unusual grammatical construction? Does anything about the wording require explanation in order to arrive at the intended interpretation? Does the proper interpretation of the step require an inference about the future state of the facility? | |
| | |
| 28. Does the step present **all information** required to identify the actions directed and their objects? | |
| | |
| 29. Does the step **contain the word "not?**" | |
| | |
| 30. Does the procedure step present diagnostic logic in which more than one condition is combined to determine the outcome? (**AND or OR or BOTH**) | |
| | |
| 31. Has the crew **practiced** executing this step in a scenario similar to this one **in** a **simulator**? | |
| | |
| 32. Does the crew **believe** that the **instructions** presented are **appropriate** to the situation (even in spite of any potential adverse consequences)? Do they have confidence in the effectiveness of the procedure for dealing with the current situation? In practice, this may come down to: have they tried it in the simulator and found that it worked? | |
| | |

**Figure 8-2. Type C Post-Initiator HFE Questionnaire (Continued)**

| Facility QRVA HRA Post-Initiator Operator Interview Questionnaire | |
|---|---|
| **Date:** | **Interviewer(s):** |
| **Interviewee(s):** | |
| **Human Action Designator:** | |
| Description of Action: | |
| 33. Execution Performance Shaping Factors (PSFs) –<br>**Environment – Lighting** (Normal, Emergency Only, Portable Only)?<br>**Heat/Humidity** (Normal, Hot/Humid, Cold)?<br>**Atmosphere** (Normal, Steam, Smoke, Respirator Required)?<br>**Tools** (Required, Adequate, Available)? **Parts** (Required, Adequate, Available)? **Clothing** (Required, Adequate, Available)? **Complexity of Execution** (Simple, Complex)?<br>**Equipment Accessibility** (Easily Accessible, Accessible with Difficulty, Inaccessible)?<br>**Facility Response as Expected** (Yes/No)?<br>**Workload** (Low/High)?<br>**PSFs Overall** (Optimal/Negative)? | |
| (normal) | |
| 34. How would you characterize the **overall execution stress** (Low, Moderate, High)? | |
| | |
| 35. Are there **any "recovery" steps** in the procedure for the specific execution steps of interest? If so, please identify them by step number. | |
| | |
| 36. If there are any "recovery" steps in the procedure for the specific execution steps of interest, how would you characterize the **interdependence** of these recovery steps relative to the original execution steps (Complete, High, Moderate, Low, Zero)? | |
| | |
| 37. In the scenarios discussed relating to this human action, are there **other human actions that would likely be associated with this scenario?** If so, what are they (please list them)? For each, how would you describe the level of interdependence: complete, high, moderate, low, zero (or no dependence)? | |
| | |

**Figure 8-2. Type C Post-Initiator HFE Questionnaire (Continued)**

### 8.2.2 Human Error Probability Evaluation and Analysis

HFE HEP values can be evaluated and determined following guidance presented in References 8-1 through 8-6. However, experience has shown that HFE HEP evaluation is most effectively and efficiently implemented via the Systematic Human Action Reliability Procedure, Revision 1 (SHARP1). Such methods are designed, to the greatest degree feasible, to implement the guidance provided in HRA procedures, such as References 8-1 through 8-6, and to provide HFE HEP values in terms of probability distributions. HFE HEP best estimate values generally range from approximately 0.0001 to 1.00 in value, with most typical HFE HEPs ranging between 0.001 and 0.1. However, HFE HEP values are highly dependent upon the facility-specific characteristics, such as the level of operator training and experience and the quality of facility procedures.

### 8.2.3 Human Action Dependency Analysis

The determination of the level of dependence among post-initiating event human actions (Type C actions) occurring in the same accident sequence (or cut set) is not an exact science and remains somewhat subjective. The specific levels of dependence applied in QRVAs are supported via operator interviews, which form a critical part of any human action dependency analysis (HADA). Many factors may influence the level of dependence among intra-sequence human actions, such as timing, location, and the relationship among persons performing the actions. In current methods typically applied for HADA, such as the Technique for Human Error Rate Prediction (Reference 8-1) applied in the widely used SHARP1 methodology, timing is deemed the most important underlying factor. The guidance most often applied in QRVA HRA HADA is to establish a minimum level of dependence based on the timing and to adjust this level of dependence higher if additional dependency factors are identified. The level of dependence based on timing between successive intra-sequence (or intra-cut set) human actions is shown in Figure 8-3.

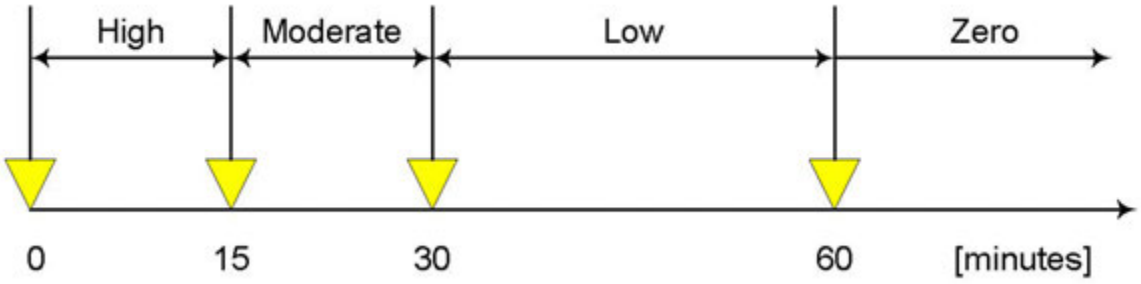



**Figure 8-3. Level of Dependence as a Function of Time**

The conditional probability of recovery step failure is quantified by determining the *level* of dependence as above and then applying the formulas from THERP (Reference 8-1) Table 20-17 that are reproduced below in Table 8-1. The formulas are functions only of the independent HEP of a recovery factor or a subsequent human action after the first action in a sequence (or cut set).

**Table 8-1. Conditional Probability Equations**

| Level of Dependence | Conditional Probability Equation (*N* = HEP) | Approximate Value for Small *N* |
|---|---|---|
| Zero Dependence (ZD) | $N$ | $N$ |
| Low Dependence (LD) | $\frac{1+19N}{20}$ | 0.05 |
| Medium Dependence (MD) | $\frac{1+6N}{7}$ | 0.14 |
| High Dependence (HD) | $\frac{1+N}{2}$ | 0.5 |
| Complete Dependence (CD) | 1.0 | 1.0 |

The steps of the HADA procedure applied via Reference 8-1 are as follows:

1. Generate a set of sequences by setting the HEPs for all post-initiator HFEs that were evaluated to be less than 0.5 to a high value (0.5) in the logic model:

    a. In the appropriate system top events, change the post-initiator operator action basic event equations to 0.5.

    b. Re-quantify the system top events affected by Step 1.a. to update the affected split fractions.

    c. Create a new point-estimate master frequency file with the updated split fraction values.

    d. Perform a Level 1 loss of fuel inventory control frequency (LOFICF) event tree quantification using the master frequency file created in Step 1.c, and a cutoff frequency of 1E-09. Ensure to select "save sequences."

    e. The saved sequence information is located in the RISKMAN.mdb database file (tables Sequence – Master Frequency File [MFF], Sequence Detail – MFF, Sequence Failed SFs – MFF).

2. Identify all combinations of two or more post-initiator HFEs in the sequences.

3. For each HFE combination, group the associated sequences.

4. Sort the HFEs in each combination in chronological order by the apparent time of the cue for each HFE.

5. Calculate the dependence importance (DI) for each combination. The DI is a risk achievement (RA) importance measure calculated by setting all the HEPs in a given combination, *except* the first HFE, equal to 1.0 in the group of sequences in which

the combination occurs. The DI for a combination is calculated as follows using the group of sequences in which the combination occurs:

a. For each HFE combination, calculate a sequence sum using the nominal HEP values = $sum_0$.

b. For each HFE combination, calculate a sequence sum by setting all HEPs = 1.0, *except* for the first HEP in the combination = $sum_1$.

c. Calculate the difference = $sum_1 - sum_0$ = DI. The DI is regarded as the potential increase in loss of fuel inventory control frequency if all the HFEs in the combination, except for the first HFE, are completely dependent. The DI is a refinement of the RA, and the DI is more relevant to HFE combinations than is RA.

6. Sort the HFE combinations by the DI in decreasing order. The purpose of this sorting is to rank the HFE combinations in order of highest potential impact on loss of fuel inventory control frequency should there be dependencies in the combination that are not accounted for.

7. Specify a DI cutoff below which the impact of potential complete dependencies would be negligible. For example, a DI of 1E-07/year for a combination represents less than 1% of a typical loss of fuel inventory control frequency in the order of 1E-05/yr.

8. The first HFE in a chronological combination is independent, unless it is not appropriate to credit for the specific initiating event, in which Case CD (complete dependence) is assigned.

9. Inspect each HFE combination to identify intervening successes. An HFE following a success is independent of the success and also independent of any HFEs preceding the success (this is a corollary to #10). For example, in a chronological combination $A\bar{B}C$, C is independent of A. This step can be labor intensive as the successes need to be inferred from the sequences (not necessarily the case for RISKMAN models) and an understanding of the procedural flow in the given scenario. As a first cut, this step can be omitted, which is conservative. For combinations of high DI, it may be justified to perform this step in a successive iteration.

10. The level of dependence between each two successive HFEs is to be determined. For example, for three chronological events, A, B, and C, the levels of dependence for B│A (B given A) and C│B (C given B) are to be determined. The level of dependence for C│A is not explicitly considered. This is based on the guidance in NUREG/CR-1278, Chapter 10, p. 10-14. The joint HEP for this combination will be P(A)*P(B│A)*P(C│B).

The criteria for applying Table 20-17 of NUREG/CR-1278 to assign the level of dependence between post-initiator HFEs are listed below and summarized in Figure 8-4.

1. If the time between the cues for the required actions exceeds the length of a shift (typically 12 hours), the actions are to be performed by different crew. In this case, the "No" branch on the "Same Crew" decision node in Figure 8-4 is selected. The different crew can be considered independent as the shift change will involve a complete re-evaluation of the facility status, so ZD can be assigned for low stress[§§] situations (Sequence Case 18 [S18] in Figure 8-4). For elevated stress, LD is assigned (S17). If the time between the cues is less than the length of a shift, the probability of a shift change during the time window needs to be considered. For a typical HFE time window of 1 hour and a shift length of 12 hours, the probability of no shift change is 1-1/12 = 0.92, so HFEs by different crew are typically only credited in scenarios where the HFE time window is longer than the length of a shift.

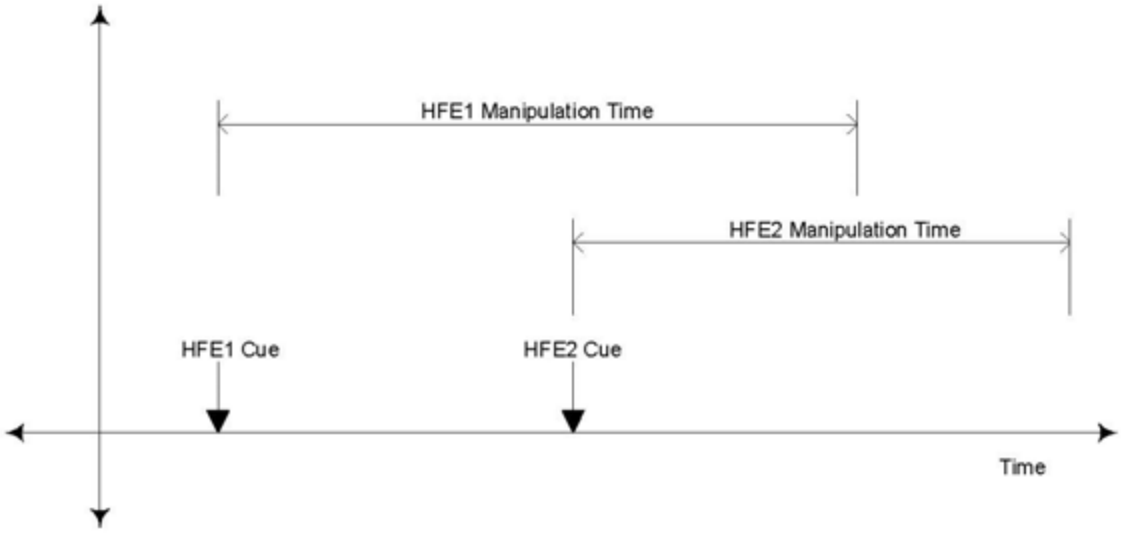
2. If the HFEs have a common cognitive element (i.e., performed by the same crew and driven by the same cue or procedural step), the "Yes" branch on the "Common Cognitive" decision node in Figure 8-4 is selected. These HFEs are regarded as completely dependent (S1).

3. For HFEs that do not share a common cognitive element, the "No" branch on the "Common Cognitive" decision node in Figure 8-4 is selected. For these HFEs, the timing is to be considered next.

4. If the cues for two HFEs occur at the same time, the "Yes" branch on the "Same Time" decision node in Figure 8-4 is selected. The required actions for these HFEs are to be performed simultaneously. If the cue for subsequent action occurs before the preceding action can be completed as illustrated below, the "Yes" branch on the "Same Time" decision node in Figure 8-4 is also selected, as the required actions would have to be performed either simultaneously or the crew may select to do either

*§§* Stress is a culmination of all other performance shaping factors. These may include preceding functional failures and successes, preceding operator errors or successes, availability of cues and appropriate procedures, workload, environment (heat, humidity, lighting, and atmosphere), requirement and availability of tools or parts, accessibility of locations. In general, stress is considered high for loss of support system scenarios or when the operators need to progress to functional restoration or emergency contingency action procedures—the closer they get to exhausting procedural options, the higher the stress.

one or the other based on some prioritization. These HFEs are termed "Simultaneous" HFEs:




a. For simultaneous HFEs, the next consideration is whether there are sufficient resources to support the required actions. This determination can be done by comparing the required tasks with the number of crew (workload). If the resources are inadequate, the "No" branch on the "Adequate Resources" branch is selected, which implies complete dependence (S6). If it can be shown that there are adequate resources to support both HFEs *and* that the scenario is feasible, the "Yes" branch on the "Adequate Resources" branch is selected. Next location and stress are considered. For the same location, the "Yes" branch on the "Same Location" decision node is selected. For high or moderate stress scenarios, assign complete dependence (S2); for low stress, assign high dependence (S3). For different locations, the "No" branch on the "Same Location" decision node is selected. (Location refers to the room or general area where the crew members are located. For example, the control room is a location—location is not differentiated down to individual panels in the control room.) For high or moderate stress scenarios, assign moderate dependence (S4); for low stress, assign low dependence (S5).

5. If the cues for the HFEs occur at different times (not simultaneously as defined above), the "No" branch on the "Same Time" decision node in Figure 8-4 is selected. Next, location is considered.

   a. For HFEs performed in the same location, the "Yes" branch on the "Same Location" decision node in Figure 8-3 is selected. Next, the timing between the cues and stress is considered as shown below:

| Time between Cues | Stress | Level | SN |
|---|---|---|---|
| 0 to 15 min. | High or Moderate | CD | S7 |
| | Low | HD | S8 |
| 15 to 30 min. | High or Moderate | HD | S9 |
| | Low | MD | S10 |
| 30 to 60 min. | High or Moderate | MD | S11 |
| | Low | LD | S12 |
| > 60 min. | High or Moderate | LD | S13 |
| | Low | ZD | S14 |

   b. For HFEs that are not performed in the same location, the "No" branch on the "Same Location" decision node in Figure 8-4 is selected. For high or moderate stress scenarios, low dependence is assigned (S15). For low stress scenarios, zero dependence is assigned (S16).

   c. For HFEs with very long time windows available for recovery relative to the time that would be required to repeat the performance of the required actions, the level of dependence can be relaxed to less than the level of dependence suggested by the timing between the cues. For example, if the timing between the cues is 25 minutes (which would suggest HD or MD) but the time window for the successive event is 2 hours with a manipulation time of 5 minutes, LD or ZD can be justified, because the required actions can be delayed/repeated for longer than an hour and still be successful.

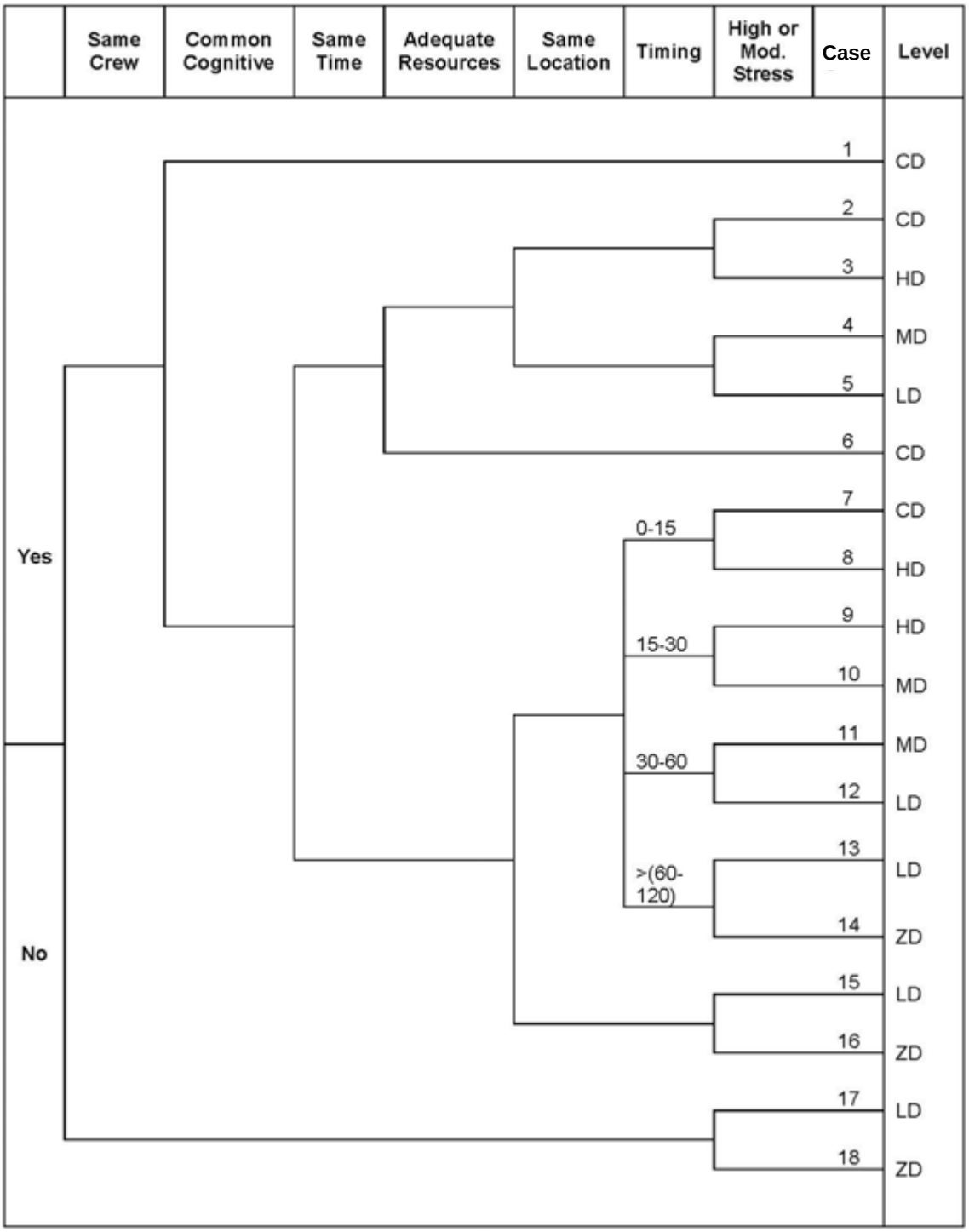



**Figure 8-4. HRA Dependency Rules for Post-Initiator HFEs**

As joint HFE HEPs evaluated via HADA are frequently significantly higher than the product of the associated independent HFE HEPs, conducting a rigorous HADA for the QRVA is critical in the development and interpretation of accurate event sequence frequency results.

## 8.3 QRVA HRA Detailed Methodology

The general objective of this human reliability analysis is to ensure that the HRA portion of the quantitative risk and vulnerability assessment accurately reflects the as-built, as-operated facility. The specific objectives of this HRA are to:

- Ensure consistency with the QRVA event sequence and systems analyses.
- Comply with industry guidelines and standards for QRVA HRA.
- Implement the HRA using SHARP1 method.

The post-initiator HFE HEPs evaluated in this assessment are summarized in Section 8.3.5 below. Note that these were developed and evaluated as new actions specifically applicable to the RHBFSF QRVA. The QRVA HFE HEPs were developed and reviewed initially by the RHBFSF QRVA HRA team and again during the RHBFSF QRVA HRA operator/technician interviews to ensure that application of these HEPs, where used in the RHBFSF QRVA, was appropriate and technically viable for the RHBFSF QRVA risk quantification.

It is important to note that the HEPs developed and evaluated as new actions specifically applicable to the RHBFSF QRVA are highly dependent upon the assumptions applied for each action and the operator/technician interviews applied [redacted].

### 8.3.1 General HRA Scope

The HRA scope includes the following types of HFEs and associated HEPs:

| | |
|---|---|
| **Type A** | HFEs during routine maintenance, testing and calibration activities that cause the unavailability of standby equipment or create precursor conditions for facility initiating events. |
| **Type B** | HFEs during normal operation that cause an initiating event. Type B HFEs were considered within the scope of the initiating events data analysis presented in Section 5 of this report. |
| **Type C** | HFEs during a response to an initiating event. These HFEs are known as post-initiator HFEs. |

Type B HEPs are typically accounted for statistically by including them in historical initiating event data. HFEs that are modeled in initiating event fault trees are not necessarily Type B HFEs—these may be either Type A or Type C HFEs. This follows the current, industry consensus in modeling HEPs.

For all types of HFEs, the HRA assumes that the operators have good intentions. Deliberate malicious acts such as sabotage are outside of the scope of the HRA.

Errors of commission—"…those errors that are associated with inappropriate interventions by operators with operating systems…"*** —are included in the scope, only as they may contribute to the scope of the HFE modeled in the QRVA event sequence analysis model or systems analysis models.

### 8.3.2 RHBFSF QRVA HRA Scope

The scope of the RHBFSF QRVA HRA consists of the following:

- A complete pre-initiator LOFICF and fuel release frequency (FRF) HRA. This includes identification, screening, definition and quantification of pre-initiator HEPs for the target facility (the RHBFSF).

- A complete post-initiator LOFICF and FRF HRA. The event sequence modeling task staff is responsible for the post-initiator HFE identification task (ASME High Level Requirement HR-E), so identification is excluded from the scope of this HRA.

- The scope is limited to the LOFICF and FRF QRVA HFEs. HFEs associated with external events such as fire are excluded from the scope of this Phase 1 QRVA. The list of post-initiator HFEs evaluated in this assessment is summarized in Section 8.3.5 of this report, and this list is consistent with the human actions described as being modeled in the event sequence analysis section of this RHBFSF QRVA.

- Thermal hydraulic analyses are not included in the scope of the HRA. The timing required and available for successful human actions are based on HRA team expert judgment and on information obtained during the operator interviews

- A dependency analysis of the most risk significant HFE combinations in the event sequences was performed and documented in this report.

### 8.3.3 Methodology

This HRA applies the EPRI Cause-Based Decision Tree Method (CBDTM), Human Cognitive Reliability/Operator Reliability Experiments (HCR/ORE) method (Reference 8-2), and the NRC THERP (Reference 8-1) to develop and quantify the HFE HEPs, consistent with the EPRI HRA Users Group HRA methodology and consistent with the state-of-the-art in the QRVA industry.

#### *8.3.3.1 Analysis of Pre-Initiator (Type A) Human Failure Events*

Pre-initiator HFEs occur during routine maintenance, testing or calibration activities—before an initiating event occurs. For maintenance, testing or calibration, facility personnel may need to disable/isolate/tag-out and/or place equipment in out-of-normal alignments, which may render the safety functions of such equipment unavailable. On completion of the maintenance, testing or calibration, these safety functions need to be restored by realigning the equipment into desired, normal configurations. The pre-initiator HRA is concerned with HFEs during routine maintenance, testing or

*** NUREG/CR-6365, A Technique for Human Error Analysis (ATHEANA), April 1996.

calibration activities that would render the equipment and associated safety functions unavailable.

Examples of pre-initiator HFEs include failure to properly realign a valve after maintenance or testing, failure to restore a system after maintenance or testing, or common cause miscalibration of sensors resulting in the unavailability of redundant trains of functionality or equipment.

The general approach to the pre-initiator HRA is summarized below and discussed in the subsequent subsections:

- IDENTIFY routine activities and practices, which if not performed correctly, may adversely impact the availability of mitigating systems.
- SCREEN out those activities for which sufficient compensating factors can be identified that would limit the likelihood or consequences of errors in those activities.
- DEFINE an HFE for each activity that cannot be screened out and incorporate these HFEs in the appropriate QRVA logic models.
- ASSESS the probability of each HFE with due consideration to dependencies.

*8.3.3.1.1 Identification*

**8.3.3.1.1.1 Procedure Review**

The purpose of the procedure review is to identify maintenance and testing activities that disable or realign equipment outside of desired normal configurations, and to identify calibration activities that may render equipment unavailable if performed incorrectly. These activities are identified by a systematic review of facility maintenance, testing and calibration procedures. The scope of the procedure review can be limited to maintenance, testing and calibration procedures, including relevant tank outage procedures, for the equipment that are relevant to the QRVA. It would therefore not be necessary to review *all* facility maintenance, testing and calibration procedures.

The maintenance and testing procedures relevant to QRVA equipment are reviewed to identify only those procedures that would require disabling or realignment of equipment outside the normal, desired alignment. Maintenance or testing procedures that do not require disabling or out-of-normal alignment equipment need not be considered further. Procedures that require the re-alignment of an entire system are of special concern, as are procedures for testing or maintenance of components that are common to two or more functionally-redundant trains of a system or two different systems.

The calibration procedures of concern are those that are performed on the control or instrumentation channels that are considered in the QRVA for equipment credited for mitigation. As a minimum, the automatic actuation channels of standby safety equipment should be considered for miscalibration, in order to satisfy the ASME standard. Of special concern are the calibrations of instrumentation channels that provide control signals to more than one system; e.g., the AFHE instrumentation provide

actuation signals to various systems. Miscalibration would impact the timely actuation of all the systems that rely on the actuation signal.

The procedure review should include an evaluation of the quality of written procedures as well as the quality of administrative controls for providing independent review.

Unfortunately, the Navy did not provide us with maintenance, inspection, or instrumentation calibration procedures for the RHBFSF other than the UFM SOP and the tank RTS SOP. Therefore, no meaningful procedure review for pre-initiating event human errors could be performed for this QRVA. The failure rates of key equipment are assumed to subsume associated human errors that may make equipment unavailable in this QRVA model.

#### 8.3.3.1.1.2 Historical Data Review

The purpose of the historical review is to identify any facility practices or events that have led to equipment unavailability. This review augments the procedure review. Facility historical data should be collected and reviewed to identify pre-initiator HFEs that have occurred. The preceding 10 years' historical data could be systematically searched using keywords such as "human error," "operator error," "maintenance error," etc. Sources of historical data include quality assurance non-conformance reports, maintenance records, corrective action records, etc. As a minimum, the facility-specific incident reports that occurred during the preceding 10 years should be reviewed. In the case of this RHBFSF QRVA, the review period recommended for application was 2007 through 2017. Incident reports from similar facilities could also provide useful insights, as can incident reports from the industry in general.

To date, the Navy has not provided records enabling or supporting such an historical data review. Therefore, the failure rates of key equipment are assumed to subsume associated human errors that may make equipment unavailable in this QRVA model.

### *8.3.3.1.2 Screening*

According to the ASME QRVA standard supporting requirements for HLR-HR-B, activities that could ***simultaneously*** impact ***multiple trains*** of ***redundant*** or ***diverse*** equipment are not to be screened out. These key terms in bold print require some interpretation and clarification.

The *simultaneous impact* is not whether an activity simultaneously impacts redundant trains while the activity is being performed, but whether the activity or activities performed in a procedure can render redundant or diverse trains unavailable simultaneously. For example, a calibration procedure would sequentially step through the calibrations of redundant channels measuring the same parameter. Although only one channel is impacted at a time, more than one channel may be miscalibrated—impacting multiple "trains" simultaneously. An activity or activities should not be screened out, because it is not performed simultaneously on redundant trains—the criterion is whether the activity or activities can result in the simultaneous unavailability of redundant or diverse trains of equipment functionality.

What constitutes *multiple trains* of redundant equipment can be interpreted at the train or component level. The flow control valves and associated flow paths can be considered redundant trains, as the flow control valve basic events would appear in the same cut sets. At this component level, redundant equipment would be simultaneously impacted, and the activity should not be screened out if the criterion for redundancy is applied at the component level. This QRVA assumes that the "*multiple trains"* statements are to be applied at the system train level and not at the component level.

#### 8.3.3.1.2.1 Screening of Activities that Do Not Impact Redundant or Diverse Equipment Simultaneously

The individual activities identified in the procedure and historical reviews—*that do not impact redundant or diverse equipment simultaneously*—are screened using the criteria in Table 8-2. These criteria were developed from NUREG/CR-4772 by incorporating project team experience in performing pre-initiator HRAs. The criteria are listed in order of descending priority; i.e., Priority 1A is the highest priority. Activities that impact redundant or diverse equipment are not screened at this stage.

**Table 8-2. Pre-Initiator Screening Criteria**

| Criterion | # | Description |
|---|---|---|
| No Impact on QRVA | 1A | Not in QRVA model. |
| | 1B | No impact on top event (LOFICF). |
| | 1C | No impact on equipment success criteria. |
| Design Methods of Detection or Correction | 2A | Compelling indication such as an annunciator or status indication in control room.<br>OR<br>System/equipment is normally in operation and unavailability will be immediately obvious. |
| | 2B | Equipment can be automatically actuated or repositioned. |
| Operability Tests and Administrative Methods | 3A | Operability test after maintenance or calibration AND verified on a periodic checklist (daily or more frequently). |
| | 3B | Operability test after maintenance or calibration AND independent verification. |
| | 3C | Independent Verification; the component is sealed. |
| | 3D | Performed during shutdown only. Maintenance activity is followed by operability test and several alignment checks during startup. |
| No or Insignificant Quantitative Impact on QRVA Results | 4 | Insignificant contributor to QRVA results. |

**Table 8-2. Pre-Initiator Screening Criteria (Continued)**

| Criterion | # | Description |
|---|---|---|
| Hardware Failures (used to screen historical events) | 5A | Manufacturing defect. |
| | 5B | Error caused by instrument drift. |
| | 5C | Resulted from equipment damage due to material defect. |
| Procedure Errors | 6 | Errors in procedure that have been corrected thus eliminating the failure mode. |
| Calibration Procedure | C | See Section 8.3.3.1.2.2 for screening of calibration activities. |

If the scope of the procedure review is not limited to maintenance, testing and calibration procedures for the equipment that are considered in the QRVA only, then Criterion 1A would screen most of the facility procedures out. If the scope of the procedure review is limited to maintenance, testing and calibration procedures for the equipment that are considered in the QRVA, then Criterion 1A would not be applicable, because all the procedures would already have been identified as relevant to QRVA equipment. Criterion 1B applies to equipment that may be modeled in the QRVA but are not relevant to the top event of interest; e.g., hydrogen recombiners may have been modeled historically but are not relevant to LOFICF or FRF. Criterion 1C would screen out procedures that do not place equipment in out-of-normal alignments; e.g., a procedure to obtain an oil sample from a pump may not require any equipment isolation or re-alignment. If the procedure review identified and eliminated these procedures already, then Criterion 1C would not be applicable at this stage. Criteria 2A to 3D are based on NUREG/CR-4772. Criteria 2A to 3A also encompass the *example* criteria stated in HR-B1 in the ASME Standard. Some of the example criteria in HR-B1 are more relaxed than the criteria presented here; e.g., in HR-B1 a post-maintenance functional test is considered sufficient to screen a procedure out. However, given that the ASME standard is not prescriptive in this regard and that the criteria are specifically example criteria, it is recommended to apply the more stringent criteria presented in Table 8-2. Criterion 4A can be applied by considering the importance metrics for the equipment in question. If the QRVA model is to be used for risk monitoring applications, great care should be exercised in applying this criterion, because the importance metrics of some equipment may be significantly different given different facility configurations. Criteria 5A, 5B, 5C, and 6 only apply to the screening of historical events

#### 8.3.3.1.2.2 Screening of Calibration Activities

Calibration activities of interest are those performed on the actuation signals of standby safety systems; e.g., facility tank and piping isolation, pump trip, etc. Each actuation signal may typically be produced from many diverse signals. Each signal in turn consists of redundant channels. Unlike mechanical systems, the definition of “train” (in terms of the ASME standard criteria) for screening purposes is somewhat subjective. It can be assumed that each of the signals that can generate an automatic actuation signal constitutes a “train”. This assumption allows one to screen calibration activities based on diversity of “trains”.

Calibration activities that impact diverse and redundant equipment may be screened by systematically considering the *diversity* in other instrumentation and control channels that provide the same function. If it can be shown that sufficient diversity exists among the instrumentation and control channels, then the relevant activities can be screened out—although they impact multiple, diverse equipment.

Two types of calibration errors are considered; miscalibration of the sensors that include the transmitters to the readout displays, and miscalibration of the logic trip (or "bistable" function) setpoints that actuate the control logic circuitry and alarms. Either type of miscalibration can cause the function to fail. The calibration of the sensors can often be screened out from further consideration, if signals provided by these sensors are continuously monitored in the control room. For example, tank level and pipeline pressure indications are monitored closely by control room personnel during normal operation. Any large deviation in all instrument channels of one of these parameters would be noticed by the operators and corrected.

As the calibration procedure for the majority of sensors is the same, it is possible to group all calibrations using the same procedure, and to derive a representative probability of miscalibration by performing a detailed analysis of the most bounding case. The potential for common cause miscalibration of a group of sensors can be determined by reviewing the instrumentation calibration schedule for each channel.

#### *8.3.3.1.3 Definition*

For each activity that cannot be screened out, a basic event should be defined in the appropriate QRVA logic structures. Basic events are also defined based on the insights gained from the review of historical data. In this QRVA, failure rates for the AFHE systems are assumed to subsume (include) failures due to human errors; e.g., miscalibration of sensors and/or control logic.

#### *8.3.3.1.4 Assessment of Probability Using THERP*

The THERP analysis and quantification is similar to that done for post-initiators. Please refer to Section 8.3.3.2.4 for details. In evaluating the potential for maintenance, testing or calibration activities rendering a component, system of function unavailable, the following are considered:

1. The frequency of the activity (testing, maintenance or calibration).

2. The probability that the component, system or function is left unavailable following the activity. The quantification of this probability is identical to the quantification of probability for quantifying post-initiator execution errors. However, for all pre-initiating operator action analyses, optimum stress is applied due to the level of experience, the nature of the operator action, and lack of being unduly challenged in performing the proceduralized tasks in a normal operating environment.

3. The frequency at which visual checks or functional tests are performed that can recover the misalignment or miscalibration. *Such recovery is limited to single check or test activities.*

4. Whether or not there is a functional test following maintenance which would reveal the fault.

Based on the period of the activity, t, and the probability of the component, system or function being left unavailable as a result of the activity, $P_D$, a mean failure rate, $\lambda$ is calculated as $P_D/t$. The period of the event credited to recover the error is the mean time to recovery (MTTR). The asymptotic unavailability of the component, system or function is then calculated as follows:

$$U = \frac{\lambda \times \text{MTTR}}{1 + \lambda \times \text{MTTR}}$$

### *8.3.3.2 Analysis of Post-Initiator (Type C) Human Failure Events*

Post-initiator human failure events occur after an initiating event and consist of a cognitive element and an execution element. The cognitive element includes detection, diagnosis and decision-making, while the execution element consists of manipulation tasks. Post-initiator human failure events occur in response to some cue; the cue may be the initiating event itself, an alarm, a procedural step or an observation. In contrast to pre-initiator human failure events, post-initiator human failure events are dynamic and subject to time constraints. This is assumed to increase the level of dependency between members of the crew, which increases the probability of failure. Some performance shaping factors may mitigate the stress level thus decreasing the probability of failure, while other performance shaping factors may aggravate the stress level thus increasing the probability of failure. Post-initiator human failure events are analyzed in a cue-response time framework.

A general framework for analyzing post-initiator human errors is shown in Figure 8-5. In response to a cue, a cognitive error can lead to failure of the human interaction if not recovered. If cognition is successful, an execution error can lead to failure of the human interaction if not recovered.

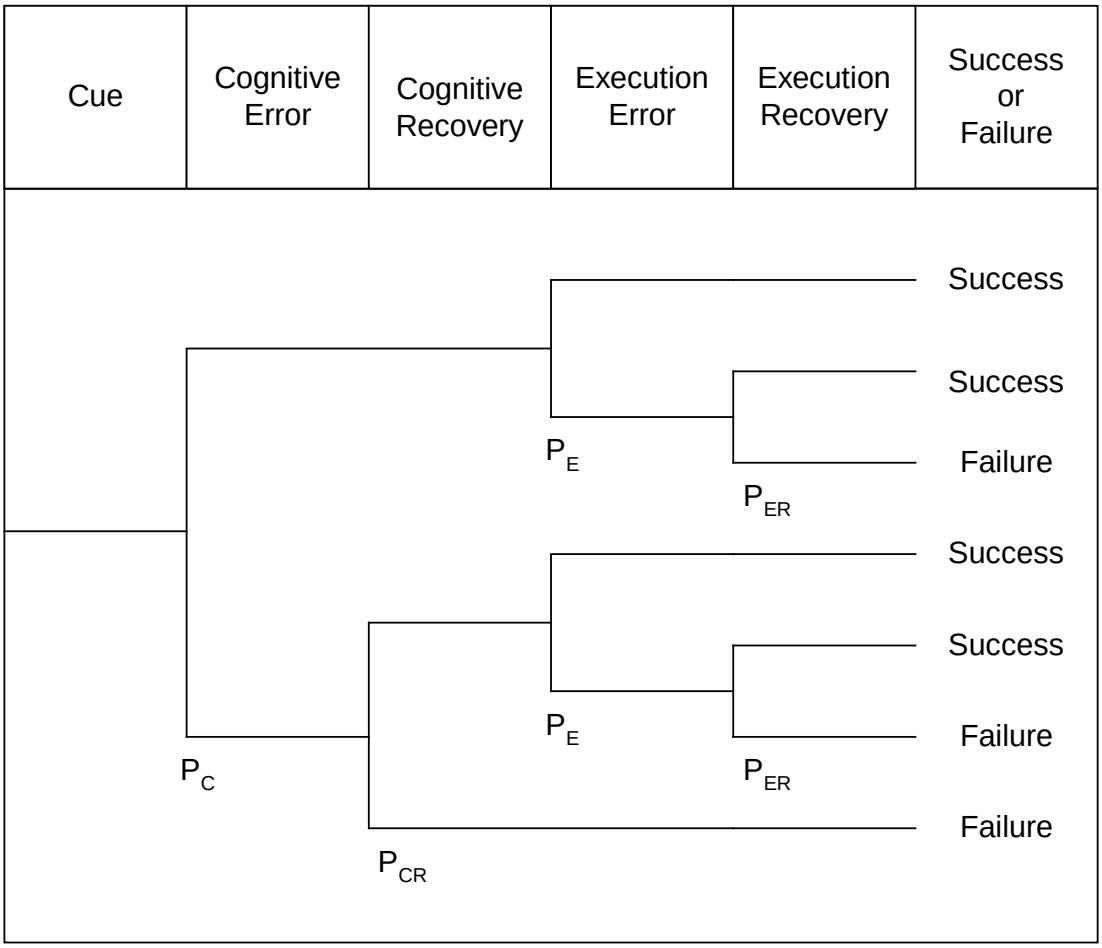



**Figure 8-5. Assessment of Post-Initiator HFE Probabilities**

The cognitive part of the HEP is denoted as $p_c$. In general, for procedure-directed actions, $p_c$ is quantified using the CBDTM. For immediate, memorized actions or time-critical actions, $p_c$ is quantified using the HCR/ORE methodology. Both the HCR/ORE and CBDTM methodologies are explained in detail in EPRI TR-100259 (Reference 8-2).

The execution part of the HEP is denoted by $p_e$, and is quantified using THERP (Reference 8-1).

The general approach to the post-initiator HRA is summarized below and discussed in the subsequent sections:

- IDENTIFY through a systematic review of the relevant procedures the set of operator responses required for each of the accident sequences.

- DEFINE human failure events that represent the impact of not properly performing the required responses, consistent with the structure and level of detail of the accident sequences.

- ASSESS the probability of each HFE using a well-defined and self-consistent process that addresses the facility-specific and scenario-specific influences on human performance, and addresses potential dependencies between human failure events in the same accident sequence.

- ASSESS recovery actions (at the cut set or scenario level) and model only if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure shall address dependency on prior human failures in the scenario.

#### *8.3.3.2.1 Identification*

The post-initiator human failure events should be identified by a systematic review of the relevant facility-specific procedures. For each initiating event considered in the QRVA, the applicable emergency operating procedures (EOP), abnormal operating procedures (AOP), annunciator response procedures, etc., are reviewed to identify all human failure events necessary for success. The post-initiator human failure events may be actions required to initiate (for those systems not automatically initiated), operate, control, isolate, or terminate those functions of systems and components used in preventing or mitigating loss of fuel inventory control as defined by the success criteria.

The procedure review should be confirmed by conducting interviews with facility operating staff such as operator trainers, qualified and nearly-qualified operators. The purpose of these interviews is to confirm the HRA analysts' understanding and assumptions of how the facility is operated and how the procedures are implemented. Each initiating event scenario should be talked through by describing the initial conditions to the operating staff and then by providing the necessary cues to elicit operator response. These interviews are also useful in estimating the time required to progress through a procedure. These interviews may result in some post-initiator human failure events being screened out, while new post-initiator human failure events may be identified.

The interviews with operating staff can be complemented by simulator observations. As a minimum, a walk-down of the simulator could be conducted to identify all the relevant instrumentation and controls. Actual simulations may be conducted to validate complex or uncertain scenarios as time and budget allowed. Simulator time is usually a precious commodity at most facilities. Results and insights obtained from previous/historical simulator exercises may also be taken into account. As the RHBFSF does not have a simulator for control room indications and actions, no simulator observations were included in this QRVA.

#### *8.3.3.2.2 Definition*

For the post-initiator human failure events identified above, define a set of HFEs as unavailabilities of functions, systems or components as appropriate to the level of detail in the accident sequence and system models. Failures to correctly perform several responses may be grouped into one HFE if the impact of the failures is similar or can be conservatively bounded.

For each HFE, specify or describe the following:

- The Accident Sequence-Specific Timeline (time available, time required, manipulation time)
- The Accident Sequence-Specific Procedural Guidance (e.g., AOPs and EOPs)
- The Availability of Cues and Other Indications for Detection and Evaluation of Failures and Corrective Action
- Degree of Clarity of the Cues/Indications
- The Necessary Tasks Required for Success of the Action
- Quality (type [classroom or simulator] and frequency) of the Operator Training or Experience
- Quality of the Written Procedures and Administrative Controls
- Human-Machine Interface
- Complexity of the Required Response
- Environment (e.g., lighting, heat, humidity) under which the Operator Is Working
- Accessibility of the Equipment Requiring Manipulation
- Necessity, Adequacy, and Availability of Special Tools, Parts, Clothing, Etc.

The accident sequence-specific timeline is obtained by thermal-hydraulic studies or by reasonable assumptions based on operator experience and operator/analyst judgment. A timeline may also be obtained from a simulator run, or from estimates obtained via operator interviews. The timeline would typically start when the initiating event occurs. The timing associated with the cues should be identified in the timeline. The timeline ends when the success criterion for the human action of interest can no longer be satisfied in the event sequence (or scenario) of interest.

*8.3.3.2.3 Assessment of Cognitive Error Probability*

#### 8.3.3.2.3.1 Annunciator Response Model

The annunciator response model is summarized in THERP (Reference 8-1) Table 20-23 and is reproduced in Table 8-3 with mean values that were calculated from the median values and error factors. It is used to quantify failure of cognition in response to alarms that occur later on in an accident sequence—after the initiating event and initial diagnosis. It is typically applied to model a recovery of the initial diagnosis failure if subsequent alarms can be identified.

**Table 8-3. THERP Annunciator Response Model**

| Item | Number of ANNs | Pr[$F_i$] | | | | | | | | | | Pr[$F_j$] | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | |
| | | a | b | c | d | e | f | g | h | i | j | k | |
| 1 | 1 | 0.0001 | | | | | | | | | | 0.0001 | 0.0003 |
| 2 | 2 | 0.0001 | 0.001 | | | | | | | | | 0.0006 | 0.0015 |
| 3 | 3 | 0.0001 | 0.001 | 0.002 | | | | | | | | 0.001 | 0.003 |
| 4 | 4 | 0.0001 | 0.001 | 0.002 | 0.004 | | | | | | | 0.002 | 0.005 |
| 5 | 5 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | | | | | | 0.003 | 0.008 |
| 6 | 6 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | | | | | 0.005 | 0.014 |
| 7 | 7 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | | | | 0.009 | 0.024 |
| 8 | 8 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | | | 0.02 | 0.04 |
| 9 | 9 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | | 0.03 | 0.08 |
| 10 | 10 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | 0.25 | 0.05 | 0.14 |
| 11 | 11 to 15 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | 0.25 | 0.12 | 0.31 |
| 12 | 16 to 20 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | 0.25 | 0.15 | 0.40 |
| 13 | 21 to 40 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | 0.25 | 0.20 | 0.53 |
| 14 | > 40 | 0.0001 | 0.001 | 0.002 | 0.004 | 0.008 | 0.016 | 0.032 | 0.064 | 0.13 | 0.25 | 0.25 | 0.67 |

#### 8.3.3.2.3.2 HCR/ORE Methodology

The HCR/ORE is an empirical method that relies on time-reliability correlations to estimate the cognitive error probability for various types of cue-response structures. The cue-response structures are defined in a timeline framework that considers $T_{SW,}$ the system time window (typically the time to loss of fuel inventory control obtained from thermal-hydraulic analyses); $T_{M,}$ the manipulation time, which is the time to complete the required actions; and $T_{1/2,}$ the median crew response time. The cue-response structures are defined in Figure 8-6:

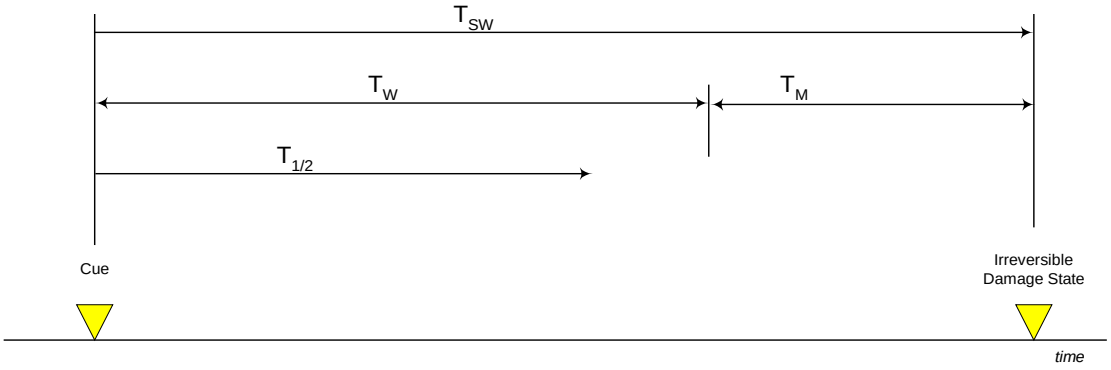



**Figure 8-6. Cue-Response Timeline**

The HCR/ORE correlation represents the cognitive error probability as a function of normalized time (the normalized time is a dimensionless unit which reflects the ratio of time available to crew median response time). Each cognitive error probability curve is characterized by two response time parameters: A crew median response time, $T_{1/2}$, and a logarithmic standard deviation of normalized time, $\sigma$. With these two parameters, the probability of cognitive error in a time window ($T_W$) is given by:

$$P_C = 1 - \Phi\left[\frac{\ln\left(\frac{T_W}{T_{1/2}}\right)}{\sigma}\right] \quad (8.1)$$

where:

$\Phi[\,]$ = Standard normal cumulative distribution (refer to standard normal distribution tables).

ln = Natural logarithm (base e).

$T_W$ = Time window available for cognition ($T_{SW} - T_M$). It must be noted that the time window ($T_W$) is assumed to be a constant; i.e., no uncertainty.

$T_{SW}$ = Thermal-hydraulic system time window available (typically the time to loss of fuel inventory control).

$T_M$ = Manipulation time, the time required to complete the required actions once they are identified.

$T_{1/2}$ = Median crew response time.

$\sigma$ = Logarithmic standard deviation (corresponds to the variability in operator response, and is estimated as described below).

The logarithmic standard deviation, $\sigma$, represents the crew-to-crew variability in responding to a specific cue. This deviation stems from a range of different factors such as cue response structure, diagnostic difficulty, degree and kind of procedural guidance, level of operator experience, communication between crew, and different response strategies.

There are two methods to determine $\sigma$. The one method is to use the "sigma decision tree," while the other method is to use the lookup table in the EPRI TR-100259 report.

The "sigma decision tree" method is based on the use of the decision tree shown in Figure 8-7. The decision tree end points have been derived based on judgment coupled with insights from simulator training.

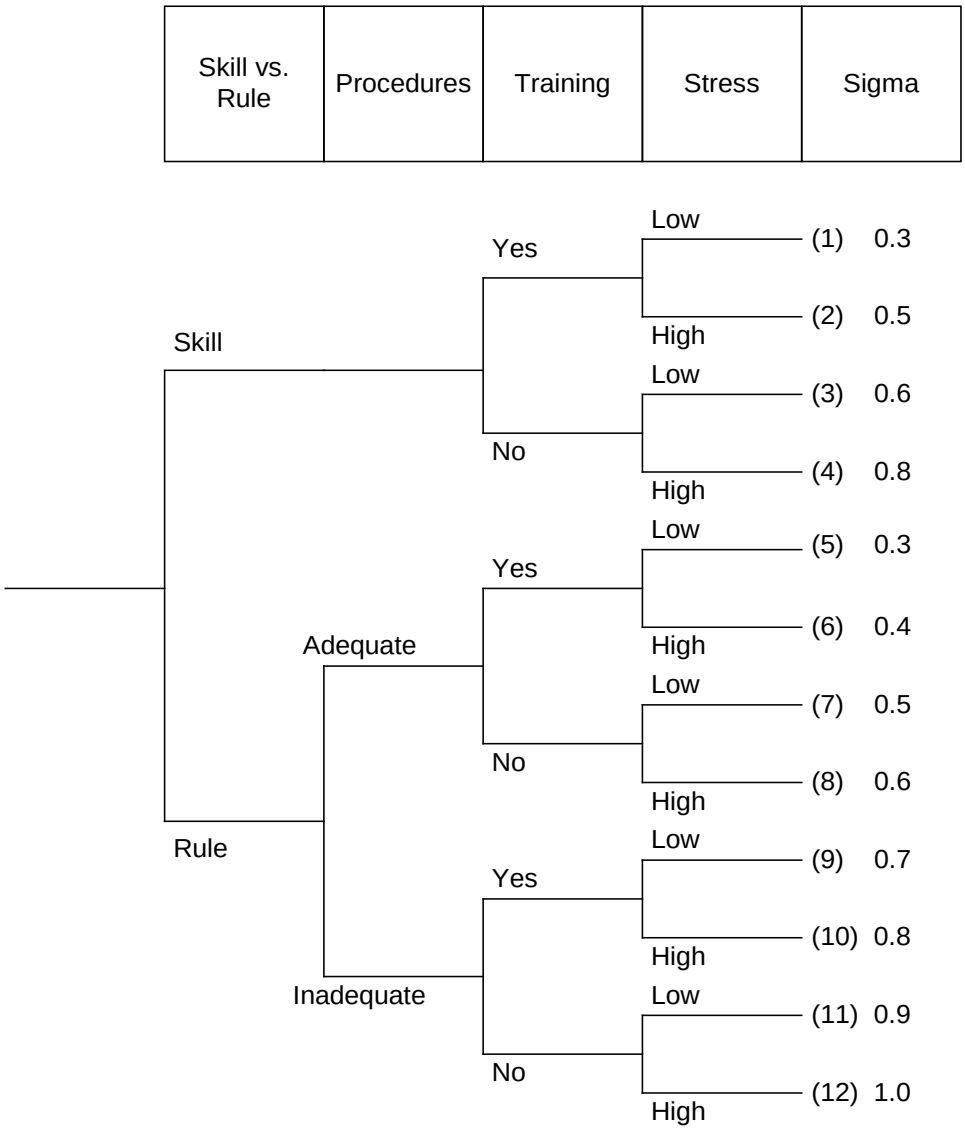



**Figure 8-7. SIGMA Decision Tree for HCR/ORE**

The paths taken on the decision tree are based on the analyst's review of the emergency procedures, and through the qualitative data obtained through discussions with the operating staff and simulator trainers. The analyst must also ascertain whether multiple strategies are possible at the facility.

A basic assumption behind the decision tree is that following an initiating event, as the accident proceeds further into the response, one can expect to see larger deviations in crew response times. A large $\sigma$ can be indicative of difficult diagnosis, the need for deriving diagnostics by monitoring meters and/or alarms, or use of different response strategies. Thus, $\sigma$ is indicative of how demanding and stressful the scenario is to the operators. The basis for defining the decision tree endpoints (the $\sigma$-values) has been a review of available operator reliability experiments data and derivation of correlation

between the calculated σ-values and the scenario descriptions coupled with observations (event chronologies).

The decision tree has four nodes, which address the response type, procedures, training, and stress. While originally employed at facilities using emergency procedures based on Industry Group Guidelines, these headings are generic and intended for all types of procedures. For each heading, questions are asked and generally, if the answer is a "yes," the up path of the decision tree is followed. Analyst judgment is required to select a path in the tree if all questions at a particular branch cannot all be answered by "yes" or "no." The set of questions associated with the decision nodes is given in Table 8-4.

**Table 8-4. Guidance on SIGMA Tree Decision Nodes**

| Decision Node | Guidance |
|---|---|
| Skill vs. Rule | This node decision relates to the type of cue-response at hand. The following questions are asked, and if either is yes, then the up branch is taken.<br>• Is the crew response concerned with immediate, memorized actions that could be regarded as skill-based?<br>• Are the required human interactions primarily concerned with assessment of need for manual back-up actions to automated safety functions? |
| Procedures | This node decision is concerned with the extent of procedural guidance and the cues available. For example, whether the procedure itself is sufficient to guide the operator or whether he/she also has to monitor meters, position indicators, etc. The following questions are asked:<br>• Is the procedural guidance simple/explicit enough; e.g., one step, clearly defined (is it unnecessary to monitor meters/alarms to make the correct decision)?<br>• Are the indications/alarms clear enough to support a decision, or is it necessary to take additional observations to reach a correct decision? Is the diagnostic straightforward without the need for consulting AFHE experts or bringing in additional crewmembers? |
| Training | From simulator experiments, it has been shown that different crews will perform consistently in highly practiced scenarios. The questions here relate to the type of training, frequency of training, and overall familiarity with the transient.<br>• Is the action highly practiced (through regular simulator training or/and actual experience) and simple to implement?<br>• Is coordination among crewmembers unimportant in responding to cue?<br>• Is no conscious planning required by operator to execute action? |
| Stress | This branch is intended to address a situation where several parallel actions have to be taken, or situations of potentially higher stress. This may cause communication problems and the shift supervisor and other on-shift personnel may become locked in a procedure loop.<br>• Is there only one critical alarm/annunciator present?<br>• Is the timing of operator response not critical (i.e., long time-window)? |

Endpoints 1 through 4 represent relatively simple, memorized actions. For highly practiced actions, the crew-to-crew variability in responding to a cue can be expected to be relatively minor; i.e., the σ-value is small. As the potential distractions (e.g., large number of more-or-less simultaneous alarms, several actions to be taken in parallel) in the control room increase, the σ-value can be expected to increase as well. Endpoints 5 through 12 represent actions of moderate to high complexity. Insights from simulator training indicate that in instances where there are clear alarms/annunciators, crews tend to perform consistently; i.e., approach the cue-response pattern of, say, Branches 1 and 2. Whenever there is the need for basing a decision on the correct interpretation of meter indications, the crew-to-crew variability tends to assume large σ-values.

The lookup table for estimating sigma from the EPRI report is reproduced in Table 8-5 below.

**Table 8-5. Estimates of σ from EPRI Report**

| Human Interaction (HI) Category | Average σ | Upper Bound | Lower Bound |
|---|---|---|---|
| CP1 | 0.7 | 1 | 0.4 |
| CP2 | 0.58 | 0.96 | 0.2 |
| CP3 | 0.75 | 0.91 | 0.59 |

#### 8.3.3.2.3.3 Caused Based Decision Tree Methodology

The CBDTM is used to assess HEPs for procedure-directed actions. It is typically applied to major decision steps such as transfers to another procedure, or the decision to initiate some process. It is generally not applied to steps that are purely directions to perform a specific task; which are considered as part of the execution.

The CBDTM methodology assesses HEPs by evaluating separate decision trees that evaluate each of the cognitive failure mechanisms shown in Table 8-6. There are two basic failure mechanisms; failure of the operator-information interface and failure of the operator-procedure interface. Each basic failure mechanism consists of four failure mechanisms.

**Table 8-6. CBDTM Failure Mechanisms**

| Type | Designator | Description |
|---|---|---|
| Failures in the Operator-Information Interface | $p_c$ a: | Data Not Available |
| | $p_c$ b: | Data Not Attended To |
| | $p_c$ c: | Data Misread or Miscommunicated |
| | $p_c$ d: | Information Misleading |
| Failures in the Operator-Procedure Interface | $p_c$ e: | Relevant Step in Procedure Missed |
| | $p_c$ f: | Misinterpret Instruction |
| | $p_c$ g: | Error in Interpreting Logic |
| | $p_c$ h: | Deliberate Violation |

Guidance on each of the CBDTM decision trees is provided below.

*8.3.3.2.3.3.1 Failure Mechanism a, Data Not Available*

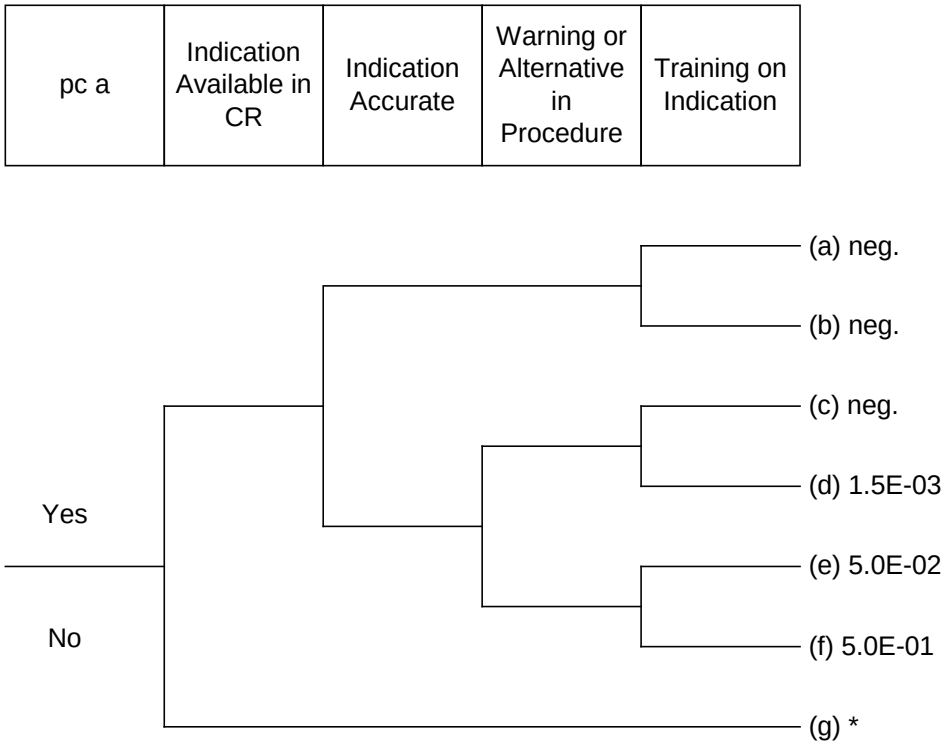



**Figure 8-8. Decision Tree for $p_c$a, Data Not Available**

## Table 8-7. Guidance on Decision Nodes for $p_c a$, Data Not Available

| Decision Node | Guidance |
|---|---|
| **Indication Available in Control Room** | Is the required indication available in the control room? |
| **Indication Accurate** | Are the available indications accurate? If they are known to be inaccurate (e.g., due to degradation because of local extreme environment conditions or isolation of the instrumentation) then select No. |
| **Warning or Alternate in Procedure** | If the normally displayed information is expected to be unreliable, is a warning or a note directing alternate information sources provided in the procedures? |
| **Training on Indication** | Has the crew received training in interpreting or obtaining the required information under conditions similar to those prevailing in this scenario? |

*8.3.3.2.3.3.2 Failure Mechanism b, Data Not Attended To*

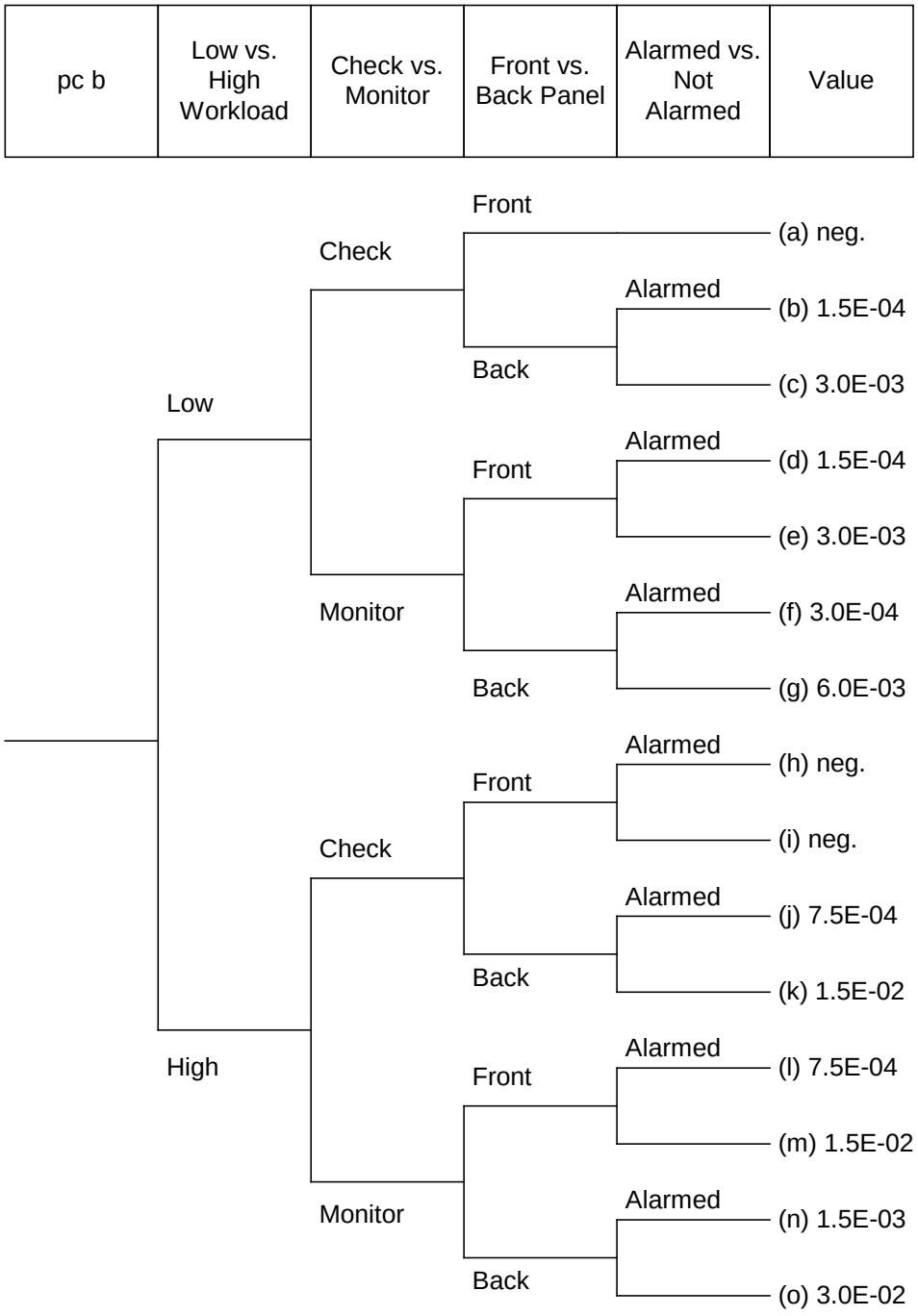



**Figure 8-9. Decision Tree for $p_c$b, Data Not Attended To**

## Table 8-8. Guidance on Decision Nodes for $p_c b$, Data Not Attended To

| Decision Node | Guidance |
|---|---|
| **Low vs. High Workload** | Do the cues critical to the human interaction (HI) occur at a time of high workload or distraction? Workload or distraction leading to a lapse of attention (omission of an intended check) is the basic failure mechanism for $p_c b$, and it interacts with the next two factors. |
| **Check vs. Monitor** | Is the operator required to perform a one-time check of a parameter, or is he required to monitor it until some specified value is reached or approached? The relatively high probabilities of failure for the monitor branches are included to indicate a failure to monitor frequently enough to catch the required trigger value prior to its being exceeded, rather than complete failure to check the parameter occasionally. |
| **Front vs. Back Panel** | Is the indicator to be checked displayed on the front panels of the main control area, or does the operator have to leave the main control area to read the indications? If so, he is more likely to be distracted or to simply decide that other matters are more pressing, and not go to look at the cue immediately. Any postponement in attending to the cue increases the probability that it will be forgotten. |
| **Alarmed vs. Not Alarmed** | Is the critical value of the cue signaled by an annunciator? If so, the operator is more likely to allow himself to check it, and the alarm acts as a preexisting recovery mechanism or added safety factor. For parameters that trigger action when a certain value is approached or exceeded (Type CP-2 and CP-3 HIs), these branches should only be used if the alarm setpoint is close to but anticipates the critical value of interest; where the alarm comes in long before the value of interest is reached, it will probably be silenced and thus not effective as a recovery mechanism. |

*8.3.3.2.3.3.3 Failure Mechanism c, Data Misread or Miscommunicated*

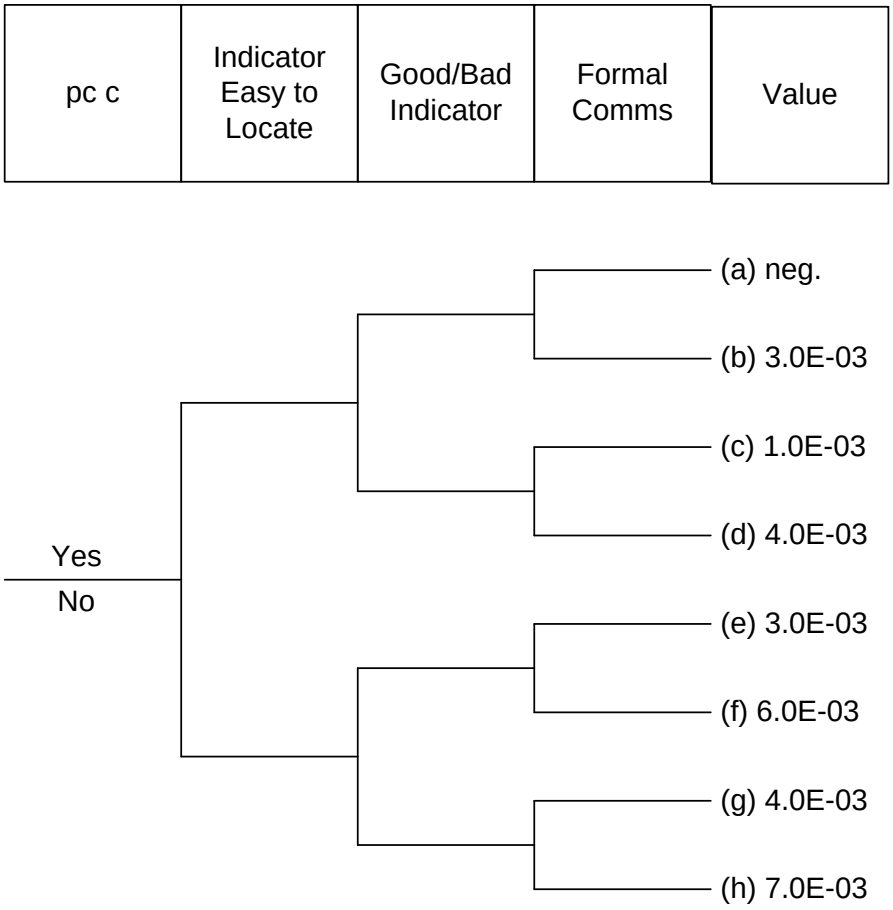



**Figure 8-10. Decision Tree for $p_c c$, Data Misread or Miscommunicated**

**Table 8-9. Guidance on Decision Nodes for $p_cc$, Data Misread or Miscommunicated**

| Decision Node | Guidance |
|---|---|
| **Indicators Easy to Locate** | Is the layout, demarcation, and labeling of the control boards such that it is easy to locate the required indicator? The answer is no if there are obvious human factor deficiencies in these areas and the plausible candidates for confusion with the correct indicator are sufficiently similar that the values displayed would not cause the operator to recheck the identity of the indicator after reading it. |
| **Good/Bad Indicator** | Does the required indicator have human engineering deficiencies that are conducive to errors in reading the display? If so, the lower branch is followed. |
| **Formal Communications** | Is a formal or semi-formal communications protocol used in which the person transmitting a value always identifies with what parameter the value is associated (this limited formality is sufficient to allow the person receiving the information to detect any mistakes in understanding his request)? |

*8.3.3.2.3.3.4 Failure Mechanism d, Information Misleading*

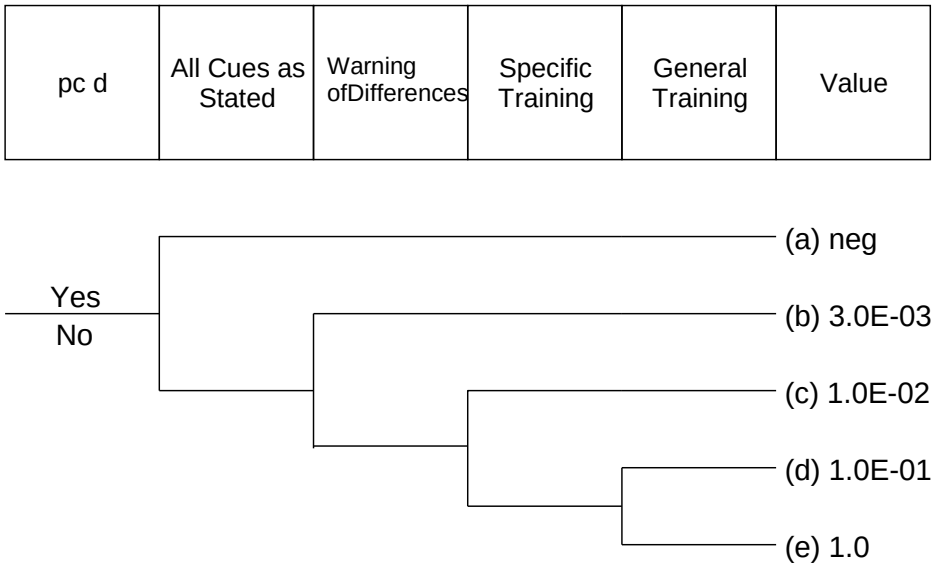



**Figure 8-11. Decision Tree for $p_cd$, Information Misleading**

## Table 8-10. Guidance on Decision Nodes for $p_c$d, Information Misleading

| Decision Node | Guidance |
|---|---|
| **All Cues as Stated** | Are cue states or parameter values as stated in the procedure? The "No" branch is to be used if an indicator is not obviously failed but would not give the value stated in the procedure. |
| **Warning of Differences** | Does the procedure itself provide a warning that a cue may not be as expected, or provide instructions on how to proceed if the cue states are not as stated? |
| **Specific Training** | Have the operators received simulator or other scenario-focused training in which the cue configuration was the same as in the situation of interest, and which emphasized the correct interpretation of the procedure in the face of the degraded cue state? |
| **General Training** | Have the operators received training that should allow them to recognize that the cue information is not correct in the circumstances? That is, is it something that every qualified operator is expected to know? Operators cannot be expected to reason from their general knowledge of instrumentation to the behavior of a specific indicator in a situation where they are not forewarned and there are many other demands on their time and attention. |

*8.3.3.2.3.3.5 Failure Mechanism e, Relevant Step in Procedure Missed*

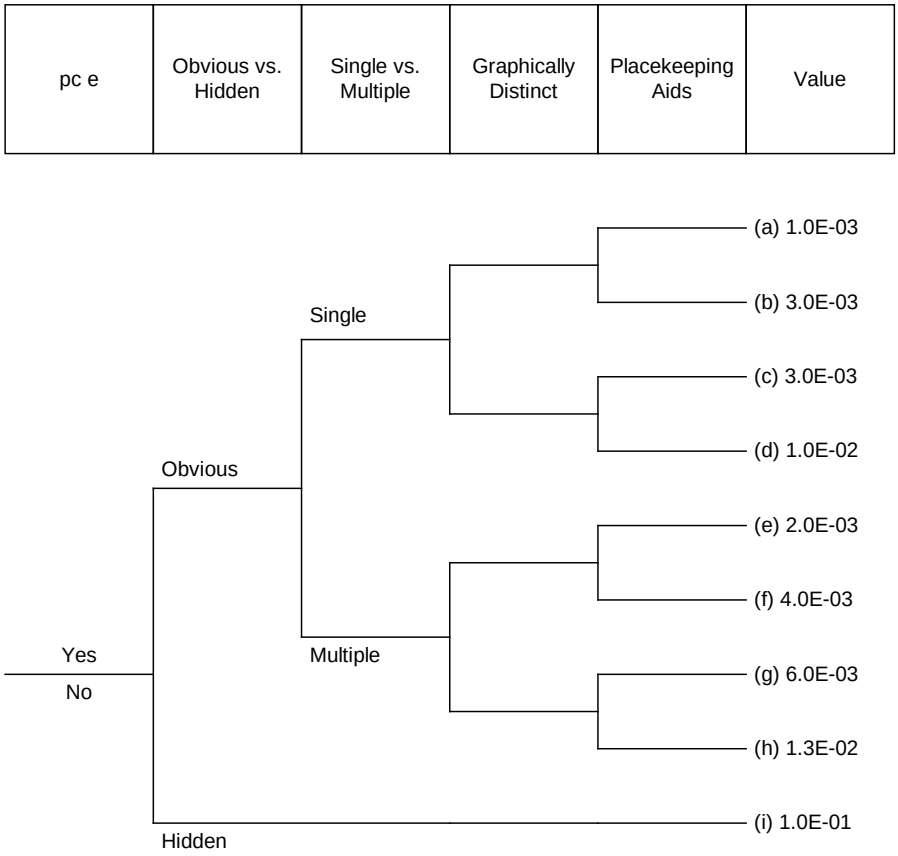



**Figure 8-12. Decision Tree for $p_c e$, Relevant Step in Procedure Missed**

## Table 8-11. Guidance on Decision Nodes for $p_c e$, Relevant Step in Procedure Missed

| Decision Node | Guidance |
|---|---|
| **Obvious vs. Hidden** | Is the relevant instruction a separate, standalone numbered step in which case the answer is Yes, or the upper branch is followed in the decision tree? Or is it "hidden" in some way that makes it easy to overlook; e.g., one of several statements in a paragraph, in a note or caution, or on the back of a page? |
| **Single vs. Multiple** | At the time of the HI, is the procedure reader using more than one text procedure or concurrently following more than one column of a flowchart procedure? If so, then answer with Yes, or follow the upper branch in the decision tree. |
| **Graphically Distinct** | Is the step governing the HI in some way more conspicuous than surrounding steps? For example, steps that form the apex of branches in flowchart procedures, steps proceeded by notes or cautions, and steps that are formatted to emphasize logic terms are more eye-catching than simple action steps, and are less likely to be overlooked simply because they look different than surrounding steps. However, this effect is diluted if there are several such steps in view at one time (as on a typical flowchart), and for this reason the only steps on flowcharts that should be credited as being graphically distinct are those at the junction of two branching flowpaths.<br>A procedure step is considered graphically distinct (as used in pc e) if it is preceded by a CAUTION, NOTE, set-off in a box, or is the only step on the page. |
| **Placekeeping Aids** | Are placekeeping aids, such as checking off or marking through completed steps and marking pending steps used by all crews?<br>The EOPs are written in a columnar "response/response not obtained" format. They may incorporate check-offs and may have provisions for placekeeping. Use of both of these aids would be noted during operator training. |

*8.3.3.2.3.3.6 Failure Mechanism f, Misinterpret Instruction*

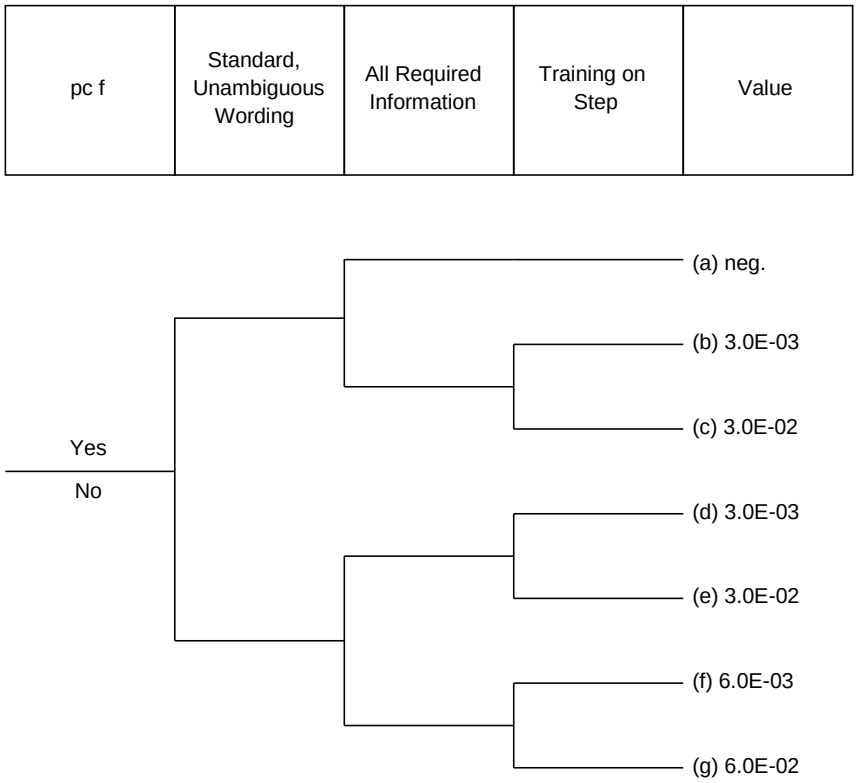



**Figure 8-13. Decision Tree for $p_cf$, Misinterpret Instruction**

**Table 8-12. Guidance on Decision Nodes for $p_cf$, Misinterpret Instruction**

| Decision Node | Guidance |
|---|---|
| **Standard Unambiguous Wording** | Does the step include unfamiliar nomenclature or an unusual grammatical construction? Does anything about the wording require explanation in order to arrive at the intended interpretation? Does the proper interpretation of the step require an inference about the future state of the facility? Standard wording = Yes, Ambiguous; Unusual = No. |
| **All Required Information** | Does the step present all information required to identify the actions directed and their objects? |
| **Training on Step** | Has the crew received training on the correct interpretation of this step under conditions similar to those in this HI? |

*8.3.3.2.3.3.7 Failure Mechanism g, Error in Interpreting Logic*

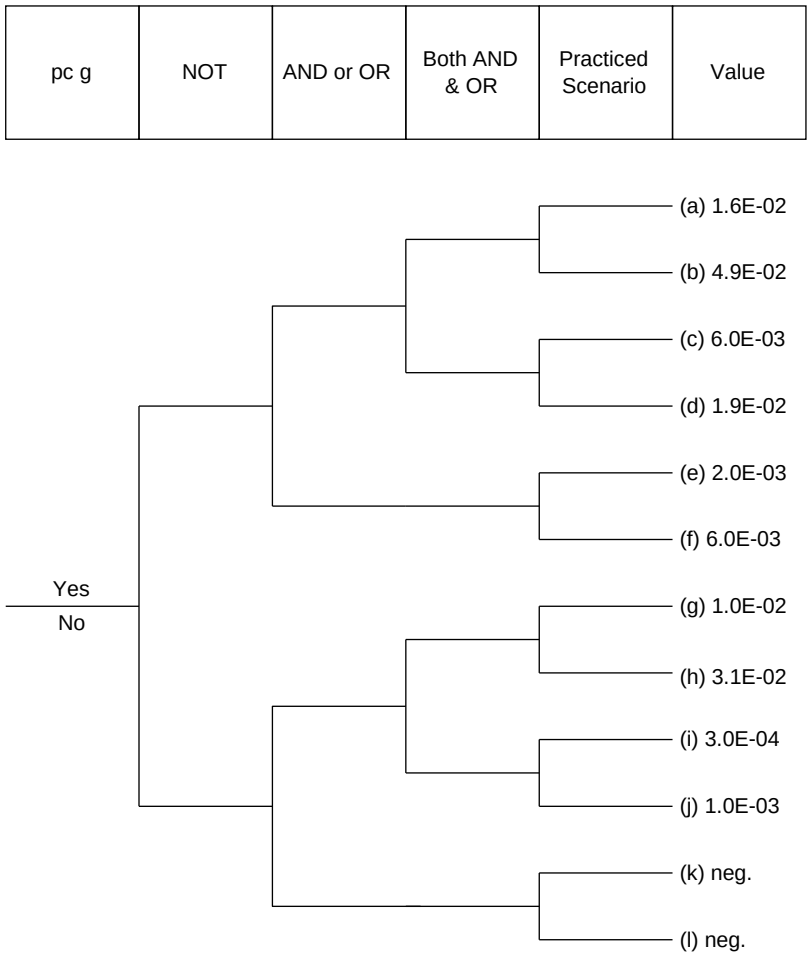



**Figure 8-14. Decision Tree for $p_cg$, Error in Interpreting Logic**

**Table 8-13. Guidance on Decision Nodes for $p_cg$, Error in Interpreting Logic**

| Decision Node | Guidance |
|---|---|
| **"NOT" Statement** | Does the step contain the word "not?" |
| **"AND" or "OR" Statement** | Does the procedure step present diagnostic logic in which more than one condition is combined to determine the outcome? |
| **Both "AND" and "OR"** | Does the step contain a complex logic involving a combination of ANDed and ORed terms? |
| **Practiced Scenario** | Has the crew practiced executing this step in a scenario similar to this one in a simulator or during scenario-focused drills or training? |

*8.3.3.2.3.3.8 Failure Mechanism h, Deliberate Violation*

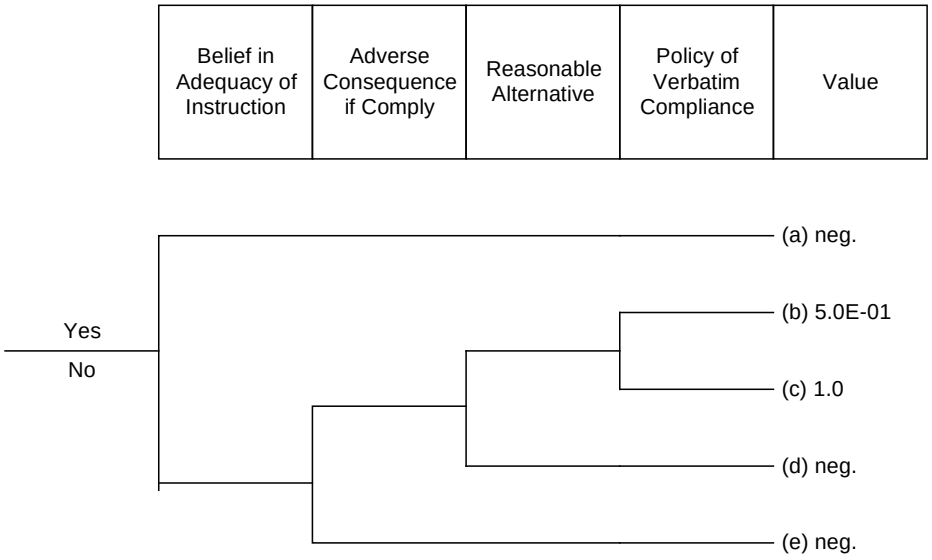



**Figure 8-15. Decision Tree for $p_c$h, Deliberate Violation**

**Table 8-14. Guidance on Decision Nodes for $p_c$h, Deliberate Violation**

| Decision Node | Guidance |
|---|---|
| **Belief in Adequacy of Instruction** | Does the crew believe that the instructions presented are appropriate to the situation (even in spite of any potential adverse consequences)? Do they have confidence in the effectiveness of the procedure for dealing with the current situation? In practice, this may come down to: have they tried it in the simulator or other scenario-focused training and found that it worked? |
| **Adverse Consequence if Comply** | Will literal compliance produce undesirable consequences, such as release of fuel, damage to the facility (e.g., thermal shock to the tank[s]), unavailability of needed systems, or violation of standing orders? A crew must have strong motivation for deliberately violating a procedure. |
| **Reasonable Alternatives** | Are there any fairly obvious alternatives, such as partial compliance or use of different systems that appear to accomplish some or all of the goals of the step without the adverse consequences produced by the step as written? Does simply delaying implementation appear to offer a reasonable hope for averting undesirable consequences? Note that simply delaying all or part of the response may not be considered a violation if the response is ultimately executed successfully. |
| **Policy of "Verbatim" Compliance** | Does the utility have and enforce policy of strict verbatim compliance with EOPs and other procedures? |

*8.3.3.2.3.3.9 Recovery*

Recovery may be accomplished by the same crewmember who initially executed the critical steps (self-review), or it could be by other crew members, or the next shift. Self-review recovery is only credited if there is a definite (compelling) cue or alarm to alert the operator to revisit the decision. Examples include an iterative path through the procedure (but taking care that this does not allow self-recovery from error modes that represent misunderstanding), an alarm (except where already credited in the decision tree). Recovery by other crew members or the next shift could only be credited when it is certain that they would be in the control room. The emergency response force (ERF) recovery factor is not applied if the human interaction takes place less than 1 hour into the sequence, or if the time available for the human interaction is less than 1 hour. The Technical Support Center and Operations Support Center are typically manned within 1 hour of an emergency plan declaration. Usually, recovery factors are effective at the times shown in Table 8-15.

**Table 8-15. When Recovery Factors Could Be Credited**

| Recovery Factor | Time Effective |
|---|---|
| Other Crew | Any time when it can be shown that there are more crew members than required. |
| Shift Technical Advisor (STA) (not applicable for this QRVA) | 15 minutes after reactor trip. |
| ERF (not applicable for this QRVA) | 1 hour after reactor trip. |
| Shift Change | 6 hours after reactor trip given 8 hour shifts.<br>9 hours after reactor trip given 12 hour shifts. |

Although multiple opportunities for recovery can typically be identified, it is prudent to only credit the single, most certain recovery factor—especially when the time window is less than an hour. This may be slightly conservative, but it is more defensible. If the time window is very long (several hours), the application of multiple recoveries is more defensible. However, for the sake of consistency in the HRA, it is advisable to adhere to policy of crediting a single recovery factor only.

Specific, allowable values for recovery factors are provided in EPRI TR-100259, Table 4-1 (Reference 8-2), which is reproduced in Table 8-16.

**Table 8-16. Recovery Factors in CBDTM**

| Tree | Branch | Self-Review | Extra Crew | STA Review (not applicable for this QRVA) | Shift Change | ERF Review (not applicable for this QRVA) |
|---|---|---|---|---|---|---|
| Pca | all | NC | 0.5 | NC | 0.5 | 0.5 |
| Pcb | all | X | NC | X | X | X |
| Pcc | all | NC | NC | X | X | X |
| Pcd | all | NC | 0.5 | X | X | 0.1 |
| Pce | a-h | X | 0.5 | NC | X | X |
| Pce | i | 0.5 | 0.5 | X | X | X |
| Pcf | all | NC | 0.5 | X | X | X |
| Pcg | all | NC | 0.5 | X | X | X |
| Pch | all | NC | X | X | NC | NC |

Where recovery factor values are listed as "X" in Table 8-16, the HEP of the associated failure mechanism is applied with due consideration of dependence between the failure mechanism and the recovery factor.

*8.3.3.2.3.3.10 Dependence*

The determination of the level of dependence between the failure mechanism and recovery factor is not an exact science and remains quite subjective. The specific levels of dependence are developed using operator interviews. Many factors may influence the level of dependence such as timing, location, and the relationship between persons performing the actions. Timing is deemed the most important underlying factor. The guidance in this document is to establish a minimum level of dependence based on the timing and to adjust this level of dependence higher if additional dependency factors are identified. The level of dependence based on timing between failure mechanism and recovery factor is shown in Figure 8-16.

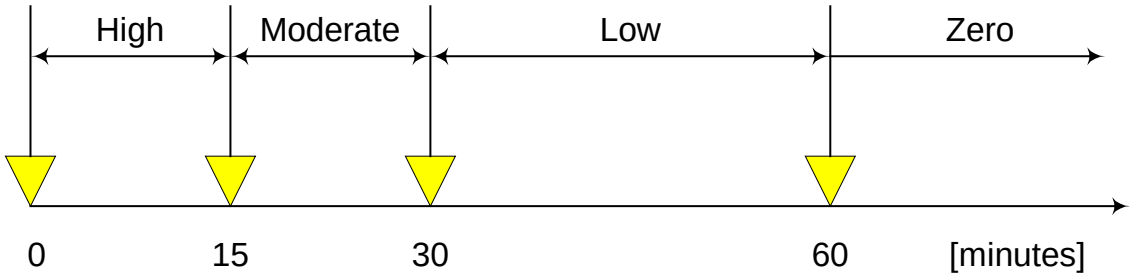



**Figure 8-16. Level of Dependence as a Function of Time**

The conditional probability of recovery step failure is quantified by determining the *level* of dependence as above and then applying the formulas from the Technique for Human

Error Rate Prediction (THERP) (Reference 8-1) Table 20-17 that are reproduced below in Table 8-17. The formulas are functions only of the independent HEP of the recovery factor.

**Table 8-17. Conditional Probability Equations**

| Level of Dependence | Conditional Probability Equation (*N* = HEP) | Approximate Value for Small *N* |
|---|---|---|
| Zero Dependence (ZD) | N | *N* |
| Low Dependence (LD) | $\frac{1 + 19\mathrm{N}}{20}$ | 0.05 |
| Medium Dependence (MD) | $\frac{1 + 6\mathrm{N}}{7}$ | 0.14 |
| High Dependence (HD) | $\frac{1 + \mathrm{N}}{2}$ | 0.5 |
| Complete Dependence (CD) | 1.0 | 1.0 |

*8.3.3.2.4 Assessment of Execution Error Using THERP*

The THERP approach develops a functional logic model of the human interaction execution failure by reviewing the procedure to identify:

1. Critical steps, which if carried out incorrectly would fail all or part of the function that is to be achieved.

2. Recovery steps, which can recover previous, failed critical steps primarily through re-visitation.

3. Alternative (redundant) steps, which are steps along an alternate success path functionally in parallel with the critical steps.

Execution errors are quantified using the THERP tables. The probabilities in the THERP tables are median values with associated error factors based on an assumed lognormal distribution. Because most QRVAs use mean values, median HEP values from THERP are converted to mean values.

**8.3.3.2.4.1 Identification of Critical Steps**

Critical steps are all those steps required (necessary and sufficient) for the success of the human interaction. The critical steps are identified by considering the success criteria for the function to be accomplished, the initial conditions such as initiating event characteristics, and preceding functional failure or successes.

**8.3.3.2.4.2 Identification of Critical Step Failure Modes**

There are two general failure modes associated with each critical step: "error of omission" (EOM) and "error of commission" (EOC). An EOM occurs when a critical step

is omitted or skipped in the procedure. An EOM is always applicable for post-initiators. However, for pre-initiators, an EOM may not always be applicable. For example, in miscalibration scenarios, skipping the calibration step will prevent miscalibration, so it is not modeled. An EOC occurs when the critical step is not omitted, but the required action is incorrectly performed. EOCs are always applicable, but may have a negligible probability in some cases. Typical EOCs for critical steps are shown in Example 1.

*Example 1: Typical EOCs for Critical Steps*

- Select wrong control on a panel.
- Turn multi-position rotary control in wrong direction.
- Turn a two-position switch in wrong direction or leave it in the wrong setting.
- Failure to complete change of state of a component if switch must be held until change is completed.
- Select wrong circuit breaker in a group of circuit breakers.
- Making an error of selection in changing or restoring a locally-operated valve.

#### 8.3.3.2.4.3 Quantification of Critical Step Failure

The various tables in Chapter 20 of THERP (Reference 8-1) are used to determine the HEPs for the critical steps as shown in Figure 8-17. Each critical step usually has two failure modes: an EOM and an EOC. The EOM occurs if the step is skipped. The EOC occurs if the step is performed incorrectly. An error factor is assigned to each HEP, based on THERP (Reference 8-1) Table 20-20.

The EOM is quantified using THERP (Reference 8-1) Table 20-7. If the human interaction takes place within ten steps from the start of the procedure, Item 20-7(1) (short list, with check-off provisions) is used. If the human interaction takes place 10 or more steps into the procedure, Item 20-7(2) (long list, with check-off provisions) is used. Items 20-7(3) and 20-7(4) (no check-off provisions) are usually used when the procedure has no check-off provisions or they are not used. The start of the procedure is used versus the start of the accident sequence based on policies for the control room supervisor to conduct a brief and thus re-synchronize the entire crew upon transfer of procedures. Based on the notes in Chapter 15 of THERP (Reference 8-1), EOM probabilities can be reduced by a factor of 3 if the procedures are not verbose but written in a step-by-step format. In the SHARP1, the EOM probabilities that are reduced by a factor of 3 are presented in Table 20-7b in the THERP.

The EOC is typically quantified using THERP (Reference 8-1) Tables 20-12 and 20-13. Critical steps require the operator to change the state of some equipment. This could be in the control room or locally. Typical actions are starting or stopping a pump and opening or closing a valve/breaker. Table 20-12 applies to the errors in manipulating controls. The EOC is committed either if the operator selects the wrong equipment to manipulate or if he does not perform the manipulation in the required manner.

Table 20-13 applies to local manual valve operation. This table is also applied to operation of other local components such as switchgear breakers and room doors.

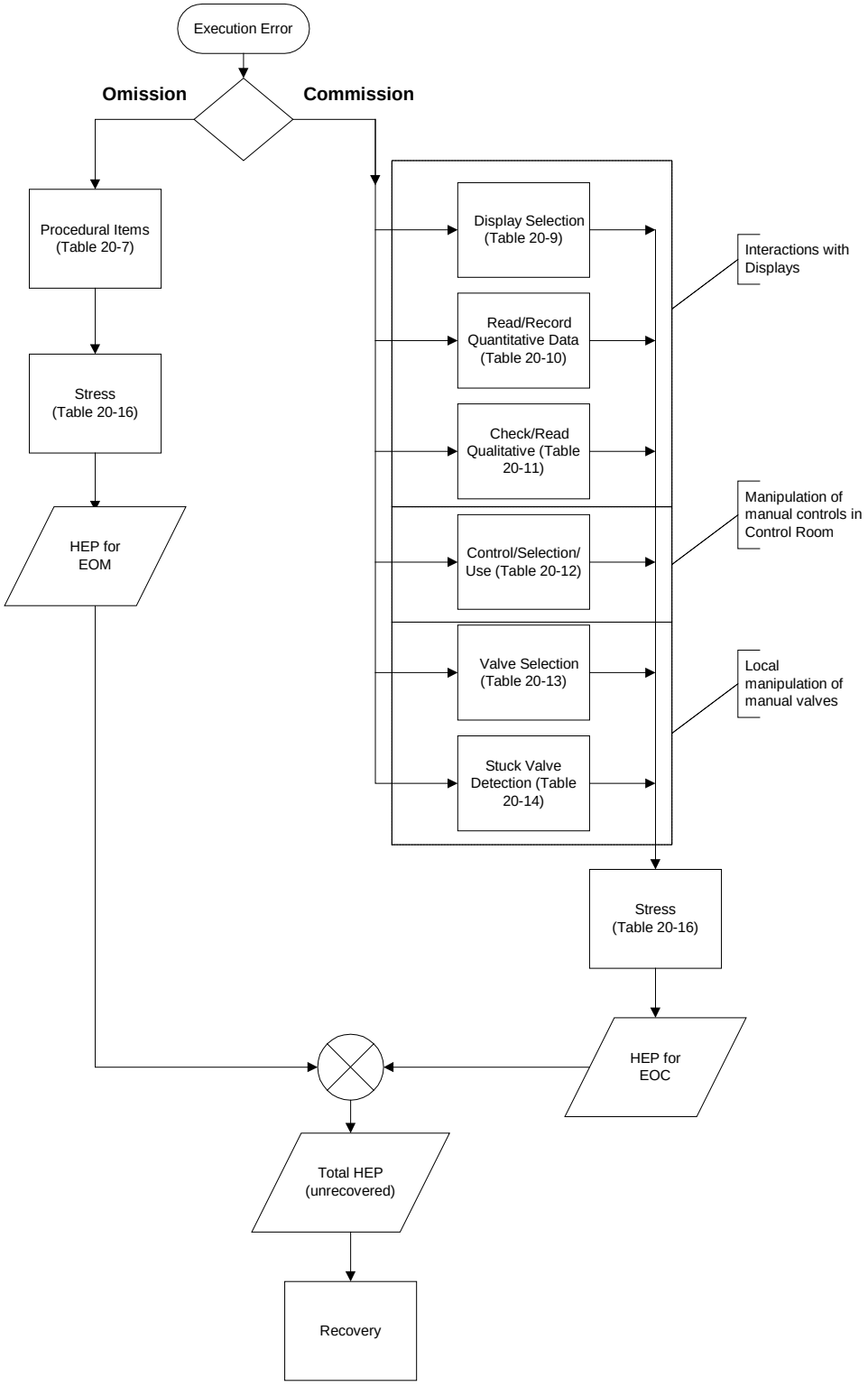



**Figure 8-17. THERP (Reference 8-1) Table Selection Flowchart**

#### 8.3.3.2.4.4 Identification of Recovery Steps

Recovery is primarily through revisitation of the critical steps due to a specific cue. The cue for revisitation may be a procedural verification step, an iterative procedural step or a compelling condition such as an annunciator alarm in the control room. A verification step directs the operator to check or verify a parameter that would confirm the success of a previous critical step. An iterative procedural step directs the operator to return to a step preceding the critical steps so that the critical steps would be repeated. An alarm would prompt the operator to rediagnose the situation and then repeat the critical steps.

In some cases, the cue for revisitation of a previous step will be the inability to execute a successive step. For example, if an interlock needs to be bypassed in order to start a pump, the pump will not start if the operator missed the step to bypass the interlock. In this case, the operator will revisit the preceding step to bypass the interlock. Although the step to bypass the interlock is "recovered" by the step to start the pump, the pump start on its own is a critical step, and quantitatively the probability of the operator failing to bypass the interlock or failing to start the pump is just the probability of failing to start the pump. Recovery can also be accomplished via alternative or redundant steps if the system success criteria allows.

Recovery is conditional on time available. If the time window is relatively long compared to the manipulation time for the critical steps, revisitation could be credited. The basic question is whether the operator would have enough time to repeat all the critical steps in the given time window? This dictates that $T_W >> T_M$. Because $T_W$ already accounts for the initial $T_M$, one needs to deduct an estimated, initial diagnosis time from the time window to determine if revisitation is credible; i.e., $T_W - T_{W(initial)} > T_M$ for revisitation to be credible.

#### 8.3.3.2.4.5 Identification of Recovery Step Failure Modes

As with critical steps, there are two general failure modes associated with each recovery step, EOM and EOC. An EOM occurs when a recovery step is omitted or skipped in the procedure. An EOC occurs when the recovery step is not omitted, but the required action is incorrectly performed.

#### 8.3.3.2.4.6 Quantification of Recovery Step Failure

The EOM is quantified using THERP (Reference 8-1) Table 20-7, as for critical steps.

The EOC is typically quantified using THERP (Reference 8-1) Table 20-9, 20-10, or 20-11. Recovery steps usually instruct the operator to verify the status of some equipment. This typically requires that the operator needs to obtain information from the control room panels by reading a gauge or checking status lights. The EOC is committed if the operator reads the wrong gauge or checks the wrong indicator, or he simply misreads the instrument to conclude that the equipment status is as required when it is not.

#### 8.3.3.2.4.7 Impact of Stress

The origins of the HEPs used in THERP (Reference 8-1) are in the nuclear weapons assembly program, which is performed under strictly controlled laboratory conditions;

i.e., in a normal working environment with little or no stress. For pre-initiators, the THERP (Reference 8-1) HEPs are applied as is, because pre-initiators are assumed to occur in a normal working environment with little or no stress. However, for post-initiators, stress needs to be taken into account for execution HEPs. The stress factors suggested in THERP (Reference 8-1) Table 20-16 are applied to both critical step HEPs and recovery step HEPs as follows:

1. Optimum stress (x1) is usually applied to tasks directed by the EOPs. In some cases, such as complex or foreboding events, the stress level is judged higher and a moderate stress (x2) is applied.

2. Moderate stress (x2) is usually applied to task directed by the functional restoration or emergency contingency action procedures.

3. Extreme stress (x5) is applied if additional human interaction is required because of subsequent equipment failure while in a functional restoration or emergency contingency action.

The above stress guidelines are based on how far the facility is from loss of fuel inventory control or how much fuel is currently assessed as releasable. These stress levels can be further increased if it is judged that there are further aggravating factors. For example, if the operator has reached the last step in a functional restoration procedure before loss of fuel inventory control would occur should the step fail, high stress would be warranted. If there were a fire, which causes the initiating event and impacts the instrumentation required to mitigate event sequence consequences, a higher stress level than those given above would be justified.

It is assumed that operators are highly skilled in performing the necessary tasks—most having more than 10 years of experience and each having more than 6 months of experience. In most cases, optimum stress is applied due to the level of experience, the nature of the event, and lack of being unduly challenged in performing the procedure-directed tasks. Some events, however, result in a high stress situation.

#### 8.3.3.2.4.8 Dependency between Critical and Recovery Steps

See Section 8.3.3.2.3.3.10.

#### 8.3.3.2.5 Uncertainty

The uncertainty in the HEPs developed specifically for the RHBFSF QRVA is reflected by the error factor, which is assigned based on the total mean HEP as shown in Table 8-18, Error Factors.

**Table 8-18. Error Factors**

| HEP (total mean value) | Reference | Error Factor |
|---|---|---|
| Estimated HEP < 0.001 | THERP (Reference 8-1) Table 20-20 | 10 |
| 0.1 > Estimated HEP ≥ 0.001 | THERP(Reference 8-1) Table 20-20 | 5 |
| 0.5 > Estimated HEP ≥ 0.1 | Mathematical Convenience | 2 |
| 0.8 > Estimated HEP ≥ 0.5 | Mathematical Convenience | 1.2 |
| Estimated HEP ≥ 0.8 | Mathematical Convenience | 1 |

#### 8.3.3.2.6 RHBFSF QRVA HRA Bases and Assumptions

The bases and assumptions applied in this assessment are listed as follows:

- The RHBFSF is operated by a minimum staff of three qualified operators from the JBPHH Navy Supply Command Fuels Department. The three operators consist of a main control room operator (locally identified as the "Papa" watch), a RHBFSF roving watchstander (locally identified as the "gauger" or Red Hill rover), and a roving watchstander on the base at JBPHH (locally identified as the "Kuahua" watch). Each of these watchstanders is qualified via a formal Navy training and qualification program, and each is required to maintain qualification via periodic re-training. In addition to these three continuous watchstanders, additional qualified watchstanders are temporarily assigned to support specific fuel movement operations.

- The RHBFSF is continuously manned.

- Facility operators are well-qualified in the application of RHBFSF standard operating procedures and evolution-specific operation orders.

- Equipment required for manually measuring main fuel storage tank fuel level, a process known as top-gauging, is maintained operational and stored in locations well-known to the qualified gauger watchstanders.

- During normal operation, all areas of the facility are adequately ventilated and lighted.

- At all times, there is a Fuels Department supervisory staff, consisting of a Fuels Department Head, Assistant Fuels Department Head, Operations Supervisor, and an

Assistant Operations Supervisor, overseeing RHBFSF operations, maintenance, inspection, and testing.

- During normal operations, multiple methods of communication are available to facility operators and supervisors. These methods include portable hand-held radios (walkie-talkies), facility telephones, cell phones, and government supported secure land-line telephones. During emergency conditions, sound-powered telephones are also available and their locations are known by the qualified watchstanders.

- During normal operations, there is a fully-functional facility video camera system controlled by the main control room operator.

- All facility communications and safety equipment is well-maintained and available for use during normal facility operations.

- During emergency conditions, emergency breathing apparatus equipment is available for operator use.

- Other bases and assumptions applied in the evaluation of specific human action HFE HEP values are documented in [redacted].

### 8.3.4 Pre-Initiators

#### *8.3.4.1 HEP Summary*

The pre-initiator HFE HEPs applied in this QRVA are summarized in Table 8-19 below. The BHEP variable in Table 8-19 simply refers to the THERP/NUREG-4772 basic human error probability value of 3.00E-02 with an error factor of 5. [redacted]

## Table 8-19. Pre-Initiator HEP Summary

| HFE Basic Event Name in Model | HFE HEP Variable Name | Description | Method | HEP | HEP Error Factor |
|---|---|---|---|---|---|
| *For Skin Valves* | | | | | |
| RHTOB102 | RHTOE | RH Staff Tag Out Valve 102B in error. | THERP | 2.90E-03 | 5 |
| NSTOB102 | CSTOE | Navy's Contractor Tag Out Valve 102B in error. | THERP | 2.90E-03 | 5 |
| ERRV102SIZE | BHEP | Mistaking the F24 (102B) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB102 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN102B | RHTOE | Error in Maintenance Plan, mistaking the F24 (102B) valve. | THERP | 2.90E-03 | 5 |
| SUEMPLN102B | BHEP | Supervisory review fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| OPEMPLN102E | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB102 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| RHTOB108 | RHTOE | RH Staff Tag Out Valve 108B in error. | THERP | 2.90E-03 | 5 |
| NSTOB108 | CSTOE | Navy's Contractor Tag Out Valve 108B in error. | THERP | 2.90E-03 | 5 |
| ERRV108SIZE | BHEP | Mistaking the JP5 (108B) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB108 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN108B | RHTOE | Error in Maintenance Plan, mistaking the JP5 (108B) valve. | THERP | 2.90E-03 | 5 |
| SUEMPLN108B | BHEP | Supervisory review fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |

## Table 8-19. Pre-Initiator HEP Summary (Continued)

| HFE Basic Event Name in Model | HFE HEP Variable Name | Description | Method | HEP | HEP Error Factor |
|---|---|---|---|---|---|
| OPEMPLN108B | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB108 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| RHTOB115 | RHTOE | RH Staff Tag Out Valve 115B in error. | THERP | 2.90E-03 | 5 |
| NSTOB115 | CSTOE | Navy's Contractor Tag Out Valve 115B in error. | THERP | 2.90E-03 | 5 |
| ERRV115SIZE | BHEP | Mistaking the F76 (115B) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB115 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN115B | RHTOE | Error in maintenance plan, mistaking the F76 (115B) valve. | THERP | 2.90E-03 | 5 |
| SUEMPLN115B | BHEP | Supervisory review fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| OPEMPLN115B | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB115 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| *For Other (non-skin) Valves* | | | | | |
| RHTOC102 | RHTOE | RH Staff Tag Out Valve 102C in error. | THERP | 2.90E-03 | 5 |
| NSTOC102 | CSTOE | Navy's Contractor Tag Out Valve 102C in error. | THERP | 2.90E-03 | 5 |
| ERRV102SIZE | BHEP | Mistaking the F24 (102C) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB102 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN102C | RHTOE | Error in maintenance plan, mistaking the F24 (102C) valve. | THERP | 2.90E-03 | 5 |

## Table 8-19. Pre-Initiator HEP Summary (Continued)

| HFE Basic Event Name in Model | HFE HEP Variable Name | Description | Method | HEP | HEP Error Factor |
|---|---|---|---|---|---|
| OPEMPLN102C | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB102 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| RHTOC108 | RHTOE | RH Staff Tag Out Valve 108C in error. | THERP | 2.90E-03 | 5 |
| NSTOC108 | CSTOE | Navy's Contractor Tag Out Valve 108C in error. | THERP | 2.90E-03 | 5 |
| ERRV108SIZE | BHEP | Mistaking the JP5 (108C) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB108 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN108C | RHTOE | Error in maintenance plan, mistaking the JP5 (108C) valve. | THERP | 2.90E-03 | 5 |
| OPEMPLN108C | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB108 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| RHTOC115 | RHTOE | RH Staff Tag Out Valve 115C in error. | THERP | 2.90E-03 | 5 |
| NSTOC115 | CSTOE | Navy's Contractor Tag Out Valve 115C in error. | THERP | 2.90E-03 | 5 |
| ERRV115SIZE | BHEP | Mistaking the F76 (115C) valve size difference. | THERP | 3.00E-02 | 5 |
| VIB115 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |
| OPCOM | BHEP | Operator does not detect the error through the communications with the contractors. | THERP | 3.00E-02 | 5 |
| EMPLN115C | RHTOE | Error in maintenance plan, mistaking the F76 (115C) valve. | THERP | 2.90E-03 | 5 |
| OPEMPLN115C | BHEP | Operator/control room fails to detect the error in the maintenance plan. | THERP | 3.00E-02 | 5 |
| VIB115 | BHEP | Vibration and sound of fuel movement in main fuel line missed. | THERP | 3.00E-02 | 5 |

#### 8.3.4.2 Miscalibration Identification and Screening

To date, the Navy has been unable to provide detailed information or data supporting identification and evaluation of miscalibration pre-initiators. In this QRVA, as in many QRVAs, the miscalibration pre-initiators are assumed to be subsumed within the instrumentation and control equipment (e.g., AFHE) basic event failure rates applied in this analysis. Miscalibration of transmitters is generally not a concern, as the same transmitters that provide signals to the protection and control systems also provide signals to the control room indications. Miscalibration of a transmitter channel will be immediately obvious via the control room indications. However, miscalibration of bistable functions used for automatic actuation signals will generally only be evident on demand.

#### 8.3.4.3 Historical Pre-Initiator Events

To date, the Navy has been unable to provide detailed historical records to support identification and evaluation of historical pre-initiator events. As is the practice for many QRVAs, historical pre-initiator event impacts are assumed subsumed within equipment basic event failure rates applied in this QRVA.

#### 8.3.4.4 Misalignment Identification and Screening

To date, the Navy has been unable to provide detailed information (e.g., equipment surveillance and testing procedures) to support identification and evaluation of misalignment human actions. Potential misalignment activities are assumed to be subsumed within equipment basic event failure rates applied in this QRVA.

### 8.3.5 Post-Initiators

#### 8.3.5.1 HEP Summary

The post-initiator HFE HEPs applied in this QRVA are summarized in Table 8-20 below. This table lists the cognitive HEP ($P_{cog}$), execution HEP ($P_{exe}$), total HEP (*Total HEP*), error factor (*EF*), and HRA method (*Method or Comment).* The QRVA post-initiator HFE HEPs were reviewed initially by the RHBFSF QRVA HRA team and again during the RHBFSF QRVA HRA operator/technician interviews to ensure that application of these HEPs, where used in the RHBFSF QRVA, was appropriate and technically viable for the RHBFSF QRVA.

It is important to note that the HEPs developed and evaluated as actions specifically applicable to the RHBFSF QRVA are highly dependent upon the assumptions applied for each action, specifically the operator/technician interviews applied. These assumptions are summarized in the basic event ID column for each RHBFSF QRVA HRA human action. For the actions specifically applicable to the RHBFSF QRVA, the project team analysts recommend application of the CBDTM/THERP method HEP results from the SHARP1 calculations. These are the results presented in Table 8-20. In many cases the SHARP1 analyses showed that the "preferred" method HEP results come from other methods, which typically yield lower HEP results. However, the HRA

team for this project has recommended the application of the CBDTM/THERP results for the spectrum of timing and facility conditions associated with the RHBFSF QRVA HRA.

## Table 8-20. Post-Initiator HFE HEP Summary

| Sequence Descriptor | Top Event Name | Split Fraction Name | HFE Basic Event Name | HFE HEP Variable Name | HFE Description | Assumed Success Time Window | Method | $P_{cog}$ | $P_{exe}$ | Total HEP | Error Factor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| S1 (idle)or S5 (MOVE) - to rock | OUFM | OUFM1 | OUFM_OUFM1 | HOUFM1 | Once leaking RHBFST is idle, operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S1 (idle)or S5 (MOVE) - to rock | OUFM | OUFM5 | OUFM_OUFM5 | HOUFM1 | Once leaking RHBFST is idle, operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S1 (idle)or S5 (MOVE) - to rock | ORGA1 | ORGA11 | ORGA1_ORGA11 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S1 (idle)or S5 (MOVE) - to rock | ORGA1 | ORGA17 | ORGA1_ORGA17 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S1 (idle)or S5 (MOVE) - to rock | OSUP | OSUP1 | OSUP_OSUP1 | HOSUP1 | Management and the RH Supervisor are contacted by the control room operator and informed that level is dropping in RH Tank. The RH supervisor directs specific actions to the control room and Rover to move fuel from the affected Tank. | 10 hours | CBDTM/THERP | 7.71E-03 | 2.03E-02 | 2.78E-02 | 5 |
| S1 (idle)or S5 (MOVE) - to rock | OXFR | OXFR1 | OXFR_OXFR1 | HOXFR1 | Red Hill facility staff implements the strategy as directed by the RH Supervisor to move fuel from the affected RHBFST. | 10 hours | CBDTM/THERP | 2.41E-02 | 2.14E-02 | 4.50E-02 | 5 |
| S8 (RTS) | OUFM | OUFM4 | OUFM_OUFM4 | HOUFM1 | Operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S8 (RTS) | OUFM | OUFM7 | OUFM_OUFM7 | HOUFM1 | Once RHBFST being returned to service is paused and skin valve closed, AFHE low level alarms; operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S8 (RTS) | ORGA1 | ORGA15 | ORGA1_ORGA15 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S8 (RTS) | ORGA1 | ORGA13 | ORGA1_ORGA13 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S8 (RTS) | OSUP | OSUP5 | OSUP_OSUP5 | HOSUP1 | Management and Red Hill Supervisor Formulate Fuel Movement Strategy. | 10 hours | CBDTM/THERP | 7.71E-03 | 2.03E-02 | 2.78E-02 | 5 |
| S8 (RTS) | OXFR | OXFR4 | OXFR_OXFR4 | HOXFR1 | Red Hill facility staff implements the strategy as directed by the RH Supervisor to move fuel from the affected RHBFST. | 10 hours | CBDTM/THERP | 2.41E-02 | 2.14E-02 | 4.50E-02 | 5 |
| S2 (Nozzle) | OSUM | OSUM1 | OSUM_OSUM1 | HOSUM1 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. If fuel movement is in progress, it is ended by CR. | 3 hours | CBDTM/THERP | 2.30E-02 | 2.29E-02 | 4.53E-02 | 5 |

**Table 8-20. Post-Initiator HFE HEP Summary (Continued)**

| Sequence Descriptor | Top Event Name | Split Fraction Name | HFE Basic Event Name | HFE HEP Variable Name | HFE Description | Assumed Success Time Window | Method | $P_{cog}$ | $P_{exe}$ | Total HEP | Error Factor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| S2 (Nozzle) | OSUM | OSUM2 | OSUM_OSUM2 | HOSUM2 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. If fuel movement is in progress, it is ended by CR. | 3 hours | CBDTM/THERP | 2.70E-02 | 2.29E-02 | 4.92E-02 | 5 |
| S2 (Nozzle) | OPAN | OPAN1 | OPAN_OPAN1 | HOPAN1 | Given fuel line leak to LAT operators and Rover decide to actuate the Panic button actions (closes skin valves and also stops any operating cargo pumps). Then manually follow up to close the ball valve(s). | 3 hours | CBDTM/THERP | 1.60E-02 | 5.65E-02 | 7.16E-02 | 5 |
| S2 (Nozzle) | OUFM | OUFM2 | OUFM_OUFM2 | HOUFM1 | Operators detect low level RHBFST level alarm(s) and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S2 (Nozzle) | ORGA1 | ORGA12 | ORGA1_ORGA12 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank; **or informs CR operators of evacuation due to fuel vapors.** | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S2 (Nozzle) | OSUP | OSUP2 | OSUP_OSUP2 | HOSUP1 | Management and the RH Supervisor are contacted by the control room operator and informed that level is dropping in RH Tank. The RH supervisor directs specific actions to the control room and Rover to move fuel from the affected Tank. | 10 hours | CBDTM/THERP | 7.71E-03 | 2.03E-02 | 2.78E-02 | 5 |
| S2 (Nozzle) | OXFR | OXFR2 | OXFR_OXFR2 | HOXFR1 | Red Hill facility staff implements the strategy as directed by the RH Supervisor to move fuel from the affected RHBFST. | 10 hours | CBDTM/THERP | 2.41E-02 | 2.14E-02 | 4.50E-02 | 5 |
| S3 (FI-LAT idle) | OPFL | OPFL1 | OPFL1 | HOPFL1 | Sequence involves noticeable drop in fuel line pressure | 1 hour | CBDTM/THERP | 6.30E-03 | 2.26E-02 | 2.88E-02 | 5 |
| S3 (FI-LAT idle) | OSUM | OSUM3 | OSUM_OSUM3 | HOSUM1 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. Presence of fuel vapor in LAT is also a cue. | 3 hours | CBDTM/THERP | 2.30E-02 | 2.29E-02 | 4.53E-02 | 5 |
| S3 (FI-LAT idle) | OSUM | OSUM4 | OSUM_OSUM4 | HOSUM2 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. Presence of fuel vapor in LAT is also a cue. | 3 hours | CBDTM/THERP | 2.70E-02 | 2.29E-02 | 4.92E-02 | 5 |
| S3 (FI-LAT idle) | OSEC | OSEC3 | OSEC_OSEC3 | HOSEC3 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section. | 3 hours | CBDTM/THERP | 1.90E-02 | 5.65E-02 | 7.44E-02 | 5 |
| S3 (FI-LAT idle) | OSEC | OSEC4 | OSEC_OSEC4 | HOSEC4 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section. | 3 hours | CBDTM/THERP | 1.90E-02 | 5.65E-02 | 7.44E-02 | 5 |
| S3 (FI-LAT MOVE) | OSUM | OSUM5 | OSUM_OSUM5 | HOSUM1 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. Presence of fuel vapor in LAT is also a cue. | 3 hours | CBDTM/THERP | 2.30E-02 | 2.29E-02 | 4.53E-02 | 5 |

**Table 8-20. Post-Initiator HFE HEP Summary (Continued)**

| Sequence Descriptor | Top Event Name | Split Fraction Name | HFE Basic Event Name | HFE HEP Variable Name | HFE Description | Assumed Success Time Window | Method | $P_{cog}$ | $P_{exe}$ | Total HEP | Error Factor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| S3 (Fl-LAT MOVE) | OSUM | OSUM6 | OSUM_OSUM6 | HOSUM2 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. Presence of fuel vapor in LAT is also a cue. | 3 hours | CBDTM/THERP | 2.70E-02 | 2.29E-02 | 4.92E-02 | 5 |
| S3 (Fl-LAT MOVE) | OSEC | OSEC2 | OSEC_OSEC2 | HOSEC3 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section. | 3 hours | CBDTM/THERP | 1.90E-02 | 5.65E-02 | 7.44E-02 | 5 |
| S3 (Fl-LAT MOVE) | OSEC | OSEC5 | OSEC_OSEC5 | HOSEC4 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section | 3 hours | CBDTM/THERP | 1.90E-02 | 5.65E-02 | 7.44E-02 | 5 |
| S3 (Fl-LAT MOVE) | OPAN | OPAN2 | OPAN_OPAN2 | HOPAN1 | Given fuel line leak to LAT operators and Rover decide to actuate the Panic button actions (closes skin valves and also stops any operating cargo pumps). Then manually follow up to close the ball valve(s). | 3 hours | CBDTM/THERP | 1.60E-02 | 5.65E-02 | 7.16E-02 | 5 |
| S3 (Fl-LAT MOVE) | OPAN | OPAN3 | OPAN_OPAN3 | HOPAN1 | Given fuel line leak to LAT operators and Rover decide to actuate the Panic button (closes skin valves and also stops any operating cargo pumps). Then manually follow up to close the ball valve(s). | 3 hours | CBDTM/THERP | 1.60E-02 | 5.65E-02 | 7.16E-02 | 5 |
| S3 (Fl-LAT MOVE) | OUFM | OUFM3 | OUFM_OUFM3 | HOUFM1 | Operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S3 (Fl-LAT MOVE) | ORGA1 | ORGA14 | ORGA1_ORGA14 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |
| S3 (Fl-LAT MOVE) | OSUP | OSUP4 | OSUP_OSUP4 | HOSUP1 | Management and Red Hill Supervisor Formulate Fuel Movement or Delayed Fuel Line Isolation Strategy. | 10 hours | CBDTM/THERP | 7.71E-03 | 2.03E-02 | 2.78E-02 | 5 |
| S3 (Fl-LAT MOVE) | OXFR | OXFR3 | OXFR_OXFR3 | HOXFR1 | Red Hill facility staff implements the strategy as directed by the RH Supervisor to move fuel from the affected Tank. | 10 hours | CBDTM/THERP | 2.41E-02 | 2.14E-02 | 4.50E-02 | 5 |
| S9 (OVERFILL) | OEV | OEV1 | OEV_OEV1 | HOEV1 | Operators correctly specify evolution and stop evolution at planned RHBFST level. | 10 hours | CBDTM/THERP | 1.30E-02 | 4.30E-04 | 1.34E-02 | 5 |
| S9 (OVERFILL) | OTRIP | OTRIP1 | OTRIP_OTRIP1 | HOTRIP1 | After AFHE high level alarm, Operators actuate an emergency stop of the cargo pumps or press the panic button, then direct the Rover to locally ensure the skin valve closed and to manually gauge the same RHBFST. | 5 hours | CBDTM/THERP | 9.30E-03 | 2.26E-02 | 3.17E-02 | 5 |
| S9 (OVERFILL) | OUFM | OUFM6 | OUFM_OUFM6 | HOUFM1 | Following the end of the inadvertent overfilling, the operators detect low level RHBFST level alarm(s) and direct RH Rover to ensure skin valve closed and manually gauge the affected tank. | 10 hours | CBDTM/THERP | 1.93E-02 | 2.29E-02 | 4.18E-02 | 5 |
| S9 (OVERFILL) | ORGA1 | ORGA16 | ORGA1_ORGA16 | HORGA11 | Rover first goes to affected RH tank AND ensures skin valve is fully closed and the ball valve is closed, then manually gauges affected tank. | 10 hours | CBDTM/THERP | 1.30E-02 | 2.60E-03 | 1.56E-02 | 5 |

**Table 8-20. Post-Initiator HFE HEP Summary (Continued)**

| Sequence Descriptor | Top Event Name | Split Fraction Name | HFE Basic Event Name | HFE HEP Variable Name | HFE Description | Assumed Success Time Window | Method | $P_{cog}$ | $P_{exe}$ | Total HEP | Error Factor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| S9 (OVERFILL) | OSUP | OSUP6 | OSUP_OSUP6 | HOSUP1 | Management and the RH Supervisor are contacted by the control room operator and informed that level is dropping in RH Tank. The RH supervisor directs specific actions to the control room and Rover to move fuel from the affected Tank. | 10 hours | CBDTM/THERP | 7.71E-03 | 2.03E-02 | 2.78E-02 | 5 |
| S9 (OVERFILL) | OXFR | OXFR5 | OXFR_OXFR5 | HOXFR1 | Red Hill facility staff implements the strategy as directed by the RH Supervisor to move fuel from the affected RHBFST. | 10 hours | CBDTM/THERP | 2.41E-02 | 2.14E-02 | 4.50E-02 | 5 |

### 8.3.5.2 Post-Initiator HFE HEP Reasonableness Checks

The reasonableness of the RHBFSF QRVA HEPs is examined in Table 8-21. The HFEs are sorted by HEP. As the approach in the SHARP1 is to reflect the culmination of the performance shaping factors in the stress level, the stress level is listed in the *Stress* column. There is not a "linear" relationship between stress and HEP in the range between 1E-04 and 1E-01, as the HEPs are also impacted by time available for recovery, recovery factors, and level of dependence, which are examined in Table 8-22. However, it is reasonable to expect that the HEPs on the high end are correlated with high stress while the HEPs at the lower end are correlated with moderate or low stress.

Assumed action timing for the RHBFSF HFEs is presented in Table 8-22 below. The ratio of $T_{rec}$ (time available for recovery) to $T_M$ (manipulation time) and $T_{1/2}$ (median response time) is calculated as $T_{ratio}$. If $T_{ratio}$ is less than 1.0, the execution cannot be repeated in the time available for recovery, and no recovery should be credited for such cases. As $T_{ratio}$ > 1.0, there are no cases for which recovery cannot be applied. For $T_{ratio}$ > 1.0, execution recovery could be credited *if* there are sufficient resources to perform the recovery.

## Table 8-21. HEP Stress Check

| HFE HEP Variable Name | HFE HEP Variable Description | Total HEP | Stress |
|---|---|---|---|
| HOPAN1 | Given fuel line leak to LAT operators and Rover decide to actuate the Panic button actions (closes skin valves and also stops any operating cargo pumps). Then manually follow up to close the ball valve(s). | 5.68E-02 | High |
| HOSEC3 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section. | 5.68E-02 | High |
| HOSEC4 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section (6"). | 5.68E-02 | High |
| HOSUM1 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. If fuel movement is in progress, it is ended by CR. | 2.31E-02 | High |
| HOSUM2 | Control room operator or Rover (from gauger station) detects fuel vapor and flow in LAT and identifies the leak location. If fuel movement is in progress, it is ended by CR. | 2.31E-02 | High |
| HOUFM1 | Operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | 2.31E-02 | Moderate |
| HOPFL1 | Control room operator detects noticeable drop in fuel line pressure. | 2.29E-02 | High |
| HOTRIP1 | After AFHE high level alarm, Operators actuate an emergency stop of the cargo pumps or press the panic button, then direct the Rover to locally ensure the skin valve closed and to manually gauge the same RHBFST. | 2.29E-02 | Moderate |
| HOXFR1 | Red Hill staff moves fuel from the leaking tank. | 2.17E-02 | High |
| HOSUP1 | Red Hill Operations Supervisor and Management formulate a plan for response. | 2.05E-02 | Moderate |
| H0CR1 | Operators notice change in affected tank level since prior midnight reading and direct the Rover to check the skin valve position and manually gauge the affected tank. | 3.14E-03 | Moderate |

## Table 8-21. HEP Stress Check (Continued)

| HFE HEP Variable Name | HFE HEP Variable Description | Total HEP | Stress |
|---|---|---|---|
| HORGA11 | RH Rover first goes to affected RH tank and ensures skin valve is fully closed and the ball valve is closed, then manually gauges the affected tank. | 2.87E-03 | Moderate |
| HOEV1 | Operators correctly specify evolution and stop evolution when planned. | 7.00E-04 | Low |

## Table 8-22. RHBFSF Post-Initiator HFE Timing

| HFE HEP Variable Name | Description | Time Unit | T(sw) | T(cog) | T(exe) | T(d) | T(rec) | T(ratio) |
|---|---|---|---|---|---|---|---|---|
| HOEV1 | Operators correctly specify evolution and stop evolution when planned. | Minutes | 600 | 10 | 1 | 5 | 584.00 | 585.00 |
| HORGA11 | RH Rover first goes to affected RH tank and ensures skin valve is fully closed and the ball valve is closed, then manually gauges the affected tank. | Minutes | 600 | 10 | 105 | 3 | 482.00 | 5.59 |
| HOUFM1 | Operators reset UFM alarm and direct Rover to ensure skin valve closed and manually gauge the affected tank. | Minutes | 600 | 10 | 3 | 3 | 584.00 | 195.67 |
| HOSUP1 | Red Hill Operations Supervisor and Management formulate a plan for response. | Minutes | 600 | 180 | 60 | 3 | 357.00 | 6.95 |
| HOPFL1 | Control room operator detects noticeable drop in fuel line pressure. | Minutes | 60 | 20 | 3 | 5 | 32.00 | 11.67 |
| HOTRIP1 | After AFHE high level alarm, Operators actuate an emergency stop of the cargo pumps or press the panic button, then direct the Rover to locally ensure the skin valve closed and to manually gauge the same RHBFST. | Minutes | 300 | 10 | 1 | 3 | 286.00 | 287.00 |
| HOPAN1 | Given fuel line leak to LAT operators and Rover decide to actuate the Panic button actions (closes skin valves and also stops any operating cargo pumps). Then manually follow up to close the ball valve(s). | Minutes | 180 | 10 | 1 | 60 | 109.00 | 110.00 |
| HOSEC3 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section. | Minutes | 180 | 10 | 1 | 60 | 109.00 | 110.00 |
| HOSEC4 | CR Operators Close Customer Valve and Fuel Line Sectional Valve(s) above leaking fuel line section (6"). | Minutes | 180 | 10 | 1 | 60 | 109.00 | 110.00 |

## Table 8-22. RHBFSF Post-Initiator HFE Timing (Continued)

| HFE HEP Variable Name | Description | Time Unit | T(sw) | T(cog) | T(exe) | T(d) | T(rec) | T(ratio) |
|---|---|---|---|---|---|---|---|---|
| H0CR1 | Operators notice change in affected tank level since prior midnight reading and direct the Rover to check the skin valve position and manually gauge the affected tank. | Minutes | 600 | 10 | 105 | 3 | 482.00 | 5.59 |
| HOXFR1 | Red Hill staff moves fuel from the leaking tank. | Minutes | 600 | 60 | 60 | 3 | 477.00 | 8.95 |
| HOSUM1 | Control room operator or Rover (from gauger station) recognizes LAT main sump pump start alarm or auto door closure, and identifies the leak location. If fuel movement is in progress, it is ended by CR. | Minutes | 180 | 10 | 3 | 120 | 47.00 | 16.67 |
| HOSUM2 | Control room operator or Rover (from gauger station) detects fuel vapor and flow in LAT and identifies the leak location. If fuel movement is in progress, it is ended by CR. | Minutes | 180 | 10 | 3 | 120 | 47.00 | 16.67 |

### 8.3.5.3 Identification

The RHBFSF QRVA post-initiator HFE identification task was performed by the event sequence analysis team using methods and guidance described in detail in NUREG-1624, *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)* (Reference 8-3), and by applying experience from other QRVA projects. The list of HFEs specifically identified for application in the RHBFSF QRVA is summarized in Table 8-20.

### 8.3.5.4 Definition and Quantification

The RHBFSF QRVA HFEs identified in this analysis were quantified using the SHARP1 method. Details of each HFE HEP quantification, including input data and assumptions are provided in [redacted]. For the actions specifically applicable to the RHBFSF QRVA, the project team analysts recommend application of the CBDTM/THERP method HEP results from the SHARP1 calculations. These are the results presented in Table 8-20. In many cases the SHARP1 analyses showed that the "preferred" method HEP results come from the Annunciator Response/THERP method, which typically yields lower HEP results. However, the HRA team for this project has recommended the application of the CBDTM/THERP results for the spectrum of timing and facility conditions associated with the RHBFSF QRVA HRA. As the HFE evaluations presented in [redacted] are taken directly from the preferred SHARP1 process, in most cases the Annunciator Response/THERP method, results are presented. This was done intentionally to allow for reviewer comparison of results. The RHBFSF QRVA HRA team maintains, however, that the CBDTM/THERP method results are more appropriate for application in the RHBFSF QRVA quantification. All other information provided in [redacted] applied equally as well for all the SHARP1 methods, including the CBDTM/THERP method.

## 8.4 Section 8 References

8-1 Swain, A. D., and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, 1983.

8-2 An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, 1992, EPRI-TR-100259.

8-3 Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Revision 1, May 2000, U.S. Nuclear Regulatory Commission, NUREG-1624.

8-4 Systematic Human Action Reliability Procedure, 1984, EPRI NP-3583.

8-5 SHARP1 – A Revised Systematic Human Action Reliability Procedure, 1990, EPRI NP-7183-SL.

8-6 Swain, A. D., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, 1987.

# 9. Event Sequence Quantification

## 9.1 Introduction

Event sequence quantification is the logical extension of event sequence analysis, wherein the initiating event data, the hardware response data, and human reliability data, and the event sequence analysis model (the comprehensive Boolean logic model, which includes event trees and fault trees) are combined to quantify risk for the QRVA.

## 9.2 Bases and Assumptions

The bases and assumptions for the development of the event sequence quantification are summarized below.

1. For equipment failures or human failure events that occur that prevent leak isolations, where applicable (e.g., isolation of a leaking fuel line), no credit is taken in the sequence models for recovery or repair.

2. A sequence quantification cutoff of 1E-12 per year is used for the base case calculation; i.e., the results are converged for this level of cutoff. All individual sequence frequencies with lower frequencies are discarded, because they are not significant.

3. A sequence quantification cutoff of 1E-15 per year is used for calculations of importance measures.

## 9.3 QRVA Event Sequence Quantification General Methodology

The likelihood of a sequence is quantified by reference to a "thought experiment" in which the facility in question is imagined to be operated for many, many billions or trillions of years. We then ask ourselves, "In this experiment, how frequently, in times per operating year, does this accident sequence occur?" This frequency is referred to as the "sequence frequency", or, if the sequence is represented by a path in an event tree, it could be called the "path frequency".

Since we have not, in fact, done this experiment, we cannot, of course, say what this sequence frequency is with complete certainty. However, we can logically infer some things about this frequency from the frequencies of the "elemental" events that make up the sequence; i.e., the split fractions.

These elemental frequencies are themselves known only within a certain degree of accuracy, which can be expressed by giving a probability curve for each elemental frequency. These elemental probability curves can then be combined or "propagated" appropriately to develop probability curves for the frequencies of the accident sequences, if desired.

In the thought experiment, let $\phi(I)$ be the frequency per facility-year with which the initiating event I occurs. This is then the frequency of the left end, or "trunk", of the tree in Figure 9-1. It is then split up into the frequencies of the various branches. Thus, now consider all the instances in our thought experiment when Event I occurred and let $f(A|I)$ be the fraction of those instances in which System A succeeded; i.e., was available. Then $f(A|I)$ is the fraction of those sequences entering Node A that emerges through the upper branch at the right of Node A.

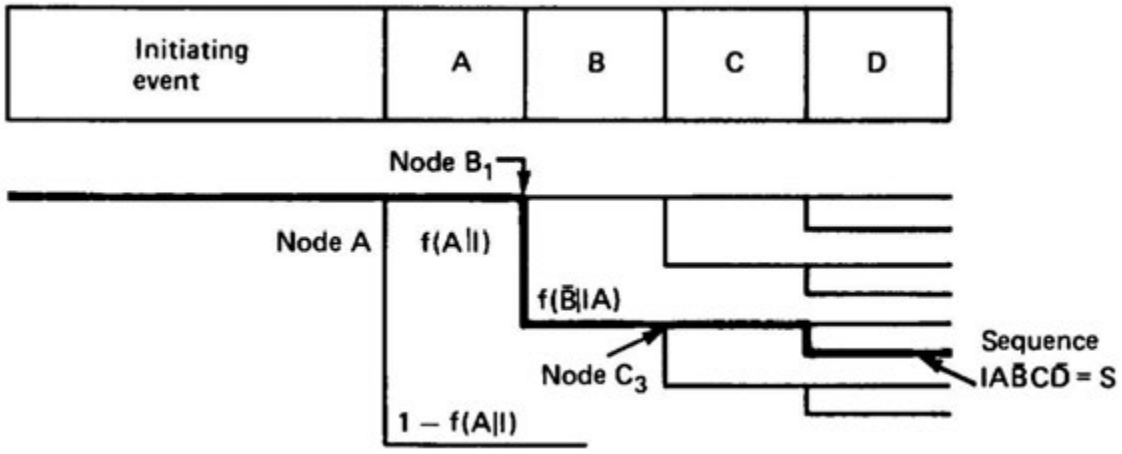



**Figure 9-1. Sample Event Tree**

In the thought experiment, then, $\phi(I)\ f(A|I)$ is the number of sequences, per facility-year, that enter Node $B_1$. Out of all those sequences, let $f(\bar{B}|IA)$ be the fraction that emerges from $B_1$ along the lower branch. The term is $f(\bar{B}|IA)$ then the split fraction at Node $B_1$.

Proceeding in this way, we can finally express the frequency of sequence s, in our thought experiment, in terms of $\phi(I)$ and the split fractions along the path. Thus,

$$\phi(S) = \phi(I)|f(A|I)\ f(\bar{B}|IA)\ f(C|IA\bar{B})\ f(\bar{D}|IA\bar{B}C)$$

where

$\phi(S)$ = the frequency of Accident Sequence S

$\phi(I)$ = the frequency of Initiating Event I

$f(A|I)$ = the frequency of success for System A, given that I has happened (i.e., the split fraction at Node A)

$f(\bar{B}|IA)$ = the frequency of failure for System B, given that I has happened and A has succeeded (the split fraction at Node B1)

$f(C|IA\bar{B})$ = the frequency of success for System C, given that I has happened, A has succeeded, and B has failed

$f(\bar{D}|IA\bar{B}C)$ = the frequency of failure for System D, given I, A, B, and C

From this equation, therefore, we can calculate the frequency of Sequence S from $\phi(I)$, which comes directly from data analysis (see Chapter 5 of NUREG/CR-2300), and from the split fractions that come from system fault trees.

Note that these fault trees must be specialized to each branch point. Thus, for example, suppose A and B were support systems. Then $f(C|IA\overline{B})$, the split fraction at Node $C_3$, must be calculated from the system model for System C with the recognition (or "boundary condition") that Support System A is working and Support System B is not.[†††]

The next section elaborates on the development of event trees and the computation of the split fractions. After that, we generalize the example of Figure 9-1 and discuss the calculation of FDB frequencies.

### 9.3.1 Event Tree Split Fraction Quantification

The first step is to develop event trees displaying all the significant intersystem dependences between the frontline systems whose performance is pertinent for the initiating event of interest. These result from common support systems and any other dependences (human error, environmental) judged to be important. The event trees include these support-system operability states as well as those of the frontline systems. Section 3.7.3 of NUREG/CR-2300 illustrates the event-tree development. Note that the pertinent dependences between support systems are to be identified and displayed in the event tree. In addition, multiple branches (reflecting partial success) rather than just binary (success or fail) branches are used where this more appropriately describes the support-system states and facilitates the quantification of the frontline system. For example, for the electric power heading of the event tree with, say, two buses supplying the safety systems, four branches would be included in the event tree to describe the availability of electric power. These branches would represent "both buses working", "Bus 1 working and Bus 2 failed", "Bus 1 failed and Bus 2 working", and "both buses failed".

When the event trees have been completed, the split fractions in the event trees are determined from logic models for the system or top event under the conditions represented by the particular branch point or node in question. The system logic models are usually in the form of fault trees, but they can be reliability block diagrams, GO models, subevent trees, FMEA models, or any other kind of model, all of these forms, if properly done, being logically equivalent.

Simple fault trees are then written to relate the state of the top event system to the states of its components. From the minimal cut sets of these trees, we can obtain the necessary condition for system failure in terms of sets of component failures. That is, the system does not fail unless at least one cut set of components fails.

The question then devolves upon what could cause the failure of one of these cut sets. The answers to this question are recorded and systematized through the use of a cause table (see Figure 9-2 for an abbreviated example). In this table, all possible causes

[†††] This can often be conveniently accomplished as suggested in Section 3.7.3.3 of NUREG/CR-2300 by writing a single fault tree for System C in which the states of Systems A and B are regarded as "house events". It is not necessary to do this, however.

("candidate" causes) are listed in the left column. Each cause is then evaluated as part of the system analysis. The components that would fail from this cause are listed in Column 3. If those components constitute a cut set, thus failing the system, this is noted in Column 4. If a particular cause does result in system failure, the frequency[###] of that failure is recorded in Column 2. (More specifically, what is recorded here is the fraction of times in our thought experiment that the system fails at the branch point in question as a result of this particular cause.)

The sum of the entries in Column 2 (i.e., the sum of all frequencies of system-failure causes) is the split fraction for system failure at the branch point in question. The bottom of the cause table can be used to accommodate the contribution from "other" causes; i.e., from all causes not otherwise called out in the table. If such entries are used, the analyst should be careful to list all contributors to "other causes".

If the system should fail as a result of a particular cause, we then ask whether that same cause might also result in some other system failing or in an initiating event. If so, then it is a potential "common" cause and needs to be called out for special treatment in the analysis. Columns 5 and 6 in the cause table are used to call attention to such situations. Because split fractions are simply multiplied together, the identification of dependent failures in the cause table and subsequently in the event tree is critical and should be given a great deal of attention.

[###] These, along with the $\phi(I)$, are examples of elemental frequencies.

| Cause | Failure Frequency | Effect | | | |
|---|---|---|---|---|---|
| | | Components | System | Other Systems | Initiating Events |
| Coincident Hardware Failures | $4.5 \times 10^{-6}$ | Mainly Pumps | Fails | No Effect | No Effect |
| Testing | $1.0 \times 10^{-10}$ | Pumps | No Effect | No Effect | No Effect |
| Maintenance and Hardware Failure | $2.0 \times 10^{-4}$ | Pumps or MV-8700A, B | Fails | No Effect | No Effect |
| Human Error and Hardware Failure | $8.2 \times 10^{-9}$ | MV-8700A, B Closed Failure on Other Side | Fails | No Effect | No Effect |
| Other | $4.6 \times 10^{-5}$ | Valves of Pumps | Fails | No Effect | No Effect |
| Total | $3.0 \times 10^{-4}$ | | | | |

*Dominant contributor = maintenance combined with hardware failure.*

**Figure 9-2. Example of Format for a Cause Table for Double Failures (buses available)**

### 9.3.1.1 Computation of PDB Frequencies

Event trees are not limited as in Figure 9-1 to nodes with two branches. Therefore, to generalize the notation, let $f_{nb}$ denote the split fraction at Node n that goes with Branch A. With these quantities established for each branch point, one can calculate the frequency of each accident-sequence path as

$$\phi(S) = \phi(I) f_{1b,1} f_{2b,2} \ldots f_{nb,n} \ldots \quad (9\text{-}1)$$

$$= \phi(I)\, f(S)$$

where $b_n$ is the branch chosen by the path at Node n.

The term f(S) on the right-hand side, the product of split fractions along a given path, thus has the meaning of "conditional frequency" that is, for all the times Initiating Event I occurs, f(S) is the fraction of times in which accident sequence S results. In this way one can compute the conditional frequency for each path in the tree. These numbers thus characterize the tree itself, without reference to the frequency of the incoming entry state. Each sequence or path culminates in an exit state; i.e., a particular state of operability-functionability with respect to frontline systems.

Now let us focus attention on a particular exit state, say $y_j$, and let $s_{ih}$ denote a particular accident sequence going from Entry State i to Exit State $y_j$. By summing over all such sequences, we obtain

$$m_{ij} = \sum_h f(S_{ih}) \quad (9\text{-}2)$$

The quantity $m_{ij}$ is thus the conditional frequency of occurrence of Exit State $y_j$ given that Initiating Event i has occurred. That is, out of all the times Entry State i occurs, $m_{ij}$ is the fraction of times that Exit State j occurs.

If we now let $\phi(I_i)$ be the frequency of Initiating Event i, then

$$\phi(I_i) m \quad (9\text{-}3)$$

is the frequency of occurrence of Exit State $y_j$ as a result of Initiating Event $I_i$. Moreover,

$$\sum_i \phi(I_i) m_{ij} \quad (9\text{-}4)$$

is the frequency of occurrence of Exit State $y_j$ as a result of all initiating events.

Equation (9-2) can now be recognized in essence as a matrix multiply operation. Thus, if we assemble the $m_{ij}$ into a facility matrix M and the $\phi(I_i)$ into an initiating-event row vector $\phi^I$, then

$$\phi^y = \phi^I M \quad (9\text{-}5)$$

where $\phi^y$ is a row vector containing the frequencies $\phi(Y_j)$ of the various facility damage states $Y_j$.

The process of Equations (9-1) through (9-5) is carried through by first using point estimates (essentially mean values) of all the frequencies and split fractions to obtain point estimates for the frequencies $\phi(Y_j)$. These point estimates can then be used to eliminate from the uncertainty analysis those sequences whose point estimates do not contribute to the point estimate of the result. When point estimates are used, the analyst should ensure that the failure-rate dependences among systems containing components assumed to be identical will not cause a nondominant sequence to become a contributor to the FDB frequency. To determine probability distributions for the $\phi(Y_j)$, we "propagate" the uncertainties in the elemental cause and initiating frequencies through the cause table and through Equations (9-1) through (9-5). In this operation, as in all probabilistic operations, attention must be paid to dependences between probability distributions. Also, as in all arithmetic, minor quantities in the calculation need not be treated with high accuracy, they can be approximated, upper bounded, or rounded off as appropriate, but such shortcuts should be well documented. Such shortcuts are especially useful in the computation of probability curves to avoid unnecessary computational labor.

### 9.3.2 Event Tree Quantification

Two approaches to accident-sequence quantification—fault-tree linking and event trees with boundary conditions—have been described. Both make use of event trees in conjunction with fault trees. Both approaches require some assumptions and approximations to be practical—for example, the truncation of cut sets or the elimination of some dependences by making use of approximations. In the fault-tree-linking technique, the event trees have been constructed at a high level in terms of the function or system success or failure definition: it is necessary to display only the frontline functions or systems. The dependences on support systems and subsystems are accommodated entirely within the fault trees. The resultant linked fault trees are thus large and complex. When the fault trees and event trees are large, the existence of automated and efficient computer reduction techniques makes analysis by this approach possible in spite of the many cut sets that can be generated for quantification.

In the other quantification method, which uses event trees with boundary conditions, the more elaborate event trees are broken down to explicitly display the significant dependences. The resultant fault trees (or reliability block diagrams) for the event tree top events are thus simpler and independent, and can be analyzed by hand without resorting to computer-assisted fault-tree reduction. Heavy reliance is placed on the analyst to identify and separate the dependences in the event tree modeling. Considerable care must therefore be taken to ensure that the significant dependences in a sequence have either been identified and included as top events in the event tree or are otherwise accounted for in generating the split fractions along an accident sequence path.

It should be noted that the use of event trees with boundary conditions generally yields many more sequences because of its evaluation for the various mutually exclusive support-system states. Several such sequences would combine to result in the same frontline-system configuration as that identified in fault-tree linking.

Overall, the basic conceptual difference between the methods is where in the process quantification (conversion from symbolic representation to numerical results) takes

place: stepwise throughout the process (for event trees with boundary conditions) or as a single step near the end (for fault-tree linking). Both methods can be successfully employed and have been used in major studies performed to date. An advantage of stepwise quantification is a reduction in the need to carry through algebraic terms, so that quantification can be performed manually. An advantage of quantification as the last step is that the symbolic representation allows computer searches for dependences as the last step before quantification and the presentation of results in terms of cut sets for dominant accident sequences.

## 9.4 Event Sequence Quantification Details

### 9.4.1 Initiating Events

The internal initiating events quantified for the acute release sequence models are presented in Table 9-1 along with their mean frequencies of occurrence. The internal event initiators were first identified in Section 6.4. The initiating event frequencies are quantified using the data variables described in Section 5, and by the use of fault trees, when the complexities of the initiating event require a detailed breakdown of the failure contributors. See Section 7.

**Table 9-1. List of Sequence Groups Evaluated in the QRVA**

| Sequence Group ID | Sequence Group Description |
|---|---|
| AGT1 | All acute IEs with fuel release |
| BGT30 | All acute IEs with fuel release >30k gallons |
| CGT60 | All acute IEs with fuel release >60k gallons |
| DGT120 | All acute IEs with fuel release >120k gallons |
| EGT250 | All acute IEs with fuel release >250k gallons |
| F24GT1 | Fuel F24 acute IEs with fuel release |
| F24GT120 | Fuel F24 acute IEs with fuel release >120k gallons |
| F24GT1M | Fuel F24 acute IEs with fuel release >1 Million gallons |
| F76GT1 | Fuel F76 acute IEs with fuel release |
| F76GT120 | Fuel F76 acute IEs with fuel release >120k gallons |
| F76GT1M | Fuel F76 acute IEs with fuel release >1 Million gallons |
| FGT500 | All acute IEs with fuel release >500k gallons |
| GGT1M | All acute IEs with fuel release >1 Million gallons |
| HGT2M | All acute IEs with fuel release >2 Million gallons |
| IDLEGT1 | While Idle All acute IEs with fuel release |
| IDLEGT120 | While Idle acute IEs with fuel release >120k gallons |
| IDLEGT1M | While Idle acute IEs with fuel release >1 Million gallons |

## Table 9-1. List of Sequence Groups Evaluated in the QRVA (Continued)

| Sequence Group ID | Sequence Group Description |
|---|---|
| IGT10M | All acute IEs with fuel release >10 Million gallons |
| ISSUEGT1 | While issuing acute IEs with fuel release |
| ISSUEGT120 | While issuing acute IEs with fuel release >120k gallons |
| ISSUEGT1M | While issuing acute IEs with fuel release >1 Million gallons |
| JLT30 | All acute IEs with fuel release between 1k &30k gallons |
| JP5GT1 | Fuel JP5 acute IEs with fuel release |
| JP5GT120 | Fuel JP5 acute IEs with fuel release >120k gallons |
| JP5GT1M | Fuel JP5 acute IEs with fuel release >1 Million gallons |
| KLT60 | All acute IEs with fuel release between 30k &60k gallons |
| LLT120 | All acute IEs with fuel release between 60k &120k gallons |
| MAINTGT1 | Maintenance error with fuel release |
| MAINTGT120 | Maintenance Error with fuel release >120k gallons |
| MAINTGT1M | Maintenance Error with fuel release >1 Million gallons |
| MLT250 | All acute IEs with fuel release between 120k &250k gallons |
| NLT500 | All acute IEs with fuel release between 250k &500k gallons |
| NOZGT1 | Nozzle with fuel release |
| NOZGT120 | Nozzle with fuel release >120k gallons |
| NOZGT1M | Nozzle with fuel release >1 Million gallons |
| OLT1M | All acute IEs with fuel release between 500k &1million gallons |
| OVFGT1 | Overfill with fuel release |
| OVFGT120 | Overfill with fuel release >120k gallons |
| OVFGT1M | Overfill with fuel release >1 Million gallons |
| PLT2M | All acute IEs with fuel release between 1 & 2 million gallons |
| QLT10M | All acute IEs with fuel release between 2 & 10 million gallons |
| RECEVGT1 | While receiving acute IEs with fuel release |
| RECEVGT120 | While receiving acute IEs with fuel release >120k gallons |
| RECEVGT1M | While Receiving acute IEs with fuel release >1 Million gallons |
| ROCKGT1 | All Leaks to Rock with fuel release |
| ROCKGT120 | Leak to Rock with fuel release >120k gallons |
| ROCKGT1M | Leak to Rock with fuel release >1 Million gallons |
| RTSGT1 | RTS Leak to Rock with fuel release |
| RTSGT120 | RTS Leak to Rock with fuel release >120k gallons |

**Table 9-1. List of Sequence Groups Evaluated in the QRVA (Continued)**

| Sequence Group ID | Sequence Group Description |
|---|---|
| RTSGT1M | RTS Leak to Rock with fuel release >1 Million gallons |
| TUNGT1 | Tunnel with fuel release |
| TUNGT120 | Tunnel with fuel release >120k gallons |
| TUNGT1M | Tunnel with fuel release >1 Million gallons |
| XFERGT1 | While inter-tank transfer acute IEs with fuel release |
| XFERGT120 | While inter-tank transfer acute IEs with fuel release >120k gallons |
| XFERGT1M | While inter-tank transfer acute IEs with fuel release >1 Million gallons |

### 9.4.2 Event Tree Linking

The event trees used for accident sequence quantification are presented earlier in Sections 6.7.1 through 6.7.8. Figure 9-3 (a repeat of Figure 6-8), shows how the different event trees are linked together to form an entire acute release accident sequence. A brief description of the role of each event tree is presented below. Refer to Section 6.7 for details on each event tree. Each complete acute release, accident sequence requires that five event trees be linked together. Each partial sequence fragment from the upstream tree then transfers to all branches of the next downstream tree.

The CONFIG event tree, as its name implies, describes the status of the different modes of operation of the Red Hill facility that may be on going at the time of an initiating event. The configuration tree also identifies the specific RHBFST that is associated with a specific leak location. The same CONFIG event tree is used for all internal initiating events. For most of the initiators, the branch point probabilities are determined simply by the fractions of time spent in different fuel movement states; i.e., idle, receiving, issuing, or undergoing inter-RHBFST gravity transfers. However, for a limited number of initiators (e.g., maintenance errors evaluated for conditions while idle separately from times when a fuel movement is in progress), then the branch probabilities are changed to reflect the conditional status of the specific initiating event. For these, the initiator occurrence frequency already includes the fraction of time spent in the single idle or fuel movement condition. Therefore, the fraction of time spent with the RHBFST idle is assigned a value of 1.0, and all other fuel movement states (as presented by Top Event MOVE) are assigned a split fraction of 0.0.

The second event tree for each internal initiating event is the ELECTRICAL event tree. This event tracks the availability of each of the electrical systems applicable to operation at the RHBFSF; i.e., both at the UGPH and at the RHBFSF. Ventilation systems used to support electrical equipment are included in the ELECTRICAL event tree.

The third event tree for each internal initiating event is the OTHERSUP event tree. This event tracks the availability of support systems other than electrical systems. It also tracks the impact on other selected systems at Red Hill. Losses of particular electrical

buses impacts the availability of power on other systems; e.g., on Red Hill sectional valves, lighting, etc.

The fourth event tree for each internal initiating event is the VALVES event tree. This event tracks the availability of key valves applicable to each sequence; e.g., the skin and ball valves of the affected RHBFST, and for a second RHBFST that may be aligned for inter-RHBFST gravity transfer. Since these valves are shared between different required fuel movement functions, it is useful to question their availability once and in a separate top event of its own.

The fifth event tree in each acute release accident sequence is a frontline event tree. The states of the top events in the early frontline trees represent the facility response to the specific initiating event. Only one frontline event tree is used in each linked sequence model, and all internal initiating events are assigned to only one frontline event tree. Section 6.7 described the frontline event tree used for each internal initiating event.

Each complete path through the linked event tree models is assigned an end state representing the gallons of fuel released for that single sequence. End state assignment logic, or binning rules, is not used for any of the earlier four event trees in the linked set; only for the last event tree in the linked set. However, the states of all top events in the linked event tree set can be used in the logic for assigning end states. The evaluation of the gallons released for each end state is described in Section 6.8. For the QRVA model, more than 500 end states are tracked in the sequence models.

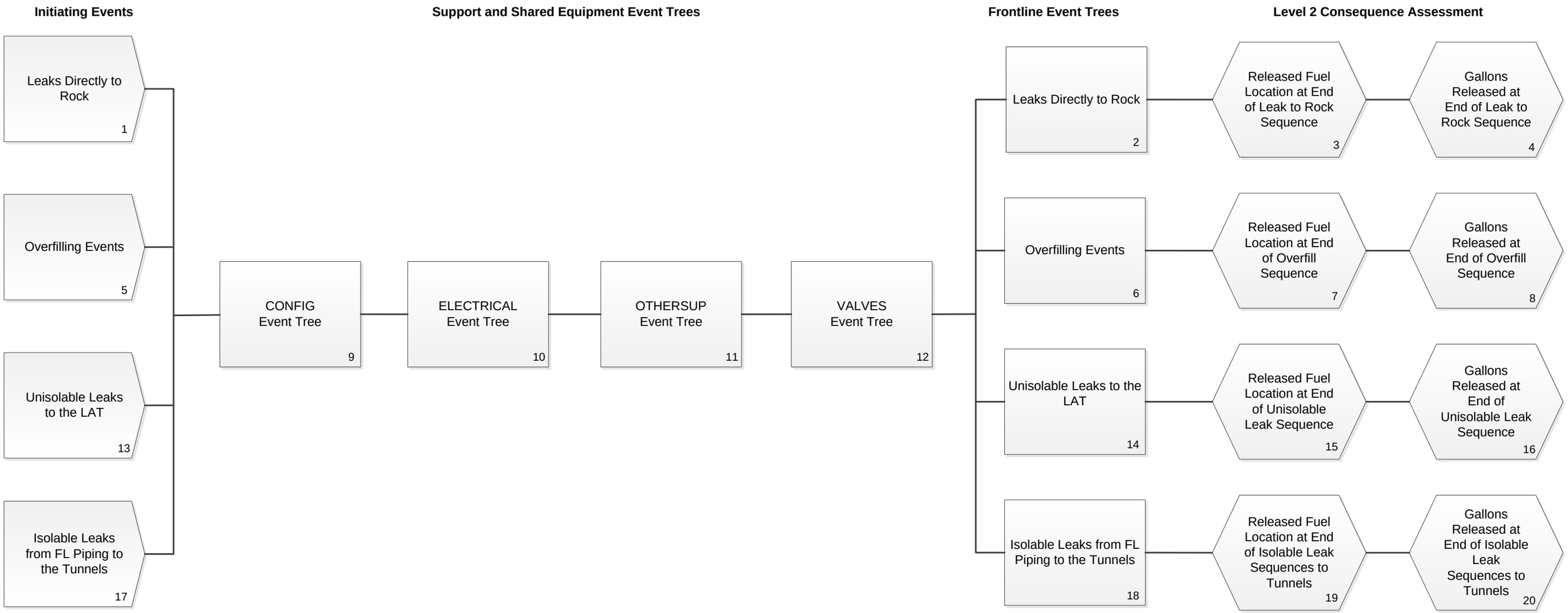



**Figure 9-3. Linking of Event Trees to Form an Entire Acute Sequence**

### 9.4.3 Assignment Logic

The split fraction and plant damage state assignment rules used in each of the event trees are presented in [redacted] in the form of the "RISKMAN Viewer" software which allows anyone to view the inputs and outputs for the RISKMAN model. The RISKMAN Viewer suppresses all quantification features of the full RISKMAN software. The RISKMAN model name for this first phase of the QRVA is RHBFSF1. The RISKMAN Viewer model inputs and outputs are provided in four modules; data analysis, systems analysis, event tree analysis, and the Big Loop Monte Carlo module. The latter is used only to propagate uncertainties in the sequence group frequencies.

The data analysis module contains all the data variable distribution used in the quantification of the RHBFSF system and sequence results. The notes associated with each data variable describe the analytical form of the distribution used and the parameters used in its creation. For some discrete probability distributions, the discrete points were entered by the analyst.

The systems module has several databases but is mostly organized by top events. The quantification of the split fractions for each top event is performed by the systems module. Many of the top events make use of fault trees to facilitate the evaluation of different split fractions. A master frequency file is a compilation of all split fraction results and the importance of basic events to each split fraction. The master frequency is file is used as a means to transfer all results from the systems module to the event tree module for accident sequence frequency quantification. Also in the systems module, is a database of initiating events. Frequency models for all initiating events are entered in this database. Some models refer to data variables developed in the data module, while other initiating event models are derived from fault trees. The initiating event frequencies are also brought over to the event tree module as an attachment to the master frequency file.

The event tree module contains the models for each event tree. This includes the event tree model structures, split fraction assignment logic, and end state assignment logic. The split fraction assignment logic accounts for the functional dependencies between the RHBFSF systems as described in the intersystem dependency tables presented in Section 6.5. In addition, initiator-specific dependencies are imposed via the split fraction assignment logic. End state (or bins) assignment logic is also provided in the RISKMAN Viewer. The assignment logic for each event tree can be reviewed by exercising the RISKMAN Viewer.

The event tree structures in model RHBFSF1 are nearly all formulated as branch everywhere sequence models. This means that every top event branches at all nodes along a single sequence. This sequence model style is in contrast to other accident sequence models which encode top event inter-dependencies by not branching at some nodes. In the RHBFSF1 model, all such dependencies are instead encoded in split fraction assignment rules. The only exception is for the first couple of sequences of the OVERFILL event tree. Refer to Section 6.7.6 for further details on this exception.

For most acute accident sequences, there is a large time available to effect a suitable response to the detection of a leak. Of course any delay in the response will lead to more fuel release before the leak location is uncovered. For the function to isolate an

initial leak, no recoveries were assumed. Instead, the failure to manually isolate a leaking pipe, or to isolate an associated RHBFST from a leaking pipe, was assumed to not be recoverable. However, this omission of recovery is not appropriate for the actions to empty a RHBFST known to be leaking. To accommodate recovery within the acute sequence models for the action to move fuel from a leaking RHBFST, the concept of time delays was used and applied for the start of fuel movement. The extent of the time delay for a specific sequence is specified as a function of top event failures throughout the sequence. If there are multiple failures in a single sequence, the longest delay time is then used in the evaluation of the amount released. The failures could involve operator response failures, or equipment failures. See Section 6.8 for more discussion on the delays, or recovery times considered. For the equipment found to be failed, to estimate the recovery time, it is important to know whether the equipment itself failed or if the supporting systems for that equipment failed preventing its operation; i.e., which equipment must be recovered determines the likely delay time for recovery. Therefore, the split fractions for equipment needed to affect moving fuel from a leaking RHBFST were initially evaluated assuming its supporting systems are available. The intersystem dependencies on supporting systems are instead considered by assignment logic macros on subsequent event responses. As an example, the top event SKIN, representing the closure of a normally open skin valve, is evaluated assuming its supports are working. Its dependence on supporting 480V electric power is instead accounted for by macros establishing the success or failure of isolation. In this way the selection of the delay times for recovery can distinguish whether the valve itself failed to close, or if it failed to close because of a loss of AC power.

### 9.4.4 Quantification Parameters

The RISKMAN software [redacted] is used to perform the acute sequence frequency quantification. All of the initiating events are evaluated in a single batch, but smaller quantification batches of just selected initiating events can also be quantified. When run, the batch evaluates the linked event tree sets of acute sequences for the initiating events listed in the batch. The end states are assigned to each sequence and running totals of the end state frequencies are maintained for later reporting. A sequence frequency cutoff is assigned so that lower frequency sequences can be truncated prior to full evaluation. However, a running sum of the truncated frequency is maintained so that the amount truncated can later be compared against the end state frequency totals to verify convergence.

The RISKMAN software provides an option to save all or some of the sequences quantified. A save sequence frequency cutoff, typically higher than the sequence frequency quantification cutoff previously mentioned, may be specified for each end state. Typically for the QRVA, the save sequence cutoff for a batch run of initiating events is set at 1E-6 per year for all end states. For reports in which more sequences are desired, a save sequence cutoff of 1E-8 per year is used for all end states. For the QRVA model, the 1E-8 per year save sequence cutoff is enough to nearly fill an entire Access database of detailed sequence information.

The specified batch of initiating events also has associated with it a list of sequence groups. These sequence groups serve two purposes. One is that they are a convenient way to define groups of sequences, other than by end states, for later reporting. As an example, a sequence group is defined for only those sequences initiated by a leakage

directly to rock; i.e., ROCKGT1. Another sequence group is for all sequences with greater than 120,000 gallons of fuel released per event; i.e., DGT120. Such sequence groups are made up of many end states. The full list of sequence groups evaluated for the QRVA is provided in Table 9-1.

The second purpose of sequence groups is to establish metrics against which importance measures can be evaluated. The importance measures can be evaluated at different levels of model elements; e.g., by basic event, by component, by split fraction, and by top event state. Sequence group by initiating events and by end states can also be determined.

The acute accident sequence models were quantified for the QRVA using an individual sequence frequency cutoff of 1E-12 per year. When quantified at a much lower individual sequence cutoff of 1E-15 per year, no sequence group frequency increased by more than 0.1%; i.e., indicating that the model has converged. Therefore, the base model is quantified with an individual sequence frequency cutoff of 1E-12 per year and this same cutoff is used for uncertainty calculations. Nevertheless, an individual sequence cutoff frequency of 1E-15 per year is used for all importance measure reports. It is typical that importance measures require greater accuracy to describe low frequency contributors, and so lower cutoffs were used.

### 9.4.5 Saved Sequence Details

When saving a sequence to the Access database within RISKMAN, all sequence details developed for the sequence frequency quantification are saved. Table 9-2 is an example detailed sequence report for one sequence. As the report header describes, this sequence is initiated by the initiating event SF76Bs, which is a small fuel line leak to Section B in the Harbor Tunnel. The sequence frequency is 3.16816E-4 per year. The end state assigned is TUN242, indicating that this analysis used the TUNLEAK frontline response event tree in its linked set of event trees. The evaluated gallons of fuel released is 242,000.

Each row in the table details the status and descriptions of the top events in the linked set of event trees. The top events represented in the five linked event trees are as follows:

- CONFIG: 1–10
- ELECTRICAL: 11–22
- OTHERSUP: 23–36
- VALVES: 37–44
- TUNLEAK: 45–63

Reading the rows of the table it is seen that this sequence involves a leak from Section B while the facility is initially idle. The fuel type is F76. There is no applicable RHBFST because all F76 RHBFSTs are idle. The leak size corresponds to a 0.5” hole. There are no failures of electrical or other support systems. Nor are there any failures of key valves. The sump at the UGPH entry operates, once leakage form the fuel line is detected. The main sump below the tank gallery is not relevant to this sequence. Staff within the Harbor Tunnel and the LAT are assumed to evacuate (Top Event EVAC=EVACU) because of the fuel released. All operator actions considered in

the frontline event tree model are successful. Especially Top Event OSEC, which represents the control room action to close the upgrade sectional valve, is successful. The valve hardware (i.e., Top Event FLISO) is also successful so isolation of the fuel line upgrade of the break location is achieved; i.e., the top event state for ISOL is YES. Leakage from the break is evaluated as 242,000 gallons because the F76 fuel line contents within the Harbor Tunnel is substantial and there is a lag time before the fuel drains to the sump at the UGPH entry and the operators affect the isolation. During this time prior to isolation, fuel upgrade of the eventually isolated sectional valve can also drain into the lower pipe section and be available for release. For this sequence, the action to empty a RHBFST is not applicable since all RHBFSTs are initially in idle. Therefore the delay time is also not relevant.

Top Event Number 63 in the table is REL which is assigned Split Fraction RELF. Split Fraction RELF represents the conditions when there is a relatively limited release of fuel in Sections A or B below the new oil door. What fuel is released from the F76 fuel line is concluded to collect at the UGPH entry. The fuel accumulated in this location is likely well below the aquifer. An assessment of how much fuel, once released to the Harbor Tunnel, seeps into the surrounding rock above the aquifer on its way down the tunnel has not yet been assessed. It is possible that this relatively high frequency sequence may have essentially no impact on the aquifer as the depth of fuel as it flows down the tunnel would be minimal.

Alternative split fractions are assigned to Top Event REL depending on the location that fuel moves to after its release from a RHBFST or a fuel line. See Section 10 for further details.

## Table 9-2. Example Detailed Sequence Report

**Model Name: RHBFSF1** **IE Frequency = 5.0302E-4**

**Master Frequency File: RH22** **End State = TUN242**

**Sequence Index No. 1 for Initiator: SF76BS** **Sequence Frequency = 3.16816E-4**

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 1 | LKLOC | SECB | LKSECB | 1.00E+00 | Location of Leak within Facility | fuel line between 2Y and 3Y |
| 2 | MOVE | IDLE | IDL761 | 9.68E-01 | Type of fuel movement initially in progress | F76 tanks are idle |
| 3 | TKID | NA | TKNOY | 1.00E+00 | RHBFST associated with Leak | leak not via RHBFST |
| 4 | FUEL | F76 | F76Y | 1.00E+00 | Type of Leaking fuel | fuel is F76 |
| 5 | TKXF | NA | TKSNAY | 1.00E+00 | Source RHBFST associated with inter-tank transfer | Inter-tank transfer not in progress |
| 6 | TKLOC | NA | TKLOCY | 1.00E+00 | LAT Fuel Line Section of associated RHBFST relative to fuel line leak to LAT (D/E/NA) | tank location relative to LAT Leak not applicable |
| 7 | HEIGHT | BOT | HIBOTY | 1.00E+00 | Height of Hole in RHBFST that is leaking to rock | FOR NOZZLE LEAKS ALWAYS BOTTOM |
| 8 | SIZE | S2 | SIZS2Y | 1.00E+00 | Size of leak from RHBFST, or Fuel Line Piping | Large leak from fuel line 50 GPM or RH tank 0.5" |
| 9 | DIREC | NA | DIRNAY | 1.00E+00 | Side of RHBFST that leak is on | Not a leak to rock or overflow to rock state NA |
| 10 | INVEN | INA | INVENY | 1.00E+00 | INVEN – Initial RHBFST Inventory Configuration. | FOR INVEN=NA STATES |
| 11 | GRID | S | GRID1 | 2.94E-03 | Offsite Grid | internal events |
| 12 | GRIDR | NOLOOP | GHRY | 1.00E+00 | Recovery from Losses of Offsite Grid | NO LOOP STATE ONLY |

## Table 9-2. Example Detailed Sequence Report (Continued)

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 13 | BUN24 | S | BUN241 | 1.35E-06 | UGPH 2.4 kV Normal Bus | DEFAULT WITH LOOP AVAILABLE |
| 14 | BUN48 | S | BUN481 | 1.35E-06 | UGPH 480V Normal Bus | DEFAULT WITH OFFSITE POWER AVAILABLE |
| 15 | BUE48 | S | BUE481 | 1.35E-06 | UGPH 480V Emergency Bus | HARDWARE FOR TRANSFORMER AND BUS |
| 16 | GEN1 | S | GEN1Y | 0.00E+00 | Backup generator at ADIT for UGPH 480V Emergency Bus | DEFAULT WITH GRID=S |
| 17 | UFAN | S | UFAN1 | 1.59E-05 | ADIT 1 Supply and Exhaust Fans for UGPH cooling Cargo Pumps | Support available fans fail to run |
| 18 | B3EA | S | B3EA1 | 9.03E-04 | ADIT 3 208V Panel A | hardware transformer and Panels B and A |
| 19 | GEN3 | S | GEN3Y | 0.00E+00 | Backup Generator at ADIT 3 for 480V Panels B and A. | DEFAULT, WITH GRID=S |
| 20 | BRN48 | S | BRN481 | 1.35E-06 | Red Hill 480V Normal Bus | Hardware transformer and 480v bus |
| 21 | BRE48 | S | BRE481 | 1.35E-06 | Red Hill 480V Emergency Bus | HARDWARE TRANSFORMER AND PANEL L |
| 22 | GEN5 | S | GEN5Y | 0.00E+00 | Red Hill 480V Emergency Bus | GRID SUCCESSFUL |
| 23 | LPRH | S | LPRH1 | 7.35E-03 | Red Hill Panels Supplying Lighting, Radios, and Cameras | DEFAULT BRE48=S |
| 24 | AFHE | S | AFHE1 | 6.29E-04 | Automatic Fuel Handling Equipment | HARDWARE ASSUMING BUE48=S FOR 24 HOURS |
| 25 | AFHR | S | AFHR1 | 1.55E-02 | AFHE Condensing and Fans for Heat Removal. | DEFAULT BUE48=S |
| 26 | EFAN | S | EFAN1 | 1.31E-05 | Fans for Tanks 1-16 in LAT & UAT fail to operate (also supply Electrical room in LAT) | Fans for Tanks 1-16 fail to run 24 hours |

## Table 9-2. Example Detailed Sequence Report (Continued)

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 27 | TFAN | S | TFAN1 | 1.31E-05 | Fans for tanks 17-20 LAT & UAT fail to operate (above bulkhead) | Fans for Tanks 17-20 to run 24 hours |
| 28 | CRM | S | CRMS | 0.00E+00 | Control Room electrical power, lighting, and Air Conditioning. | CR electrical power available from BUE48 |
| 29 | ACRM | S | ACRMS | 0.00E+00 | Alternate Control Room electrical power, lighting, and Air Conditioning. | BUN480 power is available to ACRM |
| 30 | UHMOV | S | UHMOVS | 0.00E+00 | Electrical Power to UGPH MOVs and Lower Harbor Tunnel MOVs | Electrical power from BUE48 is available |
| 31 | CARGO | S | CARF76 | 9.66E-05 | 2 or more Cargo pumps available to move leaking fuel type | CARGO PUNMPS FOR F76 AVAILABLE |
| 32 | ULIT | S | ULITS | 0.00E+00 | Electrical Power for UGPH Lighting and Lower Harbor Tunnel Lighting. | Electric power from BUN48 is available for4 lighting |
| 33 | EL72 | S | EL721 | 7.47E-03 | Personnel Elevator 72 & Controller. | Electric power from BRE48=S; random failures |
| 34 | EL73 | S | EL731 | 7.47E-03 | Cargo Elevator 73 & Controller. | Electric power from BRE48=S; random failures |
| 35 | RMOV | S | RMOVS | 0.00E+00 | Electrical Power for Red Hill Sectional Valves Down to ADIT 3Y and all LAT MOVs. | Electric power from BRE48 is available |
| 36 | RHIN | S | RHINS | 0.00E+00 | Support for Red Hill Instruments, indications, level alarms, and signals. | Success of AFHE and BRE48 for indications |
| 37 | SKIN | S | SKINS | 0.00E+00 | Successful operation of the skin valve of the RHBFST identified in top event TKID of the configuration even tree | skin valve not applicable so success assumed |
| 38 | BALL | S | BALLS | 0.00E+00 | Successful operation of the ball valve of the RHBFST identified in top event TKID of the configuration even tree | Ball valve not applicable so success assumed |

## Table 9-2. Example Detailed Sequence Report (Continued)

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 39 | SKINX | S | SKNXS | 0.00E+00 | Successful operation of the skin valve of the RHBFST identified in top event TKXF of the configuration even tree | skin valve X not applicable so success assumed |
| 40 | BALLX | S | BALXS | 0.00E+00 | BALLX - Successful operation of the ball valve of the RHBFST identified in top event TKXF of the configuration even tree | BALLX valve X not applicable so success assumed |
| 41 | FLISO | S | FLISO1 | 1.08E-03 | FLISO – Successful Closure of the Upstream Sectional Valve. | hardware failure for closure of sectional valve above section leaking |
| 42 | FLTKC | S | FLTKCS | 0.00E+00 | FLTKC – Successful Isolation of the Fuel Line Leak from All ALIGNED RHBFSTs. | Switch to track skin and ball valves are available to open |
| 43 | FLTKO | S | FLTKO1 | 1.07E-03 | FLTKO – Successful Opening of the Fuel Line from a RHBFST that is to be Emptied. | open one sectional valve |
| 44 | EVAC | EVACU | EVACY | 1.00E+00 | Sequence conditions necessitate initial evacuation from RH | Evacuation is called for by sequence conditions |
| 45 | USUMP | S | USUMP1 | 2.17E-04 | 1 of 2 Harbor Tunnel Sump Pumps At UGPH Entry Start and Transfer Leaked Fuel | 1/of 2 UGPH entry sump pumps operate |
| 46 | MSUMP | F | MSUMPF | 1.00E+00 | 1 of 2 Main Sump Pumps Below Tank Gallery Start and Transfer Leaked Fuel from LAT to S311 | Main sump pumps not effective |
| 47 | DOOR | S | DOOR1 | 2.06E-03 | Oil tight door below LAT gallery closes on high float level | Door closes when needed |
| 48 | OPFL | S | OPFL1 | 3.73E-02 | Operators Recognize Drop in Fuel Line Pressure | Operators recognize FL pressure Drop during leak to tunnels WHILE IDLE |
| 49 | OSUM | S | OSUM3 | 3.73E-02 | CR or RH rover (from gauger station) recognizes sump pump start and identifies the leak | FL leak to LAT while all idle - sump start and door closes |

## Table 9-2. Example Detailed Sequence Report (Continued)

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 50 | OPAN | S | OPAN2 | 7.86E-02 | CR Operators Actuate Cargo Pump Trip and Valve Closures Using Panic Button | Actuate panic button for FL leak to LAT |
| 51 | OSEC | S | OSEC3 | 8.00E-02 | CR Operators REMOTE MANUALLY close sectional valve(s) and ball valves as applicable; execution only | Close sectional valves FL leak to LAT, IDLE 0.5" |
| 52 | OUFM | S | OUFM3 | 3.73E-02 | CR Operators Detect Low RHBFST Alarm and Direct Top Gauger to confirm leak. | Response to low level alarm from AFHE - LEAK TO LAT WHILE UNDERGOING FUEL MOVEMENT |
| 53 | ORGA1 | S | ORGA14 | 4.63E-03 | Top Gauger Checks and confirms RHBFST that Has a Low Level Alarm. | RH gauger checks for leakage FL LEAK TO LAT STAFF EVACUATE |
| 54 | OSUP | S | OSUP4 | 3.31E-02 | Management and Red Hill Supervisor Formulate Strategy to empty RHBFST | Supervisor develops tank empty strategy - TUNLEAK - initial fuel movement |
| 55 | OXFR | S | OXFR3 | 3.70E-02 | Control Room and Red Hill Staff follow strategy & Move Fuel from the Leaking RHBFST. | RH staff implement strategy - FL LEAK TO LAT during Fuel Movement |
| 56 | ISOL | YES | ISOLY | 1.00E+00 | FL leak isolated from all RHBFSTs; by upgrade sectional, RHBFST idle or isolated - no need to empty | FL Leak isolated by sectional, tank idle, or skin or ball valves closed - switch |
| 57 | XFR1 | S | XFR11 | 2.14E-03 | Inter-tank transfer by Gravity to move fuel from leaking RHBFST | Hardware for inter-tank XFR1 available skin and ball valves |
| 58 | XFR2 | S | XFR21 | 5.35E-03 | Issue Fuel by gravity to Tanks at the Upper Tank Farm Located at Pearl Harbor. | Hardware for issue to UTF plus skin and ball valve |
| 59 | XFR3 | S | XFR31 | 8.56E-03 | Two-step Fuel Movement to Pump Fuel to other RHBFSTs | Hardware for 2-step inter-tank XFR using cargo pumps |
| 60 | XFR4 | S | XFR41 | 8.56E-03 | Gravity Feed to Ships or Other Tanks at Pearl Harbor. | Hardware for gravity feed to Pearl |

## Table 9-2. Example Detailed Sequence Report (Continued)

| # | Top | State | SF | SF Value | Top Event Description | Split Fraction Description |
|---|---|---|---|---|---|---|
| 61 | XFR5 | S | XFR51 | 3.21E-03 | Fuel Movement to Empty Bottom 7.5' of Lower Dome Using RHBFST Lower Drain Line. | Hardware for draining lower dome available including sectional valves |
| 62 | DELAY | NONE | HR0 | 1.00E+00 | Tank empty delay time based on earlier failures | O HOURS DELAY TIME |
| 63 | REL | F | RELI | 1.00E+00 | REL - Type of Fuel Release Scenario | Limited release from fuel line Sections A or B leak below New Oil Door; RHBFSTs Idle; Collects at UGPH entry and ADIT 2 with no door overpressure failures. |

### 9.4.6 List of Saved Sequences

A List of saved sequences is presented as an electronic file named [redacted], which accompanies this report and which is discussed in [redacted]. This list includes all sequences with individual frequencies greater than 1E-8 per year.

The saved sequence file contains four tabs. The first tab provides the individual sequence results. The second tab provides a roll-up of frequencies within each of nine fuel release ranges. The roll up values reported in Tab 2 are aggregated for just the saved sequences in the first tab. For the base case frequencies aggregated for all sequences quantified with individual frequencies greater than 1E-12 per year, please see Table 12-1. Also in Tab 2, an exceedance column is provided which lists the frequency of exceeding a given amount of fuel released for each of the fuel release ranges. The consolidated sequence group recurrence interval is provided in years. Finally the potential volume released in gallons per year is also provided for each interval of fuel released.

The third tab of the saved sequences file provides a list of all split fractions used in the QRVA model, their associated top events, their point estimate values, and a brief description of each split fraction. The last tab in the saved sequence file describes a legend for the names of end states (or bins) assigned to each sequence representing the amount of fuel released from each sequence in thousands of gallons.

For each saved sequence in the first tab, a number of columns of information are provided. The following describes the meanings of each of the columns.

- Sequence ID Number – This is a rank ordering number for all sequences presented in decreasing order of frequency.

- Sequence Frequency (events/year) – This is the point estimate quantified frequency of the acute sequence.

- Sequence Recurrence Interval (years) – This is the inverse of the sequence frequency indicating a point estimate for the return period.

- Sequence Probability (1 year) – The probability that the sequence will occur in the next year.

- Sequence Probability (100 years) – The probability that the sequence will occur in the next 100 years.

- RHBFSF Tank Number – If the acute sequence has a specific associated RHBFST, this columns gives the tank number. If the sequence has no specific RHBFST associated with, the entry is NA.

- Leak Direction – If the accident sequence involves leakage from an associated RHBFST, this column gives the side of the RHBFST on which the leak is on. If the sequence has no specific RHBFST associated with, the entry is NA.

- Leak Height – If the acute sequence has a specific associated RHBFST, this columns gives the release height, generally in terms of a range of fuel levels, or from the tank bottom. If the sequence has no specific RHBFST associated with, the entry is NA.

- Fuel Line Pipe Segment – If the acute sequence involves a release from a fuel line in the Harbor Tunnel or the LAT, this column identifies the pipe section and gives a brief description of the section that includes the pipe diameter in inches. If the sequence does not involve release from a fuel line, the entry is NA.

- Point Estimate Volume Released – This column identifies the amount fuel released for the sequence rounded to the nearest thousand gallons of fuel.

- Potential Volume Release Rate (gallons/year) – This column lists the product of the sequence frequency and the amount of fuel released in gallons to obtain the potential volume released rater per year.

- Release Volume Range Category – Several fuel release ranges in gallons are specified. This column identifies the range of fuel to which this sequence is assigned.

- Fuel Type – This column identifies the fuel type released in the sequence.

- Operational Phase – This column identifies the RHBFSF operational phase when the accident sequence occurs. For the fuel type released, all RHBFSTs may be idle, or one or more undergoing a fuel movement; i.e., receiving or issuing. If the associated RHBFST is also undergoing a return to service, this is also noted in the description.

- Point Estimate Release Rate (gpm) – This column provides an indication of the fuel release rate during the sequence. It may be specified in gpm, or provide an indication of the hole size through which the fuel release occurs.

- Release Category – Once the fuel is released, this column provides a brief description of where the released fuel accumulates. See Section 10 for a discussion of the different locations identified.

- Initiating Event ID – This column provides the QRVA name for the initiating event which begins the acute sequence.

- Initiating Event Description – This column describes the initiating event which begins the acute sequence.

- Response Event Sequence by Split Fraction (SF) – The entries in this column identify the split fractions which have either failed or are assigned as the multi-state branch probability for the single sequence. The point estimate value and description of each split fraction is provided in Tab 3 of the workbook. The split fractions are listed in the order they appear in the linked event tree set used to quantify the acute

sequence frequency. Additional details are available on each saved sequence, information such as that described above in Section 9.4.5 for Table 9-2.

- Consequence Bin ID – The bin ID, or end state name, identifies the amount of fuel evaluated to be released in the acute sequence. Tab 4 of the workbook provides a legend for the bin ID nomenclature.

[redacted]

# 10. Fuel Release Accident Sequence Analysis

## 10.1 Introduction

In this Level 2 QRVA, Level 1 focuses on the frequency and consequences of event scenarios leading to loss of fuel control inventory, and Level 2 focuses on the extension of the Level 1 event sequences to potential fuel release scenarios from the RHBFSF. This section describes the bases, assumptions, and evaluations performed to further characterize loss of fuel inventory control event sequences as potential fuel release event sequences. In general terms, this portion of the QRVA characterizes where in the facility we expect that fuel will be released; e.g., around or beneath the main fuel storage tanks, through ADIT doors and/or HVAC vents, though breeched underground piping, or via fuel "pooling" areas or collection points in the RHBFSF underground tunnels (Upper Access Tunnel, Lower Access Tunnel, harbor tunnel, etc.).

## 10.2 Bases and Assumptions

The bases and assumptions for the development of the fuel release accident sequence analysis are summarized below.

1. The peak operating fuel level of each RHBFST is at most 212'.

2. Fuel line leaks from Section E are assumed to occur below the Zone 7 bulkhead. Nozzle leaks associated with RHBFSTs 17, 18, or 20 are modeled to release fuel above the Zone 7 bulkhead.

3. If fuel is leaked and accumulates above the Zone 7 bulkhead, leak paths through the bulkhead are assumed at 7' above the tunnel floor and the available flow area is assumed large enough to compensate for the smaller range of leak sizes; i.e., equivalent to hole sizes of 0.5" in diameter.

4. The ADIT 6 tunnel or ventilation ducting is not sealed, so that a large accumulation of released fuel would backup to the elevation of the ADIT 6 tunnel and be released to the outside environment until the fuel level in the leaking RHBFST equilibrates with the ADIT 6 tunnel floor.

5. If a fuel line leak to the LAT occurs when two RHBFSTs are undergoing an inter-tank transfer, neither is isolated, and the new oil door below the main sump successfully closes, then the oil door has sufficient design margin so as not to fail despite the higher head of fuel available even after the LAT is filled with fuel.

6. In the event of fuel leakage to the LAT with successful oil door closure, the sequence models do not credit any long term removal of leaked fuel from above the closed oil door.

7. Seepage of accumulated fuel from the LAT into the former diesel power plant is assumed prevented by the efforts to seal these openings.

8. The normally closed fan door in Section C of the LAT is assumed to fail open if fuel accumulates behind it to the 5' level; i.e., to about 101.5' elevation.

9. The normally closed double steel doors below 3Y to ADIT 3 are assumed to fail open if fuel accumulates above them to 7'. These doors are assumed to leak spilled fuel at a modest rate if fuel accumulates at lower levels.

10. The normally closed thin metal fire door on the Harbor Tunnel side of 3Y is assumed to fail open if fuel accumulates above 7'. This door is assumed to leak spilled fuel at a modest rate, if it accumulates at lower fuel levels.

11. If fuel accumulates in the NAVFAC pump house, it is assumed there is no direct leakage path from there to the water tunnel and eventually to the aquifer. A manhole cover that was previously identified as a leak path has been sealed.

12. The UGPH fire and isolation doors are normally closed, but would fail open if fuel accumulates above 7' above the doors' base which is elevated above the Harbor Tunnel floor.

13. The normally closed double doors at ADIT 2 would fail open if fuel accumulates 7' above the doors' base level, which is elevated above the ADIT 2 tunnel floor.

14. If substantial fuel accumulates in the Harbor Tunnel, it is assumed that the UGPH entry doors would fail open at fuel levels less than would be required to fail open the ADIT 2 doors.

15. If the UGPH doors fail open, the fuel that would be left behind in the Harbor Tunnel is 500,000 gallons and the remaining would transit through the UGPH to ADIT 1.

## 10.3 General Methodology

The frequency and probability of fuel release from the facility is calculated through a natural extension of the Level 1 analysis, using the same methods and tools. If we define the Level 1 analysis as a QRVA designed to determine the frequency and probability of unplanned loss of fuel (by type) inventory control within the facility (at specified volume ranges), then the Level 2 analysis may be formulated to determine the frequency and probability of unplanned release of fuel (by type) outside the facility property boundaries (at specified volume ranges), or unplanned release of fuel (by type) to the Red Hill Water Shaft (at specified volume ranges) from the facility. Releases of fuel from the RHBFSF can occur from two general processes, acute releases from high-consequence, relatively low-probability event sequences (the primary focus of this QRVA) and chronic releases from relatively low-consequence but higher-probability (more frequent) event sequences.

### 10.3.1 RHBFSF Unscheduled Fuel Movement Data Analysis

Chronic releases can be addressed via analysis of RHBFSF UFM reports. At the RHBFSF, the computerized inventory control system automatically generates UFM reports. Based on the estimated volumes of fuel associated with individual UFM reports, and based on the experience and judgment of facility operators and supervisors,

these reports are subjected to root cause analysis and associated corrective action is formulated and implemented. In the RHBFSF QRVA, the UFM reports and available associated fuel inventory control and history records will be reviewed, evaluated, and analyzed to develop a reasonable estimate of fuel release from chronic release scenarios.

### 10.3.2 Acute Releases from Accident/Incident Event Sequences

The event sequence models developed for the QRVA are designed to support prediction of acute releases of fuel from the RHBFSF. In general, these models characterize the relatively low-frequency high-consequence event sequences applied in assessing facility risk from acute hazard sources.

#### *10.3.2.1 Probable Release Path Evaluation*

Acute releases from the facility can involve volumes and flow rates that will overwhelm the capacity of the facility normal drainage system. For such scenarios, probable release paths will be evaluated as part of the QRVA to formulate realistic release scenarios for the acute hazard event sequences. Realistic release paths include, but are not limited to, the following:

- Direct releases from ruptured tanks to the rock and soil surrounding the tanks.
- Releases into facility tunnels to the normal drainage system and/or to tunnel access entrances/exits (or "adits," a term used by the Navy referring to the Latin word "aditus"), and/or to the rock and soil outside the tunnels through tunnel structural failures or flaws.
- Releases through tank vent paths.

#### *10.3.2.2 Event-Caused Structural Failure Evaluation*

It is conceivable that, for event sequences involving large-capacity release from one or more RHBFSF tanks, the dynamic forces associated with the release could fail one or more facility structures; e.g., breach the lower tunnel walls and/or doorways. The QRVA will include evaluation of potential event-caused structural failures that could complicate expected release pathways.

#### *10.3.2.3 Integration with Level 1 Risk Results*

The Level 2 scenarios are, in general, simple extensions of the Level 1 event sequences, taking into account fuel containment failures and release pathways. Therefore, the Level 1 event trees will be expanded to characterize Level 2 results.

## 10.4 Fuel Release Accident Sequence Analysis Details

Postulated scenarios involving the flow of fuel leaked from a RHBFST or fuel line piping into the Lower Access Tunnel or Harbor Tunnel were described in Reference 10-1 for a small set of scenarios. That assessment was for the Red Hill facility conditions as of

1998. The following describes the current Red Hill conditions as applicable to a broader set of scenarios. The objective of this discussion is to identify the likely places at which the fuel released would end up after initial release from a RHBFST, fuel lines within the tunnels, or both. Seepage of fuel into the surrounding rock and potentially the aquifer below is not described. Instead, the locations where fuel is likely to accumulate is described so that such an assessment of seepage into the surrounding rock can be performed.

What follows is a description of potential releases from categories of accident sequences, organized by the location of the initial leak location. This description is based in part on the tunnel geometries and insights tabulated in Reference 10-1 and its appendices. The most important change since the 1998 study with the RHBFSTs is that the operating fuel levels have been reduced. The Reference 10-1 study assumed the initial RHBFST fuel levels would be at 236', whereas now, the peak operating fuel levels are likely to be less than 212'. The selected 212' fuel level is consistent with new annual leak tightness fuel levels. During the 90 days of RHBFST inventory levels reviewed in detail from 2017, the maximum fuel level of any RHBFST was 212' 8.25" in RHBFST 6. In many RHBFSTs, the peak fuel level within the 90-day period was much less. For example, in the smaller capacity RHBFSTs (2, 3, and 4) the maximum fuel level recorded was 201'4"; i.e., in RHBFST 3.

### 10.4.1 Direct Leaks from RHBFSTs

Release Category A: The accident sequence models identify two different leak sizes at different locations because of through holes penetrating the tank liner or piping embedded within the concrete of the lower dome. The height of the leak below the fuel level within the RHBFST, which is identified, and its orientation in terms of radial direction are noted separately for each RHBFST sequence. The volume of fuel released is noted by the sequence end state in 1000s of gallons of fuel. All such sequences are assigned to Release Category A for purposes of this description. Different classes of sequences which are assigned to Release Category A are presented in Table 10-1. The amount of fuel released to rock is largely determined by the time period in which the leaking RHBFST is emptied of fuel. The amount of fuel released is defined by the sequence bin assigned to each individual release sequence.

## Table 10-1. Fuel Release Final Locations

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELA | Direct Releases from a RHBFST through its liner to Rock. Specific leak location is specified by tank ID, leak height, and azimuthal quadrant. | All RHBFST leaks to rock of all sizes:<br>• 1.5 gpm to Rock, during Operation<br>• 0.5" Hole to Rock during Operation<br>• 1.5 gpm to Rock during RTS<br>• 0.5" Hole to Rock during RTS<br>• Lower Dome 0.5" Leaks to Rock<br>• Overfill 0.5" Leak to Rock<br>The amount of fuel released to rock is largely determined by the time period in which the leaking RHBFST is emptied of fuel. |
| RELB | Modest Fuel releases confined to Zone 7, with limited transfer by the Zone 7 sump pump to the slop system in the tank gallery. | The sequences involve a 0.5" or 6" JP5 fuel line leak into Zone 7 (fuel line Section E) with all RHBFSTs initially idle, or if a RHBFST is initially aligned but is quickly isolated.<br>There are no sequences of this type actually mapped to this release category in the QRVA. Section E includes fuel line piping above the highest sectional valves. The Section E fuel lines are both in the tank gallery and in Zone 7. Fuel line leaks involving Section E are instead assumed to occur below the Zone 7 bulkhead so as to maximize the fuel available for release; i.e., the fuel in the lines above the leak location. |

## Table 10-1. Fuel Release Final Locations (Continued)

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELC | Large accumulation of released fuel in Zone 7 with a 100,000 barrels released through ADIT 6. Remainder of fuel remains in Zone 7 or leaks through the bulkhead penetrations. The leaked fuel through the bulkhead accumulates in the tank gallery portion of the LAT with the new oil door closed. | Large leaks into Zone 7:<br>• Large 6" nozzle leak from 17-20. The new oil door closes.<br>• 6" Fuel line leak into Zone 7 (i.e., Section E) during a fuel movement in which the aligned RHBFST is not isolated from the break location. Emptying the affected RHBFST would decrease the amount of fuel available for release. The new oil door closes. There are no sequences of this type actually mapped to this Release category in the QRVA. Section E includes fuel line piping above the highest sectional valves. The Section E fuel lines are both in the tank gallery and in Zone 7. Fuel line leaks involving Section E are instead assumed to occur below the Zone 7 bulkhead so as to maximize the fuel available for release. |
| RELD | Large accumulation of released fuel in Zone 7 with no release through ADIT 6. The leakage through the bulkhead fills the tank gallery portion of the LAT and of Zone 7. Fuel level equilibrates with much of the fuel remaining in the affected RHBFST but below the level of ADIT 6. New oil door has closed. | Smaller flow rate leaks into Zone 7:<br>• Small 0.5" Nozzle leaks from RHBFST 17-20. The new oil door closes. Emptying the affected RHBFST would decrease the amount of fuel available for release.<br>• Small 0.5" hole in JP5 fuel line which is not isolated and the RHBFST is not emptied before levels reach the bulkhead penetrations above the Zone 7 isolation door.<br>The new oil door closes. There are no JP5 fuel line leaks to Zone 7 actually mapped to this release category in the QRVA. Section E includes fuel line piping above the highest sectional valves. These fuel lines are both in the tank gallery and in Zone 7. Fuel line leaks involving Section E are instead assumed to occur below the Zone 7 bulkhead so as to maximize the fuel available for release. |

## Table 10-1. Fuel Release Final Locations (Continued)

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELE | Large accumulation of released fuel in the tank gallery filling the LAT; i.e., from Section D or E. Some upgrade spillage into Zone 7 via the bulkhead penetrations occurs. New oil door has closed. Fuel level equilibrates with much of the fuel remaining in the affected RHBFST but is available to leak out if fuel penetrates into the tunnel rock. | Large leaks to tank gallery with RHBFST aligned for fuel movement that is not isolated. The new oil door closes.<br>• Large 6" or small 0.5" nozzle leaks for RHBFSTs 2–16.<br>• Small 0.5" or 6" fuel line leaks from Fuel Line Section D or E with the break located below the LAT bulkhead and without isolating a RHBFST initially undergoing a fuel movement.<br>• Maintenance error in tank gallery ball valve with an unisolated fuel movement. |
| RELF | Fuel line inventory from Section D or E only leaks to the tank gallery portion of the LAT. New oil door closes. About 20,000 gallons of the leakage is transferred by the main sump pumps to Tank S31 outside ADIT 3. | This release category involves a small or large leak to the tank gallery during a fuel movement where the RHBFST is not isolated. The new oil door closes.<br>• 0.5" or 6" fuel line leak from Section D or E with the break located below the Zone 7 bulkhead (i.e., in the lower tank gallery) and with all RHBFSTs idle, or after isolating a RHBFST initially undergoing a fuel movement.<br>• Maintenance error in tank gallery involving a ball valve with all RHBFSTs idle. |
| RELG | Fuel line inventory only from Sections C and above leaks to LAT and leaks passed doors in the lower LAT, down the Harbor Tunnel, and accumulates at the UGPH entry and in ADIT 2. UGPH doors do not fail. | This release category is for fuel line leaks in Section C, below the new oil door, in which all associated RHBFSTs are initially idle, or they are isolated quickly. Small 0.5" or 6" fuel line leaks from Fuel Line Section C with the break located below the new oil door and in which all associated RHBFSTs are initially idle, or if they are aligned for a fuel movement, they are isolated. The isolation may occur via the RHBFST skin or ball valve, or by closure of an upgrade sectional valve between the leak and the RHBFST.<br>Closure of the new oil door would not significantly affect the release for this release category. |

## Table 10-1. Fuel Release Final Locations (Continued)

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELH | Fuel line leak from Sections C and above to the LAT and leaks passed door in the lower LAT, down Harbor Tunnel and accumulates at UGPH entry and in ADIT 2. UGPH entry doors eventually fail releasing fuel out ADIT 1. | This release category is for fuel line leaks in Section C in which a RHBFSTs is initially aligned for a fuel movement and it is not isolated quickly.<br>• 0.5" or 6" fuel line leak from Section C with the break located below the new oil door and a RHBFST aligned for a fuel movement and is not isolated from the hole.<br>Closure of the new oil door would not significantly affect the release for this release category. However, its closure could shorten the time to LAT door over-pressure by reducing the volume of fuel that must be accumulated. |
| RELI | Fuel line inventory only from Section A or B and above; leaks to Harbor Tunnel and accumulates at UGPH entry and in ADIT 2. UGPH entry doors do not fail. | This release category is for fuel line leaks of all sizes (i.e. 0.5” or 6”) from Sections A or B in which all associated RHBFSTs are initially idle, or they are isolated.<br>• Small 0.5" or 6" fuel line leaks from Fuel Line Section A or B below the 3Y split in which all associated RHBFSTs are initially idle, or they are aligned for a fuel movement but then isolated. The isolation may occur via the RHBFST skin or ball valve, or by closure of an upgrade sectional valve between the leak location and the RHBFST.<br>Closure of the new oil tight door has no significant effect on the release. |
| RELJ | Fuel line inventory plus the inventory of an aligned and not isolated RHBFST leaks into Section A or B, flows downgrade in the Harbor Tunnel, and accumulates at the UGPH entry and in the ADIT 2 tunnel. Eventual overpressure (after 89,000 barrels have accumulated) of the UGPH doors occur leaving about 500,000 gallons of fuel in the lower Harbor Tunnel with the rest leaked out though ADIT 1. | This release category is for fuel line leaks of all sizes (i.e., 0.5” or 6”) from Section A or B in which a RHBFSTs is initially aligned for a fuel movement and is not isolated.<br>• Small 0.5" or large 6" fuel line leaks from fuel line Section A or B below the 3Y split in which a RHBFSTs is initially aligned for a fuel movement and is not isolated.<br>Closure of the new oil tight door has no significant effect on the release. |

## Table 10-1. Fuel Release Final Locations (Continued)

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELK | Large accumulation of released fuel in Zone 7 with a 100,000 barrels released through ADIT 6. Other fuel remains in Zone 7 or leaks through bulkhead penetrations. The leaked fuel flows down the tank gallery. The new oil door fails to close and so the fuel leaked through the bulkhead flows downgrade in the Harbor Tunnel to the UGPH entry and the ADIT 2 tunnel. Eventual overpressure (after 89,000 barrels have accumulated) of the UGPH door occurs leaving about 500,000 gallons of fuel in the lower Harbor Tunnel. Several feet of released fuel remain in Zone 7 and can potentially seep into the surrounding rock. | Similar to Release Category C but without closure of the new oil door.<br>• Large 6" nozzle leak from 17-20.<br>• 6" Fuel line leak into Zone 7 (i.e., Section E) during a fuel movement in which the connected RHBFST is not isolated from the break location. Emptying the affected RHBFST would decrease the amount of fuel available for release. There are no sequences of this type actually mapped to this release category in the QRVA. Section E includes fuel line piping above the highest sectional valves. The Section E fuel lines are both in the tank gallery and in Zone 7. Fuel line leaks involving Section E are instead assumed to occur below the Zone 7 bulkhead so as to maximize the fuel available for release. |
| RELL | Large accumulation of released fuel in Zone 7 with no release through ADIT 6. Fuel leakage through the bulkhead flows down the tank gallery portion of the LAT. The new oil door fails to close and so the fuel leaked through the bulkhead flows downgrade in the Harbor Tunnel to the UGPH entry and the ADIT 2 tunnel. Eventual overpressure (after 89,000 barrels have accumulated) of the UGPH door occurs leaving about 500,000 gallons of fuel in the lower Harbor Tunnel. Several feet of released fuel remain in Zone 7 and can potentially seep into the surrounding rock. | This release category is similar to Release Category D, except the new oil door fails to close.<br>• Small 0.5" Nozzle leaks from RHBFST 17-20. Emptying the affected RHBFST would decrease the amount of fuel available for release.<br>• Small 0.5" hole in JP5 fuel line which is not isolated and the RHBFST is not emptied before levels reach the bulkhead penetrations above the Zone 7 isolation door. There are no sequences of this type actually mapped to this release category in the QRVA. Section E includes fuel line piping above the highest sectional valves. The Section E fuel lines are both in the tank gallery and in Zone 7. Fuel line leaks involving Section E are instead assumed to occur below the Zone 7 bulkhead so as to maximize the fuel available for release. |

## Table 10-1. Fuel Release Final Locations (Continued)

| Release Category ID | Definition of Release Categories | Sequences Mapped to this Release Category |
|---|---|---|
| RELM | Large amount of released fuel to the tank gallery portion of the LAT; i.e., Section D or E. The new oil door fails to close. Leaked fuel flows downgrade in the Harbor Tunnel to the UGPH entry and the ADIT 2 tunnel. Eventual overpressure (after 89,000 barrels have accumulated) of the UGPH door occurs leaving about 500,000 gallons of fuel in the lower Harbor Tunnel. | This release category is similar to Release Category E but without closure of the new oil door.<br>• Large 6" or small 0.5" Nozzle leaks for RHBFSTs 2–16.<br>• Small 0.5" or 6" fuel line leaks from fuel line Section D or E with the break located below the LAT bulkhead and without isolating a RHBFST initially undergoing a fuel movement.<br>• Maintenance error in tank gallery ball valve with an unisolated fuel movement. |
| RELN | Fuel line inventory only from Section D or E and above only leaks to the tank gallery portion of the LAT. The new oil door fails to close. Some of the released fuel is transferred by the main sump pumps to Tank S31 outside ADIT 3. The remainder flows downgrade in the Harbor Tunnel to the UGPH entry and the ADIT 2 tunnel where it accumulates. The UGPH doors do not fail. | This release category is similar to Release Category F, except the new oil door fails to close.<br>• 0.5" or 6" fuel line leak from Section D or E with the break located below the Zone 7 bulkhead (i.e., in the lower tank gallery) and with all RHBFSTs idle, or after isolating a RHBFST initially undergoing a fuel movement.<br>• Maintenance error in tank gallery involving a ball valve with all RHBFSTs initially idle or isolated relatively quickly. |

### 10.4.2 Leaks from Fuel Lines and RHBFSTs within Zone 7

A bulkhead and isolation door separate the tank gallery portion of the LAT (with access to RHBFSTs 2 through 16) from the highest RHBFSTs; i.e., 17 through 20. This bulkhead and isolation door are designed to hold 74 psi, which is estimated to be the peak pressure that could occur following the discharge of a full RHBFST inventory from one of RHBFSTs 17 through 20. The region above this bulkhead at the level of the LAT is referred to as Zone 7. This isolation door is normally closed (but not always) and must be properly closed to achieve its function. The isolation door is liquid tight and effectively sealed at the bottom of the door. However, there are penetrations higher in the bulkhead wall which would leak or permit the flow of fuel downgrade once fuel levels above the bulkhead accumulate to the height of the penetrations. There is a relatively small capacity sump pump (P0123, estimated at 20 to 30 gpm capacity) in Zone 7 which would automatically activate on its high sump level and transfer leaked fuel to the lower side of the bulkhead via the slop line. The slop line directs the transferred fuel to the main sump below the bulkhead at the low end of the tank gallery. This smaller capacity sump pump would start automatically and continue operating unless or until the fuel levels above the door flood its electric control panel.

Release Category B: Leakage of any size from just the JP5 fuel line which penetrates the bulkhead into Zone 7 has limited fuel capacity; i.e., about 22,000 gallons. All JP5 RHBFSTs may be idle, or if initially in a fuel movement are quickly isolated from the leak location. This amount of fuel is much less than the estimated 400,000 gallons required to fill Zone 7 to a height of 7'; i.e., which is the assumed height of the penetrations above the bulkhead isolation door. The F76 and F24 fuel lines do not penetrate the bulkhead and so do not enter Zone 7. The Zone 7 sump pump may operate to transfer the leaked fuel to the main sump below the bulkhead. However, 22,000 gallons is within the capacity of Tank S311, so if the Zone 7 sump pump does operate, and the main sump pumps, which have greater capacity than the Zone 7 sump pump, also operate then only limited fuel would be left on the floor of Zone 7. Since there is so little fuel in the JP5 lines within Zone 7, the QRVA model instead assumes that any leaks from JP5 Fuel Line Section E are instead located below the bulkhead and so discharge into the tank gallery portion of the LAT.

Release Category C: However, if a large (6" hole) JP5 fuel line leakage into Zone 7 occurs with a RHBFST undergoing a fuel evolution and the fuel line and associated RHBFST are not isolated and the leaking RHBFST is not emptied, or if there is a large (6" hole) RHBFST nozzle leak from one of the RHBFSTs in Zone 7, which is not isolable, then fuel levels in Zone 7 would rise well above the bulkhead isolation door. Section 6.6.1.2 of Reference 10-1 considered a single discharge from RHBFST 20 starting with the initial RHBFST 20 fuel level at 236'. Once discharged from RHBFST 20, fuel would fill up Zone 7 to the tunnel roof and rise up the Elevator 73 shaft. The bulkhead penetrations would see rising fuel levels and begin releasing fuel to the tank gallery portion of the LAT.

Currently the outer doors at ADIT 6 are normally open, and the double fire doors inside these outer doors, though normally closed, are not believed to be leak tight. The ADIT 6 ventilation exhaust ducts may also provide a flow path for the release of any fuel backed up to the ADIT 6 floor level.

Assuming the ADIT 6 tunnel or its ventilation ducting is not sealed, the discharged fuel, after accumulation, would flow out ADIT 6 to the outside. The tunnel floor elevation at the ADIT 6 door is at 272.99'. This elevation is about 121' above the base elevation of RHBFST 20. Therefore, if ADIT 6 was not sealed so that fuel could be released to the outside, Reference 10-1 concluded that a large portion of the discharged fuel would flow out ADIT 6. The remainder would have filled up the Zone 7 floor level and the cargo elevator shaft.

The total release through ADIT 6 for this case may be estimated assuming that the ADIT 6 door is closed but would fail outward if subjected to a 7' level of fuel above the tunnel floor; i.e., at 279.00'. Once the ADIT 6 outside door fails, fuel could be released out to the environment down to the ADIT 6 tunnel floor; i.e., at 272.99'. Again, this corresponds to a RHBFST 20 fuel level of 121'. It's estimated that to fill Zone 7 and the cargo elevator shaft but excluding the ADIT 6 tunnel volume requires about 28,251 barrels. This corresponds to a drop in RHBFST 20 level of about 20.1'. Assuming the initial level in the RHBFST 20 postulated to leak is 212', its fuel level would drop to 191.9'. Then all the fuel from this level down to 121' could be released to the outside via ADIT 6; i.e., about 100,000 barrels, or 420,000 gallons. Afterwards, the RHBFST fuel level would be at 121'.

Even if ADIT 6 were sealed, Reference 10-1 concluded that the RHBFST 20 fuel level starting at 236' would equilibrate at about 196', after a level drop of 40'. Reference 10-1 also stated that by lowering the initial fuel level to less than 225', that the equilibrated fuel levels with no release through ADIT 6, would not reach the UAT floor at an elevation of about 330'. An UAT floor elevation of 330' corresponds to a RHBFST 20 fuel level of 179'. A much lower operational fuel level is already the operating practice at Red Hill, since fuel levels are now maintained at roughly 212' and below.

If an unisolated and unmitigated fuel release occurred from two of RHBFSTs 17 through 20, both of which had initial fuel levels at 212', then the release through an unsealed ADIT 6 would be correspondingly greater. Such a two RHBFST inventory leak is possible if there is an inter-RHBFST gravity transfer of fuel in progress at the time of the leak into Zone 7 and the associated skin and ball valves on both RHBFSTs all fail to close, or no manual action is taken to remotely close them.

If ADIT 6 is sealed, then the height of the connected RHBFSTs after equilibrium is reached would be higher in both RHBFSTs than in the single RHBFST leaking case, and may exceed the 179' level corresponding to the UAT floor elevation. Fortunately, the frequency of such two RHBFSTs events is very low.

The Zone 7 bulkhead and isolation door are both designed to hold up to 74 psi of liquid pressure when closed properly. This corresponds to about 196' of head for a fuel type with specific gravity of 0.85. Since the bottom of RHBFST 20 is 18' above the tunnel floor, this would correspond to a RHBFST 20 fuel level of 178'. There should be substantial margin in the design calculation, sufficient to justify a much higher fuel level. The bulkhead and isolation door are not expected to fail even if two RHBFSTs were connected to the leaking fuel line location.

Release Category D: If fuel line leakage into Zone 7 occurs via a small (0.5") RHBFST nozzle leak, which is not isolable, the leakage flow rate would be about 75 gpm. This

flow rate is large enough to accumulate fuel in Zone 7 until the leaked fuel level reaches the penetrations in the bulkhead above the isolation door. At that time flow through the bulkhead penetrations is expected to match the leakage rate through the hole so that Zone 7 leaked fuel level stabilizes. Fuel level in the leaking RHBFST would continue to drop as it discharges through the hole and exits through the bulkhead penetrations into the tank gallery portion of the LAT. Flow would not accumulate in the cargo elevator nor rise to the level of the ADIT 6 tunnel. Of course, if Red Hill staff also takes steps to empty the leaking RHBFST, the overall amount of fuel leaked into Zone 7 would be reduced. A similar sequence would involve a small hole (0.5" in a JP5 Section E fuel line which is also not isolated, and the RHBFST is not emptied before levels reached the bulkhead penetrations above the Zone 7 isolation door. Fuel released from any of RHBFSTs 17 through 20 via 0.5" size holes, and after accumulation in Zone 7, would leak through the penetrations above the isolation door. The flow from the bulkhead penetrations would flow downgrade in the tank gallery below the bulkhead, passed gauger station and the electrical room. The electrical room door is normally closed, but is not oil-tight so some fuel seepage into the electrical room is expected. In this release category, once the new oil door closes, a large amount of fuel would accumulate upgrade of the oil door; i.e., basically inventory in the connected RHBFST, except for 10,000 barrels remaining in the lower 7' of Zone 7; i.e., below the bulkhead penetrations. However, the tank gallery and space between the main sump and the new now closed oil-tight door only hold about 90,000 barrels. Once this volume fills the released fuel level in Zone 7 would rise accordingly. Both the tank gallery and Zone 7 would be filled with fuel and available for seepage into the tunnel walls and floor. Even after the loss of 100,000 barrels from a RHBFST initially at 212', the RHBFST level would still be at 140' providing substantial head for seepage into the tunnel walls and floors.

### 10.4.3 Leaks from Fuel Lines and RHBFSTs within the Tank Gallery

Any fuel leakage from RHBFSTs and fuel lines located below the Zone 7 bulkhead would not flow past gauger station or the electrical room since they are located upgrade of the RHBFSTs in the tank gallery. Fuel released to the LAT would continue flowing downgrade. For a 75 gpm flow rate (corresponding to about a 0.5" hole) spread across the tunnel floor, the fuel depth is estimated to be very shallow, about 0.1". If the 75 gpm of flow was funneled to the drainage trench in the LAT, the flow depth would be deeper and would be less subject to seepage out of the tunnel until the fuel started to accumulate. For a 6" hole releasing 11,000 gpm initially from a RHBFST, the flow depth in this part of the LAT would be about 2.5". This is a much shallower flow of fuel than calculated by WillBros Engineers, Inc. (WillBros) in Reference 10-1; i.e., 1.8', which was for a much large break of a 20" diameter hole from RHBFST 15 that was evaluated to release fuel at a rate of 75,000 gpm.

At different points in the tank gallery, there are fire doors installed. These doors are normally open. In the absence of a fire they would not close automatically. Since they do not obstruct the flow of fuel, they are not modeled in the QRVA since fire events are not yet considered.

The LAT main sump is located below the tank gallery but about 160' in distance and upgrade from the new oil-tight door. Two main sump pumps (P0100A/B with capacities of 150 gpm and 300 gpm) would actuate automatically on high sump level just below the tank gallery. Indication of their starting is provided in the control room. While these

sump pumps have different start setpoints, they do share the same strainer. Even one of these two main sump pumps would be sufficient to remove leaked fuel from a 0.5"-diameter hole releasing a maximum of 75 gpm. These main sump pumps direct fuel to Tank S311 outside of ADIT 3. The S311 tank has a nominal capacity of 950 barrels. If S311 was already half full, the available ullage would be only 475 barrels, or about 20,000 gallons. This ullage of 20,000 gallons is about equal to the fuel inventory of the F24 fuel lines above the main sump, but is only about half the inventory of the JP5 fuel lines above the main sump, and less than one-third of the inventory of the F76 fuel lines above the main sump. Of course, if a fuel evolution was also in progress, the available ullage would be insufficient for any of the three fuel types unless isolation of the leaking fuel line occurs quickly.

At 75 gpm, the available ullage in Tank S311 would be filled in just 4.4 hours. For a postulated 6" break, with both pumps operating, the ullage would be filled up in just 45 minutes. After S311 reaches capacity, the main sump pumps would have to be shut down, else the transferred fuel would overfill S311 and spill out on the ground outside ADIT 3. If, after the new oil door closes, the fuel backs up in the LAT, then the electrical panels supplying the main sump pumps would also fail stopping the main sump pumps.

For either a 75 gpm or 6" break, fuel released to the LAT would also flow down below the main sump another 160' to the new oil-door and into its sump which triggers the door to close. The new oil door is located just below the sectional valves which are downgrade from the main sump and at the bottom of the QRVA model's Fuel Line Section D; i.e., Sections D and E refer to the LAT fuel line pipe sections above and below the sectional valves in the tank gallery. The oil door would close automatically on its high sump level actuation. Following successful oil door closure, any fuel not transferred to Tank S311 would backup in the LAT, initially below the main sump. The tank gallery would fill up from the tunnel floor elevation of 120' level at the base of RHBFSTs 1 and 2, 143' at the base of RHBFSTs 15 and 16 below the bulkhead, and to 151' at the base of RHBFSTs 19 and 20 above the bulkhead separating Zone 7 from the tank gallery area.

The new oil door below the main sump has a design pressure rating of 72 psi and therefore should withstand even a RHBFST tank initially filled to 212' accounting for the released fuel needed to also fill the LAT tunnel between the new oil door and the Zone 7 bulkhead; i.e., about 90,000 barrels. Depending on the fuel type, this design pressure rating corresponds to a fuel head height of roughly 195' to 208'. The bottom of the RHBFSTs is about 18' above the floor of the LAT. This elevation difference adds to the head of discharged fuel and still backed up into the connected RHBFST. Since the RHBFSTs fuel levels are currently limited to less than about 212', and much of the fuel would have to be discharged to the LAT for the oil door to see the maximum head, it is judged that the closed oil door could withstand a full discharge from single RHBFST leak.

If, when the leak occurs, an inter-RHBFST transfer by gravity is taking place, and the leak and both initially aligned RHBFSTs are not isolated, then a greater head of fuel may develop if both RHBFSTs involved in the transfer are not isolated. However, in this case, the fuel backup above the ADIT 6 elevation (estimate as one-third the distance below the Upper Access Tunnel, or at roughly 140' fuel level in a RHBFST) would provide an escape to the surface. Since there is likely to be ample margin between the

door design pressure rating and a realistic failure pressure of the oil door, even in this extreme case of two RHBFSTs leaking, the closed oil door is assumed to hold. With the oil door closed and holding, the backed up fuel that has leaked to the LAT would then be available for seepage to the rock surrounding the LAT walls, ceiling, and floor.

It has been postulated that with time, the fuel backup up behind the closed oil-tight door could be removed from the LAT and transported to the surface by connecting the pool of fuel to pipes near the new oil-tight door. However, a scheme for doing so has not been identified and no procedure is available. Therefore, no credit for long term removal of the accumulated fuel from the LAT is assumed in the QRVA. For fuel leaks that are isolated before substantial fuel is released, this assumption may be overly conservative; e.g., leakage from fuel lines with all RHBFSTs in an idle condition so that there is no leakage from the RHBFSTs.

Release Category E: This release category involves a large amount of fuel being released to the LAT and accumulating between the new oil door which is closed and the Zone 7 bulkhead above the tank gallery. The amount of fuel released (90,000 barrels) fills these portions of the LAT tunnel with a substantial head of fuel from the incompletely emptied RHBFST that remains connected to the leak location.

This category of release involve leaks originating from fuel lines in the tank gallery portion of the LAT and below, but upstream of the new oil-tight door. Such events would include large (6” hole) or small (0.5”) nozzle leaks at the skin valve of a RHBFST, and large (6”) or small (0.5”) leaks from the fuel lines in these areas with initially a fuel movement in progress. A maintenance error resulting in opening of a fuel line while the same fuel line is undergoing a fuel movement also applies. For the fuel line leaks in this release category, the associated RHBFST undergoing the fuel movement is not isolated from the leaking fuel line.

Release Category F: This release category is similar to Release Category E, in that the release is to the LAT and accumulating between the oil door and the Zone 7 bulkhead and the oil door closes, except that the amount of fuel released is much less. The RHBFSTs on the affected fuel line may be all idle, or isolated quickly from the hole location. This Release Category F also applies for maintenance errors in opening a fuel line when all RHBFSTs on that line are in idle. The amount of fuel released is a function of the fuel line type and its fuel contents above the break location. Only the fuel inventory in QRVA Fuel Line Section D or E applies. Though normally open, if the corresponding sectional valve near RHBFSTs 11 and 12 is isolated, the amount of fuel released is reduced. With the RHBFSTs idle, only the fuel above the hole location is released. Operation of the main sumps to transfer fuel to tank S311 could effectively remove about 450 barrels of fuel making reducing the amount available for seepage through the walls and floor of the LAT.

This category of fuel releases involve leaks originating from fuel lines in the tank gallery portion of the LAT and below, but upstream of the new oil tight door. Such events would include large (6”) or small (0.5”) leaks from the fuel lines in these areas with no fuel movement in progress. A maintenance error resulting in opening of a fuel line while the

RHBFSTs of that fuel type all in idle also applies. The maximum amount of fuel only in QRVA Fuel Line Sections D and E for each fuel type is as follows:

F24 (16") – 20,000 Gallons (~500 barrels)

JP5 (18") – 39,000 Gallons (~900 barrels)

F76 (32") – 68,000 Gallons (~1600 barrels)

### 10.4.4 Leaks from Fuel Lines and RHBFSTs below the Oil Door

QRVA Fuel Line Section C represents the portion of the fuel lines which lie below the new oil tight door and above the sectional valves located just below 3Y in the Harbor Tunnel. Fuel released from Section C would flow downgrade along the narrower portion of the LAT towards the 3Y split. The narrower LAT drops down to 102' at a bend before any other doors are reached. This bend is at 18' below the base elevations of RHBFSTs 1 and 2. If the fuel line is aligned to a RHBFST at the time the hole develops, the flowing fuel depth for a release in the Section C portion of the LAT of 75 gpm is estimated to be 0.5", and for a 6" hole releasing 11,000 gpm, the flowing fuel depth is estimated to be about 1'.

Leaks originating below the oil-tight door would flow downgrade until crossing a now sealed access to the former diesel power plant and tunnel. Seepage into this abandoned power plant via its doorway was judged a potential fuel release path in the Reference 10-1 study (1998). Seepage into the former diesel power plant and tunnel is now believed unlikely. Additional effort has been made to ensure this access path is sealed and so is assumed sealed in this study. Since 1998, the openings from the LAT have been examined and plugged with grout. If the pathway were to still exist this pathway could be significant since, as described in Reference 10-1, the leaked fuel would enter the power plant riser shaft and flow down to the former diesel power station. The NAVFAC water development tunnel runs directly below the former diesel power plant but there are no known access paths to the aquifer from the diesel power station itself.

The first door (labeled Door A in Reference 10-1) that would reached in the Section C portion of the LAT is downgrade from the access to the former diesel power plant. This is a normally open door originally intended as an oil-tight door with its own sump and mechanical float for actuation. It is about 6" thick. This door is not the same design as the new oil-tight door and today has no design pressure rating. It is now acknowledged that this door is not considered oil-tight even if it is closed. The door is now referred to as an isolation door. The door is bent, is currently out of service, and would not close if released fuel was present. The QRVA models this door as always open and not able to close.

The next door downgrade in the Section C portion of the LAT is a normally closed fan door (located near Fans EF2A and 2B). This door is below the isolation Door A described above and still upgrade from the 3Y split. This fan door has no design pressure rating. The function of this fan door is to direct ventilation airflow from the LAT to the 3Y exhaust shaft. The presence of leaked fuel would push the door closed rather than open. A ventilation slide window is provided about 3 to 4 feet up the door to allow

workers to equalize tunnel pressure before manually opening the door. This normally closed door would leak fuel below the door due to the train tracks under it. Whether there is a backup of fuel above this door depends on the postulated fuel release rate. It's assumed that this door would fail open if fuel accumulates above the ventilation slide window; i.e., say 5'. When the door fails or there is gross leakage through the ventilation slide window, the fuel would flow downgrade along both splits at 3Y (at a tunnel floor elevation of 101.38', less than a 1' drop from the LAT bend) to two normally closed doors.

The amount of fuel needed to accumulate behind the normally closed fan door to cause it to fail, is that needed to fill the LAT to a height of roughly 5' above the door floor assumed to be at 101.5'; i.e., accumulate to 106.5' elevation. The new oil door is at 102.23' so the accumulation of fuel would have to back up upgrade of the new oil door. It is therefore likely the new oil door would close before the fan door fails even though the Section C leak is below the new oil door. Once the door closed the accumulated fuel would only have to fill the LAT from the fan door to the now closed fuel door elevation to a height of 5'. Neglecting the slight increase in tunnel floor elevation upgrade to the new oil door and using the tunnel lengths (1217' plus 850') and effective tunnel widths of 9.7' and 9.1', as estimated from Reference 10-1 (Section D.3), and a fuel depth of 5' yields a fuel volume of 98,000 $ft^3$ which converts to 730,000 gallons, or 17,400 barrels. There is not that much fuel even in the largest (i.e., F76, 160,000 gallons) fuel lines above in the QRVA defined Sections C, D, and E. Therefore, the leaking fuel line must be initially aligned to a RHBFST for a fuel movement and that RHBFST not isolated until that much fuel leaked out in order to accumulate sufficient fuel to fail the fan door.

More than 730,000 gallons (or 17,400 barrels) of accumulated fuel would be required to fail the fan door if the new oil door did not close. The backup of fuel would have to reach the tunnel floor elevation of 105.5' which is near RHBFSTs 5 and 6. Some accumulated fuel could also be removed by the main sump pumps. Again, there is not enough fuel in the fuel lines that the QRVA defines as Sections C, D, and E to fail the fan door.

However, if a RHBFST is aligned for a fuel movement using the fuel line postulated to be leaking, then easily enough fuel could be accumulated to fail the fan door. The new oil door closing would make the fan door fail sooner, but the fan door would fail even if the new oil door did not close.

The Harbor Tunnel side of the 3Y split has a normally closed bulkhead with thin metal fire door. This door is located just below the 3Y sectional valves, at the bottom of the QRVA model's Fuel Line Pipe Section C. The function of the door is to direct ventilation airflow from the Harbor Tunnel up through the 3Y ventilation exhaust shaft. Fuel released from the LAT side would push the door closed from above. This door also has no design pressure rating. This door would leak fuel via the train tracks beneath it. However, some fuel backup would be expected depending on the fuel release rate at the source. A realistic door failure pressure corresponding to fuel level backup of 7' is assumed.

Down the other split from 3Y towards ADIT 3, there is a normally closed, steel set of double doors which provide functions for security, fire, and ventilation purposes. These steel doors are referred to as Door B in Reference 10-1. The double doors are located

between the normally closed fan door near Fans EF2A and 2B upgrade and the NAVFAC pump house which is downgrade. This set of double doors does not have a design pressure. Fuel from above would push the doors closed. Train tracks pass under these doors so it would leak fuel from above. However, some fuel backup would be expected depending on the fuel release rate at the source. A realistic door failure pressure corresponding to fuel level backup of 7' is also assumed. This set of doors is at an elevation below 3Y in the ADIT 3 tunnel at 101.38' yet is on the Red Hill side of the water pump station which is at 101.5'.

There is again, insufficient fuel in any of the fuel lines alone, even if it is all released from a postulated hole in Section C piping, to cause these normally closed steel double doors to fail. In this case, the doors are assumed to leak fuel at a modest rate allowing it to pass down Harbor Tunnel. If a RHBFST was aligned for a fuel movement at the time of the release, and not isolated in time, then the release of fuel would be sufficient to accumulate enough fuel to fail the normally closed set of steel doors.

The NAVFAC water pump station is at a higher elevation than the normally closed double steel doors. The ADIT 3 tunnel gradually increases in elevation so that the tunnel floor at the exit is at 104.65'. Both the normally closed doors below the 3Y split would leak fuel but also hold back the same pool of backed up fuel. It is unclear which of the normally closed doors on the two 3Y splits to the Harbor Tunnel or the ADIT 3 tunnel below 3Y would fail first.

If the double doors to ADIT 3 were to fail first, a wave of fuel of less than tunnel height would enter the ADIT 3 tunnel. However, the elevated exit at ADIT 3 is at 116.65' (i.e., 12' above the tunnel floor) and should not be subject to fuel egress.

The NAVFAC water pump house is next to the ADIT 3 tunnel, near to the normally closed double steel doors. The doors to this pump house are also, but there are grated windows in the wall next to the door the lowest of which is less than one foot above the tunnel floor. The NAVFAC door and wall of filters are not designed to hold back fluids. The wall of filters into the water pump house is only about 6" above the tunnel floor. It's clear that if the double steel doors leading to ADIT 3 fail first, before the steel fire door in the Harbor Tunnel just below 3Y, and a wave of fuel was suddenly released, some portion of the fuel would enter the NAVFAC pump house. In Reference 10-1, there was a concern about an unsealed manhole cover on a platform within the pump house. Leakage passed this manhole cover was assumed to be transported down the water tunnel directly to the aquifer. This cover is mounted on an elevated platform that is about 4' above the pump house floor. NAVFAC HI freshwater division has, partly in response to a recommendation in Reference 10-1, installed a new manhole cover that is now sealed. No other known paths exist via the NAVFAC pump house to the aquifer. Owing to the sequence of events that must all occur to enter the NAVFAC pump house and that there is no known pathway from there to the water tunnel, the QRVA model assumes that this pathway is not viable even if a large volume of fuel is released to the Section C portion of the LAT. Instead, if a large amount of fuel release made its way to Section C portion of the tunnel, it is assumed that the door on the Harbor Tunnel side of the 3Y split would also fail allowing the released fuel to flow downgrade through the Harbor Tunnel.

There is again, insufficient fuel in any of the fuel lines alone, even if it is all released from a postulated hole in Section C piping, to cause the normally ventilation door below 3Y. In this case, the doors are assumed to leak fuel at a modest rate allowing the released fuel to pass down Harbor Tunnel. If a RHBFST was aligned for a fuel movement at the time of the release, and not isolated in time, then the release of fuel would be sufficient to accumulate enough fuel to fail the normally closed ventilation door.

For some postulated fuel releases in which the RHBFSTs are initially idle so that only the fuel line inventory is released, it's doubtful that a 7'-deep backup of fuel would occur that could fail any of the normally closed but not leak tight doors in the LAT. Small leakages passed the normally closed doors, or if the doors to both splits failed, would preferentially travel down the Harbor Tunnel because it's normally closed fire door is a few inches lower than the double steel doors leading to the ADIT 3 tunnel.

In conclusion then, leaks from fuel lines in Section C would either leak passed the doors in the LAT and the normally closed doors below 3Y. If the leak rate is small (i.e., 75 gpm or less) then leakage past the doors is likely to limit an accumulation of fuel at levels sufficient to fail the LAT doors. If the leak rate is larger (i.e., 6" hole) there would be fuel accumulation but likely not enough to fail the door. For leaks with a fuel line aligned to a RHBFST during a fuel movement, then accumulation behind the normally closed doors in the LAT would be expected. There would then be sufficient head from the discharge of fuel Section C fuel line aligned to a RHBFST to fail any of the doors in Section C of the LAT. With failure of the normally closed door to the Harbor Tunnel, flow from Section C should proceed downgrade via the Harbor Tunnel.

The fuel lines in the Harbor Tunnel between 2Y and 3y are referred to as Section B in the QRVA model.

As described above, fuel releases from the Section C fuel lines in the LAT or releases from the tank gallery could find their way to the Harbor Tunnel below 3Y. In addition, postulated fuel leakage from Section B, from a fuel line below 3Y could be directly released there.

In Section B of the Harbor Tunnel, there is a water line riser located at STA 31+41.8 (Elevation 8.41'), about 1.5 miles below 3Y and about two-thirds of a mile above 2Y. The water line riser also appears to be located well below the elevation at which seepage into the aquifer could occur. This riser is sealed off with concrete and therefore not a viable site for fuel leakage.

Also in Section B and above 2Y, there are located two former drainage tunnels; i.e., at STA 26+92.61 and STA 14+5.96. These former drainage tunnels are located about 0. And 0.4 miles above 2Y. Steel plates already covered these drains but since the Reference 10-1 report, the low-point sumps were removed and non-shrink concrete used to fill the drains. These drainage tunnels are no longer considered a viable fuel leakage pathway.

Just above the 2Y intersection in the Harbor Tunnel is a normally open drop track door. This door was referred to as Door C in Reference 10-1. The tunnel floor elevation at Door C is 5.21'. This door is well below the aquifer of concern. This door has no design pressure rating. The door was originally designed as an oil-tight door with a mechanical

sump float for automatic closing. Fuel from above would tend to push the door closed. Even if successfully closed the drop track door would leak due to the train tracks below it. For life safety reasons the mechanical float and this door are now disabled. The QRVA models this door as normally open and could not be closed, so it is not modeled.

There is a tunnel split at 2Y just below this now disabled door. The ADIT 2 tunnel floor is at 4.96'. However, the exit for ADIT 2 is an elevated platform whose floor is at 11.9'; i.e., this is 7' above the tunnel floor. Modest amounts of fuel from 2Y would therefore not be able to exit the ADIT 2 tunnel via this path. The double doors at the elevated ADIT 2 exit are also robust and likely more so than at the UGPH. The doors at ADIT 2 exit can be intermittently open but likely would be closed.

Below the split at 2Y, where the Harbor Tunnel meets the underground pump house (UGPH, Building 59), there is a sump and then two doors to enter the building. High sump levels in the Harbor Tunnel just outside of the UGPH entry provide an alarm on high sump level at the sump pump controls. The AFHE will also alarm on a sump high-high level event.

The UGPH door, reached first from the Harbor Tunnel, is a normally open "isolation" (not oil-tight) door. This door would close automatically on a fire alarm, or if manually actuated from the control room. The second door at this location is a fire door that is normally closed. The second door is provided for fire and ventilation purposes only. Neither door has a design pressure rating. The QRVA assumes that, if closed, both doors at the UGPH entry would fail at a realistic failure pressure corresponding to 7' of fuel above the floor of the doors. Some fuel leakage through the UGPH entry doors would be expected prior to fuel level rising to the realistic door failure pressure. Also one or more of the five sump pumps in the Harbor Tunnel at the UGPH entry would also operate to remove substantial leaked fuel from the tunnel. The UGPH entry tunnel floor is at 3.67' with seven steps leading up to the UGPH entry floor level. Assuming 7" for seven steps this is ~4' above tunnel floor, so that the bottom of the door is at ~7.67'. The realistic failure pressure of the doors then translates to a fluid elevation of 7+7.67'or 14.67' above the tunnel floor at the UGPH entry. The distance from the UGPH entry to a tunnel floor elevation of 14.67' is approximately 0.94 miles; i.e., well above both the split at 2Y and the water line riser. However, this entire distance is believed below the aquifer height which would not then be affected by any release through the tunnels walls and floor.

Tunnel floor elevation at the 2Y is at 5.16'. The ADIT 2 tunnel floor is at 4.96' and the exit platform at ADIT 2 is at 11.9'. This elevation is below the estimated realistic door failure pressure for the UGPH entry; i.e. 14.67'. However, 11.9' is the elevation at the floor of the ADIT 2 doors, not at a realistic failure pressure level. The double doors at ADIT 2 exit are also robust and likely more so than the two doors at the UGPH entry from Harbor Tunnel. Assuming the same 7' realistic failure pressure measured from the base of the door, the ADIT 2 exit doors would fail at a tunnel elevation of 18.9', or 1.03 miles from the UGPH entry. Some fuel leakage through the ADIT 2 door would be expected prior to the realistic door failure pressure. The doors at ADIT 2 can be intermittently open but likely would be closed as level rises during the incident. The QRVA therefore assumes that the doors to the UGPH would fail before the doors at the ADIT 2 exit as fuel level backs up at the base of the Harbor Tunnel.

It would take a lot of fuel to fill up the Harbor Tunnel from the UGPH to a Harbor Tunnel floor level of 14.67' because the tunnel is 10.5' tall in this region. The WillBros (Reference 10-1, Section D.3) computed the volume to completely fill the Harbor Tunnel from the UGPH entry to a Harbor Tunnel floor elevation of 15.267', plus the volume to fill the length of the ADIT 2 tunnel to its roof height of 10.5'as 555,000 $ft^3$. The 15.267' floor elevation is slightly above the 14.67' assumed as the realistic head for the failure pressure of the UGPH entry doors. Further, the 555,000 $ft^3$ result considers that the tunnel must be filled to its 10.5' roof whereas the upper portion of the tunnel need only be filled to 14.67'. So the actual figure is less than 555,000 $ft^3$ but likely more than the WillBros computed volume to fill the tunnel to 10.89'; i.e., 462,000 $ft^3$. Therefore the failure pressure volume is assumed to be 500,000 $ft^3$. This translates to 3.74 million gallons of fuel (or 89,000 barrels). Once the UGPH doors fail, much of this fuel would flow into the UGPH, and out ADIT 1. There is not enough fuel in any of the three fuel lines to accumulate this much fuel in the lower Harbor Tunnel if the RHBFSTs associated with the fuel line postulated to be leaking are all idle. If a fuel movement is in progress and is not isolated, then there would eventually be sufficient fuel leaked to exceed the estimated 3.74 million gallons needed to fail the entry doors at the UGPH.

Only the fuel filled up to the UGPH entry door floor (i.e., 7.67') would remain in the tunnels. The WillBros (Reference 10-1, Section D.3) study estimates a cumulative volume of about 350,000 $ft^3$ to fill the Harbor and ADIT 2 tunnels to this tunnel floor elevation. However, this volume is to fill the tunnels to 10.5'. The Harbor Tunnel floor at the UGPH entry is already at 3.67', so after failure of the doors the tunnel need only be filled another 4' rather than 10.5'. Further, the tunnel is slanted so that the height of the fuel in the tunnel remaining is just half that much on average. Therefore, the total volume remaining after the doors fail is estimated as 350,000 $ft^3$*(4/10.5)*(.5) = 66,700 $ft^3$, which translates to 500,000 gallons (or 12,000 barrels) of fuel. All fuel released to the Harbor Tunnel above that value is assumed released through the failed doors at the entry to UGPH and then out ADIT 1.

The above assessment is largely based on the assumption that the UGPH entry doors and the ADIT 2 exit door have the same failure pressures. Because the ADIT 2 exit is further up the tunnel (1' higher in tunnel floor elevation) and the ADIT 2 door platform is higher than the entry platform to the UGPH (7' instead of 4'), then the latter doors would fail first as fuel accumulates.

Release Category G: This release category is for fuel line leaks of all sizes (i.e., 0.5" or 6") from Section C in which all associated RHBFSTs are initially idle, or they are isolated prior to significant fuel release from the connected RHBFST. The fuel would accumulate behind the LAT doors but would not accumulate high enough (i.e., <5') to fail them. Leakage past all LAT doors would occur at a modest rate (10s of gallons per minute) until all fuel is leaked into the Harbor Tunnel. The released fuel would accumulate in the lower Harbor Tunnel and the ADIT 2 tunnel but not at a level that would over-pressurize the entry doors to the UGPH nor sufficiently to egress through ADIT 2. The amount of fuel accumulated initially behind the LAT doors and eventually at the lower end of Harbor Tunnel would depend on the specific accident sequence.

Release Category H: This release category is for fuel line leaks of all sizes (i.e., 0.5" or 6") from Section C in which a RHBFST is initially aligned for a fuel movement and is not isolated prior to significant fuel release from the connected RHBFST. With the

added head of the connected RHBFST, the released fuel would accumulate behind the LAT doors high enough (i.e., >5') to fail them. Leakage past all LAT doors would occur at a modest rate (10s of gallons per minute) until the doors fail. At that time, all fuel would be released into the Harbor Tunnel. The released fuel would accumulate in the lower Harbor Tunnel and the ADIT 2 tunnel at a level that would over pressurize the entry doors to the UGPH; i.e., after more than 3.74 million gallons (or 89,000 barrels) had accumulated. Once the entry doors to the UGPH fail, most of the accumulated fuel would be released into the UGPH and out ADIT 1. Only 500,000 gallons would remain the Harbor Tunnel. The amount of fuel accumulated initially behind the LAT doors or eventually released into the UGPH at the lower end of Harbor Tunnel would depend on the specific accident sequence. Steps taken to empty the aligned RHBFST would decrease the total amount of fuel released.

Release Category I: This release category is for fuel line leaks of all sizes (i.e., 0.5" or 6") from Sections A or B in which all associated RHBFSTs are initially idle, or they are isolated prior to significant fuel release from the connected RHBFST. The released fuel would flow directly down Harbor Tunnel and accumulate in the lower Harbor Tunnel and the ADIT 2 tunnel, but not at a level that would over-pressurize the entry doors to the UGPH or to sufficiently to egress through ADIT 2. The amount of fuel accumulated at the lower end of Harbor Tunnel would depend on the specific accident sequence.

Release Category J: This release category is for fuel line leaks of all sizes (i.e., 0.5" or 6") from Section A or B in which a RHBFST is initially aligned for a fuel movement and is not isolated prior to significant fuel release from the connected RHBFST. The released fuel would flow directly down Harbor Tunnel and accumulate in the lower Harbor Tunnel and the ADIT 2 tunnel. With the added release from the connected RHBFST, the released fuel would accumulate in the lower Harbor Tunnel and the ADIT 2 tunnel at a level that would over-pressurize the entry doors to the UGPH; i.e., after more than 3.74 million gallons (or 89,000 barrels) had accumulated. Once the entry doors to the UGPH fail, most of the accumulated fuel would be released into the UGPH and out ADIT 1. Only 500,000 gallons would remain the Harbor Tunnel. The amount of fuel accumulated and then released through the UGPH would depend on the specific accident sequence. Steps taken to empty the aligned RHBFST would decrease the total amount of fuel released.

### 10.4.5 Leaks from Fuel Lines and RHBFSTs if the New Oil Door Does Not Close

This section presents the release categories which are similar to those already discussed above but are changed here for conditions involving the added failure of the new oil tight door to close. Only those release categories where the failure to close the door would matter are presented.

Release Category K: This release category is like Release Category C except that the new oil-tight door fails to close. It involves a large (6" hole) JP5 fuel line leakage into Zone 7 with a RHBFST undergoing a fuel evolution, the leaking fuel line and the associated RHBFST are not isolated, or there is a large (6" hole) RHBFST nozzle leak from one of the RHBFSTs in Zone 7, which is not isolable. Fuel levels in Zone 7 would rise well above the bulkhead isolation door. Once discharged from RHBFST 20, fuel would fill up Zone 7 to the tunnel roof and rise up the Elevator 73 shaft. The bulkhead

penetrations would see rising fuel levels and begin releasing fuel to the tank gallery portion of the LAT. The Zone 7 sump pump would may also transfer fuel to the tank gallery until its electrical controls are flooded. As described for Release Category C, as much as 100,000 barrels may be released out ADIT 6. Afterwards, the leaking RHBFST fuel level would equilibrate at about 121'. The Zone 7 bulkhead and isolation door maintain their integrity despite the accumulated fuel in Zone 7. There it may seep via the Zone 7 walls and tunnel floor into the surrounding rock under the add pressure. Additionally, fuel would be leaking from the floor and walls of the tank gallery portion of the LAT and from Harbor Tunnel and ADIT 2. At a flow rate of 75 gpm, it would take more than a month for the released fuel that flows down the Harbor Tunnel to accumulate sufficiently to over-pressurize the normally closed doors at the UGPH.

Release Category L: This release category is like Release Category D, except that the new oil door also fails to close. If fuel line leakage into Zone 7 occurs via a small (0.5") RHBFST nozzle leak, which is not isolable, the leakage flow rate would be about 75 gpm. This flow rate is large enough to accumulate fuel in Zone 7 until the leaked fuel level reaches the penetrations in the bulkhead above the isolation door. At that time flow through the bulkhead penetrations is expected to match the leakage rate through the RHBFST nozzle so that fuel level in Zone 7 stabilizes. Fuel level in the leaking RHBFST would continue to drop as it discharges through the hole and exits through the bulkhead penetrations into the tank gallery portion of the LAT. Flow would not accumulate in the cargo elevator nor rise to the level of the ADIT 6 tunnel. Of course, if Red Hill staff also take steps to empty the leaking RHBFST, the overall amount of fuel leaked into Zone 7 would be reduced. A similar sequence would involve a small hole (0.5") in a JP5 Section E fuel line which is also not isolated, and the RHBFST is not emptied before levels reached the bulkhead penetrations above the Zone 7 isolation door. Fuel released from any of RHBFSTs 17 through 20 via 0.5" size holes, and after accumulation in Zone 7, would leak through the penetrations above the bulkhead isolation door. The flow from the bulkhead penetrations would flow downgrade in the tank gallery below the bulkhead, passed Gauger station and the electrical room. The electrical room door is normally closed, but is not oil-tight so some fuel seepage into the electrical room is expected. In this release category, the new oil door fails to close. Fuel released to the tank gallery would flow down the LAT leaking passed the normally closed doors in the LAT, and then downgrade to the lower Harbor Tunnel. There would be almost no depth of fuel in the tank gallery. Even after the loss of 100,000 barrels from a RHBFST initially at 212', the RHBFST level would still be at 121' sustaining the 75 gpm flow rate for some time. The fuel released through the bulkhead penetrations eventually flows down the tank gallery, through the failed open new oil door, and leaks passed the normally closed doors in the LAT and below 3Y. Later, fuel would be leaking from the floor and walls of the tank gallery portion of the LAT, from Harbor Tunnel and ADIT 2, and from Zone 7, which would have the added pressure from the elevated head of the fuel remaining in the RHBFST connected to Zone 7. The fuel released through the bulkhead penetrations eventually flows down the tank gallery, through the failed open new oil door, and leaks passed the normally closed doors in the LAT and below 3Y. Later, fuel would be leaking from the floor and walls of the tank gallery portion of the LAT, the ADIT 3 tunnel, from Harbor Tunnel and ADIT 2, and from Zone 7, which would have the added pressure from the head of fuel remaining in the RHBFST connected to Zone 7. It may take a month before sufficient fuel would accumulate at the UGPH entry to fail its two doors.

This category of fuel releases involve leaks originating from fuel lines in the tank gallery portion of the LAT and below the main sump, but upstream of the new oil tight door. Such events would include large (6" hole) or small (0.5") nozzle leaks at the skin valve of a RHBFST, and large (6") or small (0.5") leaks from the fuel lines in these areas with fuel movement in progress. A maintenance error resulting in opening of a fuel line while that fuel type is undergoing a fuel movement also applies. For the fuel line leaks in this release category, there is also a fuel movement in progress and the associated RHBFST is not isolated from the leaking fuel line.

Release Category M: This release category is similar to Release Category E except that the new oil door also fails to close. It involves a large amount of fuel being released to the tank gallery portion of the LAT; i.e., near RHBFSTs 1–16, via a fuel line in Section D or E. The released fuel flows down the tank gallery, through the failed open, new oil door, and either leaks passed the normally closed doors in the LAT and below 3Y, or accumulates sufficiently above them to cause the normally closed doors to fail. Later, fuel would be leaking from the floor and walls of the tank gallery portion of the LAT, from Harbor Tunnel, ADIT 3 tunnel, and the ADIT 2 tunnel. The fuel depth at every portion of the tank gallery and tunnels would be limited, except at the bottom of Harbor Tunnel. At a flow rate of 75 gpm, it is estimated that it would take more than a month to increase the accumulated fuel level at the bottom of Harbor Tunnel sufficiently above the UGPH entry doors to fail them. For a larger leak rate corresponding to a 6" hole, the time would be much shorter (within several hours), and well before the aligned RHBFST fully empties.

This category of fuel releases involve leaks originating from fuel lines in the tank gallery portion of the LAT and below, but upstream of the new oil tight door. Such events would include large (6" hole) or small (0.5") nozzle leaks at the skin valve of a RHBFST, and large (6") or small (0.5") leaks from the fuel lines in these areas with a fuel movement in progress at the time the hole develops. A maintenance error resulting in the inadvertent opening of a fuel line undergoing a fuel movement at the same time also applies. For the fuel line leaks in this release category, there is also a fuel movement in progress and the associated RHBFST is not isolated from the leaking fuel line.

Release Category N: This release category is similar to Release Category F, in that the release is to the LAT below the Zone 7 bulkhead but in this case the new oil door fails to close. The amount of fuel released is much small than for Release Category M. The RHBFSTs on the affected fuel line are all idle, or if not then isolated relatively quickly from the hole location. The amount of fuel released is a function of the fuel line type and its fuel contents above the break location. Only the fuel inventory in QRVA Fuel Line Sections D or E applies. Though normally open, if the corresponding sectional valve near RHBFSTs 11 and 12 is isolated, the amount of fuel released is further reduced. With the RHBFSTs idle, only the fuel above the hole location is released. Operation of the main sumps to transfer fuel to Tank S311 may remove up to 450 barrels of fuel by transferring them to Tank S311 outside ADIT 3. Operation of the sump pumps at the entry to the UGPH could remove much more fuel as it accumulates at that location.

Without closure of the new oil-tight door, the released fuel would proceed down the tank gallery passing through the new oil door bulkhead and downgrade through the LAT to the normally closed doors. There, leakage passed the normally closed doors would occur. There is insufficient fuel leaked for these scenarios to accumulate enough head

to fail the normally closed doors. For either size leak rate, the leaked fuel would then proceed below 3Y and down the Harbor Tunnel. Eventually, fuel would be leaking from the floor and walls of the tank gallery portion of the LAT from relatively shallow fuel depths, from ADIT 3 tunnel, and from Harbor Tunnel and the ADIT 2 tunnel at increasing fuel depths.

The maximum amount of fuel in QRVA Fuel Line Sections D and E (i.e., above the new oil tight door) for each fuel type are as follows:

F24 (16") – 20,000 Gallons (~500 barrels)

JP5 (18") – 39,000 Gallons (~900 barrels)

F76 (32") – 68,000 Gallons (~1,600 barrels)

For these amounts of fuel accumulated at the base of Harbor Tunnel, there would be insufficient head to fail the doors at the entry to the UGPH. Even for a full accumulation of the F76 inventory (68,000 gallons, or 9,090 $ft^3$.) this would result in just a one foot deep pool of fuel backed upgrade about 900' from the UGPH entry.

This category of fuel releases involve leaks originating from fuel lines in the tank gallery portion of the LAT and below, but upstream of the new oil tight door. Such events would include large (6") or small (0.5") fuel line leaks in these areas with no fuel movement in progress. Release Category N also applies for maintenance errors that result in a full opening of a fuel line, if all RHBFSTs on that line are in idle.

### 10.4.6 Summary

A summary of the different release categories (i.e., RELA through RELN) is provided in Table 10-1. The summarized definitions of the release categories are extracted from the above descriptions. A summary of sequence types that are mapped to each release category are also provided in the table. The total amount of gallons of fuel released in a given release category varies with the individual sequence assigned to the release category.

## 10.5 Section 10 Reference

10-1. "Red Hill Complex Fire, Safety, Life Safety, and Environmental Risk Assessment/Analysis Volume I of II, Final Submittal," prepared by WillBros Engineers, Inc., for Department of the Navy Pacific Division Naval Facilities Engineering Command, Pearl Harbor, Hawaii, August 1998.

# 11. Risk Uncertainty Analysis

## 11.1 Introduction

In QRVA, while point estimate quantification of risk can provide a general illustration of risk assessment results, it cannot provide a comprehensive presentation of risk. To provide a valid basis for decision-making support, risk results must be expressed via a presentation of not only best estimates but also the uncertainty we can express in those results. In general, there are two major types of uncertainty considered in QRVA, aleatory uncertainty and epistemic uncertainty, which are described herein. In laymen terms, these types of uncertainty roughly translate to data uncertainty and modeling uncertainty. The data uncertainty for QRVA input variables has been presented in Sections 5 and 8 of this report via the presentation of probability distributions for initiating event data, hardware response data, and HFE HEPs. In QRVA uncertainty analysis, these probability distributions are propagated through the event sequence quantification process to develop probability distributions about the QRVA results.

## 11.2 Bases and Assumptions

The bases and assumptions for the development of the risk uncertainty analysis are summarized below.

1. Parameter uncertainties are propagated through the full QRVA models to provide an estimate of the uncertainties in the frequencies of each sequence group.

2. The sequence quantification used for uncertainty analysis is 1E-12 per year.

3. The Monte Carlo uncertainty propagation was performed for 2,000 samples.

## 11.3 QRVA Uncertainty Analysis General Methodology

The probability or frequency estimates that are obtained by analyzing fault trees or event trees are generally associated with considerable uncertainty. The uncertainty comes from the following principal sources:

- The specified models are incorrect. Basic assumptions about the accident sequences, system-failure modes, and the application of the quantification formulas may not be correct.

- Important failure modes have been overlooked (completeness problem). The scope of the risk assessment may preclude the analysis of all initiating events, the analyst may not have all the required information, or the quantification process may have truncated large numbers of low-probability events that sum to a significant probability.

- The values of the input parameters are not exactly known. Data limitations or uncertainties in component-failure rates require the use of probability distributions or

interval estimates to model frequencies for initiating events and probabilities for system failures.

Although it may be possible to quantify the contribution to total uncertainty made by each of these sources, in practice it is very difficult to develop credible quantitative measures for all the sources of uncertainty in the analysis. It is usually more practical to perform additional analyses to ensure that the modeling is correct than to try estimating a particular quantitative uncertainty. This section discusses these uncertainty sources and describes a method for evaluating their contribution to total uncertainty in the analysis.

### 11.3.1 Sources of Uncertainty

Table 11-1 lists the uncertainties that can affect the estimates of accident-sequence frequencies as well as the sections of this guide that discuss these uncertainties. The major sources of uncertainty that are directly related to accident-sequence quantification are truncation schemes that eliminate accident sequences or accident-sequence cut sets that are determined to be insignificant. The errors they produce are nonconservative. Another source of error in quantification is the rare-event approximation used to develop a probability expression for the accident sequences; it produces conservative errors. Accident-sequence quantification provides the opportunity for assessing the effect of uncertainties in the input data on the calculated frequencies of accident sequences.

**Table 11-1. Contributors to Uncertainty in Estimates of Accident-Sequence Frequency**

| Uncertainty Type | Source of Uncertainty | QRVA Procedures Guide Section |
|---|---|---|
| Model Uncertainties | Event and fault-tree models do not correctly account for time-dependent component failures, component dependences, etc. | 3.9 |
| | Failure modes improperly defined | 3.9 |
| | Component-failure models may not be correct (i.e., exponential failure model) | 5.7 |
| | Approximations are used to sum large numbers of cut sets (i.e., rare-event approximation) | 6.4.1 |
| | Human Errors | 4 |
| | External Events | 10.4, 11.2, 11.3, 11.4 |
| Completeness | Event- and fault-tree models do not contain important failure modes | 3.9 |
| | Database may not include all pertinent failures or experience | 5.7 |
| | Large numbers of low-probability accident sequences and cut sets may have been eliminated through truncation | 6.4.1 |
| Input-Parameter Uncertainty | Mission time for the operation of various systems may not be known exactly | 3.9 |
| | There are uncertainties in the frequencies of initiating events, component-failure rates, and test and maintenance parameters | 5.7, 6.4.1 |

### 11.3.2 Some Procedures for Uncertainty and Sensitivity Analysis

The uncertainty introduced through Boolean manipulations, truncations, and screenings should be small in comparison with that in the accident sequence logic models and the database. However, significant uncertainty can be introduced through the elimination of large numbers of low-frequency cut sets or accident sequences whose sum contributes significantly to the FDB frequency. In order to quantify this contribution, the cut sets must be generated and quantified. Unfortunately, most truncation schemes used in fault-tree analysis have no capability for estimating this contribution.

One way to estimate the total contribution of many low-frequency events is to use a direct-quantification code like WAM-BAM (see Section 6.6 of NUREG/CR-2300). The direct-quantification codes are very efficient and can use a much lower truncation value because they do not have to perform cut-set manipulations. Moreover, WAM-BAM has the capability to estimate an upper bound on the sum total of the truncated terms. By comparing the direct-quantification result obtained with a lower truncation value against the result of the cut-set solution, the analyst can determine whether a lower truncation value would significantly affect the result. In addition, the WAM-BAM output can be examined to determine the upper bound probability of the terms eliminated during the direct quantification. If the value is small, the use of truncation can be shown to have a small effect on the cut-set solution process.

When trying to evaluate the contribution to system-failure probability from variations in input parameters, the analyst can either perform a probabilistic importance analysis to get a qualitative feel for the effect of input parameters on the results or derive probability distributions or interval estimates for the result.

Probabilistic importance measures are a means of estimating the contribution of a primary event to the accident-sequence frequency. There are three principal types of measure: the Barlow-Proschan (Reference 11-1), the Fussell-Vesely (Reference 11-2), and the Birnbaum (Reference 11-3) measures; they have been defined and described by Lambert and Gilman (Reference 11-4). The Barlow-Proschan and the Fussell-Vesely measures are more closely related to each other than to the Birnbaum measure. The exact nature of the relationships among these and other measures is discussed by Engelbrecht-Wiggans and Strip (Reference 11-5).

The Barlow-Proschan and the Fussell-Vesely measures compute the probability that a primary event is contributing to the failure of a system and therefore provide information on which primary events, if made more failure resistant through improved quality or redundancy, will most decrease the probability of a system failure.

The Barlow-Proschan measure of the importance of a primary event i is the probability of the system failing because a minimal cut set containing i fails, with Primary Event i failing last. By this definition, the most important primary event in a system is the most unlikely primary event in the most likely minimal cut set.

The Fussell-Vesely measure of the importance of a primary event is the probability Primary Event i is contributing to system failure, given the system has failed. It is estimated by dividing the sum of the failure probabilities of the minimal cut sets that contain Primary Event i by the failure probability of the system. The most important primary event in the system according to this definition is the primary event in the most likely group of minimal cut sets. Thus, this definition gives some measure of the probability that the recovery of a primary event will restore the system.

The Birnbaum measure indicates the sensitivity of the overall system failure probability to the probability of an individual primary event. Thus, it measures the rate of change in system-failure probability to change in primary-event probability. The upgrading function, which is closely related to the Birnbaum measure, can be used in many circumstances to help decide which primary events would contribute most to reducing system-failure probability.

As described by Engelbrecht-Wiggans and Strip (Reference 11-5), these measures are intimately linked, and their differences are quite subtle. It is therefore difficult to recommend which measures are appropriate in different situations. The choice between the Barlow-Proschan/Fussell-Vesely and the Birnbaum measures is difficult because they measure slightly different aspects of system-failure probability, although frequently the former measures are more appropriate for measuring system improvement.

However, Lambert (Reference 11-6) demonstrates the use of the upgrading function (a variant of the Birnbaum measure) for selecting primary events for change to improve system-failure probability.

Chapter 12 of NUREG/CR-2300 discusses various methods for performing sensitivity studies and for propagating probability distribution and interval estimates based on the simplified equation for the frequency. Section 6.6 of NUREG/CR-2300 discusses the computer codes (e.g., SAMPLE) that can be used in the actual propagation. The manner in which the propagation is performed should be consistent with the data used in the analysis.

A consideration in the propagation of primary event uncertainty through a top event probability expression is the method of treating the uncertainty distribution or interval estimates of two primary event probabilities derived from components that are identical. Their uncertainty parameters are considered to be correlated. In evaluating the probability expression, only one distribution should be used to represent uncertainty for every primary event whose probability is derived from components assumed to be identical. Consider, for example, the probability expression

$$\begin{aligned} \mathrm{P(top)} = {} & \mathrm{P(pump\ A)} * \mathrm{P(pump\ B)} \\ & + \mathrm{P(pump\ A)} * \mathrm{P(control\ B)} \\ & + \mathrm{P(pump\ B)} * \mathrm{P(control\ A)} \\ & + \mathrm{P(control\ A)} * \mathrm{P(control\ B)} \end{aligned}$$

If Pumps A and B along with Controls A and B are assumed to have identical failure rates, the probability expression should be changed to the form

$$\mathrm{P(top)} = [\mathrm{P(pump)}]^2 + 2[\mathrm{P(pump)\ P(control)}] + [\mathrm{P(control)}]^2$$

In this way, the assumption that the primary events are identical can be correctly evaluated. With independent primary events and distributions, the sums or products of the means of the distributions for the individual primary events will yield the correct mean for the top event. The potential cause for error in assuming that components are identical has been discussed by Apostolakis and Kaplan (Reference 11-7). In practice, the propagation of uncertainty in primary-event probability may be very difficult to perform by methods other than Monte Carlo for large numbers of independent modules containing similar components.

## 11.4 Monte Carlo Uncertainty Analysis

The RHBFSF QRVA systematically identified and quantified the frequency of acute sequences involving fuel releases from both the RHBFSTs and the associated fuel lines located in the LAT and Harbor Tunnel. As described in Section 12, there are numerous ways to characterize the assessed fuel release results. The frequencies of sequence groups within a range of amounts of fuel released, in gallons, are selected for uncertainty analysis.

The data variable, or parameter, uncertainties are propagated through the acute sequence models using Monte Carlo simulation to develop uncertainty distributions of the frequencies for each of the selected sequence group. The Monte Carlo propagation is performed using the Big Loop Monte Carlo module of the RISKMAN software; [redacted]. During each sample of the simulation, the initiating event frequencies, the split fraction probabilities, and the sequence frequencies are calculated using the QRVA models. Sampling is performed on each of the data variable distributions and then used to quantify the entire model. No truncation limits are needed for the evaluation of initiating event frequencies or of the split fraction values. A sequence frequency cutoff of 1E-12 per year is used for the event sequence models, consistent with the base case quantification cutoff.

Table 11-2 summarizes the uncertainty analysis results. Key percentiles of the resulting uncertainty distributions and the mean values are provided for each sequence group. The 90% confidence range is taken as between the 5% and 95% percentiles.

Included in Table 11-2 are common measures of the uncertainty of each sequence group frequency. The error factor provides an indication of the spread of the distribution above the median. The range factor provides an indication of the full spread of the distribution between the low (i.e., 5%) and high side (95%). As expected, the spread in the uncertainty is larger when assessing the frequencies of sequence groups for the larger amounts of fuel released, which are also correspondingly much less likely.

## Table 11-2. Uncertainty Distribution Characteristics for Selected Sequence Group Frequencies

| Sequence Group ID | 5th % | 50th % | 95th % | Mean | Sequence Group Description | Error Factor (95%/50%) | Range Factor (95%/5%)$^{1/2}$ |
|---|---|---|---|---|---|---|---|
| *Sequence Groups for the Frequency of Exceeding a Given Amount of Fuel Released* | | | | | | | |
| AGT1 | 0.225 | 0.315 | 0.521 | 0.346 | All acute IEs with fuel release | 1.7 | 1.5 |
| BGT30 | 8.24E-03 | 1.50E-02 | 4.11E-02 | 1.99E-02 | All acute IEs with fuel release >30k gallons | 2.7 | 2.2 |
| CGT60 | 1.67E-03 | 5.40E-03 | 1.43E-02 | 6.48E-03 | All acute IEs with fuel release >60k gallons | 2.6 | 2.9 |
| DGT120 | 9.56E-04 | 3.52E-03 | 9.57E-03 | 4.22E-03 | All acute IEs with fuel release >120k gallons | 2.7 | 3.2 |
| EGT250 | 5.06E-04 | 2.30E-03 | 7.77E-03 | 3.06E-03 | All acute IEs with fuel release >250k gallons | 3.4 | 3.9 |
| FGT500 | 1.18E-04 | 5.23E-04 | 1.49E-03 | 6.38E-04 | All acute IEs with fuel release >500k gallons | 2.9 | 3.6 |
| GGT1M | 1.00E-04 | 4.64E-04 | 1.35E-03 | 5.65E-04 | All acute IEs with fuel release >1 Million gallons | 2.9 | 3.7 |
| HGT2M | 5.61E-06 | 9.09E-05 | 6.97E-04 | 1.87E-04 | All acute IEs with fuel release >2 Million gallons | 7.7 | 11.2 |
| IGT10M | 2.83E-06 | 7.27E-05 | 5.76E-04 | 1.52E-04 | All acute IEs with fuel release >10 Million gallons | 7.9 | 14.3 |
| *Sequence Groups for the Frequency of Fuel Released within a Given Range of Gallons* | | | | | | | |
| JLT30 | 2.14E-01 | 2.99E-01 | 4.82E-01 | 3.26E-01 | All acute IEs with fuel release between 1k & 30k gallons | 1.6 | 1.5 |
| KLT60 | 5.47E-03 | 9.06E-03 | 3.13E-02 | 1.34E-02 | All acute IEs with fuel release between 30k & 60k gallons | 3.5 | 2.4 |
| LLT120 | 3.17E-04 | 1.39E-03 | 6.32E-03 | 2.26E-03 | All acute IEs with fuel release between 60k & 120k gallons | 4.6 | 4.5 |

**Table 11-2. Uncertainty Distribution Characteristics for Selected Sequence Group Frequencies (Continued)**

| Sequence Group ID | 5th % | 50th % | 95th % | Mean | Sequence Group Description | Error Factor (95%/50%) | Range Factor $(95\%/5\%)^{1/2}$ |
|---|---|---|---|---|---|---|---|
| MLT250 | 2.68E-04 | 9.90E-04 | 2.61E-03 | 1.16E-03 | All acute IEs with fuel release between 120k & 250k gallons | 2.6 | 3.1 |
| NLT500 | 3.25E-04 | 1.81E-03 | 6.41E-03 | 2.43E-03 | All acute IEs with fuel release between 250k & 500k gallons | 3.5 | 4.4 |
| OLT1M | 8.54E-06 | 4.29E-05 | 2.21E-04 | 7.31E-05 | All acute IEs with fuel release between 500k & 1million gallons | 5.2 | 5.1 |
| PLT2M | 3.76E-05 | 2.76E-04 | 1.02E-03 | 3.78E-04 | All acute IEs with fuel release between 1 & 2 million gallons | 3.7 | 5.2 |
| QLT10M | 1.81E-06 | 1.89E-05 | 1.25E-04 | 3.49E-05 | All acute IEs with fuel release between 2 & 10 million gallons | 6.6 | 8.3 |

## 11.5 Section 11 References


11-1 Barlow, R. E., and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York, 1975.

11-2 Fussell, J. B., "How to Hand Calculate System Reliability Characteristics," IEEE Transactions of Reliability, Vol. R-24, No. 3, 1975.

11-3 Birnbaum, Z. W., "On the Importance of Different Components in a Multi-System in Multivariate Analysis," Academic Press, New York, 1969.

11-4 Lambert, H. E., and F. M. Gilman, "The Importance Computer Code," ERDA Report UCRL-79269, Lawrence Livermore National Laboratory, Livermore, California, 1977.

11-5 Engelbrecht-Wiggans, R., and D. R. Strip, "On the Relation of Various Reliability Measures to Each Other and to Game Theoretic Values," SANDB0-2624, Sandia National Laboratories, Albuquerque, New Mexico, 1981.

11-6 Lambert, H. E., "Fault Trees for Decision-Making in Systems Analysis," Ph.D. thesis, UCRL-51829, Lawrence Livermore National Laboratory, Livermore, California, 1975.

11-7 Apostolakis, G. E., and S. Kaplan, "Pitfalls in Risk Calculations," Reliability Engineering, Vol. 2, pp. 135–145, 1981.

# 12. Facility Risk Quantitative Results (Phase 1)

This section describes the frequency high level quantification results for the acute release sequences from internal initiating events only. The acute accident event sequence models are described earlier in Section 6.7. Three parts of results are presented in this section, for sequence group frequencies, for initiating event contributions to selected sequence groups, and end state frequencies.

## 12.1 Bases and Assumptions

The bases and assumptions for the development of the facility risk quantitative results are summarized below.

1. The assessment of contributors is performed by examining the point estimate sequence frequencies; i.e., where the split fractions and sequence frequencies are quantified using the mean values of each data parameter.

2. A sequence quantification cutoff of 1E-12 per year is used for the base case calculation of sequence group frequencies and end state frequencies; i.e., the results are converged for this level of cutoff. All individual sequence frequencies with lower frequencies are discarded, because they are not significant.

3. A sequence quantification cutoff of 1E-15 per year is used for calculations of importance measures reported in this section.

## 12.2 Sequence Group Frequency Results

The acute sequence frequency results for internal initiating events are discussed in this section. Table 12-1 presents the summation of all internal initiating event sequences for a number of sequence groups. The sequence quantification results presented utilized an individual sequence cutoff of 1E-12 per year; i.e., all sequences with cutoffs less than 1E-12 were eliminated. There are seven sets of sequence groups presented in the table. The first set presents the exceedance frequencies for the summation of sequence frequencies above a given number of gallons of fuel. The amount of fuel released is tabulated in thousands of gallons. Nine different release measures are listed. Sequence Group AGT1 lists the frequency of all acute release sequences in which at least 1,000 gallons of fuel are released. This group's frequency total is nearly the same as the sum of all initiating event frequencies, with one exception. The overfill challenge frequencies are not likely to end in any release. This challenge frequency is for the number of times per year that fuel level is being raised near the maximum operating levels; e.g., in preparation for the annual leak tightness tests. The other sequence groups in Set I are also exceedance frequencies but involve different levels of gallons released.

## Table 12-1. Acute Sequence Group Frequencies per Year

| Sequence Group Name | Frequency (events per year) of Single Sequence Group | Sequence Group Description |
|---|---|---|
| **Set I** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater for All Initiating Events** | |
| AGT1 | 3.43E-01 | All acute Initiating Events with fuel release >1,000 gallons |
| BGT30 | 1.95E-02 | All acute Initiating Events with fuel release >30k gallons |
| CGT60 | 6.51E-03 | All acute Initiating Events with fuel release >60k gallons |
| DGT120 | 4.25E-03 | All acute Initiating Events with fuel release >120k gallons |
| EGT250 | 3.06E-03 | All acute Initiating Events with fuel release >250k gallons |
| FGT500 | 6.34E-04 | All acute Initiating Events with fuel release >500k gallons |
| GGT1M | 5.64E-04 | All acute Initiating Events with fuel release >1 Million gallons |
| HGT2M | 1.87E-04 | All acute Initiating Events with fuel release >2 Million gallons |
| IGT10M | 1.52E-04 | All acute Initiating Events with fuel release >10 Million gallons |
| **Set II** | **Frequency (events per year) of a Range of Fuel Releases for All Initiating Events** | |
| JLT30 | 3.24E-01 | All acute Initiating Events with fuel release between 1k & 30k gallons |
| KLT60 | 1.30E-02 | All acute Initiating Events with fuel release between 30k & 60k gallons |
| LLT120 | 2.26E-03 | All acute Initiating Events with fuel release between 60k & 120k gallons |
| MLT250 | 1.18E-03 | All acute Initiating Events with fuel release between 120k & 250k gallons |
| NLT500 | 2.43E-03 | All acute Initiating Events with fuel release between 250k & 500k gallons |
| OLT1M | 6.92E-05 | All acute Initiating Events with fuel release between 500k & 1million gallons |
| PLT2M | 3.77E-04 | All acute Initiating Events with fuel release between 1 & 2 million gallons |
| QLT10M | 3.49E-05 | All acute Initiating Events with fuel release between 2 & 10 million gallons |

## Table 12-1. Acute Sequence Group Frequencies per Year (Continued)

| Sequence Group Name | Frequency (events per year) of Single Sequence Group | Sequence Group Description |
|---|---|---|
| **Set III** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater Only for Initiating Events Involving a Specific Fuel Type** | |
| F24GT1 | 9.57E-02 | Fuel F24 acute Initiating Events with fuel release >1,000 gallons |
| F24GT120 | 1.01E-03 | Fuel F24 acute Initiating Events with fuel release >120k gallons |
| F24GT1M | 6.90E-05 | Fuel F24 acute Initiating Events with fuel release >1 Million gallons |
| F76GT1 | 2.82E-02 | Fuel F76 acute Initiating Events with fuel release >1,000 gallons |
| F76GT120 | 1.01E-03 | Fuel F76 acute Initiating Events with fuel release >120k gallons |
| F76GT1M | 3.65E-04 | Fuel F76 acute Initiating Events with fuel release >1 Million gallons |
| JP5GT1 | 2.19E-01 | Fuel JP5 acute Initiating Events with fuel release >1,000 gallons |
| JP5GT120 | 2.24E-03 | Fuel JP5 acute Initiating Events with fuel release >120k gallons |
| JP5GT1M | 1.30E-04 | Fuel JP5 acute Initiating Events with fuel release >1 Million gallons |
| **Set IV** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater for Indicated Types of Initiating Events** | |
| ROCKGT1 | 2.90E-01 | All Leak to Rock Initiating Events with fuel release >1,000 gallons |
| ROCKGT120 | 6.09E-04 | All Leak to Rock Initiating Events with fuel release >120k gallons |
| ROCKGT1M | 3.89E-05 | All Leak to Rock Initiating Events with fuel release >1 Million gallons |
| OVFGT1 | 4.66E-02 | All Overfill Initiating Events with fuel release >1,000 gallons |
| OVFGT120 | 0.00E+00 | All Overfill Initiating Events with fuel release >120k gallons |
| OVFGT1M | 0.00E+00 | All Overfill Initiating Events with fuel release >1 Million gallons |
| NOZGT1 | 3.00E-03 | All Initiating Events involving leaks from a RHBFST Nozzle with a fuel release >1,000 gallons |

## Table 12-1. Acute Sequence Group Frequencies per Year (Continued)

| Sequence Group Name | Frequency (events per year) of Single Sequence Group | Sequence Group Description |
|---|---|---|
| NOZGT120 | 2.79E-03 | All Initiating Events involving leaks from a RHBFST Nozzle with a fuel release >120k gallons |
| NOZGT1M | 5.20E-04 | All Initiating Events involving leaks from a RHBFST Nozzle with a fuel release >1 Million gallons |
| TUNGT1 | 3.21E-03 | All Initiating Events involving leaks to a Red Hill Tunnel with a fuel release >1,000 gallons |
| TUNGT120 | 8.49E-04 | All Initiating Events involving leaks to a Red Hill Tunnel with a fuel release >120k gallons |
| TUNGT1M | 4.59E-06 | All Initiating Events involving leaks to a Red Hill Tunnel with a fuel release >1 Million gallons |
| **Set V** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater for Initiating Events Resulting from Maintenance Errors** | |
| MAINTGT1 | 2.74E-05 | All Maintenance Error Initiating Events with fuel release >1,000 gallons |
| MAINTGT120 | 9.14E-07 | All Maintenance Error Initiating Events with fuel release >120k gallons |
| MAINTGT1M | 8.50E-07 | All Maintenance Error Initiating Events with fuel release >1 Million gallons |
| **Set VI** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater for Initiating Events Involving Leak to Rock at the time of a RHBFST Return to Service (i.e., following extended RHBFST maintenance when the RHBFST liner if most susceptible to leaking)** | |
| RTSGT1 | 1.00E-01 | Initiating Events involving leaks to rock during a RHBFST return to service with fuel releases >1,000 gallons |
| RTSGT120 | 2.51E-04 | Initiating events involving leaks to rock during a RHBFST return to service with fuel releases >120k gallons |
| RTSGT1M | 0.00E+00 | Initiating Events involving leaks to rock during a RHBFST return to service with fuel releases >1 Million gallons |
| **Set VII** | **Frequency (events per year) of Indicated Amount of Fuel Released or Greater, but Only for Events Occurring during a Particular Fuel Movement State (i.e., while all RHBFSTs are idle, one or more is receiving fuel, one or more is issuing fuel, or during a gravity transfer between RHBFST)** | |
| IDLEGT1 | 2.83E-01 | Sequences initiated while all RHBFSTs are Idle resulting in a fuel release >1,000 gallons |
| IDLEGT120 | 4.13E-03 | Sequences initiated while all RHBFSTs are Idle resulting in a fuel release >1,000 gallons >120k gallons |

## Table 12-1. Acute Sequence Group Frequencies per Year (Continued)

| Sequence Group Name | Frequency (events per year) of Single Sequence Group | Sequence Group Description |
|---|---|---|
| IDLEGT1M | 5.45E-04 | Sequences initiated while all RHBFSTs are Idle resulting in a fuel release >1,000 gallons >1 Million gallons |
| RECEVGT1 | 5.92E-02 | Sequences initiated while one or more RHBFSTs are receiving fuel when a fuel release >1,000 gallons occurs |
| RECEVGT120 | 7.44E-05 | Sequences initiated while one or more RHBFSTs are receiving fuel when a fuel release >120k gallons occurs |
| RECEVGT1M | 9.07E-06 | Sequences initiated while one or more RHBFSTs are receiving fuel when a fuel release >1 million gallons occurs |
| ISSUEGT1 | 1.21E-03 | Sequences initiated while one or more RHBFSTs are issuing fuel when a fuel release >1,000 gallons occurs |
| ISSUEGT120 | 3.77E-05 | Sequences initiated while one or more RHBFSTs are issuing fuel when a fuel release >120k gallons occurs |
| ISSUEGT1M | 9.30E-06 | Sequences initiated while one or more RHBFSTs are issuing fuel when a fuel release >1 million gallons occurs |
| XFERGT1 | 1.23E-04 | Sequences initiated while there is an ongoing RHBFST inter-tank fuel transfer and a fuel release >1,000 gallons occurs |
| XFERGT120 | 3.43E-06 | Sequences initiated while there is an ongoing RHBFST inter-tank fuel transfer and a fuel release >120k gallons occurs |
| XFERGT1M | 1.04E-06 | Sequences initiated while there is an ongoing RHBFST inter-tank fuel transfer and a fuel release >1 million gallons occurs |

Figure 12-1 illustrates the data from Set 1, of Table 12-2. The exceedance curve in Figure 12-1 indicates the frequency of events per year of acute sequences each of which would potentially release the indicated amount of gallons or more shown on the x-axis. This type of curve provides a way to aggregate the results from many acute sequences into one curve.

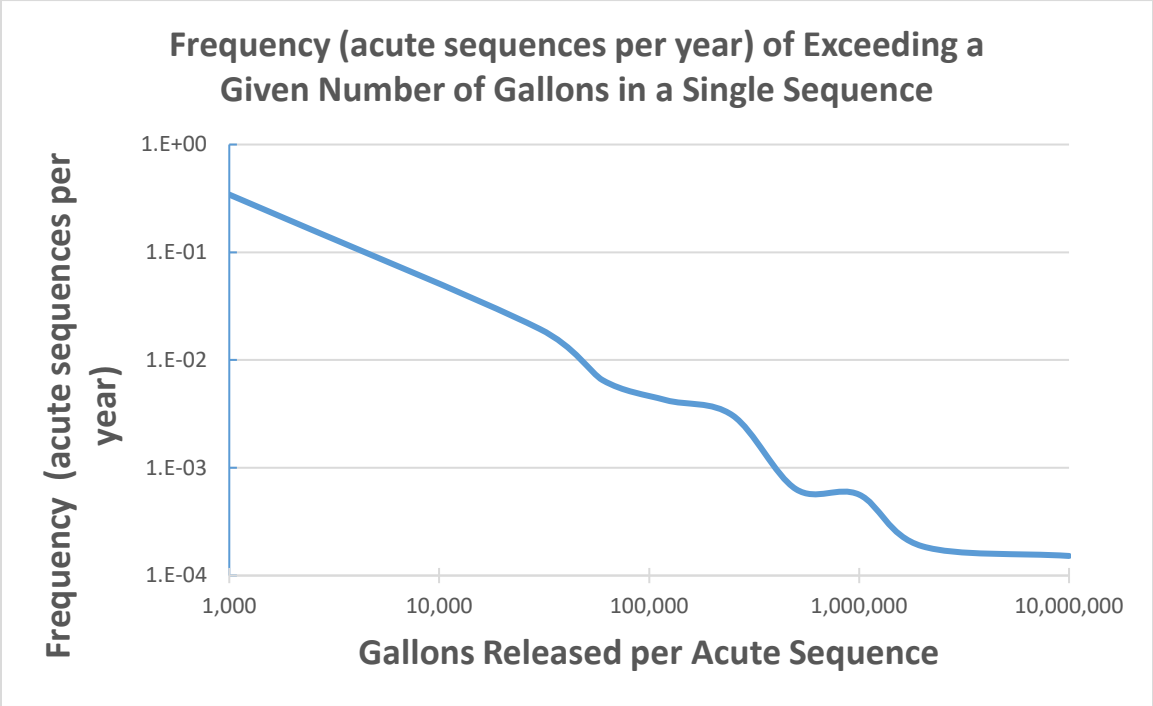



**Figure 12-1. Frequency per Year of Exceeding a Given Number of Gallons in Any Single Acute Sequence**

The second set of sequence groups presents the interval frequencies for the summation of sequences within a given range of gallons of fuel released, also in thousands of gallons. Again nine different release intervals are listed. The ranges of the intervals are uneven. Generally, but not always, the frequency of each interval for fuel released decreases as the interval ranges represent greater amounts of fuel released.

Figure 12-2 provides an alternate way of presenting the aggregated acute sequence results. This figure is consistent with data set II in Table 12-1. The bar chart in Figure 12-2 indicates the frequency of all acute sequences whose potential release in gallons lies within the specified range of gallons released. The vertical axis is presented as a logarithmic scale.

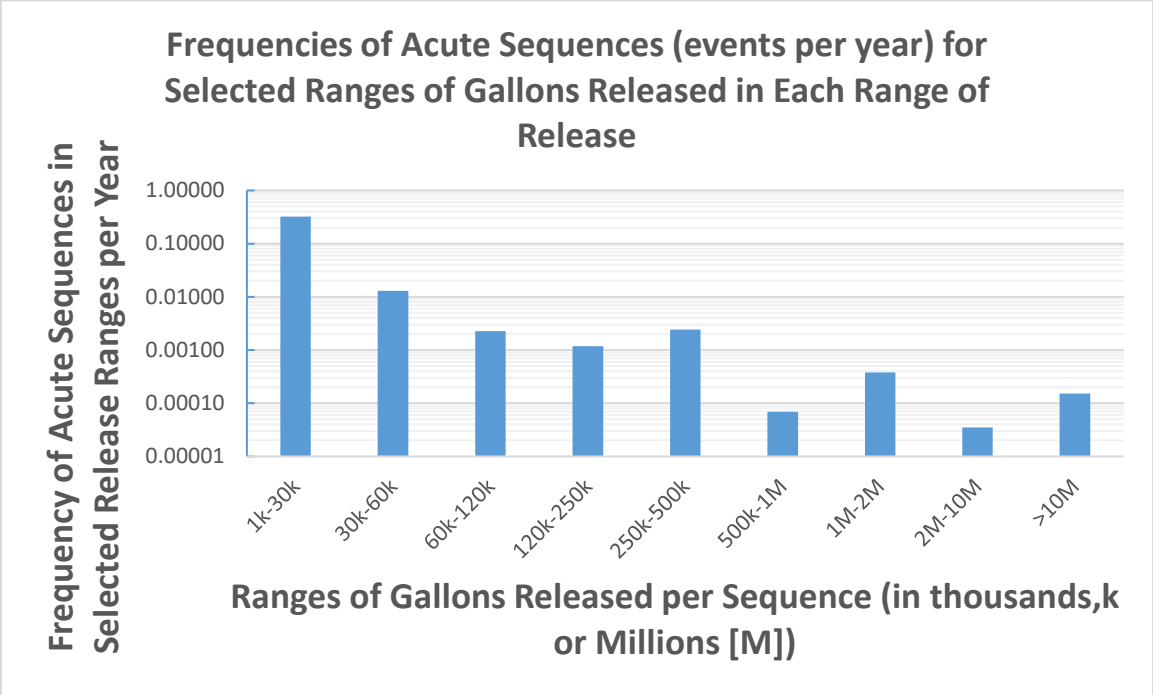



**Figure 12-2. The Frequencies Acute Sequences whose Potential Release, in Gallons, Lies within a Specified Range of Release**

The third set of sequence groups in Table 12-1 presents the frequencies for the summation of sequences releasing the same fuel type for three separate exceedance thresholds; i.e., for greater than 1,000 gallons, greater than 120,000 gallons, and for greater than 1 million gallons of fuel released. The JP5 fuel type has the greatest frequency of acute accident sequences with more than 1,000 or more than 120,000 gallons released. This is attributed to the larger number of RHBFSTs holding JP5 than for other fuel types. For greater than 1 million gallons released, the F76 fuel type has the largest frequency. The model assumes there is insufficient ullage available to fully empty an F76 RHBFST that is leaking. This leads to delays in fully emptying a leaking F76 RHBFST and therefore to a greater frequency of large fuel releases than for the other fuel types. This increase is more than enough to offset the smaller number of RHBFSTs holding F76 fuel.

The fourth set of sequence groups presents the frequencies for the summation of sequences, this time over the types of initiating events. Results for four different initiating event groups are presented; i.e., for leaks to rock, overfill leaks to rock, nozzle leaks to the LAT, and all other leaks to the LAT or Harbor Tunnel. The sequence group for leaks directly to rock from a RHBFST (ROCKGT1) dominates the release frequency of sequences releasing at least 1,000 gallons, with overfill initiating events next most in importance. The leaks to rock, nozzle, and tunnel initiating event groups (ROCKGT120, NOZGT120, and TUNGT120) have similar contributions to the total frequency of acute accident sequences releasing more than 120,000 gallons of fuel, while overfill initiating events are unlikely to leak more than 120,000 gallons. The NOZZLE initiating event sequence group (NOZGT1M) contributes by far the most frequency to the total frequency of sequences releasing more than 1 million gallons of fuel.

The fifth set of sequence groups presents the frequencies for a subset of initiating events; i.e., only those from maintenance errors leading to fuel line leaks into the LAT. The maintenance error events are split between the NOZXXX and TUNXXX sequence groups in Set IV above. The acute sequence model assesses these errors as unlikely, but if they do occur, the resulting flow area is modeled as large resulting in substantial fuel released.

The sixth set of sequence groups presents the frequencies for a subset of initiating events; i.e., only those involving leaks from a RHBFST directly to rock during a RHBFST return to service condition. These initiating events are also grouped with the ROCK initiating events in Set IV. The acute sequence model assesses these errors as a significant contributor to the frequency of sequences involving more than 1,000 gallons released per event, but as lower contributors to larger fuel release scenarios; i.e., to Sequence Groups RTSGT120 or RTSGT1M. The acute sequence model assumes that ullage is likely to be readily available in the event there is a need to empty the RHBFST while it is being returned to service, should that become necessary. This minimizes the effective delay times in accomplishing the fuel offloading, and since such leak flow rates are not expected to be large, the actions to empty a leaking RHBFST that was being returned to service are found to be relatively effective.

The seventh and final set of sequence groups in Table 12-1 presents the frequencies for a subset of all initiating events. The subsets are separated by whether the RHBFSF is idle, or undergoing a fuel movement at the time of the initiating event; i.e., receiving, issuing, of inter-RHBFST gravity transferring. As expected, since most of the time RHBFSTs are not aligned for a fuel movement, the idle facility configuration contributes the most to each of the three fuel release measures evaluated; i.e., greater than 1,000, greater than 120,000, or greater than 1 million gallons of fuel released. It might be anticipated that fuel movements periods would contribute more to the greater than 1 million gallons released group. That they do not reflects the models findings that NOZZLE leaks (i.e., leaks located at or inside the nearest skin valve which may be closed) directly to the LAT are significant in assessed frequency and these frequencies are not assessed to vary with whether the RHBFST is idle or undergoing a fuel movement.

## 12.3 Initiating Event Frequency Contribution Results

Table 12-2 presents the individual initiating event contributions to the sequence group representing the summation of all acute accident sequences that release more than 1,000 gallons of fuel (AGT1). Only initiating events contributing more than 0.15% of the total are presented. It is readily seen that leaks directly from a RHBFST to rock dominate the total sequence group frequency. The initiating events involving random leaks directly to rock for RHBFSTs 16, 15, 3, and 18 are found to contribute less than from the other RHBFSTs. This is because the sequence model assumes these RHBFSTs have initial fuel levels less than the maximum operating fuel level consistent with the reviewed operating practices. The lower initial fuel levels limit the potential release for leak events located high in the RHBFST. These four RHBFSTs are not always kept at lower levels, but they were at lower levels throughout the historical experience data reviewed and so it is judged to be standard practice to keep some RHBFSTs at lower levels. The other RHBFSTs, whose leak to rock initiating events are ranked higher in Table 12-2, were assumed always at 212'.

## Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1)

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1,000 Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1,000 Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| LTK06 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak F24 to rock per calendar year for RHBFST 006 |
| LTK05 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak F24 to rock per calendar year for RHBFST 005 |
| LTK04 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak F24 to rock per calendar year for RHBFST 004 |
| LTK02 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak F24 to rock per calendar year for RHBFST 002 |
| LTK20 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 020 |
| LTK17 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 017 |
| LTK14 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 014 |
| LTK13 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 013 |
| LTK12 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 012 |
| LTK11 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 011 |
| LTK10 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 010 |
| LTK09 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 009 |
| LTK08 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 008 |
| LTK07 | 1.24E-02 | 1.24E-02 | 3.60% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 007 |
| LRTS04 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 004 |

**Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1,000 Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1,000 Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| LRTS03 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 003 |
| LRTS02 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 002 |
| LRTS06 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 006 |
| LRTS07 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 007 |
| LRTS17 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 017 |
| LRTS05 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 005 |
| LRTS18 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 018 |
| LRTS16 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 016 |
| LRTS15 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 015 |
| LRTS14 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 014 |
| LRTS13 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 013 |

**Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1,000 Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1,000 Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| LRTS12 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 012 |
| LRTS11 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 011 |
| LRTS10 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 010 |
| LRTS09 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 009 |
| LRTS08 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 008 |
| LRTS20 | 5.54E-03 | 5.54E-03 | 1.62% | 1.5gpm leak to rock per year during a Return to Service TK 018 |
| LTK16 | 1.24E-02 | 5.19E-03 | 1.51% | 1.5gpm leak F76 to rock per calendar year for RHBFST 016 |
| LTK15 | 1.24E-02 | 5.19E-03 | 1.51% | 1.5gpm leak F76 to rock per calendar year for RHBFST 015 |
| LTK03 | 1.24E-02 | 3.22E-03 | 0.94% | 1.5gpm leak F24 to rock per calendar year for RHBFST 003 |
| OVFL14 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK14 |
| OVFL17 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK17 |
| OVFL16 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK16 |

**Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1,000 Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1,000 Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| OVFL20 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK20 |
| OVFL18 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK18 |
| OVFL09 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK09 |
| OVFL15 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK15 |
| OVFL13 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK12 |
| OVFL12 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK12 |
| OVFL11 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK11 |
| OVFL10 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK10 |
| OVFL08 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK07 |
| OVFL07 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK07 |
| OVFL06 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK06 |

**Table 12-2. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 1,000 Gallons (Sequence Group ID = AGT1) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1,000 Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1,000 Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| OVFL05 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK05 |
| OVFL04 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK04 |
| OVFL03 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK03 |
| OVFL02 | 1.00E+00 | 2.59E-03 | 0.75% | CHALLENGE FOR OVERFILL LEAK TO ROCK PER YEAR TK02 |
| LTK18 | 1.24E-02 | 1.98E-03 | 0.58% | 1.5gpm leak JP5 to rock per calendar year for RHBFST 018 |

Table 12-3 presents the individual initiating event contribution to the sequence group representing the summation of all acute accident sequences that release more than 120,000 gallons of fuel (Sequence Group DGT120). Only initiating events contributing more than 0.3% of the total are presented. The top ranked initiating event involves a small fuel line leak into the Harbor Tunnel (i.e., SF76BS, Section B) from the largest diameter fuel line (32"); i.e., that for F76 type fuel. Small nozzle leaks from each of the RHBFSTs then contribute next in frequency. Larger nozzle leaks from each RHBFST are lower in the ranking to Sequence Group DGT120. Fuel line leaks into the Harbor Tunnel from other fuel types contribute about 2% each to this sequence group.

## Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120)

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| SF76BS | 5.03E-04 | 5.03E-04 | 11.84% | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y, Small Leak, 0.5" φ |
| NSTK17 | 2.10E-04 | 2.10E-04 | 4.95% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 017 |
| NSTK02 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 002 |
| NSTK04 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 004 |
| NSTK05 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 005 |
| NSTK15 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 015 |
| NSTK03 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 003 |
| NSTK16 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 016 |
| NSTK06 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 006 |
| NSTK14 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 014 |

**Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NSTK13 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 013 |
| NSTK12 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 012 |
| NSTK11 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 011 |
| NSTK10 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 010 |
| NSTK09 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 009 |
| NSTK08 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 008 |
| NSTK07 | 1.51E-04 | 1.51E-04 | 3.55% | RHBFST Nozzle 0.5”φ leak to LAT per tank year; i.e., between skin valve and RHBFST 007 |
| NSTK20 | 1.20E-04 | 1.20E-04 | 2.83% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 020 |
| SJP5BS | 5.03E-04 | 9.41E-05 | 2.22% | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y, Small Leak, 0.5" φ |
| SF76BL | 7.61E-05 | 7.61E-05 | 1.79% | Green F76 32" line from normally closed Sectional Valve 153 down to Sectional Valve 152 at ADIT 2Y, Large leak, pipe rupture |

**Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| SJP5BL | 7.61E-05 | 7.61E-05 | 1.79% | Gold JP5 18" line from normally closed Sectional Valve 157 at ADIT 3Y down to Sectional Valve 156 at ADIT 2Y, Large leak, pipe rupture |
| SF76AS | 1.09E-04 | 2.10E-05 | 0.49% | Green F76 32" line from Sectional Valve 152 at ADIT 2Y to Sectional Valve 151 at PH59, Small Leak, 0.5" φ |
| SF24AS | 1.09E-04 | 2.10E-05 | 0.49% | Blue F24 16" line, from Sectional Valve 160 at ADIT 2Y down to Sectional Valve 159 at PH59, Small Leak, 0.5" φ |
| SJP5AS | 1.09E-04 | 2.09E-05 | 0.49% | Gold JP5 18" line from Sectional Valve 156 at ADIT 2Y down to Section Valve 155 at PH59, Small Leak, 0.5" φ |
| MTK06 | 6.65E-05 | 1.95E-05 | 0.46% | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 006 |
| MTK05 | 6.65E-05 | 1.95E-05 | 0.46% | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 005 |
| MTK04 | 6.65E-05 | 1.95E-05 | 0.46% | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 004 |
| MTK02 | 6.65E-05 | 1.95E-05 | 0.46% | MEDIUM LEAK 0.5" leak F24 to rock per calendar year for RHBFST 002 |
| MTK20 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 020 |
| MTK17 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 017 |

**Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| MTK09 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 009 |
| MTK14 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 014 |
| MTK13 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 013 |
| MTK12 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 012 |
| MTK10 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 010 |
| MTK08 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 008 |
| MTK07 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 007 |
| MTK11 | 6.65E-05 | 1.94E-05 | 0.46% | MEDIUM LEAK 0.5" leak JP5 to rock per calendar year for RHBFST 011 |
| MTK16 | 6.65E-05 | 1.75E-05 | 0.41% | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 016 |
| MTK15 | 6.65E-05 | 1.75E-05 | 0.41% | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 015 |
| NLTK18 | 1.48E-05 | 1.48E-05 | 0.35% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 018 |

**Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NLTK17 | 1.48E-05 | 1.48E-05 | 0.35% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 017 |
| MRTS18 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 018 |
| MRTS20 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 020 |
| MRTS17 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 017 |
| MRTS02 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 002 |
| MRTS04 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 004 |
| MRTS14 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 014 |
| MRTS13 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 013 |
| MRTS12 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 012 |
| MRTS11 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 011 |
| MRTS10 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 010 |
| MRTS07 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 007 |
| MRTS05 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 005 |
| MRTS06 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 006 |
| MRTS03 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 003 |

**Table 12-3. Frequency of Individual Initiating Events Contributing to All Acute Sequences Releasing Greater than 120,000 Gallons (Sequence Group ID = DGT120) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >120k Gallons | Frequency Contribution of Initiating Event to Total of All Releases >120k Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| MRTS09 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 009 |
| MRTS08 | 3.87E-05 | 1.40E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 008 |
| MRTS16 | 3.87E-05 | 1.39E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 016 |
| MRTS15 | 3.87E-05 | 1.39E-05 | 0.33% | MEDIUM leak to rock per year during a Return to Service TK 015 |

Table 12-4 presents the individual initiating event contribution to the sequence group representing the summation of all acute accident sequences that release more than 1 million gallons of fuel per event (GGT1M). The base model sequence cutoff frequency of 1E-12 per year was used to develop these results. Only initiating events contributing more than 0.30% of the total are presented. The top two ranked initiating events involve small Nozzle leaks from the F76 RHBFSTs; i.e., 15 and 16. The acute sequence model assumes that there is insufficient ullage on hand to fully empty either RHBFST 15 or 16 so that there is a substantial delay to fully empty either of them in the event of a small nozzle leak. The next two ranked initiating events to GGT1M also involve RHBFSTs 15 and 16, but this time from medium leaks (i.e., equivalent to a 0.5" hole) directly to rock. The next contributors (around 1.9% each) are larger nozzle leaks (i.e., 6" equivalent diameters) in which no credit is given for emptying the affected RHBFST in time to limit the total fuel release. Small nozzle leaks for the other RHBFSTs (i.e., holding F24 or JP5 fuel) contribute most of the remaining sequence group frequency. These sequences are judged, having more ullage readily available, to be more easily mitigated by emptying the affected RHBFST than is assumed for RHBFSTs 15 and 16.

## Table 12-4. Frequency of Initiating Events Contributing to Acute Sequences Releasing Greater than 1 Million Gallons (Sequence Group ID = GGT1M)

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1 Million Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1 Million Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NSTK15 | 1.51E-04 | 1.51E-04 | 26.69% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 015 |
| NSTK16 | 1.51E-04 | 1.51E-04 | 26.69% | RHBFST Nozzle 0.5”φ leak to LAT per tank year; i.e., between skin valve and RHBFST 016 |
| MTK16 | 6.65E-05 | 1.73E-05 | 3.06% | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 016 |
| MTK15 | 6.65E-05 | 1.73E-05 | 3.06% | MEDIUM LEAK 0.5" leak F76 to rock per calendar year for RHBFST 015 |
| NLTK17 | 1.48E-05 | 1.48E-05 | 2.62% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 017 |
| NLTK13 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 013 |
| NLTK02 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 002 |
| NLTK14 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 014 |
| NLTK12 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 012 |
| NLTK15 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 015 |
| NLTK11 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 011 |

**Table 12-4. Frequency of Initiating Events Contributing to Acute Sequences Releasing Greater than 1 Million Gallons (Sequence Group ID = GGT1M) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1 Million Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1 Million Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NLTK10 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 010 |
| NLTK09 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 009 |
| NLTK08 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 008 |
| NLTK07 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 007 |
| NLTK06 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 006 |
| NLTK05 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 005 |
| NLTK04 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 004 |
| NLTK03 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 003 |
| NLTK16 | 1.06E-05 | 1.06E-05 | 1.88% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 016 |
| NLTK20 | 8.47E-06 | 8.47E-06 | 1.50% | NOZZLE RUPTURE to LAT per tank year; i.e., between skin valve and RHBFST 018 |
| NSTK02 | 1.51E-04 | 3.23E-06 | 0.57% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 002 |

## Table 12-4. Frequency of Initiating Events Contributing to Acute Sequences Releasing Greater than 1 Million Gallons (Sequence Group ID = GGT1M) (Continued)

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1 Million Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1 Million Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NSTK04 | 1.51E-04 | 3.23E-06 | 0.57% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 004 |
| NSTK05 | 1.51E-04 | 3.23E-06 | 0.57% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 005 |
| NSTK06 | 1.51E-04 | 3.23E-06 | 0.57% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 006 |
| NSTK17 | 2.10E-04 | 2.94E-06 | 0.52% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 017 |
| LDTK16 | 6.70E-06 | 2.18E-06 | 0.39% | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 016 |
| LDTK15 | 6.70E-06 | 2.18E-06 | 0.39% | Lower dome 0.5"φ pipe leaks to ROCK per tank year applies to RHBFST 015 |
| NSTK03 | 1.51E-04 | 2.12E-06 | 0.38% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 003 |
| NSTK14 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 014 |
| NSTK13 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 013 |
| NSTK12 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 012 |
| NSTK11 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 011 |

**Table 12-4. Frequency of Initiating Events Contributing to Acute Sequences Releasing Greater than 1 Million Gallons (Sequence Group ID = GGT1M) (Continued)**

| Initiating Event Name | Initiating Event Frequency (events per year) | Frequency Contribution of Initiating Event to Releases >1 Million Gallons | Frequency Contribution of Initiating Event to Total of All Releases >1 Million Gallons (%) | Initiating Event Description |
|---|---|---|---|---|
| NSTK10 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 010 |
| NSTK09 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5”φ leak to LAT per tank year; i.e., between skin valve and RHBFST 009 |
| NSTK08 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 008 |
| NSTK07 | 1.51E-04 | 2.11E-06 | 0.37% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 007 |
| NSTK20 | 1.20E-04 | 1.68E-06 | 0.30% | RHBFST Nozzle 0.5"φ leak to LAT per tank year; i.e., between skin valve and RHBFST 020 |

The QRVA sequence model is quantified by tracing the sequence paths each of which start with a single initiating event. Table 12-2, Table 12-3, and Table 12-4 document the contributions of individual initiating events to different release thresholds. However, this granularity can be a bit overwhelming when trying to understand the high level results. One alternative way to describe the risk is to roll up the frequencies of all individual initiating events into initiating event categories and using these categories to discuss their contribution to risk. All individual initiating events assigned to the same category have largely the same impact on the Red Hill facility, though often impacting different RHBFSTs or different fuel line piping sections.

Table 12-5 summarizes the initiating event categories defined for this purpose of a high level understanding, and provides the total initiating event category frequency found by summing the frequency of each individual initiating event assigned to that category. The frequencies in Table 12-5 are not the frequencies of entire sequences, but rather the starting points of many acute sequences which may be traced from a single initiating event assigned to that category.

The initiating event categories in Table 12-5 are sorted by their frequencies of occurrence. The first initiating event category has a very high frequency. This value is not the frequency of a release, but rather the frequency of a challenge to the plant staff

to respond correctly by ending the receiving fuel movement before an overfilling occurs. The initiating event categories defined in Table 12-5 are used to contribute to the discussions of contributors below.

| Frequency of Initiating Event Category (events per year) | Initiating Event Category |
|---|---|
| 18 | Challenge to an Inadvertent RHBFST Overfilling with Hole above Operating Level |
| 0.322 | RHBFST Liner Small Leaks to Rock at Low Leak Rates |
| 2.808E-03 | Small Hole in Fuel Line Piping |
| 2.801E-03 | Small Nozzle Hole 0.5" Diameter |
| 1.893E-03 | RHBFST Liner Leaks to Rock via 0.5" Hole |
| 3.780E-04 | Large Hole in Fuel Line Piping |
| 1.971E-04 | Large Nozzle Hole 6" Diameter |
| 1.206E-04 | Small Hole in Lower Dome Piping |
| 2.745E-05 | Maintenance Error Opening Incorrect Valve |

A roll up of all initiating event frequencies with greater than 1,000 gallons released, by initiating event category is presented in the pie chart displayed in Figure 12-3. This chart uses the data of Table 12-2. By far the largest category contributor are initiating events involving RHBFST liner leaks at very low leak rates; i.e., on the order of 1.5 gpm. The next highest frequency group of initiating events involve an inadvertent overfilling of a RHBFST above the tank's maximum operating level; i.e., currently around 212'. The QRVA model considers the possibility that an undetected hole is located just above this RHBFST level and so release through the liner may result from such initiating events. It is noted that each RHBFST is filled to its maximum operating level each year in preparation for its annual leak tightness test.

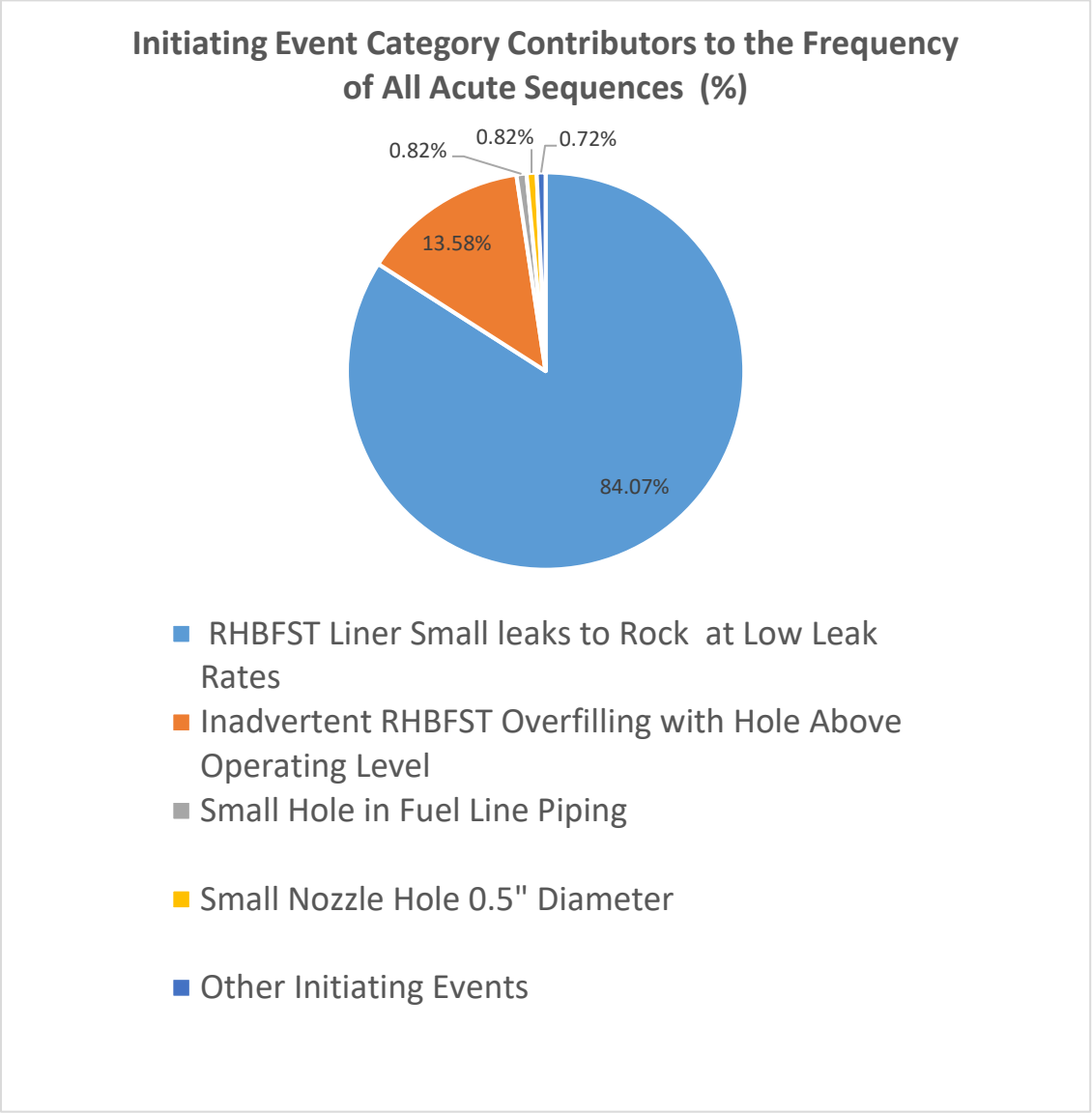



**Figure 12-3. Initiating Event Category Frequency Contribution to the Frequency of All Acute Sequences**

The next two initiating event categories contribute less than 1% each as do the sum of the frequencies of all other initiating events not represented in the first four initiating event categories presented in the figure.

A roll up of all initiating event frequencies with greater than 120,000 gallons released, by initiating event category, is presented in the pie chart displayed in Figure 12-4. This chart uses the data of Table 12-3. The largest contributor involves initiating events with small holes in the RHBFST nozzle area which are not isolable. The next highest frequency category of initiating events involve small holes in fuel line piping to the LAT or to the Harbor Tunnel. The third highest initiating event category involves RHBFST leaks in the liner from hole sizes larger than have ever resulted in leakage in the operating history at Red Hill. The next two initiating event categories contribute 4 to 5% of the total

frequency of acute sequences that may potentially release greater than 120,000 gallons in a single event. These categories involve large holes either in a RHBFST nozzle or from other fuel line sections within the tunnels. The frequencies of all other initiating events not represented in the first five initiating event categories are further grouped in Figure 12-4 as other initiating events.

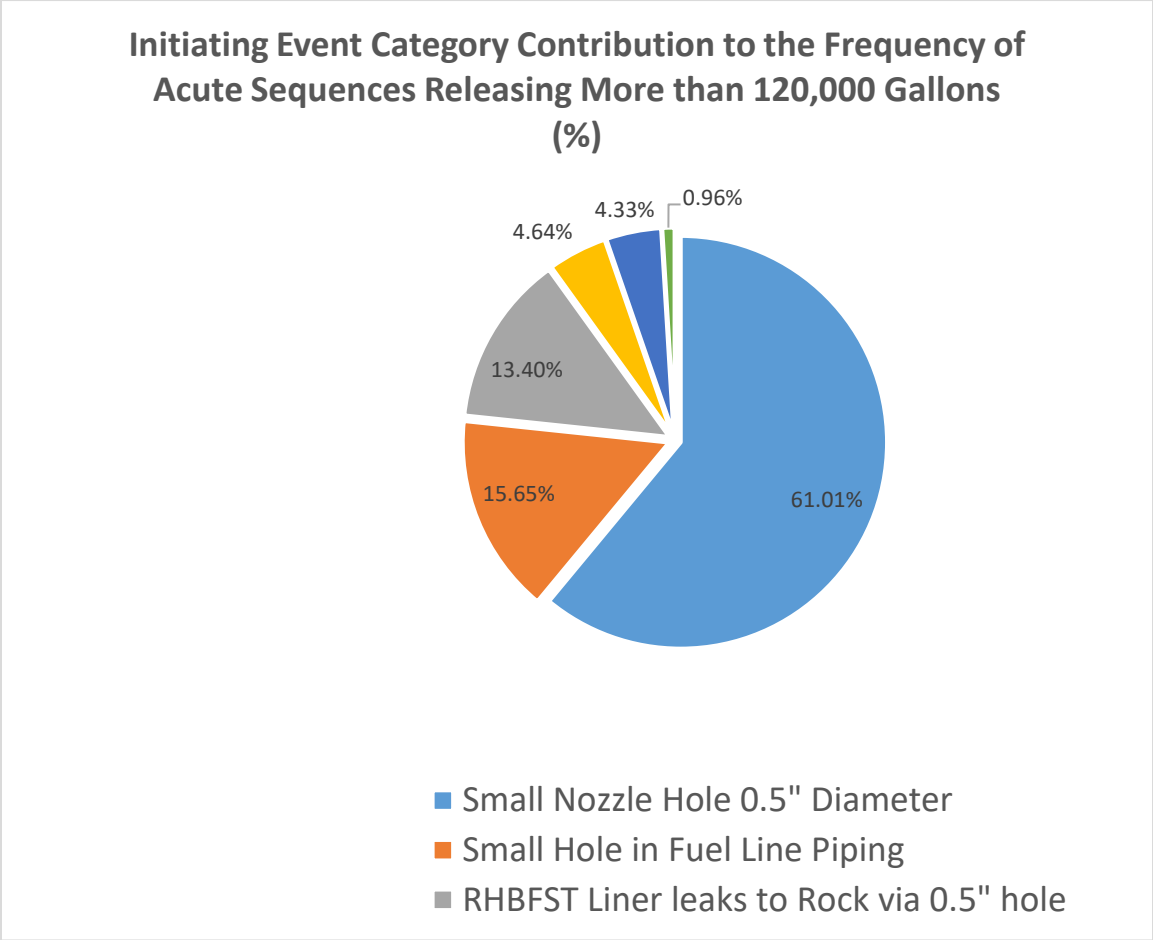



**Figure 12-4. Initiating Event Category Frequency Contribution to the Frequency of Acute Sequences Each Potentially with a Release of Greater than 120,000 Gallons**

A roll up of all initiating event frequencies with greater than 1,000,000 gallons released, by initiating event category, is presented in the pie chart displayed in Figure 12-5. This chart uses the data of Table 12-4. The largest contributor, amounting to two-thirds of the total, involve initiating events with small holes in the RHBFST nozzle area. Such holes are not isolable but can be mitigated by moving further from the affected RHBFST. The next highest frequency category of initiating events involves large holes in the RHBFST nozzle area. The third highest initiating event category involves RHBFST leaks in the liner from hole sizes larger than have ever occurred in the operating history of Red Hill. The fourth highest initiating event category involves leaks from the piping of a RHBFST that passes through the lower dome. Due to these pipes being embedded in concrete, hole sizes from these pipes are judged limited to holes sizes equivalent to a

0.5”-diameter hole. Such holes sizes also have not occurred in the history of Red Hill operation. Finally, the other categories of initiating events sum to less than 1% of the total for those that contribute to acute sequences that potentially release more than 1 million gallons.

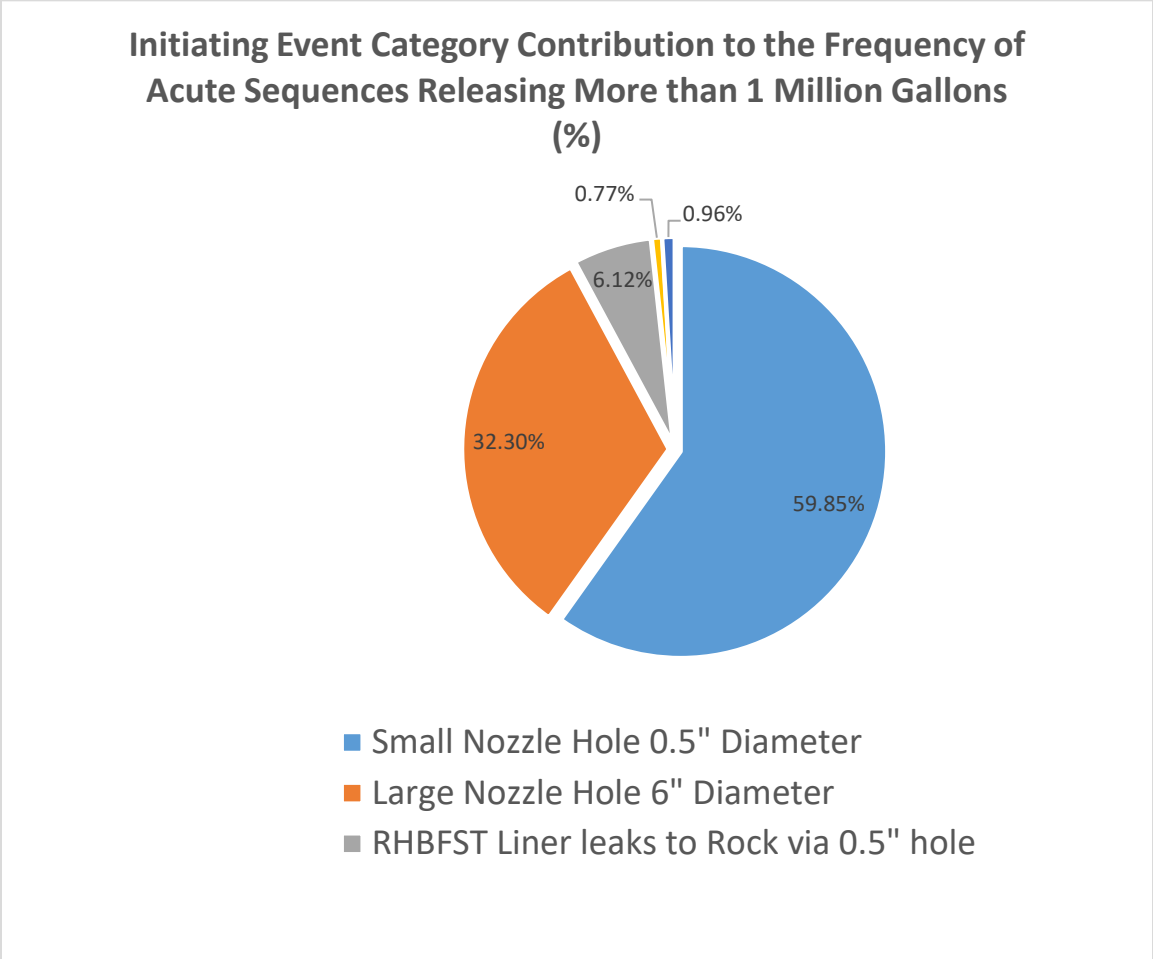



**Figure 12-5. Initiating Event Category Frequency Contributions to the Frequency of Acute Sequences Each Potentially with a Release of Greater than 1 Million Gallons**

Table 12-5 presents the sequence frequency contributions of initiating event categories to the potential volume release (gallons per year) from acute sequences. The total potential volume released from all acute sequences is 6,584 gallons per year. The initiating event categories include initiators of the same type, including all the individual initiating events for the different RHBFSTs, or for all fuel line pipe sections. The headers of Table 12-5, shown above, identify the meaning of each initiating event group. The first row below the header of Table 12-5 shows the % contribution from each initiating event category to the total potential volume released. The average release per acute release event and the average potential volume release per year are also indicated.

**Table 12-5. Initiating Event Category % Contributions to Potential Volume Release by Release Range (gallons) and to Total Potential Volume Release (gallons per year)**

| Fuel Release Volume Range Category (gallons) | FLPLRG – Large Hole in Fuel Line Piping 6" Diameter | FLPSML – Small Hole in Fuel Line Piping 0.5" Diameter | LDP5 – 0.5" Holes in Lower Dome Piping to Rock | MAINT – Maintenance Error Opening Incorrect Valve | NOZLRG – Large Nozzle Hole 6" Diameter | NOZSML – Small Nozzle Hole 0.5" Diameter | OVERF – Inadvertent RHBFST Overfilling with Hole above Fuel Level | ROC1P5 – RHBFST Liner Leaks at 1.5 gpm | ROCMED – RHBFST Liner Leaks via 0.5" Hole | Average Release in Range (gallons/event) | Potential Volume Released – Point Estimate (gallons/year) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| % Contribution of Initiating Event Category to Potential Volume Released (gallons/year from acute releases) | 1.23% | 4.11% | 0.36% | 0.13% | 29.09% | 23.32% | 8.08% | 29.81% | 3.88% | 19,228 | **6,584** |
| 1,000 to 30,000 | 0.01% | 0.31% | 0.00% | 0.01% | 0.00% | 0.00% | 12.46% | 87.16% | 0.05% | 6,068 | 1,960 |
| 30,000 to 60,000 | 0.38% | 1.50% | 0.47% | 0.00% | 0.00% | 1.58% | 41.80% | 49.41% | 4.86% | 39,681 | 515 |
| 60,000 to 120,000 | 4.49% | 41.66% | 1.09% | 0.00% | 0.00% | 0.15% | 37.79% | 0.00% | 14.82% | 86,641 | 191 |
| 120,000 to 250,000 | 8.50% | 45.99% | 1.26% | 0.01% | 1.25% | 12.43% | 0.00% | 0.00% | 30.56% | 190,012 | 219 |
| 250,000 to 500,000 | 3.13% | 3.84% | 0.83% | 0.00% | 0.00% | 85.29% | 0.00% | 0.00% | 6.90% | 456,251 | 1,097 |
| 500,000 to 1,000,000 | 8.24% | 33.89% | 0.87% | 0.00% | 0.00% | 50.09% | 0.00% | 0.00% | 6.91% | 669,170 | 42 |
| 1,000,000 to 2,000,000 | 0.00% | 0.19% | 1.15% | 0.00% | 0.00% | 89.50% | 0.00% | 0.00% | 9.16% | 1,641,706 | 604 |
| 2,000,000 to 10,000,000 | 0.61% | 7.42% | 0.00% | 0.79% | 91.17% | 0.00% | 0.00% | 0.00% | 0.00% | 7,547,154 | 253 |
| > 10,000,000 | 0.70% | 0.00% | 0.00% | 0.38% | 98.74% | 0.19% | 0.00% | 0.00% | 0.00% | 11,415,250 | 1,703 |

The subsequent rows show the % contributions of initiating event categories for different ranges of gallons released. The average release in gallons, for each range of release, is provided in the last column of Table 12-5. These average amounts released in gallons for each range of fuel release are used to weight the % contribution in each range to obtain the % contributions of each initiating event category to the total potential volume release in the first row.

It is seen that the largest contributions to potential volume release averaged over all fuel release ranges come from three of the nine initiating event categories; i.e., large and small RHBFST nozzle holes, and smaller sized RHBFST liner leaks. Overfilling events contribute next in importance.

The second and subsequent rows of Table 12-5 indicate how the % contributions from each initiating event category vary with a single range of potential volume of fuel released. In the smallest range of potential volumes released (1,000 to 30,000 gallons) small release rates through the RHBFST liner dominate; i.e., initiating event category name ROC1P5. This release range contributes substantially to the total potential volume released; i.e., 1,960 out of 6,584 gallons per year.

In the second smallest release range (i.e., 30,000 to 60,000 gallons), ROC1P5 also contributes substantially, but there is also a substantial contribution (42%) from initiators involving an inadvertent overfilling combined with a hole being present in the liner above the maximum fuel operating level. The overall potential volume release from this release range is only about a fourth of the first range; i.e., 515 gallons per year versus 1,960 gallons per year.

The third potential volume release range (60,000 to 120,000 gallons) is dominated again by inadvertent overfill events and a second initiating event category; i.e., the initiating event group involving a small hole in fuel line piping, releasing to the LAT or Harbor Tunnel. The previously important category involving small leaks through the RHBFST liner (i.e., ROC1P5) contributes not at all to this range. This is because the consequence assessment for ROC1P5 events indicates that the potential release does not exceed 60,000 gallons; i.e., an RHBFST leaking at rate of 1.5 gpm is very likely to be emptied before releasing more than 60,000 gallons of fuel. Note that this third range of release contributes little to the overall potential volume release; i.e., 191 versus 6,584 gallons per year.

The fourth potential volume release range (120,000 to 250,000 gallons) is no longer dominated by inadvertent overfill events. Overfill events are unlikely to lead to more than 120,000 gallons released since the postulated hole is high in the RHBFST and therefore it is relatively easy to uncover the hole by moving fuel. The initiating event category involving a small hole in fuel line piping releasing to the LAT or Harbor Tunnel becomes the highest contributor to this range. The initiating event category, ROCMED, involves leaks from a RHBFST liner, this time through a larger hole, of a size beyond any that have been experienced at Red Hill contributes substantially. The larger hole size than for ROC1P5, is assessed as resulting in larger release before the leaking RHBFST can be emptied. A third initiating event category begins to contribute in this fourth range of fuel release; i.e., that of small holes in a RHBFST nozzle. Because a hole in the nozzle is not isolable, substantial fuel is assessed as being released before

the affected RHBFST can be emptied. This fourth range of release, however, contributes minimally to the total potential volume released in gallons per year.

The fifth potential volume release range (250,000 to 500,000 gallons) is dominated (i.e., 85%) instead by the initiating event category that involves small holes in RHBFST nozzle piping. These events are not isolable and so typically are assessed as resulting in larger releases. This range of release contributes significantly to the total potential volume release; i.e., 1,097 out of 6,584 gallons per year.

The sixth potential volume release range (500,000 to 1,000,000 gallons) is again dominated (i.e., 50%) by the initiating event category that involves small holes in RHBFST nozzle piping. However, two other initiating event categories become important; i.e., small (FLPSML) and large (FLPLRG) holes in fuel line piping releasing to the LAT or Harbor Tunnel. These categories were also significant contributors to higher frequency low fuel release ranges. Their importance here comes from the added failure to isolate the initially leaking pipe section so that the release from a RHBFST undergoing a fuel movement at the time of the leak also occurs. This range of release contributes only minimally to the total potential volume release per year.

The seventh potential volume release range (1,000,000 to 2,000,000 gallons) is dominated (i.e., 90%) again by the initiating event category that involves small holes in RHBFST nozzle piping. These events are not isolable and so typically are assessed as resulting in larger fuel releases. This range of release, however, contributes about 10% to the total potential volume release; i.e., 604 out of 6,584 gallons per year.

The eighth potential volume release range (2,000,000 to 10,000,000 gallons) is dominated (i.e., 91%) again by RHBFST nozzle piping holes but this time the dominant contributor is from large holes rather than small holes. These events are also not isolable and so are assessed as resulting in large fuel releases. This range of release contributes about 4% to the total potential volume release; i.e., 254 out of 6,584 gallons per year.

The ninth and largest potential volume release range (greater than 10,000,000 gallons) is dominated (i.e., 99%) again by the initiating event category that involves large holes in RHBFST nozzle piping. These events are not isolable and so typically are assessed as resulting in larger fuel releases. No credit is assumed for emptying a RHBFST subject to such an event. The release per event may include sequences in which the entire inventory of an RHBFST is released (down to 7.5'), or possibly more, if two RHBFSTs were undergoing an inter-tank transfer when the nozzle leak occurs and neither RHBFST could be isolated. Because of the very high fuel releases possible within this range, this range of releases, despite the lower frequencies of the events occurring, contributes significantly to the total potential volume release; i.e., 1,703 out of 6,584 gallons per year.

Figure 12-6 displays in a pie chart the initiating event categories % contributions to total acute risk expressed as potential fuel volume release in gallons per year; i.e., averaged over all acute sequences and weighted by the gallons released in each sequence. For convenience , the three lower frequency contributing initiating event categories have been combined into the "other" contribution; i.e., MAINT, LDP5, and FLPLRG contributions are grouped into "other".

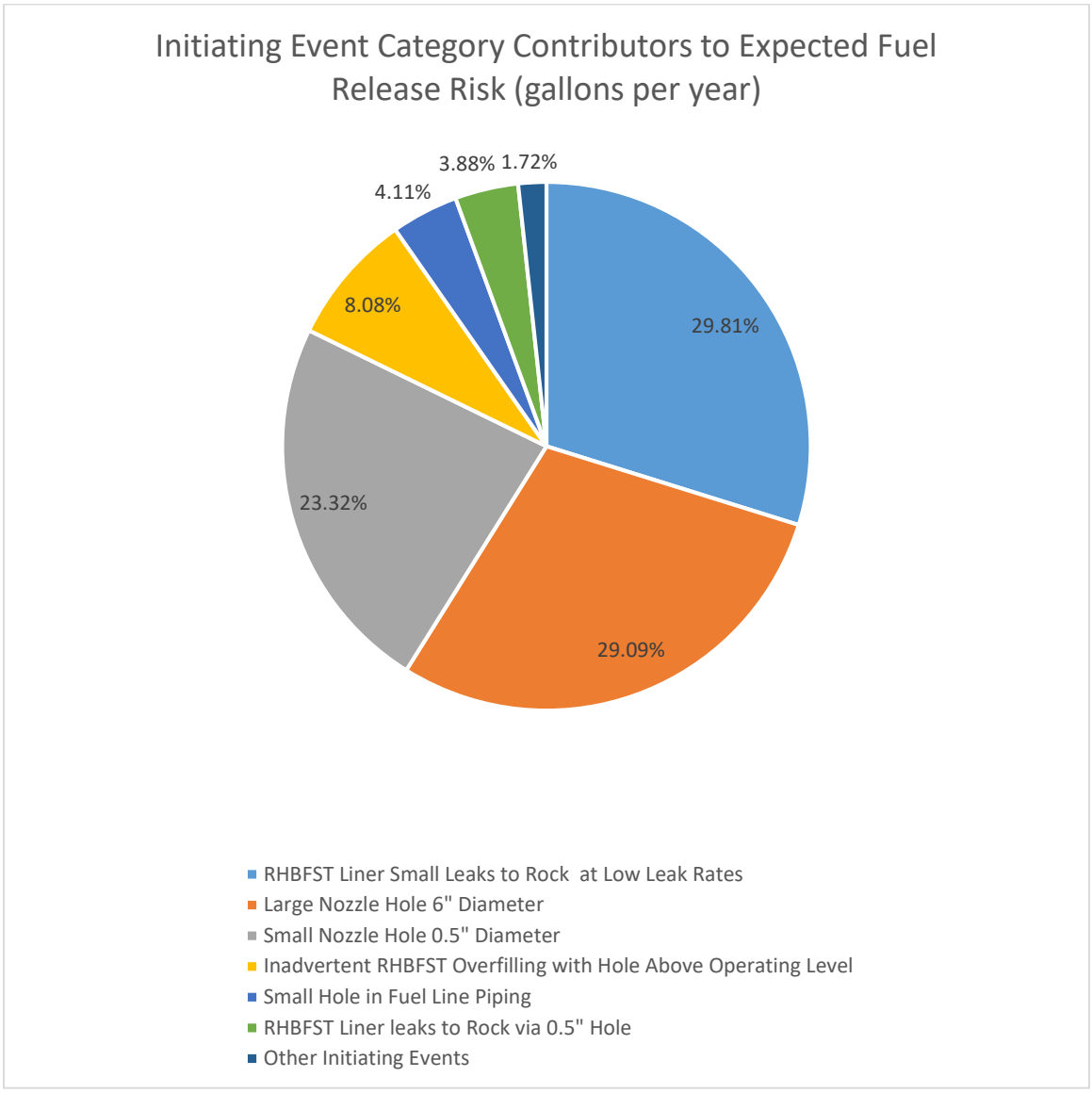



**Figure 12-6. Initiating Event Category Contributions to Acute Expected Risk**

## 12.4 End State Frequency Contribution Results

The end state frequencies summed over all internal initiating events are presented in Table 12-6. All end states with frequencies greater than 1E-6 per year included. There are more than 500 end states of which 337 have frequencies greater than zero frequency when quantified with an individual sequence cutoff of 1E-12 per year. Per Table 12-6, end states with frequencies greater than 1E-2 per year are for fuel releases less than 10,000 gallons per event, with one exception. End State OFG22 has a frequency greater than 1E-2 per year and an evaluated release of 22,000 gallons. This end state is made up of sequences involving an overfill condition. If the extent of overfilling is high enough, and a hole is present above the maximum operating level, then leakage to rock can occur. Even after the filling with fuel is ended, fuel leakage can continue until its determined there is a leak and actions to move fuel are carried out.

End states with frequencies between 7E-4 to 1E-2 per year have associated fuel releases less 40,000 gallons, with one exception. The exception is End State NOZ469, which has an assessed fuel release of 469,000 gallons at a frequency of 2.07E-3 per year. The initiating events contributing to this end state are small, unisolable nozzle leaks from each RHBFST (i.e., 0.5" equivalent holes) directly to the LAT.

The next two large fuel release end states are NOZ1649 at 3.01E-4 per year and NOZ11413 at 1.51E-4 per year. NOZ1649 (i.e., 1,649,000 gallons) is dominated by small nozzle leaks from F76 RHBFSTs 15 and 16. The initiating event contributors to end state NOZ11413 (i.e., 11,413,000 gallons) are for large (e.g., 6" equivalent holes), postulated nozzle leaks directly to the LAT from one of the RHBFSTs.

The initiating events contributing to other end states can be determined using the RISKMAN Viewer, see [redacted].

## Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| ROC2 | 1.26E-01 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC4 | 4.73E-02 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC3 | 4.45E-02 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG22 | 3.47E-02 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC8 | 2.64E-02 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC5 | 2.44E-02 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG45 | 4.87E-03 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC10 | 4.06E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC37 | 3.96E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC7 | 3.86E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG29 | 3.20E-03 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC34 | 2.48E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC9 | 2.14E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| NOZ469 | 2.07E-03 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| OFG23 | 1.78E-03 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC6 | 1.57E-03 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC15 | 8.93E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC11 | 7.79E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG99 | 7.30E-04 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| OFG25 | 6.08E-04 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC35 | 5.55E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC12 | 4.68E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN81 | 4.05E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN66 | 4.00E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN242 | 3.96E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |

## Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released (Continued)

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| NOZ1649 | 3.01E-04 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| OFG48 | 2.74E-04 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| OFG32 | 2.60E-04 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| TUN10 | 2.25E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC81 | 2.10E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| NOZ36 | 2.06E-04 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC131 | 1.69E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN137 | 1.69E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC28 | 1.67E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN98 | 1.65E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN392 | 1.65E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| NOZ11413 | 1.51E-04 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| NOZ197 | 1.46E-04 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC360 | 1.28E-04 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG90 | 1.23E-04 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| TUN21 | 1.20E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN17 | 1.19E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN52 | 1.17E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN11 | 1.15E-04 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN13 | 9.64E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |

## Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released (Continued)

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| TUN22 | 9.36E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC78 | 8.53E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN8 | 8.53E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN27 | 8.52E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN9 | 8.37E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC202 | 8.03E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC50 | 6.25E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN53 | 4.63E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN31 | 4.51E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN114 | 4.51E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN30 | 4.28E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC40 | 3.74E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC154 | 3.70E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN46 | 3.49E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| NOZ684 | 3.47E-05 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| NOZ1868 | 3.42E-05 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| OFG27 | 3.29E-05 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC141 | 3.25E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC101 | 3.01E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC201 | 2.67E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC66 | 2.63E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| OFG36 | 2.43E-05 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |

## Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released (Continued)

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| ROC1586 | 2.39E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN216 | 2.29E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN160 | 2.24E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN650 | 2.24E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| NOZ9361 | 2.15E-05 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC463 | 1.96E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC33 | 1.82E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| NOZ146 | 1.59E-05 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC1148 | 1.50E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC164 | 1.36E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN248 | 1.29E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN71 | 1.23E-05 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC286 | 1.23E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC394 | 1.18E-05 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| NOZ4833 | 1.06E-05 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| OFG33 | 9.79E-06 | OFG"nnn" is Leak following OVERFILL of "nnn" gallons in 1,000s |
| ROC42 | 9.73E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN121 | 9.69E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN115 | 9.48E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN136 | 9.46E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC23 | 9.28E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC230 | 7.39E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |

## Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released (Continued)

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| ROC669 | 5.39E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC343 | 5.36E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC261 | 5.24E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC144 | 4.40E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC91 | 3.68E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN86 | 3.55E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| NOZ91 | 3.45E-06 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC57 | 3.42E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN23 | 3.06E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC142 | 2.97E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC75 | 2.96E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC455 | 2.82E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN28 | 2.61E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| NOZ345 | 2.45E-06 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| TUN12 | 2.36E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC377 | 2.24E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| NOZ1157 | 2.10E-06 | NOZ"nnn" is Leak from RHBFST Nozzle into LAT of "nnn" gallons in 1,000s |
| ROC47 | 1.97E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| TUN663 | 1.96E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN472 | 1.86E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN2572 | 1.47E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC216 | 1.41E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |
| ROC49 | 1.38E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |

**Table 12-6. Frequencies of Assigned Sequence End States which Track the Amount of Fuel Released (Continued)**

| End State Name | End State Frequency (events per year) | End State Description |
|---|---|---|
| TUN12600 | 1.05E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN34 | 1.04E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| TUN408 | 1.00E-06 | TUN"nnn" is Leak to LAT or Harbor Tunnel of "nnn" gallons in 1,000s |
| ROC111 | 1.00E-06 | ROC"nnn" is Leak to ROCK of "nnn" gallons in 1,000s |

## 12.5 Importance of Human Failure Events and Equipment Failures to Risk

The importance to risk of individual QRVA basic events can be measured against a variety of risk metrics. One such risk metric is the frequency of acute sequences that have the potential to exceed 120,000 gallons of fuel released. A limitation of this risk metric is that it only captures the impact on the metric if the failure increases the frequency of a sequence that already exceeds 120,000 gallons released, or if the amount of gallons released changes from less than 120,000 gallons per event to greater than 120,000 gallons released. Other basic event failures that increase the assigned gallons of fuel released but do not cross the 120,000 gallons threshold do not contribute to this metric. An alternative risk metric is therefore defined for use in this section to develop importance measures.

The risk metric used here is defined as the product of each sequence frequency times its gallons released, and then these products are summed up over all acute sequences. This risk metric is often referred to by a statistical name; i.e., expected risk. This name is in part a misnomer. Sequences developed in this study only have the potential for fuel release; i.e., they are not expected. Table 12-7 presents the list of basic events in the QRVA model sorted by Fussell-Vesely importance to expected risk; i.e., sorted from largest to smallest importance. Basic events with zero Fussell-Vesely importance are removed from this table. Other standard risk importance measures to expected risk are also listed in the table along with the basic event value and basic event description.

A column labeled “Basic event type” is also included in Table 12-7. This column simply identifies which basic events refer to a human failure event, or to an equipment failure. There are other basic events in the QRVA Model which are not presented in Table 12-7. These omitted basic events include fault tree house events, and basic events which track different initial sequence conditions. These basic events include those which track whether a fuel movement is in progress when the initiating event occurs, if so what type of fuel movement, and the fuel level at which a leak is assumed to occur in a RHBFST if the initiating events involves such a leak. These basic events that have been omitted

from Table 12-7 are referred to as flags, although they often have values less than 1.0. The full set of basic events with importance to expected risk are included in tab "BE Importance to Expected Risk" in the attached Excel file named Master Frequency File and Importance Measures.xlsx

Table 12-7 indicates that the top basic event to expected risk is a human failure event; i.e., OEV_OEV1. This action is defined for conditions when a RHBFST is being filled to its maximum operating level to prepare for its annual leak tightness test. While this human action is a routine event at Red Hill, experience data for failures of this routine action (i.e., in total and as a function of the amount of overfilling) were not available to be incorporated into the QRVA. Further, the RHBFST high level alarm level settings are well above their maximum operating levels and so would not affect the assessment of OEV_OEV1.

The second ranked human failure event is OSEC_OSEC6. This action is to remotely close the sectional valves on a leaking fuel line so as to isolate the leak and thereby limit the fuel release to the LAT or to the Harbor Tunnel, to that initially contained in the leaking section between sectional valves. Closure of the appropriate sectional valves is not directed by procedures, but may be expected based on general operator training once a start of sump pumps is detected and investigated. No credit for this action is used if earlier in the sequence the operators failed to actuate the panic button; i.e., when top event OPAN has already failed. Credit is taken for this action when the applicable fuel line postulated to be leaking is initially idle; no fuel movement is in progress. This condition is represented by human failure event OSEC_OSEC3.

Human Failure Event OPAN_OPAN2 has a Fussell-Vesely importance to expected risk metric of 6.04E-3. This action is credited when the leak to the LAT is not from a RBFST nozzle, and the operators identify the start of sump pumps or the staff at Red Hill initiate an evacuation due to the size of the fuel leak.

Other human failure events with Fussell-Vesely importance of 1E-3 or higher are the basic events representing the actions to identify the need for (Top Event ORGA1), notify management (Top Event OUFM), plan a response (Top Event OSUP), and execute the strategy and plans created to empty a RHBFST (Top Event OXFR) when necessary. The basic events representing these actions include: OXFR_OXFR5, OSUP_OSUP6, OXFR_OXFR1, OUFM_OUFM2, OSUP_OSUP1,OXFR_OXFR4, OUFM_OUFM1, OSUP_OSUP5, and ORGA1_ORGA16. The QRVA assumes that failure of one or more of these actions introduces a delay in the staff response to performing the actions needed to empty the affected RHBFST. The delays in the response then leads to higher fuel releases.

Basic events representing equipment failures generally have lower Fussell-Vesely importance to expected risk than from human failure events. This is because equipment failures needed to mitigate an initial leak are less probable than the assessed human failure events. Only four equipment failures have Fussell-Vesely importance measures greater than 1E-3. Two of these (i.e., MDCFTS and FANFTS) involve failures of the room cooling system for the AFHE system. Failure of either equipment is judged to result in a temporary loss of the AFHE system. The AFHE system is needed for continuous detection of any drop in RHBFST fuel levels. The delay in restoring the AFHE system, whose failure must occur coincident with an initiating event before it can

be mitigated, leads to a greater amount of fuel evaluated as being released for these sequence that depend on the AFHE system for detection and mitigation.

The other two equipment failures with Fussell-Vesely importance greater than 1E-3 (i.e., XFR31SF and XFR51) represent the hardware failures involving equipment that is needed to move fuel from a RHBFST that needs to be emptied. Top Event XFR3 represents the failures of hardware needed to move fuel from one RHBFST to another using the cargo pumps at the underground pump house. Top Event XFR5 represents the hardware needed to drain the lowest 7.5' of fuel from a leaking RHBFST. The equipment response represented by XFR5 is only needed if there is a leak in the RHBFST liner in the lower dome. Failure of either of these events is modeled as delaying the RHBFST emptying process and therefore leading to higher fuel releases than otherwise would occur. While hardware failures may initially preclude remote actions to align the equipment needed to empty a RHBFST, local actions to manually align or repair the equipment failed are also possible.

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| OEV_OEV1 | 2.16E-02 | Human Failure Event | 1.85E-01 | 1.85E-01 | 8.57E+00 | 9.39E+00 | 1.23E+00 | Operators fail to correctly specify evolution or to stop evolution before overfilling |
| MDCFTS | 2.09E-04 | Equipment Failure | 2.54E-02 | 1.20E-02 | 8.87E-01 | 1.87E+00 | 1.01E+00 | AFHE Condenser Fails to Start |
| OSEC_OSEC6 | 1.000 | Human Failure Event | 1.09E-02 | 1.09E-02 | 1.09E-02 | 1.00E+00 | 1.01E+00 | Failure to close sectionals during Idle or Fuel Movement given successful detection of sump pump start |
| OXFR_OXFR5 | 6.67E-02 | Human Failure Event | 2.16E-02 | 9.93E-03 | 1.49E-01 | 1.14E+00 | 1.01E+00 | Failure to implement strategy to empty RHBFST given Leak following overfill |
| OSUP_OSUP6 | 4.49E-02 | Human Failure Event | 1.45E-02 | 6.49E-03 | 1.45E-01 | 1.14E+00 | 1.01E+00 | Failure to formulate strategy to empty RHBFST given Leak following overfill |
| OPAN_OPAN2 | 9.63E-02 | Human Failure Event | 1.05E-02 | 6.04E-03 | 6.27E-02 | 1.06E+00 | 1.01E+00 | Failure to push panic button given Fuel Line Leak to LAT during Fuel Movement |
| XFR31SF | 8.56E-03 | Equipment Failure | 1.05E-02 | 4.48E-03 | 5.23E-01 | 1.52E+00 | 1.00E+00 | Hardware fails for 2-step inter-tank transfer to empty RHBFST using cargo pumps |
| OXFR_OXFR1 | 6.67E-02 | Human Failure Event | 1.50E-02 | 4.05E-03 | 6.07E-02 | 1.06E+00 | 1.00E+00 | Failure to Implement RHBFST empty strategy given leak to rock |
| OUFM_OUFM2 | 6.35E-02 | Human Failure Event | 4.76E-02 | 3.29E-03 | 5.18E-02 | 1.05E+00 | 1.00E+00 | Failure to detect RHBFST low level alarm given nozzle leak |
| OSEC_OSEC3 | 9.94E-02 | Human Failure Event | 6.13E-03 | 3.23E-03 | 3.25E-02 | 1.03E+00 | 1.00E+00 | Failure to close sectionals during for 0.5" hole; idle; with successful detection of sump start |
| OSUP_OSUP1 | 4.49E-02 | Human Failure Event | 1.00E-02 | 2.65E-03 | 5.90E-02 | 1.06E+00 | 1.00E+00 | Failure to Formulate RHBFST empty strategy given leak to rock |
| OXFR_OXFR4 | 6.67E-02 | Human Failure Event | 6.14E-03 | 2.41E-03 | 3.61E-02 | 1.03E+00 | 1.00E+00 | Failure to implement strategy to empty RHBFST given Return to Service |
| XFR51 | 3.21E-03 | Equipment Failure | 3.99E-03 | 1.74E-03 | 5.42E-01 | 1.54E+00 | 1.00E+00 | Hardware for draining lower dome available including sectional valves |
| OUFM_OUFM1 | 6.35E-02 | Human Failure Event | 1.04E-02 | 1.62E-03 | 2.55E-02 | 1.02E+00 | 1.00E+00 | Failure to detect RHBFST low level alarm given 1.5 gpm leak rate |
| FANFTS | 7.96E-04 | Equipment Failure | 3.35E-03 | 1.59E-03 | 8.76E-01 | 1.87E+00 | 1.00E+00 | AFHE Fan for room cooling Fails To Start |
| OSUP_OSUP5 | 4.49E-02 | Human Failure Event | 4.12E-03 | 1.58E-03 | 3.51E-02 | 1.03E+00 | 1.00E+00 | Failure to formulate strategy to empty RHBFST given leak during Return to Service |
| ORGA1_ORGA16 | 2.52E-02 | Human Failure Event | 5.03E-03 | 1.03E-03 | 4.10E-02 | 1.04E+00 | 1.00E+00 | Failure to confirm 0.5" hole in RHBFST after overfill ends |
| ORGA1_ORGA18 | 7.39E-02 | Human Failure Event | 6.85E-03 | 9.37E-04 | 1.27E-02 | 1.01E+00 | 1.00E+00 | Dependent Failure to confirm RHBFST leak to rock given failure to initially detect low level alarm (OUFM=F) |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| XFR21SF | 5.35E-03 | Equipment Failure | 4.48E-03 | 7.20E-04 | 1.35E-01 | 1.13E+00 | 1.00E+00 | Hardware failure for issuing to Upper tank farm plus skin and ball valve |
| OTRIP_OTRIP1 | 5.12E-02 | Human Failure Event | 9.55E-03 | 6.48E-04 | 1.27E-02 | 1.01E+00 | 1.00E+00 | Operators fail to stop overfill after receiving high level alarm |
| OUFM_OUFM4 | 6.35E-02 | Human Failure Event | 3.72E-03 | 6.10E-04 | 9.61E-03 | 1.01E+00 | 1.00E+00 | Failure to detect RHBFST low level given leak at 1.5 gpm during pause in Return to Service |
| ORGA1_ORGA11 | 2.52E-02 | Human Failure Event | 3.79E-03 | 5.56E-04 | 2.21E-02 | 1.02E+00 | 1.00E+00 | Failure to confirm leak to rock given 1.5 gpm leak |
| OUFM_OUFM8 | 0.110 | Human Failure Event | 3.47E-03 | 4.27E-04 | 3.87E-03 | 1.00E+00 | 1.00E+00 | Dependent Failure to detect RHBFST low level alarm given any leak to LAT a previous human failure event (i.e. OPAN, OSEC, or OTRIP=F) |
| OPAN_OPAN1 | 9.63E-02 | Human Failure Event | 4.86E-02 | 2.94E-04 | 3.05E-03 | 1.00E+00 | 1.00E+00 | Failure to Push Panic Button during nozzle leak (small or large) to LAT |
| XFR11SF | 2.14E-03 | Equipment Failure | 1.79E-03 | 2.87E-04 | 1.34E-01 | 1.13E+00 | 1.00E+00 | Hardware for inter-RHBFST gravity transfer to empty affected RHBFST |
| OSEC_OSEC5 | 9.94E-02 | Human Failure Event | 3.53E-04 | 2.71E-04 | 2.72E-03 | 1.00E+00 | 1.00E+00 | Failure to close sectionals during Fuel Movement for 6" hole with successful detection of sump pump start |
| OSUM_OSUM5 | 6.71E-02 | Human Failure Event | 5.89E-04 | 2.46E-04 | 3.66E-03 | 1.00E+00 | 1.00E+00 | Failure to detect leak to LAT during Fuel Movement; with sump start and door closing |
| OUFM_OUFM5 | 6.35E-02 | Human Failure Event | 1.99E-03 | 2.08E-04 | 3.27E-03 | 1.00E+00 | 1.00E+00 | Failure to detect low level alarm 0.5" hole size |
| ORGA1_ORGA15 | 2.52E-02 | Human Failure Event | 1.34E-03 | 1.87E-04 | 7.41E-03 | 1.01E+00 | 1.00E+00 | Failure to confirm 1.5 gpm leak to rock when in pause during RHBFST Return to Service |
| EL72_FOD | 6.56E-04 | Equipment Failure | 7.65E-03 | 1.87E-04 | 2.50E-02 | 1.02E+00 | 1.00E+00 | Elevator 72 Fails or is not available on demand |
| EL73_FOD | 6.56E-04 | Equipment Failure | 7.65E-03 | 1.87E-04 | 2.50E-02 | 1.02E+00 | 1.00E+00 | Elevator 73 Fails or is not available on demand |
| OXFR_OXFR3 | 6.67E-02 | Human Failure Event | 3.69E-03 | 1.69E-04 | 2.53E-03 | 1.00E+00 | 1.00E+00 | Failure to Implement strategy to empty RHBFST given FL Leak to LAT |
| OSUP_OSUP4 | 4.49E-02 | Human Failure Event | 2.49E-03 | 1.11E-04 | 2.47E-03 | 1.00E+00 | 1.00E+00 | Failure to formulate strategy to empty RHBFST given FL Leak to LAT |
| OSEC_OSEC2 | 9.94E-02 | Human Failure Event | 1.96E-04 | 1.10E-04 | 1.11E-03 | 1.00E+00 | 1.00E+00 | Failure to close sectionals during Fuel Movement for 0.5" hole to LAT |
| FLMAINT | 0.109 | Human Failure Event | 1.10E-04 | 1.10E-04 | 1.00E-03 | 1.00E+00 | 1.00E+00 | Fuel Line Maintenance Requiring opening of a fuel line or a valve |
| OUFM_OUFM7 | 6.35E-02 | Human Failure Event | 6.57E-04 | 1.08E-04 | 1.70E-03 | 1.00E+00 | 1.00E+00 | Failure to detect low level alarm given pause during Return to Service 0.5" hole |
| OSEC_OSEC4 | 9.94E-02 | Human Failure Event | 8.59E-04 | 1.03E-04 | 1.03E-03 | 1.00E+00 | 1.00E+00 | Failure to close sectionals for 6" hole fuel line; idle; with successful detection of sump start |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| M0117D | 3.28E-04 | Equipment Failure | 1.62E-04 | 9.37E-05 | 8.70E-02 | 1.09E+00 | 1.00E+00 | M0117D - RHBFST 17 Skin Valve Fails to Open or Close |
| M0117E | 3.28E-04 | Equipment Failure | 1.62E-04 | 9.37E-05 | 8.70E-02 | 1.09E+00 | 1.00E+00 | M0117E - RHBFST 17 Ballx Valve Fails to Open or Close |
| AFHEFTOP | 1.08E-03 | Equipment Failure | 7.15E-04 | 8.53E-05 | 1.36E-01 | 1.14E+00 | 1.00E+00 | Process Logic Fail to Operate |
| M0105D | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.06E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0105D - RHBFST 5 Skin Valve Fails to Open or Close |
| M0105E | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.06E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0105E - RHBFST 5 Ballx Valve Fails to Open or Close |
| M0106D | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.06E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0106D - RHBFST 6 Skin Valve Fails to Open or Close |
| M0106E | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.06E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0106E - RHBFST 6 Ballx Valve Fails to Open or Close |
| M0104D | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0104D - RHBFST 4 Skin Valve Fails to Open or Close |
| M0104E | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0104E - RHBFST 4 Ballx Valve Fails to Open or Close |
| M0107D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0107D - RHBFST 7 Skin Valve Fails to Open or Close |
| M0107E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0107E - RHBFST 7 Ballx Valve Fails to Open or Close |
| M0108D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0108D - RHBFST 8 Skin Valve Fails to Open or Close |
| M0108E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0108E - RHBFST 8 Ballx Valve Fails to Open or Close |
| M0109D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0109D - RHBFST 9 Skin Valve Fails to Open or Close |
| M0109E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0109E - RHBFST 9 Ballx Valve Fails to Open or Close |
| M0110D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0110D - RHBFST 10 Skin Valve Fails to Open or Close |
| M0110E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0110E - RHBFST 10 Ballx Valve Fails to Open or Close |
| M0111D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0111D - RHBFST 11 Skin Valve Fails to Open or Close |
| M0111E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0111E - RHBFST 11 Ballx Valve Fails to Open or Close |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| M0112D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0112D - RHBFST 12 Skin Valve Fails to Open or Close |
| M0112E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0112E - RHBFST 12 Ballx Valve Fails to Open or Close |
| M0113D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0113D - RHBFST 13 Skin Valve Fails to Open or Close |
| M0113E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0113E - RHBFST 13 Ballx Valve Fails to Open or Close |
| M0114D | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0114D - RHBFST 14 Skin Valve Fails to Open or Close |
| M0114E | 3.28E-04 | Equipment Failure | 1.36E-04 | 8.05E-05 | 7.48E-02 | 1.07E+00 | 1.00E+00 | M0114E - RHBFST 14 Ballx Valve Fails to Open or Close |
| M0102D | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.05E-05 | 7.47E-02 | 1.07E+00 | 1.00E+00 | M0102D - RHBFST 2 Skin Valve Fails to Open or Close |
| M0102E | 3.28E-04 | Equipment Failure | 1.37E-04 | 8.05E-05 | 7.47E-02 | 1.07E+00 | 1.00E+00 | M0102E - RHBFST 2 Ballx Valve Fails to Open or Close |
| MDCFTR | 1.32E-04 | Equipment Failure | 1.69E-04 | 8.03E-05 | 8.75E-01 | 1.87E+00 | 1.00E+00 | AFHE Compressor Fails to Run |
| M0120D | 3.28E-04 | Equipment Failure | 1.23E-04 | 7.37E-05 | 6.85E-02 | 1.07E+00 | 1.00E+00 | M0120D - RHBFST 20 Skin Valve Fails to Open or Close |
| M0120E | 3.28E-04 | Equipment Failure | 1.23E-04 | 7.37E-05 | 6.85E-02 | 1.07E+00 | 1.00E+00 | M0120E - RHBFST 20 Ballx Valve Fails to Open or Close |
| OPFL1 | 4.65E-02 | Human Failure Event | 2.29E-03 | 7.21E-05 | 1.55E-03 | 1.00E+00 | 1.00E+00 | Operators Recognize Drop in Fuel Line Pressure for leak to LAT while RHBFSTs are idle |
| OSUM_OSUM7 | 0.114 | Human Failure Event | 3.24E-04 | 7.18E-05 | 6.31E-04 | 1.00E+00 | 1.00E+00 | Failure to detect leak to LAT during Idle or Fuel Movement given fuel line pressure drop not detected |
| ORGA1_ORGA17 | 2.52E-02 | Human Failure Event | 7.26E-04 | 6.71E-05 | 2.66E-03 | 1.00E+00 | 1.00E+00 | Failure to confirm leak to rock given liner 0.5" hole |
| M0103D | 3.28E-04 | Equipment Failure | 9.10E-05 | 6.02E-05 | 5.59E-02 | 1.06E+00 | 1.00E+00 | M0103D - RHBFST 3 Skin Valve Fails to Open or Close |
| M0103E | 3.28E-04 | Equipment Failure | 9.10E-05 | 6.02E-05 | 5.59E-02 | 1.06E+00 | 1.00E+00 | M0103E - RHBFST 3 Ballx Valve Fails to Open or Close |
| EMPLN108C | 9.29E-04 | Equipment Failure | 4.93E-05 | 4.93E-05 | 1.70E-02 | 1.02E+00 | 1.00E+00 | Error in Maintenance Plan; mistaking the JP5 (108C) valve |
| OPEMPLN108C | 8.89E-02 | Human Failure Event | 4.93E-05 | 4.93E-05 | 1.64E-03 | 1.00E+00 | 1.00E+00 | Operator / control room fails to detect the error in the maintenance |
| OXFR_OXFR2 | 6.67E-02 | Human Failure Event | 1.60E-02 | 4.04E-05 | 6.05E-04 | 1.00E+00 | 1.00E+00 | Failure to implement strategy to empty RHBFST given nozzle leak |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| M0118D | 3.28E-04 | Equipment Failure | 5.62E-05 | 3.90E-05 | 3.62E-02 | 1.04E+00 | 1.00E+00 | M0118D - RHBFST 18 Skin Valve Fails to Open or Close |
| M0118E | 3.28E-04 | Equipment Failure | 5.62E-05 | 3.90E-05 | 3.62E-02 | 1.04E+00 | 1.00E+00 | M0118E - RHBFST 18 Ballx Valve Fails to Open or Close |
| B3EA1 | 4.55E-05 | Equipment Failure | 8.25E-05 | 3.71E-05 | 8.15E-01 | 1.82E+00 | 1.00E+00 | Hardware transformer and panels B and A (U.E.) |
| SVFTC | 3.28E-04 | Equipment Failure | 9.18E-05 | 3.59E-05 | 3.34E-02 | 1.03E+00 | 1.00E+00 | Sectional Valve Fail to Close |
| M0115D | 3.28E-04 | Equipment Failure | 1.33E-04 | 3.57E-05 | 3.31E-02 | 1.03E+00 | 1.00E+00 | M0115D - RHBFST 15 Skin Valve Fails to Open or Close |
| M0115E | 3.28E-04 | Equipment Failure | 1.33E-04 | 3.57E-05 | 3.31E-02 | 1.03E+00 | 1.00E+00 | M0115E - RHBFST 15 Ballx Valve Fails to Open or Close |
| M0116D | 3.28E-04 | Equipment Failure | 1.32E-04 | 3.57E-05 | 3.31E-02 | 1.03E+00 | 1.00E+00 | M0116D - RHBFST 16 Skin Valve Fails to Open or Close |
| M0116E | 3.28E-04 | Equipment Failure | 1.32E-04 | 3.57E-05 | 3.31E-02 | 1.03E+00 | 1.00E+00 | M0116E - RHBFST 16 Ballx Valve Fails to Open or Close |
| ORGA1_ORGA13 | 2.52E-02 | Human Failure Event | 2.37E-04 | 3.40E-05 | 1.35E-03 | 1.00E+00 | 1.00E+00 | Failure to confirm 0.5" hole during pause in Return to Service |
| EMPLN102C | 2.90E-03 | Equipment Failure | 3.36E-05 | 3.36E-05 | 1.16E-02 | 1.01E+00 | 1.00E+00 | Error in Maintenance Plan; mistaking the F24 (102C) valve |
| OPEMPLN102C | 3.00E-02 | Human Failure Event | 3.36E-05 | 3.36E-05 | 1.12E-03 | 1.00E+00 | 1.00E+00 | Operator / control room fails to detect the error in the maintenance |
| OUFM_OUFM3 | 6.35E-02 | Human Failure Event | 2.23E-03 | 3.19E-05 | 5.01E-04 | 1.00E+00 | 1.00E+00 | Failure to detect low level alarm after Fuel Movement during nozzle leak |
| EDGFTS | 1.15E-03 | Equipment Failure | 6.92E-05 | 2.73E-05 | 6.00E-03 | 1.01E+00 | 1.00E+00 | Emergency Diesel Generator (Standby) Fail to Start |
| EMPLN115C | 9.29E-04 | Equipment Failure | 2.66E-05 | 2.66E-05 | 9.15E-03 | 1.01E+00 | 1.00E+00 | Error in Maintenance Plan; mistaking the F76 (115C) valve |
| OPEMPLN115C | 8.89E-02 | Human Failure Event | 2.66E-05 | 2.66E-05 | 8.85E-04 | 1.00E+00 | 1.00E+00 | Operator / control room fails to detect the error in the maintenance |
| ORGA1_ORGA14 | 2.52E-02 | Human Failure Event | 1.25E-03 | 2.42E-05 | 9.62E-04 | 1.00E+00 | 1.00E+00 | Failure to confirm FL leak to LAT and RHBFST Losing fuel |
| VIB102 | 8.89E-02 | Human Failure Event | 2.16E-05 | 2.16E-05 | 7.20E-04 | 1.00E+00 | 1.00E+00 | Vibration and sound of fuel movement in main fuel line missed |
| [P0206FTR P0207FTR] | 8.29E-05 | Equipment Failure | 6.57E-05 | 2.03E-05 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPR, JP5 Pumps FTR, 2/3 |
| [P0206FTR P0208FTR] | 8.29E-05 | Equipment Failure | 6.57E-05 | 2.03E-05 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPR, JP5 Pumps FTR, 3/3 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [P0207FTR P0208FTR] | 8.29E-05 | Equipment Failure | 6.57E-05 | 2.03E-05 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:F24MDPR, F24 Pumps FTR, 2/3 |
| ABTFTOP | 2.39E-09 | Equipment Failure | 3.71E-05 | 1.84E-05 | 5.99E-03 | 1.01E+00 | 1.00E+00 | Automatic Bus Transfer Switch Fail to Operate |
| OSUP_OSUP2 | 4.49E-02 | Human Failure Event | 1.05E-02 | 1.76E-05 | 3.93E-04 | 1.00E+00 | 1.00E+00 | Failure to formulate strategy to empty RHBFST given nozzle leak |
| EDGFTR1 | 7.23E-04 | Equipment Failure | 4.41E-05 | 1.74E-05 | 5.99E-03 | 1.01E+00 | 1.00E+00 | Emergency Diesel Generator Fail to Run During First Hour of Operation |
| [P0206FTR P0207FTR P0208FTR] | 6.67E-05 | Equipment Failure | 5.28E-05 | 1.64E-05 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:F24MDPR, F24 Pumps FTR, 2/3 |
| FANFTR | 6.74E-06 | Equipment Failure | 2.00E-05 | 9.48E-06 | 8.75E-01 | 1.87E+00 | 1.00E+00 | AFHE room cooling Fan Fails To Run |
| VIB115 | 8.89E-02 | Human Failure Event | 9.23E-06 | 9.23E-06 | 3.08E-04 | 1.00E+00 | 1.00E+00 | Vibration and sound of fuel movement in main fuel line missed |
| [P0209FTR P0210FTR] | 8.29E-05 | Equipment Failure | 2.92E-05 | 8.89E-06 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 2/3 |
| [P0209FTR P0211FTR] | 8.29E-05 | Equipment Failure | 2.92E-05 | 8.89E-06 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 2/3 |
| [P0210FTR P0211FTR] | 8.29E-05 | Equipment Failure | 2.92E-05 | 8.89E-06 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 2/3 |
| EDGFTR3 | 1.56E-03 | Equipment Failure | 2.14E-05 | 8.56E-06 | 5.04E-03 | 1.01E+00 | 1.00E+00 | Emergency Diesel Generator Fail to Run During 3 Hours of Operation |
| [P0209FTR P0210FTR P0211FTR] | 6.67E-05 | Equipment Failure | 2.35E-05 | 7.15E-06 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 3/3 |
| VIB108 | 8.89E-02 | Human Failure Event | 6.55E-06 | 6.55E-06 | 2.18E-04 | 1.00E+00 | 1.00E+00 | Vibration and sound of fuel movement in main fuel line missed |
| ORGA1_ORGA12 | 2.52E-02 | Human Failure Event | 1.26E-02 | 5.12E-06 | 2.03E-04 | 1.00E+00 | 1.00E+00 | Failure to detect low level alarm given nozzle leak |
| [P0206FTR] | 3.01E-03 | Equipment Failure | 1.56E-05 | 4.82E-06 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPR; JP5 Pumps FTR; 1/3 |
| [P0207FTR] | 3.01E-03 | Equipment Failure | 1.56E-05 | 4.82E-06 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPR; JP5 Pumps FTR; 1/3 |
| [P0208FTR] | 3.01E-03 | Equipment Failure | 1.56E-05 | 4.82E-06 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPR; JP5 Pumps FTR; 1/3 |
| EDGFTR12 | 8.61E-03 | Equipment Failure | 1.30E-05 | 4.66E-06 | 4.99E-04 | 1.00E+00 | 1.00E+00 | Emergency Diesel Generator Fail to Run During 12 Hours of Operation |
| TFMFTOP | 3.99E-08 | Equipment Failure | 8.75E-06 | 4.19E-06 | 4.59E+00 | 5.59E+00 | 1.00E+00 | Transformer to Red Hill 480v Emergency bus Fails to Operate |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [SF1AFTR SF1BFTR] | 3.26E-06 | Equipment Failure | 7.32E-06 | 4.06E-06 | 1.24E+00 | 2.24E+00 | 1.00E+00 | CCF:ESF1FTR, Red Hill Ventilation Fans ES1A & 1B FTR, 2/2 |
| [EF1AFTR EF1BFTR] | 3.26E-06 | Equipment Failure | 7.32E-06 | 4.06E-06 | 1.24E+00 | 2.24E+00 | 1.00E+00 | CCF:EEF1FTR; Red Hill Ventilation Fans EF1A & 1B FTR; 2/2 |
| [EF2AFTR EF2BFTR] | 3.26E-06 | Equipment Failure | 7.32E-06 | 4.06E-06 | 1.24E+00 | 2.24E+00 | 1.00E+00 | CCF:EEF2FTR; Red Hill Ventilation Fans EF2A & 2B FTR; 2/2 |
| XFR41SF | 8.56E-03 | Equipment Failure | 6.03E-03 | 2.83E-06 | 3.31E-04 | 1.00E+00 | 1.00E+00 | Hardware for gravity feed to Pearl |
| [SF5AFTR SF5BFTR] | 3.26E-06 | Equipment Failure | 5.92E-06 | 2.66E-06 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:USF5FTR; Red Hill Ventilation Fans SF5A & 5B FTR; 2/2 |
| [P0209FTR] | 3.01E-03 | Equipment Failure | 6.92E-06 | 2.11E-06 | 6.99E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 1/3 |
| [P0210FTR] | 3.01E-03 | Equipment Failure | 6.92E-06 | 2.11E-06 | 6.99E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 1/3 |
| [P0211FTR] | 3.01E-03 | Equipment Failure | 6.92E-06 | 2.11E-06 | 6.99E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPR; F24 Pumps FTR; 1/3 |
| BUSFTOP | 7.92E-08 | Equipment Failure | 4.17E-06 | 2.00E-06 | 4.59E+00 | 5.59E+00 | 1.00E+00 | 480v Red Hill Emergency Bus Fails to Operate |
| EDGFTR6 | 3.91E-03 | Equipment Failure | 4.54E-06 | 1.71E-06 | 4.04E-04 | 1.00E+00 | 1.00E+00 | Emergency Diesel Generator Fail to Run During 6 Hours of Operation |
| [EF6DFTR] | 2.57E-04 | Equipment Failure | 3.16E-06 | 1.42E-06 | 5.53E-03 | 1.01E+00 | 1.00E+00 | CCF:UEF6FTR; USF 6A 6B 6C & 6D FTR; 1/4 |
| [EF6AFTR] | 2.57E-04 | Equipment Failure | 3.16E-06 | 1.42E-06 | 5.53E-03 | 1.01E+00 | 1.00E+00 | CCF:UEF6FTR; USF 6A 6B 6C & 6D FTR; 1/4 |
| [EF6BFTR] | 2.57E-04 | Equipment Failure | 3.16E-06 | 1.42E-06 | 5.53E-03 | 1.01E+00 | 1.00E+00 | CCF:UEF6FTR; USF 6A 6B 6C & 6D FTR; 1/4 |
| [EF6CFTR] | 2.57E-04 | Equipment Failure | 3.16E-06 | 1.42E-06 | 5.53E-03 | 1.01E+00 | 1.00E+00 | CCF:UEF6FTR; USF 6A 6B 6C & 6D FTR; 1/4 |
| [P0206FTS P0207FTS P0208FTS] | 4.15E-06 | Equipment Failure | 3.28E-06 | 1.02E-06 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 3/3 |
| LPRH1SF | 1.41E-05 | Equipment Failure | 1.51E-05 | 1.01E-06 | 7.13E-02 | 1.07E+00 | 1.00E+00 | DEFAULT BRE48=S |
| EDGFTR24 | 1.80E-02 | Equipment Failure | 3.08E-06 | 9.36E-07 | 4.79E-05 | 1.00E+00 | 1.00E+00 | Emergency Diesel Generator Fail to Run During 24 Hours of Operation |
| [EF6AFTR EF6BFTR EF6CFTR EF6DFTR] | 1.03E-06 | Equipment Failure | 1.88E-06 | 8.42E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; Red Hill Ventilation Fans USF 6A 6B 6C & 6D FTR; 4/4 |
| [P0206FTS P0207FTS] | 3.15E-06 | Equipment Failure | 2.50E-06 | 7.73E-07 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 2/3 |
| [P0206FTS P0208FTS] | 3.15E-06 | Equipment Failure | 2.50E-06 | 7.73E-07 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 2/3 |
| [P0207FTS P0208FTS] | 3.15E-06 | Equipment Failure | 2.50E-06 | 7.73E-07 | 2.45E-01 | 1.25E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 2/3 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [EF1AFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:EEF1FTR; EF1A & 1B FTR; 1/2 |
| [SF1AFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:ESF1FTR; ES1A & 1B FTR; 1/2 |
| [SF1BFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:ESF1FTR; ES1A & 1B FTR; 1/2 |
| [EF1BFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:EEF1FTR; EF1A & 1B FTR; 1/2 |
| [EF2AFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:EEF2FTR; EF2A & 2B FTR; 1/2 |
| [EF2BFTR] | 2.57E-04 | Equipment Failure | 1.30E-06 | 7.23E-07 | 2.81E-03 | 1.00E+00 | 1.00E+00 | CCF:EEF2FTR; EF2A & 2B FTR; 1/2 |
| FLTK02 | 5.00E-07 | Equipment Failure | 1.07E-06 | 6.00E-07 | 1.20E+00 | 2.20E+00 | 1.00E+00 | 5 SECTIONAL VALVES MUST REMAIN OPEN TOP EMPTY A RHBFST |
| FLTKO1 | 1.07E-03 | Equipment Failure | 5.60E-05 | 5.97E-07 | 5.58E-04 | 1.00E+00 | 1.00E+00 | Open one sectional valve |
| [SF5AFTR] | 2.57E-04 | Equipment Failure | 1.06E-06 | 4.74E-07 | 1.84E-03 | 1.00E+00 | 1.00E+00 | CCF:USF5FTR; SF5A & 5B FTR; 1/2 |
| [SF5BFTR] | 2.57E-04 | Equipment Failure | 1.06E-06 | 4.74E-07 | 1.84E-03 | 1.00E+00 | 1.00E+00 | CCF:USF5FTR; SF5A & 5B FTR; 1/2 |
| [P0209FTS P0210FTS P0211FTS] | 4.15E-06 | Equipment Failure | 1.46E-06 | 4.45E-07 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 3/3 |
| [SFPS1AFTR SFPS1BFTR] | 3.26E-06 | Equipment Failure | 3.69E-06 | 4.27E-07 | 1.31E-01 | 1.13E+00 | 1.00E+00 | CCF:TSF1FTR; TSF1A & 1B FTR; 2/2 |
| [PE1AFTR PE1BFTR] | 3.26E-06 | Equipment Failure | 3.69E-06 | 4.27E-07 | 1.31E-01 | 1.13E+00 | 1.00E+00 | CCF:TEF1FTR; TE1A & 1B FTR; 2/2 |
| [SFPS2AFTR SFPS2BFTR] | 3.26E-06 | Equipment Failure | 3.69E-06 | 4.27E-07 | 1.31E-01 | 1.13E+00 | 1.00E+00 | CCF:TSF2FTR; TSF2A & 2B FTR; 2/2 |
| [P0208FTS] | 2.60E-04 | Equipment Failure | 1.34E-06 | 4.14E-07 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 1/3 |
| [P0206FTS] | 2.60E-04 | Equipment Failure | 1.34E-06 | 4.14E-07 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 1/3 |
| [P0207FTS] | 2.60E-04 | Equipment Failure | 1.34E-06 | 4.14E-07 | 1.60E-03 | 1.00E+00 | 1.00E+00 | CCF:JP5MDPS; JP5 Pumps FTS; 1/3 |
| [EF6AFTR EF6BFTR EF6CFTR] | 5.07E-07 | Equipment Failure | 9.21E-07 | 4.13E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 3/4 |
| [EF6AFTR EF6BFTR EF6DFTR] | 5.07E-07 | Equipment Failure | 9.21E-07 | 4.13E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 3/4 |
| [EF6AFTR EF6CFTR EF6DFTR] | 5.07E-07 | Equipment Failure | 9.21E-07 | 4.13E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 3/4 |
| [EF6BFTR EF6CFTR EF6DFTR] | 5.07E-07 | Equipment Failure | 9.21E-07 | 4.13E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 3/4 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [P0209FTS P0210FTS] | 3.15E-06 | Equipment Failure | 1.11E-06 | 3.38E-07 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 2/3 |
| [P0209FTS P0211FTS] | 3.15E-06 | Equipment Failure | 1.11E-06 | 3.38E-07 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 2/3 |
| [P0210FTS P0211FTS] | 3.15E-06 | Equipment Failure | 1.11E-06 | 3.38E-07 | 1.07E-01 | 1.11E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 2/3 |
| [P0201FTR P0202FTR P0203FTR P0204FTR] | 1.60E-05 | Equipment Failure | 3.59E-06 | 2.62E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 4/5 |
| [P0201FTR P0202FTR P0203FTR P0205FTR] | 1.60E-05 | Equipment Failure | 3.59E-06 | 2.62E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 4/5 |
| [P0201FTR P0202FTR P0204FTR P0205FTR] | 1.60E-05 | Equipment Failure | 3.59E-06 | 2.62E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 4/5 |
| [P0201FTR P0203FTR P0204FTR P0205FTR] | 1.60E-05 | Equipment Failure | 3.59E-06 | 2.62E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 4/5 |
| [P0202FTR P0203FTR P0204FTR P0205FTR] | 1.60E-05 | Equipment Failure | 3.59E-06 | 2.62E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 4/5 |
| [EF6AFTR EF6BFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |
| [EF6AFTR EF6CFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |
| [EF6AFTR EF6DFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |
| [EF6BFTR EF6CFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |
| [EF6BFTR EF6DFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |
| [EF6CFTR EF6DFTR] | 3.14E-07 | Equipment Failure | 5.70E-07 | 2.56E-07 | 8.15E-01 | 1.81E+00 | 1.00E+00 | CCF:UEF6FTR; UGPH Exhaust Fans 6A 6B 6C & 6D FTR; 2/4 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [USUMP1FTR USUMP2FTR] | 1.97E-04 | Equipment Failure | 1.07E-05 | 2.43E-07 | 1.23E-03 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTR; Harbor Tunnel Sump Pumps FTR; 2/2 |
| [P0201FTR P0202FTR P0203FTR P0204FTR P0205FTR] | 1.12E-05 | Equipment Failure | 2.52E-06 | 1.84E-07 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 5/5 |
| [P0209FTS] | 2.60E-04 | Equipment Failure | 5.95E-07 | 1.81E-07 | 6.97E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 1/3 |
| [P0210FTS] | 2.60E-04 | Equipment Failure | 5.95E-07 | 1.81E-07 | 6.97E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 1/3 |
| [P0211FTS] | 2.60E-04 | Equipment Failure | 5.95E-07 | 1.81E-07 | 6.97E-04 | 1.00E+00 | 1.00E+00 | CCF:F24MDPS; F24 Pumps FTS; 1/3 |
| ERRV108SIZE | 8.89E-02 | Equipment Failure | 1.43E-07 | 1.43E-07 | 4.76E-06 | 1.00E+00 | 1.00E+00 | Mistaking the JP5 (108B) valve size difference |
| NSTOC108 | 5.97E-04 | Equipment Failure | 1.43E-07 | 1.43E-07 | 4.93E-05 | 1.00E+00 | 1.00E+00 | Navy's Subcontractor Tag out valve 108C in error |
| RHTOC08 | 5.97E-04 | Human Failure Event | 1.24E-07 | 1.24E-07 | 4.27E-05 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 108C in error |
| OSUM_OSUM8 | 1.000 | Human Failure Event | 9.30E-08 | 9.30E-08 | 9.30E-08 | 1.00E+00 | 1.00E+00 | Failure to detect leak to LAT with none of sump start; door clos |
| [PE1AFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TEF1FTR; TE1A & 1B FTR; 1/2 |
| [SFPS1AFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TSF1FTR; TSF1A & 1B FTR; 1/2 |
| [SFPS1BFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TSF1FTR; TSF1A & 1B FTR; 1/2 |
| [PE1BFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TEF1FTR; TE1A & 1B FTR; 1/2 |
| [SFPS2AFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TSF2FTR; TSF2A & 2B FTR; 1/2 |
| [SFPS2BFTR] | 2.57E-04 | Equipment Failure | 6.58E-07 | 7.61E-08 | 2.96E-04 | 1.00E+00 | 1.00E+00 | CCF:TSF2FTR; TSF2A & 2B FTR; 1/2 |
| [MSUMP1FTR MSUMP2FTR] | 1.97E-04 | Equipment Failure | 1.06E-04 | 6.48E-08 | 3.29E-04 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTR; Main Sump Pumps FTR; 2/2 |
| ERRV102SIZE | 3.00E-02 | Equipment Failure | 6.35E-08 | 6.35E-08 | 2.12E-06 | 1.00E+00 | 1.00E+00 | Mistaking the F24 (102C) valve size difference |
| NSTOC102 | 2.90E-03 | Equipment Failure | 6.35E-08 | 6.35E-08 | 2.19E-05 | 1.00E+00 | 1.00E+00 | Navy's Subcontractor Tags out valve 102C in error |
| RHTOC02 | 5.97E-04 | Human Failure Event | 6.25E-08 | 6.25E-08 | 2.15E-05 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 102C in error |
| OSUM_OSUM6 | 7.25E-02 | Human Failure Event | 2.01E-07 | 5.15E-08 | 7.11E-07 | 1.00E+00 | 1.00E+00 | Failure to detect leak to LAT during Fuel Movement; neither sump start nor door closes |
| ERRV115SIZE | 8.89E-02 | Equipment Failure | 2.82E-08 | 2.82E-08 | 9.40E-07 | 1.00E+00 | 1.00E+00 | Mistaking the F76 (115B) valve size difference |
| NSTOC115 | 5.97E-04 | Equipment Failure | 2.82E-08 | 2.82E-08 | 9.72E-06 | 1.00E+00 | 1.00E+00 | Navy's Subcontractor Tag out valve 115C in error |
| RHTOC115 | 5.97E-04 | Human Failure Event | 2.67E-08 | 2.67E-08 | 9.20E-06 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 115C in error |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| RHTOC108 | 5.97E-04 | Human Failure Event | 1.90E-08 | 1.90E-08 | 6.53E-06 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 108C in error |
| [P0201FTS P0202FTS P0203FTS P0204FTS P0205FTS] | 1.01E-06 | Equipment Failure | 2.26E-07 | 1.65E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 5/5 |
| [USUMP1FTR] | 3.05E-03 | Equipment Failure | 5.49E-07 | 1.25E-08 | 4.10E-06 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTR; Harbor Tunnel Sump Pumps FTR; 1/2 |
| [USUMP2FTR] | 3.05E-03 | Equipment Failure | 5.49E-07 | 1.25E-08 | 4.10E-06 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTR; Harbor Tunnel Sump Pumps FTR; 1/2 |
| [USUMP1FTS USUMP2FTS] | 9.35E-06 | Equipment Failure | 5.07E-07 | 1.15E-08 | 1.23E-03 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTS; Harbor Tunnel Sump Pumps FTS; 2/2 |
| [P0201FTS P0203FTS P0204FTS P0205FTS] | 6.82E-07 | Equipment Failure | 1.53E-07 | 1.12E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 4/5 |
| [P0202FTS P0203FTS P0204FTS P0205FTS] | 6.82E-07 | Equipment Failure | 1.53E-07 | 1.12E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 4/5 |
| [P0201FTS P0202FTS P0203FTS P0204FTS] | 6.82E-07 | Equipment Failure | 1.53E-07 | 1.12E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 4/5 |
| [P0201FTS P0202FTS P0203FTS P0205FTS] | 6.82E-07 | Equipment Failure | 1.53E-07 | 1.12E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 4/5 |
| [P0201FTS P0202FTS P0204FTS P0205FTS] | 6.82E-07 | Equipment Failure | 1.53E-07 | 1.12E-08 | 1.64E-02 | 1.02E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 4/5 |
| [MSUMP1FTR] | 3.05E-03 | Equipment Failure | 5.44E-06 | 3.33E-09 | 1.09E-06 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTR; Main Sump Pumps FTR; 1/2 |
| [MSUMP2FTR] | 3.05E-03 | Equipment Failure | 5.44E-06 | 3.33E-09 | 1.09E-06 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTR; Main Sump Pumps FTR; 1/2 |
| [MSUMP1FTS MSUMP2FTS] | 9.35E-06 | Equipment Failure | 5.03E-06 | 3.08E-09 | 3.29E-04 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTS; Main Sump Pumps FTS; 2/2 |
| [P0201FTR] | 2.98E-03 | Equipment Failure | 4.21E-08 | 3.08E-09 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 1/5 |
| [P0202FTR] | 2.98E-03 | Equipment Failure | 4.21E-08 | 3.08E-09 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 1/5 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [P0203FTR] | 2.98E-03 | Equipment Failure | 4.21E-08 | 3.08E-09 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 1/5 |
| [P0204FTR] | 2.98E-03 | Equipment Failure | 4.21E-08 | 3.08E-09 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 1/5 |
| [P0205FTR] | 2.98E-03 | Equipment Failure | 4.21E-08 | 3.08E-09 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR; F76 Pumps FTR; 1/5 |
| OPCOM | 3.00E-02 | Human Failure Event | 2.56E-09 | 2.56E-09 | 8.54E-08 | 1.00E+00 | 1.00E+00 | Operator does not detect the error via communications with the |
| [P0201FTR P0202FTR P0203FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0201FTR P0202FTR P0204FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0201FTR P0202FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0201FTR P0203FTR P0204FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0201FTR P0203FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0201FTR P0204FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0202FTR P0203FTR P0204FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0202FTR P0203FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 3/5 |
| [P0202FTR P0204FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF Group F76MDPS 3 Cargo Pumps (202, 204, and 205) Fail to run |
| [P0203FTR P0204FTR P0205FTR] | 1.48E-05 | Equipment Failure | 2.26E-08 | 1.65E-09 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF Group F76MDPS 3 Cargo Pumps (203, 204, and 205) Fail to run |
| RHTOC15 | 5.97E-04 | Human Failure Event | 1.51E-09 | 1.51E-09 | 5.21E-07 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 115C in error |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [USUMP1FTS] | 2.61E-04 | Equipment Failure | 4.68E-08 | 1.07E-09 | 4.08E-06 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTS, Harbor Tunnel Sump Pumps FTS, 1/2 |
| [USUMP2FTS] | 2.61E-04 | Equipment Failure | 4.68E-08 | 1.07E-09 | 4.08E-06 | 1.00E+00 | 1.00E+00 | CCF:USUMPFTS, Harbor Tunnel Sump Pumps FTS, 1/2 |
| RHTOC102 | 2.90E-03 | Human Failure Event | 1.05E-09 | 1.05E-09 | 3.63E-07 | 1.00E+00 | 1.00E+00 | RH Staff Tag Out Valve 102C in error |
| [MSUMP1FTS] | 2.61E-04 | Equipment Failure | 4.65E-07 | 2.84E-10 | 1.09E-06 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTS; Main Sump Pumps FTS; 1/2 |
| [MSUMP2FTS] | 2.61E-04 | Equipment Failure | 4.65E-07 | 2.84E-10 | 1.09E-06 | 1.00E+00 | 1.00E+00 | CCF:MSUMPFTS; Main Sump Pumps FTS; 1/2 |
| [P0201FTS] | 2.58E-04 | Equipment Failure | 3.65E-09 | 2.66E-10 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 1/5 |
| [P0202FTS] | 2.58E-04 | Equipment Failure | 3.65E-09 | 2.66E-10 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 1/5 |
| [P0203FTS] | 2.58E-04 | Equipment Failure | 3.65E-09 | 2.66E-10 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 1/5 |
| [P0204FTS] | 2.58E-04 | Equipment Failure | 3.65E-09 | 2.66E-10 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0205FTS] | 2.58E-04 | Equipment Failure | 3.65E-09 | 2.66E-10 | 1.03E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0201FTR P0202FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0201FTR P0203FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0201FTR P0204FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0201FTR P0205FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0202FTR P0203FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0202FTR P0204FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0202FTR P0205FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0203FTR P0204FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0203FTR P0205FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |
| [P0204FTR P0205FTR] | 2.62E-05 | Equipment Failure | 1.31E-09 | 9.56E-11 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPR, F76 Pumps FTR, 2/5 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [P0201FTS P0202FTS P0203FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0201FTS P0202FTS P0204FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0201FTS P0202FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0201FTS P0203FTS P0204FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0201FTS P0203FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0201FTS P0204FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0202FTS P0203FTS P0204FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0202FTS P0203FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0202FTS P0204FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| [P0203FTS P0204FTS P0205FTS] | 6.71E-07 | Equipment Failure | 1.02E-09 | 7.47E-11 | 1.11E-04 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 3/5 |
| MSUMP1SPLUG | 1.12E-09 | Equipment Failure | 1.46E-08 | 3.85E-11 | 5.17E-06 | 1.00E+00 | 1.00E+00 | Main Sump Pump 1 Strainer Plug |
| MSUMP2SPLUG | 1.12E-09 | Equipment Failure | 1.46E-08 | 3.85E-11 | 5.17E-06 | 1.00E+00 | 1.00E+00 | Main Sump Pump 2 Strainer Plug |
| MSUMP1FLOAT | 3.88E-06 | Equipment Failure | 3.45E-09 | 9.11E-12 | 5.17E-06 | 1.00E+00 | 1.00E+00 | Float Actuation for Main Sump Pump 1 Fails To Operate |
| MSUMP2FLOAT | 3.88E-06 | Equipment Failure | 3.45E-09 | 9.11E-12 | 5.17E-06 | 1.00E+00 | 1.00E+00 | Float Actuation for Main Sump Pump 2 Fails To Operate |
| [P0201FTS P0202FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| [P0201FTS P0203FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0201FTS P0204FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0201FTS P0205FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0202FTS P0203FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0202FTS P0204FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0202FTS P0205FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0203FTS P0204FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS, F76 Pumps FTS, 2/5 |
| [P0203FTS P0205FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 2/5 |
| [P0204FTS P0205FTS] | 1.02E-06 | Equipment Failure | 5.08E-11 | 3.71E-12 | 3.64E-06 | 1.00E+00 | 1.00E+00 | CCF:F76MDPS; F76 Pumps FTS; 2/5 |
| M0206A | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206A fails to operate |
| M0206B | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206B fails to operate |
| M0206C | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206C fails to operate |
| M0206E | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206E fails to operate |
| M0206F | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206F fails to operate |
| M0206G | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0206G fails to operate |
| M0207A | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207A fails to operate |
| M0207B | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207B fails to operate |
| M0207C | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207C fails to operate |
| M0207E | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207E fails to operate |
| M0207F | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207F fails to operate |
| M0207G | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0207G fails to operate |
| M0208A | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208A fails to operate |
| M0208B | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208B fails to operate |
| M0208C | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208C fails to operate |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| M0208E | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208E fails to operate |
| M0208F | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208F fails to operate |
| M0208G | 3.28E-04 | Equipment Failure | 6.43E-12 | 1.99E-12 | 1.85E-09 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0208G fails to operate |
| M0209A | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209A fails to operate |
| M0209B | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209B fails to operate |
| M0209C | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209C fails to operate |
| M0209E | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209E fails to operate |
| M0209F | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209Ffails to operate |
| M0209G | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0209G fails to operate |
| M0210A | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210A fails to operate |
| M0210B | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210B fails to operate |
| M0210C | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210C fails to operate |
| M0210E | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210E fails to operate |
| M0210F | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210F fails to operate |
| M0210G | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0210G fails to operate |
| M0211G | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211 Fails to operate |
| M0211A | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211A fails to operate |
| M0211B | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211B fails to operate |
| M0211C | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211C fails to operate |
| M0211E | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211E fails to operate |
| M0211F | 3.28E-04 | Equipment Failure | 2.86E-12 | 8.70E-13 | 8.08E-10 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0211E fails to operate |
| OSUM_OSUM4 | 7.25E-02 | Human Failure Event | 1.45E-15 | 1.44E-15 | 1.44E-15 | 1.00E+00 | 1.00E+00 | Failure to Detect leak to LAT given neither sump start nor door closes |
| M0201A | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201A fails to operate |
| M0201B | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201B fails to operate |
| M0201C | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201C fails to operate |
| M0201E | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201E fails to operate |
| M0201F | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201F fails to operate |
| M0201G | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0201G fails to operate |
| M0202A | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202A fails to operate |

**Table 12-7. Basic Event Importance to Expected Risk Sorted by Fussell-Vesely Importance for Human Failure Events and Equipment Failures (Continued)**

| Basic Event Name | Basic Event Value | Basic Event Type | Fractional Importance (FI) | Fussell-Vesely Importance (FVI) | Birnbaum Importance (BI) | Risk Achievement Worth (RAW) | Risk Reduction Worth (RRW) | Basic Event Description |
|---|---|---|---|---|---|---|---|---|
| M0202B | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202Bfails to operate |
| M0202C | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202C fails to operate |
| M0202E | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202E fails to operate |
| M0202F | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202F fails to operate |
| M0202G | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0202G fails to operate |
| M0203A | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203A fails to operate |
| M0203B | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203B fails to operate |
| M0203C | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203Cfails to operate |
| M0203E | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203E fails to operate |
| M0203F | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203F fails to operate |
| M0203G | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0203G fails to operate |
| M0204A | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204A fails to operate |
| M0204B | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204B fails to operate |
| M0204C | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204C fails to operate |
| M0204E | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204E fails to operate |
| M0204F | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204F fails to operate |
| M0204G | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0204G fails to operate |
| M0205A | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205A fails to operate |
| M0205B | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205B fails to operate |
| M0205C | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205C fails to operate |
| M0205E | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205E fails to operate |
| M0205F | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205F fails to operate |
| M0205G | 3.28E-04 | Equipment Failure | 1.76E-14 | 1.33E-15 | 1.20E-12 | 1.00E+00 | 1.00E+00 | Motor Operated Valve M0205G fails to operate |
| OSUM_OSUM2 | 6.71E-02 | Human Failure Event | 1.34E-15 | 1.33E-15 | 1.33E-15 | 1.00E+00 | 1.00E+00 | Failure to identify and locate nozzle leak neither sump start nor door closes |

# 13. Facility Risk Vulnerability Assessment

The total aggregate risk results discussed in Section 12 are interesting from the perspective of comparison with other general sources of risk, but they are of limited value in supporting an understanding of the risk characteristics in enough detail to support meaningful decision-making regarding risk mitigation and risk management for the RHBFSF. To adequately support meaningful decision-making, it is necessary to perform a vulnerability assessment based on the QRVA quantified risk. By applying a detailed event sequence analysis to implement the QRVA, analysts have an ideal tool to decompose or deconstruct the risk into its elemental or component parts to aid in the identification and characterization of facility vulnerabilities to risk.

## 13.1 Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences)

Because we have developed the QRVA applying an event sequence analysis approach, we can decompose the total aggregate risk into its logical contributors in several different ways, which are valuable in characterizing and understanding the facility risk. There are several ways that the facility total aggregate risk can be decomposed to provide valuable risk insights. The most common ways of decomposing the risk for presentation to decision-makers are the following:

- By Hazard Source or Initiating Event Category
- By Individual Initiating Event
- By Event Sequence Category
- By Individual Event Sequence
- By Consequence Bin Category

These decompose risk results can be presented in prioritized lists of rank order based on contribution to total aggregate risk. These results can be presented in tabular, pie chart, or bar chart formats for facilitation of risk communication. Similarly, the individual elements of event sequences (initiating events, event tree top events, event tree conditional split fractions, human errors [the HFEs previously discussed], fault tree basic events [component failure modes], etc.) can be analyzed to develop a variety of risk importance measures, which can be evaluated via rank order lists to identify and characterize specific facility risk vulnerabilities. Risk importance measures are discussed in Section 13.2.

## 13.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events

Calculation of the risk importance measures or “risk worths” as a standard part of a QRVA is straightforward. Most of the information needed to calculate the risk worths is available from a QRVA. The success requirements, the system and component unavailabilities, the assumed human actions, the system dependencies, and the containment response for each sequence are quantified when performing the QRVA.

The sequences are also classified into release categories according to containment response and mitigative system success. Much of the information presented in this section is an adaptation of NUREG/CR-3385.

### 13.2.1 Fractional Importance

For individual event sequences or for logical groups of event sequences, such as all those sequences associated with a specific initiating event or initiating event category, the fractional importance can be derived by simply taking the ratio of the risk associated with that individual sequence or group of sequences divided by the total aggregate risk. Often, in a risk model encompassing thousands of event sequences, a relative few sequences dominate the total risk. For example, in a model encompassing 50,000 sequences, we may find that 30 or 40 individual sequences account for over 90 percent of the total risk. In attempting to identify facility-specific vulnerabilities to risk, it is frequently instructive to focus more attention on these 30 to 40 risk-dominating sequences. Similarly, if we find that sequences associated with only one or two initiating event categories dominate the total risk, then we should focus more attention on those initiating event category sequences in our search for vulnerabilities. However, this approach does not provide a complete picture of risk for vulnerability determination. It is also important to investigate other importance measures assessed for individual elements of the event sequences; e.g., fault tree basic events (failure modes) and human errors, to determine facility-specific vulnerabilities (see discussion of additional importance measures below).

### 13.2.2 Risk Achievement Worth

To measure the worth of a feature in achieving the present risk, a logical approach is to remove the feature and then determine how much the risk has increased. Thus, the risk achievement worth is formally defined to be the increase in risk if the feature were assumed not to be there or to be failed.

Depending on how the increase in risk is measured, the risk achievement worth can either be defined as a ratio or an interval. Let

$$R_i^t = \text{the increased risk level without feature i or with feature i assumed failed,} \quad (13.1)$$

and

$$R_0 = \text{the present risk level,} \quad (13.2)$$

where the risk can be any measure such as loss of fuel inventory control frequency, acute fuel release frequency, etc. Then, on a ratio scale, the risk achievement worth $A_i$ of feature i is defined as:

$$A_i = R_i^t / R_0 \quad (13.3)$$

On an interval scale the risk achievement worth $A_i$ is defined as:

$$A_i = R_i^t - R_0 \quad (13.4)$$

In calculating $R_i^t$ with feature i removed, it is important to consider other features that are also effectively removed because of interrelationships or dependencies with feature i. Whether the ratio or interval definition is most pertinent will depend upon the particular utilization. When risk achievement worth values are calculated for a given facility in order to prioritize the features then the ratio and interval definitions will generally give the same rankings. When the features of different facilities are compared or when cost-benefit evaluations are performed, even for a single facility, then the interval definition is generally more appropriate. If different risk measures $R_0$, such as expected early fatalities, are used, then different priorities can result and therefore it generally is useful to examine various risk measures to obtain a more complete picture of a feature's risk worth. Utilization of risk achievement worth in decision making is further discussed in Section 5.0 of NUREG/CR-3385.

### 13.2.3 Risk Reduction Worth

To measure the worth of a feature in reducing the present risk, a logical approach is to "optimize" the feature and then determine how much the risk has been decreased. Thus, the risk reduction worth is formally defined to be the decrease in risk if the feature were assumed to be optimized or were assumed to be made perfectly reliable.

Again, depending on how the decrease in risk is measured, the risk reduction worth can either be defined as a ratio or an interval. Let

$R_{\bar{1}}$ = the decreased risk level with the feature optimized or assumed to be perfectly reliable, (13.5)

and again let $R_0$ be the present risk level. Then on a ratio scale, the risk reduction worth $D_i$ of feature i (the letter "D" denotes decrease) is defined as:

$$D_i = R_0 / R_{\bar{1}} \quad (13.6)$$

On an interval scale the risk reduction worth $D_i$ is:

$$D_i = R_0 - R_{\bar{1}} \quad (13.7)$$

As defined in the above manner, the risk reduction worth, $D_i$ or $D_i$, is always greater than or equal to one or is always positive, respectively.

In calculating $R_{\bar{1}}$ with feature i optimized, other interrelated features which are also effectively optimized should be included. Again, whether the ratio or interval definition is used will depend upon the specific application. For a given facility and for a given risk measure, the ratio and interval will generally give the same ranking of the features. The risk reduction worths of features will depend on the risk measure being examined. As for the risk achievement worths, when the features of different facilities are compared or when cost-benefit analyses are performed, then the interval definition is generally more appropriate. Utilizations of calculated risk reduction worths are further discussed in Section 5.0 of NUREG/CR-3385.

### 13.2.4 Fussell-Vesely Importance (risk participation index)

Another generally applied importance measure is the fractional contribution of i to the risk, or the Fussell-Vesely (Reference 13-1) measure of importance, $I_i$, which can be expressed as:

$$I_i = \frac{R_0 - R_{\bar{i}}}{R_0} \tag{13.8}$$

where the numerator represents the risk due to contributor i. Equation (13.8) can be expressed as:

$$I_i = 1 - \frac{1}{D_i} \tag{13.9}$$

or

$$I_i = \frac{D_i - 1}{D_i} \tag{13.10}$$

Thus, the importance $I_i$ is simply related to the risk reduction worth on a ratio scale, $D_i$. The risk reduction worth on a ratio scale, however, gives only partial information about the risk importance of i; the interval measure and the risk achievement worth give important additional information about the importance of 1.

### 13.2.5 Birnbaum Importance (risk derivative)

If the risk measure is defined to be the system unavailability or unreliability, then the more generally applied Birnbaum (Reference 13-2) importance $\Delta_i$ of Component i can be defined as:

$$\Delta_i = R_i^t - R_{\bar{i}} \tag{13.11}$$

where $R_i^t$ is the system availability with Component i assumed failed and $R_{\bar{i}}$ is the system unavailability with the component assumed working. Barlow and Proschan (Reference 13-3) call the $\Delta_i$ reliability importance of Component i.

By adding and subtracting the nominal unavailability $R_0$ to the right side of Equation (13.11), it can be seen that

$$\Delta_i = A_i - D_i \tag{13.12}$$

Thus, the Birnbaum importance is the sum of the risk achievement and risk reduction worth of Component i on an interval scale. The risk achievement worth and the risk reduction worth together are thus more informative than the Birnbaum importance.

## 13.3 Risk Contribution Sensitivity Analysis

Another valuable asset of the event sequence analysis approach to QRVA is that it supports sensitivity analysis of most elements of the QRVA risk results, such as:

- Individual Initiating Event Frequency
- Individual Event Sequence Frequency
- Event Tree Top Events
- Event Tree Split Fractions
- Fault Tree Basic Events (e.g., grouped or specific component failure rates, component unavailability values, human error rates or specific HFE HEP values, etc.)

In practice, we review the risk importance measure results, then based on those results, select risk model elements; e.g., specific component failure rates, for risk sensitivity analysis. The risk sensitivity analyses are performed by selecting a QRVA input element, then changing the input data for the target parameter by a specified percentage or factor, and requantifying the risk model with the revised parameter value to produce the sensitivity case value for the total aggregated risk.

## 13.4 Vulnerability Assessment Results Presentation and Interpretation

Key elements of the QRVA are presentations of the sequence group frequencies, initiating event frequencies, end state frequencies, and risk element risk importance measures and associated sensitivity case studies.

These results are presented in the QRVA report with an accompanying discussion developed by analysts experienced with the RHBFSF risk model designed to facilitate meaningful interpretation of vulnerability assessment results.

### 13.4.1 Insights from Sequence Group, Initiating Event, and End State Frequency Results

The contributors to the sequence group and initiating event frequency results presented in Section 12 reveal some insights regarding the fuel release risk vulnerabilities for RHBFSF. These are summarized below.

1. RHBFST leakage events through the liner, though historically these events have been at relatively small flow rates (i.e., 1.5 gpm or less), they contribute most of the frequency of fuel releases greater than 1,000 gallons. In the event of liner leakage, the continuous level monitoring system provides a low level warning alarm only after 2,500 gallons have already been lost. If initially undergoing a fuel movement when

the leakage begins, the RHBFST must be isolated before the change in level can again be continuously measured.

2. RHBFST leakage events through the liner during a return to service have historically occurred. See Section 5.4.3.5 where 12 small leak events out of 91 estimated RHBFST returns to service were found to occur. The early 2014, RHBFST 5 leakage event occurred during its return to service. Tests using water to check for leaks prior to filling the RHBFST with fuel are no longer permitted. However, the requirements for 100% liner inspections and improved inspection techniques prior to initiating the return to service may more than compensate for no longer performing the tests with water. Multiple pauses of 24 hours in duration each during the refilling process to monitor for changes in fuel level, are helpful to detect and alarm leaks on the order of 1.5 gpm or larger. Smaller leak rates occurring during a return to service may only be detected by careful level trending analysis.

3. For the sequences involving smaller amounts of fuel released (i.e., greater than 1,000 gallons or greater than 120,000 gallons), the RHBFSTs holding JP5 fuel contribute the most. This is because there are more RHBFSTs in operation that hold JP5 fuel than those holding either F24 or F76 fuel.

4. The RHBFSTs holding F76 fuel contribute disproportionately to the frequency of sequences with large amounts of fuel; i.e., greater than 1 million gallons. This is because there is insufficient ullage initially available at RHBFSF or the upper tank farm to fully empty a leaking RHBFST that contains F76 fuel. This would lead to a time delay in fully emptying a leaking F76 RHBFST when needed until additional ullage is located. Adding readily accessible ullage for F76 fuel when needed, would limit the delay time in emptying the affected RHBFST. While the lack of ullage for emptying a leaking F76 RHBFST is the most acute problem, the available ullage at RHBFSF for F24 and JP5 fuel may be spread out over two or more RHBFSTs, complicating the strategy for emptying. Consolidating the available ullage in one RHBFST of the same fuel type would simplify the strategy for moving fuel in an emergency.

5. The RHBFST overfill sequences contribute roughly the same frequency to smaller fuel release (i.e., less than 120,000 gallons) sequences as do leaks from a RHBFST nozzle, or from other fuel lines into the LAT or Harbor Tunnels. For the larger volume RHBFSTs, which is most of them, there is about 10’ difference in fuel level between the fuel level that RHBFSTs are tested for leak tightness annually and where the first high-high level alarm probe. Past RHBFST inspections have detected larger size holes (i.e., 1/8” to 3/4” equivalent diameters) in the RHBFST liner above the normal fuel operating levels. RHBFSTs which have not yet under gone 100% surface inspections are most at risk at having holes at these higher tank levels. There is no procedure available for the actions to take in the event that an overfilling occurs. The QRVA models a response to lower fuel level in the RHBFST once a low level alarm occurs indicating a leak may be in progress.

6. Nozzle leaks contribute the most frequency to large fuel release sequences; i.e., those releasing greater than 1 million gallons. These larger fuel releases are to the LAT and not directly through the RHBFST liner. As a result, once initiated, they are not isolable. The initiating event frequency for nozzle leaks is made of all three

lines which penetrate the RHBFST lower dome and exit the concrete into the LAT. One way to reduce the frequency of such events is to isolate the piping lines within the RHBFST for those lines which are not needed for fuel movements or other operational considerations. No nozzle leak postulated of any size has occurred in the history of RHBFSF. The standard operating procedure in response to a RHBFST low fuel level alarm, is to perform a top gauge of the affected RHBFST to confirm the RHBFST is leaking. This may be difficult since, even for relatively small fuel leaks, evacuation of the LAT and Upper Access Tunnels is required.

7. The initiating event with the largest frequency contribution to sequences releasing more than 120,000 gallons of fuel is that of a small leak (i.e., 0.5" hole equivalent in the 32"-diameter pipe) from the F76 fuel line into the Harbor Tunnel. This section of the F76 fuel line is very long and it is entirely located below the new oil door. There are no abnormal operating procedures for the operators to follow should such an event occur. There is general operator training to push the "panic" button if a leak to either the LAT or Harbor Tunnels occurs and in other cases. This operator action would isolate any initially aligned RHBFST undergoing a fuel movement and, at the same time, would trip any operating cargo pumps. However, this action does not isolate the leaking fuel line from fuel flowing by gravity from upgrade to the leak location. An action is nevertheless credited in the QRVA risk model to close the fuel line upgrade sectional valve as applicable. Depending on the size of the fuel line leak postulated, it may also be effective for the operators to gravity drain the leaking fuel line (e.g., to the upper tank farm) so as to minimize the amount of fuel available to leak out the postulated hole.

### 13.4.2 Insights from Importance Measures

Importance measures provide a summary of the impact of different QRVA model elements to selected risk metrics. Importance measures indicate the effect of changing one model element at a time. The importance measures roll up the results across all acute sequences. For this assessment, the sequence group representing fuel releases greater than 120,000 gallons (DGT120) is used as the risk metric. The following Excel workbook file contains the importance measures for two sets of model elements; basic events and split fractions: Master Frequency File and Importance Measures.xlsx.

The basic event importance measures are presented in tab, BEIMP-ALL, of that workbook. Basic event importance values are presented for the following importance measures: fractional importance, Fussell-Vesely importance, Birnbaum importance, risk achievement worth (RAW), and risk reduction worth. The basic event importance table is sorted in decreasing order of Fussell-Vesely importance.

The column labeled "BE TYPE" assigns each basic event to one of three types of events; i.e., FLAG, HFE, or EF. These are defined below:

FLAG – This type of basic event describes the configuration of the facility at the time of the initiating event, and is typically a stochastic event, but does not represent an operator or equipment failure mode.

HFE – This type of basic event stands for human failure event. Operator actions that are included in the QRVA logic models are represented as failure events, generally as failure s to perform the desired action.

EF – This type of basic event represents equipment failures.

Most of the highest ranked basic events by Fussell-Vesely importance are FLAG events. These basic events describe the status of the facility (e.g., which fuel type is associated with the initiating event, and whether a fuel movement of different types is in progress). Basic events representing the fraction of time the postulated leak is at a given level in the RHBFST are also assigned to the BE TYPE FLAG. Often the various alternatives to these FLAG events sum to a total probability of 1.0 and are evaluated on multi-state top events in the same model. It is for this reason that this type of basic event often has high Fussell-Vesely importance.

Other than FLAG events, the highest ranked basic events sorted by Fussell-Vesely importance involve human failure events (HFE type). The actions are modeled in the four frontline event trees; see Sections 6.7.5 through 6.7.8. Typically human failure events are assigned relatively high failure probabilities as compared to equipment failure probabilities. The operator actions to close sectional valves under different conditions (e.g., OSEC_OSEC6 and OSEC_OSEC3) and to push the panic button (OPAN_OPAN2) have the highest rankings to the sequence group DGT120. Other HFE basic events also show up high in the ranked list of basic events.

The three highest ranked actions listed above are important because they are directed at the first response to the initiating event; i.e., that of partial leak isolation. Failure to close the sectional valve upgrade of a fuel line leak would allow more fuel to be released. In this case, the HFE is not lowering the initiating event frequency of the sequence, but rather is changing the fuel released from one that would have released less than 120,000 gallons had the action been successful, to one that releases more than 120,000 gallons when it fails. Similarly the action to push the panic button and have the equipment respond as intended could limit the release of fuel to less than 120,000 gallons in fuel line leak sequences in which the associated RHBFST is initially aligned for a fuel movement; i.e., the pipeline fuel inventory above the leak location may be less than 120,000 gallons, but if initially aligned to a RHBFST, more fuel than that could still be released.

Changes to the facility that would have the effect of lowering these HFE failure probabilities could lower the frequency of sequences releasing greater than 120,000 gallons by as much as the amount indicated by the Fussell-Vesely importance measures, expressed as a fraction of the total sequence group frequency. Often relatively low cost changes may be used to achieve a large part of the possible reduction in risk; e.g., develop procedures for the class of sequences contributing, and/or provide

better cues to the operators in the form of enhanced alarms or other indications to improve the probabilities of successful response, or of success sooner in time than what now may be predicted. The QRVA models the first detection of leaks to the LAT or Harbor Tunnel by indications of sump pumps starting or of the new oil door closing. For smaller leak flow rates, there could be substantial time between the leak initiation and such indications being received in the control room. Fuel vapor monitoring within these tunnels, especially if alarmed in the control room, may shorten the times to detection.

The EF type basic events ranked highest by Fussell-Vesely importance to Sequence Group DGT120 are assessed as MDCFTS and FANFT. These events are used to model heat removal from the AFHE system. If heat removal is lost, eventual overheating and failure of the AFHE system is assumed. The model tracks failure of AFHE as the cause of a time delay for successfully initiating the activities to empty a leaking RHBFST. Hence, failure of Top Event AFHR results in a sequence with greater release, in some sequences, changing the release from less than 120,000 to a release greater than 120,000 gallons.

The next ranked Type EF basic event is SVFTC, which represents the failure of a sectional valve to close. Its failure influences the affected sequences in the same way as failure of HFE Type Event OSEC_OSEC3, but at a lower failure probability.

The Fussell-Vesely importance of these three EF type events are very low; i.e., less than 5E-3. For the RAW importance measure, a value of 2 or greater is usually selected as defining a basic event that is risk significant. Only two basic events have RAW values for Sequence Group DGT120 greater than 2; i.e., TFMTOP and BUSTOP. These events represent the failure of the transformer or bus to supply emergency power at the Red Hill 480V bus via Top Event BRE48. Since the usual criterion for risk significance as measured by RAW is barely exceeded, this indicates that equipment failures are not that risk significant to Sequence Group DGT120.

A second table of importance measures is provided in Tab SFIMP-ALL of the Excel workbook file Master Frequency File and Importance Measures.xlsx. Recall that split fractions represent the total branch probability for a specific top event subject to a specific boundary condition imposed by the sequence of events up to that node in the event tree structure. It represents a higher level of model element than does a basic event. When sorted by Fussell-Vesely importance, the highest ranked split fractions also involve FLAG type split fractions; e.g., for the status of the RHBFSF, such as whether all RHBFSTs are idle, or what level in a RHBFST does the hole postulated by an initiating event occur. The split fractions in which the HFE type basic events are used also appear in the split fraction importance ranking; i.e., Split Fractions OPAN2 and OSEC3. Similarly, the split fraction representing the condensation unit which provides heat removal for AFHE also shows in the higher rankings; i.e., Split Fraction AFHR1. It is concluded that reviews of the split fraction importance for HFE and EF type split fractions show no additional insights from those already determined by reviewing the basic event importance tab.

### 13.4.3 Insights from Release Category Importance Measures

Fuel release categories are described in Section 10. The release categories provide an indication of where the released fuel accumulates, or ends up, after its accidental

release from a RHBFST or fuel line in the LAT. One of these release categories is assigned to each acute sequence by the assignment of a split fraction, each with a value of 1.0, to Top Event REL of the linked sequence model. Split fraction importance reports are generated for each selected range of fuel release in gallons to determine the frequency of each Release Category to each range. These frequencies are reported in Table 13-1. The total frequency and a description for each release category are also reported in Table 13-1. The cells of the table with darkened borders identify the highest frequency release category contribution for each fuel release interval; i.e., one release category for each fuel release interval. Similarly, the shaded cells in the table identify the range of fuel release which has the highest frequency of occurrence for each release category; i.e., one cell per release category. Release Category RELE contributes the most frequency in each of five fuel release intervals. Release Category RELA is the highest frequency contributor to three other fuel release intervals. In selecting the range of fuel release to use for an evaluation of transport of released fuel to the aquifer, it is the release interval corresponding to the shaded cells that should be used.

For each of the fuel release intervals of greater than 250,000 gallons, the highest frequency release category is described by RELE. For each of the fuel release intervals of less than 120,000 gallons, the highest frequency release category is RELA. The remaining fuel release interval (i.e., between 120,000 and 250,000 gallons) has its highest frequency contribution from Release Category RELI, and RELA is its second highest. Release Category RELI is unique in that its initial point of release is below the new old door into the Harbor Tunnel. An assessment of whether this type of release scenario can impact the aquifer as the fuel flows downgrade through the Harbor Tunnel to ADIT 2 and the UGPH, is of interest.

The frequencies in Table 13-1 can be summed across the columns for fuel release intervals greater than 120,000 gallons to obtain the exceedance frequency for fuel release sequences greater than 120,000 gallons; i.e., 4.25E-3 per year. The fuel releases are judged to be more likely to transport to the water table if they accumulate at locations above the water table. Fuel releases from sequences where the fuel flows unimpeded down the Harbor Tunnel to lower elevations at the UGPH, are judged less likely to result in the released fuel reaching the water table. A bounding, sensitivity assessment is performed to see the frequency of exceeding 120,000 gallons released if such sequences are excluded from the total. In this sensitivity, all frequencies for sequences with greater than 120,000 gallons of fuel released were excluded for Release Categories RELG, RELH, RELI, RELJ, RELK, RELL, RELM, and RELN. These excluded sequences include those for which the release point is below the new oil door, or above the new oil door but it also fails to close. This leaves the contributions from Release Categories RELA, RELB, RELC, RELD, RELE, and RELF in the summation. The frequency of sequences with fuel releases greater than 120,000 gallons and with more significant potential to reach the water table is then 3.40E-3 per year; i.e., about a 20% reduction in the frequency total for all sequences which release greater than 120,000 gallons. Nearly all of the reduction comes from omitting sequences assigned to Release Category RELI; i.e., sequences with limited fuel release directly to the Harbor Tunnel.

## Table 13-1. Fuel Release Category Frequencies (events per year) for Selected Fuel Release Ranges in Gallons (1), (2)

| | | Sequence Group ID and Fuel Release Interval Range in Gallons | | | | | | | | | Release Category Description |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | JLT30 | KLT60 | LLT120 | MLT250 | NLT500 | OLT1M | PLT2M | QLT10M | IGT10M | |
| Release Category ID | Total Release Category Frequency | 1k–30k | 30k–60k | 60k–120k | 120k–250k | 250k–500k | 500k–1M | 1M–2M | 2M–10M | >10M | |
| RELA | 3.37E-01 | 3.23E-01 | 1.26E-02 | 1.21E-03 | 3.77E-04 | 1.88E-04 | 5.41E-06 | 3.89E-05 | 0.00E+00 | 0.00E+00 | Release to Rock from a RHBFST Liner. |
| RELC | 3.80E-05 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.48E-05 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 2.32E-05 | Large accumulation in Zone 7 with RHBFSTs not Idle or nozzle leak; Release through ADIT 6; New Oil Door Closes. |
| RELD | 5.40E-04 | 0.00E+00 | 2.05E-04 | 3.45E-06 | 1.15E-06 | 3.20E-04 | 5.37E-06 | 4.60E-06 | 0.00E+00 | 3.63E-08 | Accumulation in Zone 7; RHBFST Not Idle or nozzle leak; & New Oil Door Closes. No release through ADIT 6. |
| RELE | 2.42E-03 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.46E-04 | 1.75E-03 | 2.93E-05 | 3.33E-04 | 3.21E-05 | 1.28E-04 | Accumulation in Tank Gallery Sections D or E with RHBFST Not Idle or a nozzle leak; LAT fills; New Oil Door Closes. |
| RELF | 6.08E-04 | 5.70E-04 | 3.56E-05 | 4.30E-07 | 1.42E-06 | 1.28E-07 | 0.00E+00 | 0.00E+00 | 1.15E-07 | 1.02E-07 | Limited release to Tank Gallery Sections D or E with RHBFST Idle or successfully isolated from leak; New Oil Door Closes. |
| RELG | 5.02E-04 | 2.41E-04 | 2.10E-04 | 4.91E-05 | 4.79E-07 | 1.80E-08 | 1.15E-06 | 0.00E+00 | 2.06E-08 | 1.57E-08 | Limited release from Section C fuel line below New Oil door; RHBFSTs Idle; Collects at ADIT 2 and UGPH Entry. |
| RELH | 1.14E-06 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.67E-07 | 3.81E-07 | 7.97E-09 | 4.57E-07 | 1.26E-07 | Large accumulation from Section C below New Oil door with RHBFSTs Not Idle; Collects at UGPH until entry doors fail; large release via ADIT 1. |
| RELI | 2.09E-03 | 2.63E-04 | 0.00E+00 | 9.93E-04 | 6.44E-04 | 1.69E-04 | 2.52E-05 | 5.57E-09 | 9.79E-08 | 7.37E-08 | Limited release from fuel line Sections A or B leak below New Oil Door; RHBFSTs Idle; Collects at UGPH entry and ADIT 2 with no door overpressure failures. |
| RELJ | 5.27E-06 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 2.42E-06 | 9.41E-08 | 2.11E-06 | 6.50E-07 | Large release from Section A or B fuel lines below New Oil Door; RHBFSTs Not Idle; Accumulation at UGPH fails doors; large release through ADIT 1. |
| RELK | 3.66E-08 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.42E-08 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 2.24E-08 | Accumulation in Zone 7 with RHBFSTs Not Idle or nozzle leak; Large release through ADIT 6; New Oil Door Fails to Close; Eventual overpressure of UGPH doors. |
| RELL | 5.20E-07 | 0.00E+00 | 1.98E-07 | 3.32E-09 | 1.10E-09 | 3.09E-07 | 5.17E-09 | 4.43E-09 | 0.00E+00 | 3.47E-11 | Accumulation in Zone 7; RHBFST Not Idle nor nozzle leak; No release through ADIT 6. New Oil Door Fails to Close; Eventual overpressure of UGPH doors. |
| RELM | 2.33E-06 | 0.00E+00 | 0.00E+00 | 0.00E+00 | 1.41E-07 | 1.69E-06 | 2.82E-08 | 3.21E-07 | 3.09E-08 | 1.23E-07 | Large release to Tank Gallery Sections D or E with RHBFST Not Idle or nozzle leak; New Oil Door Fails to Close; Eventual overpressure of UGPH doors. |
| RELN | 5.85E-07 | 5.49E-07 | 3.43E-08 | 4.13E-10 | 1.37E-09 | 1.20E-10 | 0.00E+00 | 0.00E+00 | 1.09E-10 | 9.54E-11 | Release from Fuel Line only to Tank Gallery Sections D or E with RHBFST Idle; New Oil Door Fails to Close; Collects at UGPH entry doors which remain intact. |

*(1) The shaded cells indicate the highest frequency fuel release intervals for each release category.*

*(2) Darkened cell borders identify the highest frequency release category for each fuel release interval.*

## 13.5 Section 13 References

13-1 Lambert, H. E., "Measures of Importance of Events," in Reliability and Fault Tree Analyses, ed. R. E. Barlow, J. B. Fussell, and N. D. Singpurwalla, SIAM Press, Philadelphia, Pennsylvania, pp. 77–100 (1975).

13-2 Birnbaum, Z. W., "On the Importance of Different Components in a Multi-System in Multivariate Analysis," Academic Press, New York, 1969.

13-3 Barlow, R. E., and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York, 1975.

# 14. Phase 1 QRVA Conclusions

The first phase of this baseline QRVA, which is the topic of this report, has been designed to focus on internal events (not including the risk from internal fires or internal floods). This includes, but is not limited to equipment or structural failures in both frontline and support systems, human errors, etc., at the RHBFSF. This Phase 1 QRVA provides a rigorous, comprehensive, technically-sound risk assessment suitable to support prudent decision-making for effective and efficient RHBFSF risk management now and into the future.

In the baseline QRVA model developed for this Phase 1 project, 3,691,380 event sequences (or scenarios) were quantified. Of these, the top 32,889 event sequences were found to comprise 99% of the total calculated risk for the RHBFSF.

Based on Reference 14-1, the current risk thresholds of concern for the safety of the water table potentially affected by RHBFSF fuel release to the environment are:

- Acute (sudden, scenario-specific, one-time) fuel release incidents of 120,000 gallons or greater.

- Chronic (generally undetected, potentially continuous) releases of 2,300 gallons or greater per tank per year. For 18 active tanks at the facility (the configuration of the facility at the time of this assessment) this equates to 41,400 gallons or greater per year for the entire facility.

Given these risk thresholds of interest, the Phase 1 QRVA shows that the best point estimate cumulative frequency of event sequences leading to 120,000 gallons or greater of fuel release to the environment (outside the control and physical boundaries of the RHBFSF) that could potentially impact water table safety is 0.00417 events per year (or about one event every 240 years). This yields an annual probability of occurrence of 0.00416 and a probability of occurrence over 100 years of 0.341 (or about a 34% chance of occurrence sometime during the next 100 years). Another way to think of this risk is that there is about a 66% likelihood that such an event will not occur over the next 100 years of facility operation. For chronic releases, the Phase 1 QRVA shows that the expected fuel release is 5,803 gallons per year for the entire facility (please see Section 5.4.6 of this report for details), well below the threshold of concern. These results are based on the as-built, as-operated, and as-maintained RHBFSF at the design freeze date for this risk assessment, July 27, 2017. The full spectrum of results for this Phase 1 QRVA is presented in detail in Section 12 of this report. The uncertainty analysis performed for this QRVA is presented in Section 11 of this report.

The important quantitative results of this Phase 1 QRVA are summarized, then, as follows:

- **For acute risk, 0.00417 events per year**, or about **one event every 240 years**, for event sequences leading to 120,000 gallons or greater of fuel release potentially threatening water table safety.

- **For chronic risk, 5,803 gallons per year** expected fuel release for the entire facility, well below the risk threshold of interest.

It is important to note that these results are for events and conditions leading only to fuel release from the facility but not necessarily directly into the water table. The propagation of potential fuel releases from the facility to the water table is not within the scope of this risk assessment but is a focus of the activity associated with AOC Sections 6 and 7.

While the quantitative results of the QRVA are important to help facilitate prudent decision-making for the facility, the risk insights gained as a result of performing the QRVA may be even more valuable to RHBFSF decision-makers. While the charter of this risk assessment does not include development of detailed recommendations for specific risk management actions or alternatives for the RHBFSF, some of the general high-level risk insights resulting from the Phase 1 QRVA are summarized as follows:

1. The availability of tank ullage to accommodate emergency movement of fuel from a leaking tank to a safe storage tank or other safe container is important to risk.

2. The availability and quality of potential fuel release emergency response procedures and associated operator training are important to risk.

3. The capability and reliability of tank fuel inventory (fuel level) instrumentation and control systems are important to risk.

4. In response to potential fuel release scenarios, operator actions are generally more important than equipment failures to overall risk. Specific examples are identified in Sections 8 and 13 of this report.

5. Following tank inspections and maintenance, quality control during the tank return−to−service process is important to risk.

6. Strategies for responding to fuel releases inside the RHBFSF Lower Access Tunnel (e.g., strategies for removing and controlling fuel released into the Lower Access Tunnel) are important to risk.

7. Potential fuel releases from the tank nozzles (the main fuel flow piping leading into and out of the main storage tanks up to the upstream flange connections for the tank skin valves) are important to risk.

8. The capability and reliability of fuel piping isolation in response to fuel release incidents in the RHBFSF Lower Access Tunnel are important to risk.

9. Safety management and control of specific maintenance actions at the facility (e.g., tank nozzle and skin valve maintenance) is important to risk.

10. The design and proximity of the RHBFSF Lower Access Tunnel and the Red Hill Water Pump Area is important to risk. This is because potential fuel releases into the RHBFSF Lower Access Tunnel could potentially propagate to this area and flow (in a near-direct path) to the water table.

These insights are roughly ordered by predicted importance to potential risk mitigation based on a review of the vulnerability assessment reported in this Phase 1 QRVA (please see Section 13 of this report). Alternative-specific risk case studies are required to provide an accurate prioritization of these risk insights and to appropriately account for risk-benefit-to-cost considerations. Risk alternative-specific case studies are not within the scope of this Phase 1 baseline risk assessment project; however, this baseline risk assessment is the first fundamental building block of the tool enabling risk case studies to be performed to support prudent decision-making for the RHBFSF regarding risk and safety. While many of these insights may be apparent without a QRVA, the QRVA provides a critically valuable tool to help focus and prioritize these insights for effective and efficient decision support regarding facility risk management actions; e.g., improvements to facility design, operation, maintenance, inspection, and testing over the remaining life of the facility.

**Section 14 Reference**

14-1 E-mail message from Steven L. Chow, NAVFAC Hawaii, to James K. Liming, ABSG Consulting Inc., dated July 27, 2018, 11:27 AM Pacific Time.

# 15. Considerations for Future Facility Risk Case Studies

Although it is important to remember that the scope of the Phase 1 QRVA includes only internal events (without fire or flooding), the QRVA can be applied to investigate and evaluate the potential cost-benefit-risk impacts associated with proposed modifications or improvement options at the facility. These improvement options could include modification of any individual or logical set of multiple aspects of the facility, including, but not limited to changes in facility design, operation, maintenance, inspection, or testing. These modifications could include new or refined operator or maintenance technician procedures and training as well as modifications to facility hardware; e.g., structures, systems, and/or components. This is generally accomplished via development and evaluation of risk management action, risk improvement option, or more aptly named risk reduction option, case studies.

In general, the QRVA can be applied to predict the potential benefit (risk reduction) associated with a proposed improvement option and linking that to the implementation cost associated with the improvement option. In that way, proposed improvement options can be prioritized based on the quantitative value of the ratio of risk reduction per dollar invested. For example, the QRVA could be applied to evaluate potential risk reduction associated with AOC Section 3 tank upgrade alternatives and, using the case study results and the ratio of risk reduction to alternative cost, prioritize the tank upgrade alternatives by predicted risk reduction per dollar invested, by alternative case. While no such case studies are included in the QRVA Phase 1 baseline risk assessment, the application of a mature QRVA could be applied to support case study evaluation of risk reduction alternatives in the future.

In cases where the baseline risk is determined to be unacceptably high, the QRVA vulnerability assessment can be applied to support development, evaluation, and prioritization of risk-reducing improvements to the facility.

In the vulnerability assessment presented in Section 13, the consolidated baseline risk is decomposed into elements contributing to risk in a number of ways to help facilitate prudent decision-making concerning potential risk reduction alternatives for the facility. By reviewing all the ranked lists of importance measure results, we can obtain an understanding of facility-specific risk-dominating vulnerabilities.

Using QRVA results to support decision-making is relatively straightforward. For example, as stated above, the baseline QRVA results can be applied to determine whether or not we have adequate confidence that the facility presents acceptable or unacceptable risk. If we determine that predicted risk is too high for the facility, we can use the results of the vulnerability assessment to help identify potential facility improvement options that can effectively reduce risk.

The QRVA can be applied to investigate and evaluate the potential cost-benefit-risk impacts associated with proposed improvement options at the facility. This is generally accomplished via development and evaluation of risk improvement option case studies.

In general, the QRVA can be applied to predict the potential benefit (risk reduction) associated with a proposed improvement option and linking that to the implementation cost associated with the improvement option. In that way, proposed improvement options can be prioritized based on the quantitative value of the ratio of risk reduction per dollar invested.

The scope of this Phase 1 QRVA does not include making or evaluating specific recommendations for detailed risk management actions or improvement options at the facility. However, through the risk insights gained as a result of performing this risk assessment, the QRVA team has identified some conceptual areas where the Navy may wish to investigate options or alternatives for future RHBFSF risk management improvements, such as:

1. Consider implementing strict controls on tank return-to-service processes following tank outages for inspection and maintenance to reduce the probability of recurrence of events like the reported January 2014 Tank 5 event. These controls should include requirements to plug any holes drilled through the steel tank liner with acceptable material and to implement 100% quality-controlled hole patch welds. This should also include required quality assurance verification from both the contractor performing the work and subsequently by a competent Navy authority prior to tank close-out for RTS.

2. Consider separating the RHBFSF and Red Hill Water Plant tunnels physically and permanently.

3. Reconsider the location and functionality of the fuel blocking doors in the Lower Access Tunnel (remove or change the location and ensure there exists remote opening capability against spilled fuel).

4. Consider installing submersible emergency shutoff valves inside the tanks on lines upstream of the skin valves. Similarly, consider applying double-wall piping from the interior of each tank to the skin valves. These options could mitigate risk of nozzle rupture between the inlet of the fuel piping inside the tank up to the connection to the skin valve. Pipe breaks or breeches in this area could lead to uncontrolled release of effectively all the fuel in the tank.

5. Consider dedicating and designating one or two existing main fuel storage tanks as “Emergency Ullage Tanks”. Preferably, these would be the lowest elevation tanks feasible; e.g., Tank 1 or Tank 2.

6. If Item 4 above is considered impractical, consider installing one large dedicated emergency ullage tank somewhere on the base, JBPHH, and ensure that it is “protected” as a normally empty tank.

7. Consider developing and implementing improved procedures and training associated with response to risk-dominating loss of fuel inventory control and fuel release scenarios.

8. As part of Item 6 above (or as an extension of Item 6), consider developing emergency strategies for fuel movement, ullage management, etc., at relates to loss of fuel inventory control scenarios.

9. Consider implementing strict supervisory controls regarding main storage tank skin valve and nozzle maintenance; e.g., formal two- or three-person checking and authorization for procedure step implementation.

10. Consider developing formal guidelines, procedures, and associated training for facility maintenance; e.g., at the component type level of detail.

11. Consider implementing periodic (e.g., at least semi-annual) formal emergency scenario walk-through/talk-through exercises for facility operators and supervisors.

12. Consider developing emergency procedures for a potential fuel leak entering the water pump house to include conditions for water pump shutdown.

13. Consider developing emergency procedures for leaks to the Lower Access Tunnel, to include direction for isolation of sectional valves, use of the panic button, securing electric-powered components and buses for explosion protection, and when to close ball valves.

14. Consider labeling tank gallery areas with the associated tank number in large block letters on the tunnel wall.

15. Consider adding fuel vapor sensors and fuel flow sensors in the RHBFSF Lower Access Tunnel.

16. Consider adding improved AFHE (redundant and diverse) fuel level sensors for each main fuel storage tank (likely already under consideration).

17. Consider adding sensors with visible indicators for pipeline pressure and/or flow on the fuel piping in the Lower Access Tunnel.

18. Consider design and implementation of automated pump and valve alignment “fail-safe” schemes for loss of electric power scenarios.

Conceptual risk management actions or improvement options like these or others identified by the Navy or other AOC section teams can be addressed individually via QRVA case studies, or they can be grouped into logical sets of actions for QRVA case study evaluation. Experience has shown that evaluation of potential risk management actions or improvement options via such case studies can be very valuable in supporting prudent, cost-effective facility risk management throughout the life of the facility.

# Appendix A. RISKMAN Software User Manual

[REDACTED FOR PUBLIC RELEASE]

# Appendix B. Information Applied for the QRVA

[REDACTED FOR PUBLIC RELEASE]

# Appendix C. Supporting Engineering Analyses

[REDACTED FOR PUBLIC RELEASE]

# Appendix D. Bibliography

A list of useful QRVA information sources is presented in the following bibliography:


1. Naval Facilities Engineering Command, Hawaii, "Section 8.2: Risk/Vulnerability Assessment Scope of Work," April 13, 2017.

2. United States Navy Contract N62742-14-D-1884, Task Order 0028, Amendment 64 Statement of Work, June 1, 2017.

3. Administrative Order on Consent for the Red Hill Bulk Fuel Storage Facility, U.S. Environmental Protection Agency, 2015 (https://www.epa.gov/red-hill/red-hill-administrative-order-consent).

4. E-mail message from Steven L. Chow, NAVFAC Hawaii, to James K. Liming, ABSG Consulting Inc., dated July 27, 2018, 11:27 AM Pacific Time.

5. American Nuclear Society and Institute of Electrical and Electronic Engineers, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," sponsored by the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute, NUREG/CR-2300, April 1983.

6. U.S. Nuclear Regulatory Commission, "PSA Procedures Guide," NUREG/CR-2815, 1985.

7. American Institute of Chemical Engineers Center for Chemical Process Safety, "Guidelines for Chemical Process Quantitative Risk Analysis," 2nd Edition, October 1999.

8. OREDA 2015 Handbook, Offshore and Onshore Reliability Database, 2015.

9. NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, 2007.

10. Kaplan, S., "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems (preprint), 1981.

11. Chhikara, R. S., and J. L. Folks, "The Inverse Gaussian Distribution as a Lifetime Model," Technometrics, Vol. 19, pp. 461–468, 1977.

12. Hahn, G. J., and S. S. Shapiro, Statistical Models in Engineering, John Wiley & Sons, Inc., New York, Chapter B, 1967.

13. Mann, N. R., R. E. Shafer, N. D. Singpurwalla, Methods for Statistical Analysis of Reliability and Life Data, John Wiley & Sons, Inc., New York, 1974.

14. Barlow, R. E., and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York, 1975.

15. Lapides, M. E., and E. L. Zebroski, Use of Nuclear Plant Operating Experience to Guide Productivity Improvement Programs, EPRI SR-26-R, Electric Power Research Institute, Palo Alto, California, 1975.

16. U.S. Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), Washington, D.C., 1975.

17. McClymont, A., and G. McLagan, Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis, EPRI NP-2433, Electric Power Research Institute, Palo Alto, California, 1982.

18. Green, A. E., and A. J. Bourne, Reliability Technology, Wiley-Interscience, New York, 1972.

19. Hald, A., Statistical Theory with Engineering Applications, John Wiley & Sons, Inc., New York, 1952.

20. Apostolakis, G., S. Kaplan, B. J. Garrick, and R. J. Duphily, "Data Specialization for Plant-Specific Risk Studies," Nuclear Engineering and Design, Vol. 56, pp. 321–329, 1980.

21. Parry, T. W., and P. W. Winter, "Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis," Nuclear Safety, Vol. 22, pp. 28–42, 1981.

22. Bayes, T., "Essay Toward Solving a Problem in the Doctrine of Chances" (reprinted), Biometrika, Vol. 45, pp. 293–315, 1958.

23. Ahmed, S., D. R. Metcalf, R. E. Clark, and J. A. Jacobsen, BURD – A Computer Program for Bayesian Updating of Reliability Data, NPGD-TM-582, Babcock & Wilcox, Lynchburg, Virginia, 1981.

24. Martz, H. F., and R. Waller, Bayesian Reliability Analysis, John Wiley & Sons, New York, 1982.

25. Jeffreys, H., Theory of Probability, 3rd ed., Clarendon Press, Oxford, England, 1961.

26. Apostolakis, G., and A. Mosleh, "Expert Opinion and Statistical Evidence: An Application to Reactor Core Melt Frequency," Nuclear Science and Engineering, Vol. 70, pp. 135–149, 1979.

27. Smith, A. M., and I. A. Watson, "Common Cause Failures – A Dilemma in Perspective," Reliability Engineering, Vol. 1, pp. 127–142, 1980.

28. Watson, J. A., and G. T. Edwards, A Study of Common-Mode Failures, R-146, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, London, England, 1979.

29. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operation Experience Involving Dependent Events," Pickard Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

30. Fleming, K. N., "A Reliability Model for Common Mode Failure in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A1 3284, April 23–25, 1975.

31. Parry, G. W., "Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty," 1984 Annual Meeting of the Society for Risk Analysis.

32. Fleming, K. N., and A. M. Kalinowski, "An Extension of the Beta Factor Method to Systems with High Levels of Redundancy," Pickard, Lowe and Garrick, Inc., PLG-0289, June 1983.

33. Poucet, A., A. Amendola, and P. C. Carriabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Center Report, EUR-11054 EN, Ispra, Italy, 1987.

34. Mosleh, A., "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data," Nuclear Engineering and Design, August 1985.

35. Paula, H. M., "Comments on the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation," Nuclear Safety, Vol. 27, No. 2, April/June 1986.

36. Mosleh, A., and N. O. Siu, "A Multi-Parameter, Event-Based Common Cause Failure Model," Paper M7/3, Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, 1987.

37. Atwood, C. L., "Common Cause Fault Rates for Pumps," NUREG/CR-2098, prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.

38. Burdick, G. R., N. H. Marshall, and J. R. Wilson, "COMCAN – A Computer Program for Common Cause Failure Analysis," ERDA Report ANCR-1314, Aerojet Nuclear Company, 1976.

39. Rooney, J. J., and J. B. Fussell, "BACFIRE II – A Computer Program for Common Cause Failure Analysis of Complex Systems," Department of Nuclear Engineering, University of Tennessee, Knoxville, Tennessee, 1978.

40. Worrell, R. B., and O. W. Stack, "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, California, pp. 363–366, 1981.

41. Wagner, O. P., C. L. Cate, and J. B. Fussell, "Common Cause Failure Analysis for Complex Systems," in Nuclear Systems Reliability and Risk Assessment, J. B. Fussell and G. R. Burdick (editors), Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania, 1977.

42. Rasmuson, D. M., N. H. Marshall, J. R. Wilson, and G. R. Burdick, COMCAN II – A Computer Program for Automated Common Cause Failure Analysis, U.S. Department of Energy Report TREE-1361, EG&G Idaho, Inc., Idaho Falls, Idaho, 1979.

43. Putney, B. F., WAMCOM, Common Cause Methodologies Using Large Fault Trees, NP-1851, Electric Power Research Institute, Palo Alto, California, 1981.

44. Lindley, D. V., Introduction to Probability and Statistics. Part 1: Probability, Part 2: Inference, Cambridge University Press, 1970.

45. Kaplan, S., "On a 'Two-Stage' Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 1, January 1983.

46. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG/75-014), October 1975.

47. Nuclear Power Engineering Committee of the IEEE Power Engineering Society, "IEEE Guide to the Collection and Presentation of Electrical, Electronic and Sensing Component Reliability Data for Nuclear Power Generation Stations," IEEE Std 500-1984, New York, New York, December 13, 1983.

48. Mosleh, A., and G. Apostolakis, "Models for the Use of Expert Opinions," Proceedings, Workshop on Low-Probability/High-Consequence Risk Analysis, Arlington, Virginia, June 15-17, 1982, Plenum Press, New York, 1983.

49. Dalkey, N. C., An Experimental Study of Group Opinion, The RAND Corporation, RM-5888-PR, Santa Monica, California, 1969.

50. Hubble, W. H., and C. F. Miller, "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants," NUREG/CR-1363, EGG-EA-5125, June 1980.

51. ABSG Consulting Inc., "RISKMAN™ for Windows Version 14.4 User Manual II: Data Analysis," Irvine, California, December 2015.

52. Mosleh, A., and G. Apostolakis, "Combining Various Types of Data in Estimating Failure Rate Distributions," Transactions of the 1983 Winter Meeting of the American Nuclear Society, San Francisco, California, 1983.

53. Hannaman, G. W., "GCR Reliability Data Bank Status Report," General Atomic Company, GA-A14839 UC-77, July 1978.

54. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, September 1981.

55. Apostolakis, G., "Data Analysis in Risk Assessments," Nuclear Engineering and Design, Vol. 71, pp. 375-381, 1982.

56. Lichtenstein, S., B. Fischhoff, and L. D. Phillips, “Calibration of Probabilities: The State of the Art,” Decision Making and Change in Human Affairs, J. Jungermann and G. de Zeeuw, editors, D. Reidel Publishing Co., Dordrecht, Holland, 1977.

57. Slovic, P., B. Fischhoff, and S. Lichtenstein, “Facts versus Fears: Understanding Perceived Risk,” Societal Risk Assessment, R. C. Schwing and W. A. Albers, Jr., editors, Plenum Press, 1980.

58. OGP Risk Assessment Data Directory, Report No. 434, March 2010. (434.PDF)

59. OGP Risk Assessment Data Directory, Report No. 434-3 March 2010. (434-03.PDF)

60. RH_Tank1_UnverifiedHistory.pdf

61. RH_Tank2_UnverifiedHistory.pdf

62. RH_ Tank 3_UnverifiedHistory.pdf

63. RH_ Tank 4_UnverifiedHistory.pdf

64. RH_ Tank 5_UnverifiedHistory.pdf

65. RH_ Tank 6_UnverifiedHistory.pdf

66. RH_ Tank 7_UnverifiedHistory.pdf

67. RH_ Tank 8_UnverifiedHistory.pdf

68. RH_ Tank 9_UnverifiedHistory.pdf

69. RH_ Tank 10_UnverifiedHistory.pdf

70. RH_ Tank 11_UnverifiedHistory.pdf

71. RH_ Tank 12_UnverifiedHistory.pdf

72. RH_ Tank 13_UnverifiedHistory.pdf

73. RH_ Tank 14_UnverifiedHistory.pdf

74. RH_ Tank 15_UnverifiedHistory.pdf

75. RH_ Tank 16_UnverifiedHistory.pdf

76. RH_ Tank 17_UnverifiedHistory.pdf

77. RH_ Tank 18_UnverifiedHistory.pdf

78. RH_ Tank 19_UnverifiedHistory.pdf

79. RH_ Tank 20_UnverifiedHistory.pdf

80. Whitacre 2014a.pdf

81. Whitacre 2014b.pdf

82. Whitacre 2014c.pdf

83. Whitacre 2014d.pdf

84. Whitacre 2014e.pdf

85. Whitacre 2014f.pdf

86. Whitacre 2014g.pdf

87. Whitacre 2014h.pdf

88. Whitacre 2014i.pdf

89. Audit Report – Department of the Navy Red Hill and Upper Tank Farm Fuel Storage Facilities N2010-0049, August 16, 2010. (N2010-0049 Final Audit Report-16aug2010.pdf)

90. Board of Water Supply Comments on the Proposed Administrative Order on Consent (AOC) and Attachment A, Statement of Work (SOW) on the Red Hill Bulk Fuel Storage Facility, July 20, 2015. (EPA-R09-UST-2015-0441-0559 (1).pdf)

91. Unverified Histories: Releases Vs Tell-tales AND Verified Reporting: Since 1988 (RH_CompUnverLeakHistories_DEC17-NAVFACcomments.xlsx)

92. AFHE Pearl Harbor Tank 0105 Findings, February 6, 2014. (Pearl Harbor Tank 0105 AFHE Findings_02_6_2014=chronology.pdf)

93. Administrative Order on Consent Statement of Work Section 2.4 TIRM Procedures Decision Document and Implementation, Red Hill Bulk Fuel Storage Facility, Joint Base Pearl Harbor-Hickam, Oahu, Hawaii, April 24, 2017. (RH_AOC_Section2_TIRMDecisionDocument_24APR17-RHBFST5.pdf)

94. Final API 653 Inspection Report, PRL 03-12: Internal Inspection of Tank 6, Red Hill, FISC Pearl Harbor, Hawaii, January 2007. (Final API 653 Inspection Report-Tk 6_2007.pdf)

95. RedHill_ Tank 07InspectionReport_1998.pdf

96. RedHill_ Tank 08InspectionReport_1998.pdf

97. RedHill_ Tank 10InspectionReport_1998.pdf

98. Consolidated Construction Projects for FISC, Pearl Harbor, Hawaii, Clean and Repair Tanks 1 and 15, 6 and 16, Weld Repair As Built Record, June 2005. (Tank 15 Repair As Built Jun05.pdf)

99. Final API-653 Inspection Report, PRL 99-21: Clean, Inspect, and Repair Tank 15, Red Hill, FISC Pearl Harbor, Hawaii, January 2007. (API-653 Inspection Report-Tk15_2007.pdf)

100. Final API 653 Inspection Report, PRL 02-11: Clean, Inspect, and Repair Tank 16, Red Hill, FISC Pearl Harbor, Hawaii, January 2007. (Tank 16 API 653 Final Inspection Report_2007.pdf)

101. Repair Tank, Red Hill, FISC Pearl Harbor, Hawaii, DESC Project PRL 98-9, August 1998. (Tank 19 Rpr.pdf)

102. Modified API-653 Out-of-Service, Tank 20, Red Hill, December 5, 2008. (RedHill_API653Report_ Tank 20_05DEC08.pdf)

103. RHBFST 20, Engineering Review and Suitability, for Service Evaluation, API 653 Out-of-Service Tank Inspection by Others, January 2009. (SUMMARY Tank 20 Engineering Review - Final Report 01-27-09.pdf)

104. RHBFST 2 Repair Certification Report Clean, Inspect, and Repair Red Hill Storage Tank s Fleet and Industrial Supply Center Pearl Harbor, Revision 2, July 2010. (DO 31 Final, Rv2 Tank 2 Repair Certification Rpt.pdf)

105. Muhlbauer, W. Kent, "Pipeline Risk Management Manual Ideas, Techniques and Resources," Third Edition, ELSEVIER.

106. Michael Baker Jr., Inc., "Final 2015 Biennial Leak Detection Testing Report of 14 Bulk Field-Constructed Underground Storage Tanks at Red Hill Underground Fuel Storage Facility," prepared for Defense Logistics Agency Energy, Ft. Belvoir, Virginia, June 12, 2015.

107. ESTCP Final Report, "Validation of the Low-Range Differential Pressure (LRDP) Leak Detection System for Small Leaks in Bulk Fuel Tanks," Prepared by Environmental Security Technology Certification Program, U. S. Department of Defense. (EPA-R09-UST-2015-0441-0344-LRDP-24.pdf)

108. Center for Chemical Process Safety of the American Institute of Chemical Engineers, "Guidelines for Process Equipment Reliability Data with Data Tables," New York, New York, 1989.

109. Blanton, C. H., and S. A. Eide, "Savannah River Site Generic Data Base Development (U)," Westinghouse Savannah River Company, WSRC-TR-93-262, June 30, 1993.

110. Pickard, Lowe & Garrick, Inc., "Database for Probabilistic Risk Assessment for Light Water Nuclear Power Plants," proprietary, PLG-0500.

111. Lees, F. P., and M. S. Mannan, Lees' Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control, Fourth Edition, Volumes 1–3, August 2012.

112. Turhanlar, Daniel, Yaping He, and Glenn Stone, "The Use of Lifts for Emergency Evacuation – a reliability study," The 9th Asia-Oceania Symposium on Fore and Science Technology, www.sciencedirect.com, Procedia Engineering 62 (2013) 680-689, by School of Computing, Engineering and Mathematics, University of Western Sydney, Penrith NSW 2751, Australia.

113. U.S. Nuclear Regulatory Commission, "CCF Parameter Estimations, 2015 Update," October 26, 2015.

114. "Red Hill Complex Fire, Safety, Life Safety, and Environmental Risk Assessment/Analysis Volume I of II, Final Submittal," prepared by WillBros Engineers, Inc., for Department of the Navy Pacific Division Naval Facilities Engineering Command, Pearl Harbor, Hawaii, August 1998.

115. Victor L. Streeter, "Fluid Mechanics," Fifth Edition. McGraw Hill Company, 1973. Pages 278–281.

116. Fault Tree Handbook, NUREG-0492, 1981.

117. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, 1980.

118. Swain, A. D., and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, 1983.

119. An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, 1992, EPRI-TR-100259.

120. Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Revision 1, May 2000, U.S. Nuclear Regulatory Commission, NUREG-1624.

121. Systematic Human Action Reliability Procedure, 1984, EPRI NP-3583.

122. SHARP1 – A Revised Systematic Human Action Reliability Procedure, 1990, EPRI NP-7183-SL.

123. Swain, A. D., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, 1987.

124. Fussell, J. B., "How to Hand Calculate System Reliability Characteristics," IEEE Transactions of Reliability, Vol. R-24, No. 3, 1975.

125. Birnbaum, Z. W., "On the Importance of Different Components in a Multi-System in Multivariate Analysis," Academic Press, New York, 1969.

126. Lambert, H. E., and F. M. Gilman, “The Importance Computer Code,” ERDA Report UCRL-79269, Lawrence Livermore National Laboratory, Livermore, California, 1977.

127. Engelbrecht-Wiggans, R., and D. R. Strip, “On the Relation of Various Reliability Measures to Each Other and to Game Theoretic Values,” SANDB0-2624, Sandia National Laboratories, Albuquerque, New Mexico, 1981.

128. Lambert, H. E., “Fault Trees for Decision-Making in Systems Analysis,” Ph.D. thesis, UCRL-51829, Lawrence Livermore National Laboratory, Livermore, California, 1975.

129. Apostolakis, G. E., and S. Kaplan, “Pitfalls in Risk Calculations,” Reliability Engineering, Vol. 2, pp. 135–145, 1981.

130. Lambert, H. E., “Measures of Importance of Events,” in Reliability and Fault Tree Analyses, ed. R. E. Barlow, J. B. Fussell, and N. D. Singpurwalla, SIAM Press, Philadelphia, Pennsylvania, pp. 77–100 (1975).

131. RHBFST 2 Engineering Review and Suitability for Service Evaluation API 653 Out-of-Service RHBFST Inspection by Others, October 2008. (2008 Oct 13_API 653 - Final Report_Tank 2.pdf)

132. RHBFST 5 & 17 Cleaning, Inspection and Repairs Project, RHBFST 5 Inspection Report, November 18, 2010. (RedHill_RHBFST05InspectionReport_18NOV10.pdf)

133. Director Aaron Poentis, “Red Hill Complex, Soil Sampling Results for January 2016, DOH Facility ID No. 9-102271, DOH Release ID No. 990051, 010011, 020028, and 140010,” Department of the Navy letter to Mr. Richard Takaba, Hawaii State Department of Health, dated February 10, 2016, 5090 SER N45/ 0443.

# Appendix E. Glossary

This glossary is an adaptation of information found in NUREG-2122.

## E.1. Terms and Definitions

Table E-1 provides the terms and their definitions with the associated discussion. The terms are listed alphabetically. Hazard-specific terms are listed, but their definitions are provided in the noted appendix.

**Table E-1. Terms and Definitions**

| Term and Definition | Discussion |
|---|---|
| **Accident Consequence** | |
| The health effects or the economic costs resulting from a facility accident. *(see Health Effects, Accident Consequence Analysis)* | In a Level 3 (or 4) QRVA, the consequences can be measured by health effects and economic costs resulting from a facility accident.<br>The accident consequences analyzed in a risk analysis generally involve evaluating the extent to which the health of the surrounding population or the condition of the surrounding environment is affected. The health effects and economic costs of a facility accident can be incurred both on the facility site as well as in the surrounding community. In most cases, the focus is on offsite consequences (i.e., (1) fuel chemical exposure from various exposure pathways and consequent health effects to the public, and (2) the economic costs associated with protective measures, such as evacuation and relocation of the public, destruction of contaminated foodstuffs, and decontamination or interdiction of contaminated land and property). |
| **Accident Consequence Analysis** | |
| The calculation of the extent of health effects or the economic costs resulting from a facility accident. *(see Accident Consequence)* | In a QRVA, the accident consequence analysis is the actual quantification of the potential magnitude of health effects and/or economic costs that can result from a facility accident. Accident consequence analysis attempts to answer the third of the three questions used to define risk: (1) What can go wrong? (2) How likely is it? (3) What might be its consequences? |
| **Accident Event Sequence** | |
| *(see Accident Sequence)* | The term accident event sequence has the same meaning as accident sequence and is defined under “Accident Sequence.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Accident Mitigation** | |
| Actions taken to reduce the severity of an accident. *(see Accident Prevention, Emergency Preparedness, Emergency Response)* | In a QRVA, accident mitigation typically refers to actions taken to reduce the severity of an accident once loss of fuel inventory control has started, as opposed to actions to prevent a loss of fuel inventory control event from occurring. Successful accident mitigation implies that a loss of fuel inventory control event occurred, but its consequences were minimized.<br>Some strategies used for accident mitigation include preventing fuel chemical releases by maintaining barrier integrity, or reducing fuel chemical releases by filtration.<br>Also, accident mitigation measures typically refer to plans or actions taken on the facility site, while emergency preparedness measures and emergency response (e.g., evacuation, sheltering) refer to plans or actions taken to reduce exposure of onsite workers, as well as the surrounding population offsite. |
| **Accident Mitigation** | |
| Actions taken to reduce the severity of an accident. *(see Accident Prevention, Emergency Preparedness, Emergency Response)* | In a QRVA, accident mitigation typically refers to actions taken to reduce the severity of an accident once loss of fuel inventory control has started, as opposed to actions to prevent a loss of fuel inventory control event from occurring. Successful accident mitigation implies that a loss of fuel inventory control event occurred, but its consequences were minimized.<br>Some strategies used for accident mitigation include preventing fuel chemical releases by maintaining barrier integrity, or reducing fuel chemical releases by filtration.<br>Also, accident mitigation measures typically refer to plans or actions taken on the facility site, while emergency preparedness measures and emergency response (e.g., evacuation, sheltering) refer to plans or actions taken to reduce exposure of onsite workers, as well as the surrounding population offsite. |
| **Accident Precursor, Precursor Event** | |
| A change in facility status that could lead to loss of fuel inventory control accidents. | A QRVA is used to evaluate an event to determine if it will be considered an accident precursor. A conditional loss of fuel inventory control probability (CLOFICP) is calculated for the event. The event is considered a precursor event, according to the NRC's Performance and Accountability Report, if the event has a probability of greater than 1 in 1 million of leading to substantial loss of fuel inventory control. An event is considered to be a "significant precursor" when the event "has a probability of 1 in 1,000 (or greater) of leading to substantial damage to the reactor fuel."<br>The terms accident precursor and precursor event generally have the same meaning. In some documents, the definition of accident precursor or precursor event includes quantitative criteria (e.g., as in the definition above), whereas some other definitions do not include quantitative criteria. |

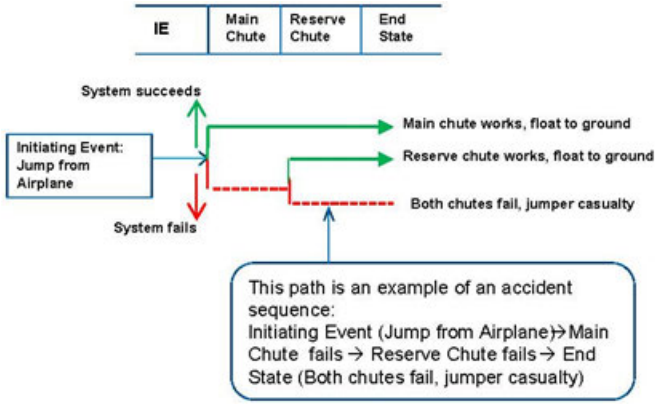
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Accident Prevention** | |
| Actions taken to reduce the likelihood of an accident. *(see Accident Mitigation )* | In a QRVA, accident prevention typically refers to actions taken to prevent a loss of fuel inventory control event from occurring, as opposed to reducing the severity once loss of fuel inventory control has started. Successful accident prevention implies that a loss of fuel inventory control event does not occur.<br>Some strategies used for accident prevention include: physical protection, maintaining facility stable operation, reactor protective systems, and maintaining barrier integrity. |
| **Accident Progression Event Tree** | |
| A logic diagram that begins with the onset of loss of fuel inventory control and identifies the potential responses of the containment and associated equipment, as well as operator actions, to the severe accident loads. *(see Bridge Tree, Containment Event Tree, Event Tree)* | In the QRVAs documented in the NUREG-1150 series of reports, an accident progression event tree (APET) was used to analyze containment response to severe accident loads. An APET is a detailed representation of the containment response to severe accident loads, including the interaction of phenomena, the availability of equipment, and the performance of operators. For most modern QRVAs, a containment event tree (CET), which is a less complex representation, is used to emphasize the status of the containment and containment equipment during a severe accident. The end states of both the APET and the CET are no containment failure, various containment failure modes, or containment bypass. |
| **Accident Scenario** | |
| *(see Accident Sequence)* | The term accident scenario has the same meaning as accident sequence and is defined under “Accident Sequence.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Accident Sequence Analysis, Event Sequence Analysis** | |
| The process used to determine the series of events that can lead to undesired consequences. (see Accident Sequence) | In a QRVA, accident sequence analysis is the process used to determine the combination of events that can lead to the undesired end state (e.g., loss of fuel inventory control or acute fuel release). The results of the accident sequence analysis are expressed in terms of individual accident sequences, each of which includes an initiating event followed by the necessary set of failures or successes of additional events (such as system, function, or operator performance) that will cause the undesired event.<br>The terms accident sequence analysis and event sequence analysis are similar in meaning and often correctly used interchangeably. However, generally the terminology "accident" refers to leading to loss of fuel inventory control, and the terminology "event" does not necessarily reflect a negative outcome such as loss of fuel inventory control.<br>The ASME/ANS PRA Standard defines accident sequence analysis as "the process to determine the combinations of initiating events, safety functions, and system failures and successes that may lead to loss of fuel inventory control or large early release." |
| **Accident Sequence Class, Accident Sequence Group, Accident Sequence Type, Event Sequence Class, Event Sequence Group, Event Sequence Type** | |
| A grouping of accident sequences with similar characteristics or end states. *(see Accident Sequence)* | In a QRVA, the accident sequences typically are combined into accident sequence classes (groups or types). For example, an accident sequence class might represent a set of accident sequences with similar initiating events or similar safety function responses. The purpose for combining like sequences is generally done to understand the type of sequences contributing to the risk.<br>The terms accident sequence class, accident sequence group, and accident sequence type are similar in meaning and often correctly used interchangeably. Moreover, accident sequence is also used interchangeably with event sequence. Consequently, the terms event sequence class, event sequence group, and event sequence type also are similar in meaning and used interchangeably. |
| **Accident Sequence Frequency** | |
| *(see Frequency)* | Accident sequence frequency is a type of frequency used in QRVA and is defined in the discussion under "Frequency." |
| **Accident Sequence Group** | |
| *(see Accident Sequence Class)* | The term accident sequence group has the same meaning as accident sequence class and is defined under "Accident Sequence Class." |
| **Accident Sequence Type** | |
| *(see Accident Sequence Class)* | The term accident sequence type has the same meaning as accident sequence class and is defined under "Accident Sequence Class." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Accident Sequence, Accident Event Sequence, Accident Scenario, Event Sequence, Event Scenario, Event Tree Sequence** | |
| A series of events that can lead to undesired consequences. *(see Accident Sequence Analysis, Severe Accident, End State, Event Tree)* | In a QRVA, this series of events (e.g., an accident sequence, scenario, or event sequence) refers to an event tree pathway that follows from a particular initiating event, through system and operator responses, and ultimately to a well-defined end state, such as loss of fuel inventory control. If the end state involves extensive loss of fuel inventory control and fuel chemical release into the containment, with potential release to the environment, the accident sequence would represent a severe accident sequence. The system and operator responses may involve success, failure, or both.<br>The terms accident sequence, accident event sequence, accident scenario, event scenario, event sequence, and event tree sequence are similar in meaning and are often correctly used interchangeably.<br>The ASME/ANS PRA Standard defines an accident sequence as "a representation in terms of an initiating event followed by a sequence of failures or successes, of events (such as system, function or operator performance) that can lead to undesired consequences with a specified end state (e.g., loss of fuel inventory control or large early release)."<br>The following figure is an example of an accident sequence:<br>  <br> |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Active Component** | |
| A component whose operation or function depends on an external source of power (e.g., air, electrical, hydraulic). *(see Passive Component)* | In a QRVA, important elements of the model include both active and passive components. NUREG/CR-5695 defines active component as: "A component which normally is operating or can and should change state under normal operating conditions or in response to accident conditions (e.g., pumps, valves, switches)."<br>Some examples of active components include pumps, fans, relays, and transistors. These are identified as active components because they rely on an external driving mechanism to perform their function.<br>The International Atomic Energy Agency (IAEA) Safety Glossary mentions "certain components, such as rupture discs, check valves, safety valves, injectors, and some solid state electronic devices, have characteristics that require special consideration before designation as an active or passive component." This special consideration implies that some components are not easily labeled as either active or passive because they may have characteristics of both.<br>The ability to change state is sometimes considered as the defining characteristic of whether a component is active or passive. For example, a check valve normally has a passive function, but in a safety injection system it could be considered active since it needs to open and then reclose to prevent backflow. |
| **Acute Exposure** | |
| *(see Exposure)* | The term acute exposure is a type of exposure and is defined in the discussion under "Exposure." |
| **Acute Fuel Release** | |
| *(see Fuel chemical Release)* | The term acute fuel release is a type of fuel chemical release and is defined in the discussion under "Fuel Release." |
| **Acute Fuel Release Frequency (AFRF)** | |
| *(see Frequency)* | The term acute fuel release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency." |
| **Acute Fuel Release Frequency Analysis** | |
| *(see* Fuel *Release Frequency Analysis)* | The term acute fuel release frequency analysis is a type of fuel release frequency analysis and is defined under "Fuel Release Frequency Analysis." |
| **Acute Health Effects** | |
| *(see Health Effects)* | The term acute health effect refers to a type of health effect and is defined in the discussion under "Health Effects." |

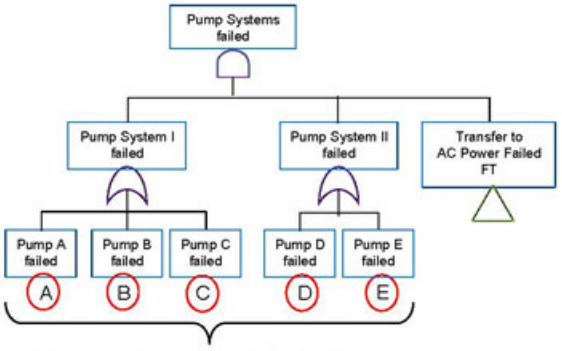
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Aging** | |
| General process in which characteristics of a structure or component gradually change (e.g., degrade) with time or use. *(see Bathtub Curve)* | In a PRA, the aging of a component is generally not explicitly modeled but is sometimes assumed to be reflected in the failure probability used to represent the performance of the component.<br>The performance of structures or components may degrade with time (e.g., increasing failure rates, new failure modes) because of wearout and exposure to environmental conditions. Aging can lead to increasing failure rates in the later stages of life of a component. During the early life (burn-in) of a component, failure rates can decrease until a plateau is reached, as seen in the bathtub curve.<br>The definition provided is based on the definition in the IAEA Safety Glossary. |
| **Air Submersion** | |
| *(see Cloudshine)* | Air submersion has the same meaning as cloudshine and is defined under "Cloudshine." |
| **Aleatory Uncertainty** | |
| *(see Uncertainty)* | The term aleatory uncertainty is a specific type of uncertainty and is defined under the term "Uncertainty." |
| **As-Built As-Operated (As-Designed)** | |
| The accurate and current design and operation of the facility. *(see QRVA Configuration Control, Living QRVA, Facility Configuration Control)* | When applied to a QRVA, as-built as-operated refers to the fidelity of the QRVA model matching the current facility design, configuration, procedures, and performance data (e.g., component failure rates). Similarly, as-designed refers to the QRVA matching the facility configuration in the design certification stage, in which the facility is not yet built or operated.<br>Because the facility's configuration and operating procedures are continuously upgraded and modified and operating experience is accrued, the QRVA model needs to be updated from time to time to reflect the as-built, as-operated facility. In that case, the model is said to be up-to-date (i.e., current). A QRVA that is continuously updated to incorporate facility changes is called a living QRVA.<br>In the ASME/ANS PRA Standard, as-built as-operated is defined as "a conceptual term that reflects the degree to which the PRA matches the current plant design, plant procedures, and plant performance data, relative to a specific point in time." |
| **As-Designed** | |
| *(see As-Built As-Operated)* | The term as-designed is defined in the discussion of the term "As-Built As-Operated." |

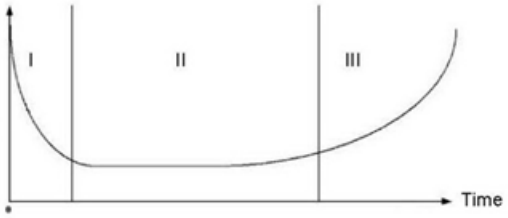
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Assumption (Key)** | |
| A decision or judgment that is made in the development of a model or analysis. *(see Model Uncertainty)* | In a QRVA, an assumption is either related to a source of model uncertainty or to scope or level of detail. An assumption related to a model uncertainty is made about the choice of the data, approach, or model used to address an issue because there is no consensus. A credible assumption is one that has a sound technical basis, such that the basis would receive broad acceptance within the relevant technical community. An assumption related to scope or level of detail is one that is made for modeling convenience.<br>An assumption is considered to be key to a risk-informed decision when it could affect the QRVA results that are being used in a decision and, consequently, may influence the decision being made. An effect on the QRVA results could include the introduction of a new functional accident sequence or other changes to the risk profile (e.g., overall loss of fuel inventory control frequency [LOFICF] or AFRF, event importance measures). Key sources of model uncertainty are identified in the context of an application.<br>The definition provided is based on the definition in the ASME/ANS PRA Standard. The NRC Website Glossary states, "in the context of individual plant examinations, individual plant examinations for external events, and probabilistic risk assessments, assumptions are those parts of the mathematical models that the analyst expects will hold true for the range of solutions used for making decisions." |
| **Availability (Unavailability)** | |
| The probability that a system, structure, or component of interest is functional at a given point in time. (*see Reliability)* | In a QRVA, unavailability is one of the attributes of a system, structure, or component that may affect the facility's response to an initiating event.<br>Unavailability is the complement of availability (i.e., shortfall between availability and unity). In the ASME/ANS PRA Standard, unavailability is defined as "the probability that a system or component is not capable of supporting its function including, but not limited to, the time it is disabled for test or maintenance."<br>The definition provided is based on the definition in NFPA-805. |
| **Base QRVA, Baseline QRVA** | |
| *(see QRVA)* | The terms base QRVA and baseline QRVA represent a specific type of QRVA and are defined under "QRVA." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Basic Event** | |
| An element of the QRVA model for which no further decomposition is performed because it is at the limit of resolution consistent with available data. *(see Component, Fault Tree)* | In a QRVA, in developing the fault trees, the basic events represent those failures for which there is available data, and as such, represent the termination of a branch of the fault tree. There are typically two types of failures (or basic events): equipment unavailability and human errors.<br>The term basic event can have other (more specific) definitions, as stated below:<br>• "An event in a fault tree model that requires no further development, because the appropriate limit of resolution has been reached." (NUREG-0492).<br>• The individual events that collectively form a cut set, which is a combination of failures needed to result in the occurrence of a condition of interest (e.g., accident sequence, system failure).<br>In the quantification process of the QRVA, the model uses or manipulates the basic events to model the LOFICF. At this point, the initiating event is part of the quantification process; consequently, an initiating event is sometimes referred to as a basic event.<br>The following figure is an example of a basic event:<br>  |
| **Basic Event Failure Probability** | |
| *(see Probability)* | The term basic event failure probability is a specific type of failure probability and is defined under "Probability." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Bathtub Curve** | |
| Graphical representation of failure rate time dependency in the life of a typical component. *(see Aging)* | In a QRVA, the mid-life or constant failure rate stage in the life of a component is the one typically modeled. However, the life of certain types of components is often considered to have three stages of failure rate behavior: I) burn-in (or infant mortality) stage, characterized by failure rates decreasing with time, II) mid-life or constant failure rate stage, and III) wearout stage in which failure rates increase with time. These three stages together form a curve that looks like the cross-section of a bathtub. The following figure represents a bathtub curve:<br>  <br><br>• Region I – The failure rate is usually high at the beginning of a component's life because of defects. It decreases if the component survives.<br>• Region II – The failure rate becomes stable and remains constant in the middle of the component's life.<br>• Region III – The failure rate increases toward the end of the component's life. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Bayesian Analysis, Bayesian Estimation, Bayesian Statistics** | |
| Type of data analysis in which an initial estimate about a parameter value is combined with evidence to arrive at a more informed estimate. *(see Frequentist, Bayesian Update)* | In a QRVA, Bayesian analysis is commonly used in the computation of the frequencies and failure probabilities in which an initial estimation about a parameter value (e.g., event probability) is modified based on actual occurrences of the event. The initial parameter value may have a probability distribution associated with it. Thus, the event probability to be determined is based on a belief, rather than on occurrence ratios. Any actual occurrence or lack of occurrence of the event is used to measure consistency with the original hypothesis, which is then modified to reflect this evidence. The modified or updated hypothesis is the most meaningful estimate of the parameter.<br>The initial hypothesis is called the "prior". The prior should be as relevant as possible to the parameter value in question. The final parameter estimate will depend on the prior chosen to a certain extent. For example, industry average (generic) data may be used as the prior. Noninformative priors can be used if no basis for making an educated guess exists. The prior is modified by actual observations of the event occurrences (e.g., facility-specific data) to calculate the "posterior" or best estimate of the parameter. The process is called "Bayesian update."<br>Bayesian analysis is used when occurrences of an event are sparse or nonexistent, such that probability estimates using the proportion of actual event occurrences (frequentist approach) are not reliable. It also can be used to produce a probability distribution for the parameter in question.<br>In risk analysis, both frequentist and Bayesian analysis may be used. Frequentist analysis is used when the occurrence data is sufficiently abundant, Bayesian analysis is used otherwise.<br>The terms Bayesian analysis, Bayesian estimation, and Bayesian statistics are used interchangeably. |
| **Bayesian Estimation** | |
| *(see Bayesian Analysis)* | The term Bayesian estimation has the same meaning as Bayesian analysis and is defined the same as the term "Bayesian Analysis." |
| **Bayesian Statistics** | |
| *(see Bayesian Analysis)* | The term Bayesian statistics has the same meaning as Bayesian analysis and is defined the same as the term "Bayesian Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Bayesian Update** | |
| Modification of a probability (frequency) of an event by incorporating additional observations of event occurrence. *(see Bayesian Analysis)* | In a QRVA, Bayesian update is the process of using the Bayesian approach to incorporate new information and combine it with existing information to come up with a new characterization of the state-of-knowledge about a parameter. It is used to incorporate new information as it becomes available or to account for facility-specific information when primarily relying on generic data (or some other initial guess) to generate event failure probabilities or frequencies. For example, an initial guess of a pump failure rate is based on industry generic data.<br>Observations of a certain number of failures (or no failures) of that type of pump over a certain time period in the facility are used in the Bayesian update to obtain a better estimate of the pump failure rate in that particular facility.<br>Industry generic failure rates might be used as the starting estimate (called the prior). These would be combined with the observed occurrences of failure of such components to calculate the updated failure rates. A similar process may be used to obtain facility-specific initiating event frequencies, by starting from generic data and updating with facility-experienced occurrences to arrive at the updated initiating event frequencies. |
| **Best Estimate** | |
| Approximation of a quantity based on the best available information. *(see Mean, Point Estimate)* | In a QRVA, the term best estimate is not generally used. The term is sometimes mistakenly used in place of point estimate or mean value to characterize a parameter value estimate used in a QRVA.<br>The term is used for deterministic calculations, in which best estimate designates inputs or results obtained by using the most realistic assumptions available to the analyst (i.e., not biased by conservatism or optimism). For example, best estimate codes may be used to deterministically predict the pressure rise in containment from a hydrogen burn. |

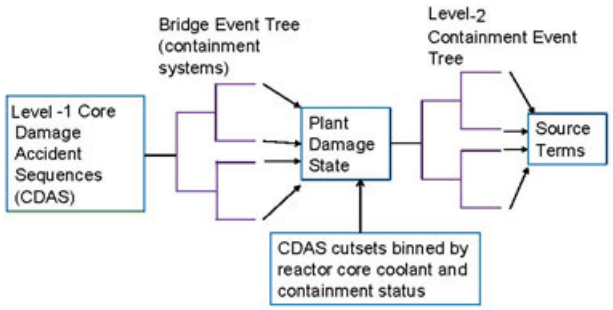
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Beyond-Design-Basis Accident** | |
| A postulated accident that is more severe than those accidents used to establish the design of a facility. *(see Design-Basis Accident, Severe Accident)* | In a QRVA, beyond-design-basis accidents (BDBA) are a major focus of the analysis.<br>A facility must be designed and built to withstand a design-basis accident (DBA) without threatening public health and safety. However, the facility is not necessarily designed to withstand BDBAs. Therefore, an important role of QRVA is to determine how a facility will behave in a BDBA and analyze the adequacy of the systems, structures, and components that are included to ensure public health and safety are maintained. Although BDBAs might exceed the design envelope, they do not necessarily result in significant consequences. Those BDBAs that do result in significant consequences are termed severe accidents. All severe accidents are by definition BDBAs since their challenges exceed the design envelope of the facility.<br>The NRC Website Glossary defines the term beyond-design-basis accident as "a technical way to discuss accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely. (In that sense, they are considered beyond the scope of design-basis accidents that a facility must be designed and built to withstand.) As the regulatory process strives to be as thorough as possible, beyond-design-basis accident sequences are analyzed to fully understand the capability of a design." |
| **Beyond-Design-Basis Event** | |
| An event more severe than the events for which the facility was designed to withstand and specified in the safety analysis. *(see Design-Basis Event, Severe Accident)* | In a QRVA, beyond-design-basis events (BDBE) represent conditions beyond the facility design envelope and, therefore, exceed the already considered anticipated transients, anticipated operational occurrences (AOO), DBAs, and design-basis natural phenomena.<br>A BDBE challenges the systems, structures, and components that are included in the design to ensure public health and safety. Generally, BDBEs have been excluded from the design-basis because they were considered to have a low probability of occurrence. Extremely unlikely earthquakes or aircraft impacts would be considered beyond-design-basis events which, while not considered in the facility design, can be analyzed in the QRVA to determine how the facility would respond given such an event. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Bin, Binning** | |
| A group of initiating events or accident sequences with similar characteristics. | In a QRVA, binning is a process used to group similar types of initiating events, accident scenarios, or sequences together to simplify the analysis. The term bin generally is associated with binning event tree sequences into groups that have similar characteristics and lead to similar end states called facility damage states. Initiating events also are grouped by similar characteristics<br>Bin is the actual group and binning is the process. |
| **Birnbaum Importance** | |
| *(see Importance Measure)* | The term Birnbaum importance is one type of importance measure and is defined under "Importance Measure." |
| **Bounding Analysis** | |
| An analysis that uses assumptions such that the assessed outcome will meet or exceed the maximum severity of all credible outcomes, both in magnitude as well as frequency. (*see Conservative Analysis)* | In a QRVA, a bounding analysis of a contributor or parameter may be performed to bound the risk or to screen the QRVA item as a potential contributor to risk. When used for screening, the bounding analysis demonstrates that the item can be omitted from the QRVA model because, even in the worst case, the impact on calculated risk is insignificant.<br>As discussed in NUREG-1855, in the context of a specific QRVA scope or level of detail item, a bounding analysis includes the worst credible outcome of all known possible outcomes that result from the risk assessment of that item. The worst credible outcome is the one that has the greatest impact on the defined risk metric(s). Thus, a bounding probabilistic analysis must be bounding both in terms of the potential outcome and the likelihood of that outcome. Consequently, a bounding analysis considers both the frequency of the event and the outcome of the event.<br>NUREG-1855 states that if a bounding analysis is being used to bound the risk (i.e., determine the magnitude of the risk impact from an event), then both its frequency and outcome must be considered. However, if a bounding analysis is being used to screen the event (i.e., demonstrate that the risk from the event does not contribute to the defined risk metric(s)), then the event can be screened based on frequency, outcome, or both, depending on the specific event.<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |
| **Bridge Event Tree** | |
| *(see Bridge Tree)* | The term bridge event tree has the same meaning as bridge tree and is defined under "Bridge Tree." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Bridge Tree, Bridge Event Tree** | |
| An event tree used to transfer information from one analysis stage to another in a manner that ensures the critical information is preserved. *(see Containment Event Tree, Event Tree, Accident Progression Event Tree)* | In a QRVA, the most common use of bridge trees is in linking the loss of fuel inventory control states, which are the end points of the Level 1 QRVA analysis, with the facility damage states. The facility damage states often are used as the starting point of the accident progression event tree or the containment event tree (i.e., Level 2 analysis). In this case, the bridge trees provide the information on the status of systems that were not relevant for determining consequences, but that can influence further accident progression. The terms bridge tree and bridge event tree are similar in meaning and often correctly used interchangeably.<br>The figure below is an example of a bridge tree:<br>  <br> |
| **Capability Categories** | |
| Categories used to indicate different levels of detail, facility specificity, and realism in defining technical requirements for an acceptable QRVA. | For a QRVA used with a risk-informed application, the level of detail, facility specificity, and realism needs to be commensurate with the scope of the specific application under consideration, as recognized in NRC Regulatory Guide 1.200.<br>Capability categories are used in the ASME/ANS PRA Standard to recognize that the various elements in the QRVA model can be constructed to different levels of detail, levels of facility-specificity, and levels of realism. The QRVA standard defines three categories of the acceptable level of detail, facility-specificity and realism, starting at the minimal for capability Category I, and increasing through Category II, and Category III. The use of capability categories supports the concept that a QRVA needs only to have the scope and level of detail necessary to support the application for which it is being used, but it always needs to be technically acceptable.<br>As stated in the ASME/ANS PRA Standard, "as the capability category increases, the depth of the analysis required also increases." As further stated in the ASME/ANS PRA Standard, "the level of conservatism may decrease as the capability category increases and more detail and more realism are introduced into the analysis. However, this is not true for all requirements and should not be assumed." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Chemical Element Group** | |
| A group of fuel chemicals with similar physical and chemical properties used to simplify the estimate for offsite health effects. *(see Source Term)* | In a QRVA, the source term used to characterize the fuel release is based on the defined chemical element groups.<br>During a fuel release accident, the number of different materials released from the facility containment to the environment can be quite large. The number of materials considered can be reduced to a manageable size by grouping those with similar physical and chemical properties. |
| **Chronic Exposure** | |
| *(see Exposure)* | The term chronic exposure is a type of exposure and is defined in the discussion under "Exposure." |
| **Cohort** | |
| A group of individuals that is defined by some statistical or demographic factor. (see Emergency Response) | In the emergency response modeling of a Level 3 (or 4) QRVA, a cohort is a subset of the offsite population that mobilizes or moves differently from others. The planning and analysis of the offsite response to a severe accident is driven by the demographics of the surrounding population (i.e., the attributes (e.g., age, location) of the various cohorts (e.g., school children, hospital patients, prisoners) and their potential for being exposed to severe health effects). |
| **Common Cause Component Group** | |
| Similar components that are modeled as a group because they are subject to failure by a common cause. (see Common-Cause Failure) | In a QRVA, one failure mechanism of a component may be from a common cause that also fails other components.<br>A common cause component group is a collection of like components considered to have the potential to fail by the same cause. For example, redundant diesel generators in a facility are modeled as having the potential to fail by common cause (as well as independently) and form a common cause component group. Turbine-driven and motor-driven pumps in a secondary cooling system may form a common cause component group (failures because of a common environment), while at the same time the motor-driven pumps may form a separate common cause group because of separate common cause failures.<br>Common cause failure among like components usually is not modeled to occur across system boundaries. This is because the operating regime may be different and thus failure rates may be different. An exception may be in external events, such as seismic events, in which components may be subject to similar stresses. |

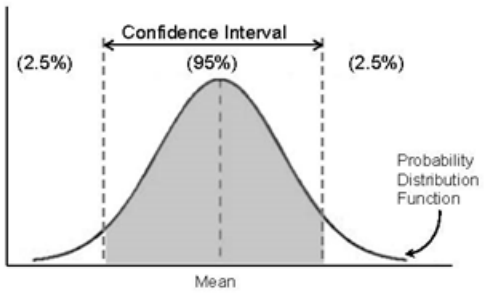
## Table E-1. Terms and Definitions (Continued)

<table>
<tr><th>Term and Definition</th><th>Discussion</th></tr>
<tr><td colspan="2">Common Cause Failure</td></tr>
<tr><td>A failure of two or more structures, systems, or components as a result of a single shared cause. (see Common-Mode Failure, Failure Mode)</td><td>
In a QRVA, CCF is a special form of dependent failure in which the failure of the SSCs has occurred from the same fault. CCF faults generally reflect errors occurring as a result of a common manufacturer, environment, maintenance, etc.<br><br>
The CCF term is often incorrectly used interchangeably with common-mode failure (CMF). CCF only accounts for the SSCs failing because of the same, single cause, not if they ultimately fail in the same manner (or in the same mode), which is CMF. In data provided to quantify CCF events, the failure mode is usually presented (i.e., failure to start, fail to run), and the cause is not always provided about why the failure mode occurs. There could be multiple causes lumped into the data presentation for a given failure mode. Thus, the available failure data dictate whether the QRVA model is modeling CCF or CMF.<br><br>
To illustrate the relationship between CCF and CMF, consider potential causes of failure for emergency diesel generators (EDG) as shown in the figure below. Potential failure causes include a plugged radiator, a failed load sequencer, bad fuel oil, or faulty bearings. As indicated in the figure below, each of these causes can result in failure of multiple diesel generators in either the same failure mode or in different failure modes. Diesel failure modes included in this example are fails to start and fails to run.<br><br>
<table>
<tr><th rowspan="2">Failure Cause</th><th colspan="2">Failure Mode</th><th rowspan="2">Basic Event</th><th rowspan="2">Comments</th><th rowspan="2">CCF Types</th></tr>
<tr><th>EDG A</th><th>EDG B</th></tr>
<tr><td>Plugged radiator</td><td>FTS</td><td>FTR</td><td>CCF-DG-AB-FTS/R-1</td><td>Same cause results in a different failure mode of each DG</td><td>CCF without CMF</td></tr>
<tr><td>Failed load sequencer</td><td>FTR</td><td>FRT</td><td>CCF-DG-AB-FTR</td><td>Same cause results in the same failure mode of both EDGs</td><td>CCF with CMF</td></tr>
<tr><td>Bad fuel oil</td><td>FTS</td><td>FTS</td><td>CCF-DG-AB-FTS</td><td>Same cause results in the same failure mode of both EDGs</td><td>CCF with CMF</td></tr>
<tr><td>Faulty Bearings</td><td>FTS</td><td>FTR</td><td>CCF-DG-AB-FTS-R2</td><td>Same cause results in a different failure mode of each DG</td><td>CCF without CMF</td></tr>
</table>
<br>
The definition provided was based on the definition in the ASME/ANS PRA Standard.
</td></tr>
</table>

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Common-Mode Failure** | |
| A failure of two or more structures, systems, or components in the same manner or mode as the result of a single shared cause. *(see Common-Cause Failure, Failure Mode)* | In a QRVA, CMF is a special form of dependent failure that reflects (1) a common manner of failure (e.g., failure to start, failure to run) and (2) failure from a common cause. Consequently, CMF is actually a type of CCF in which the SSCs fail in the same way and from the same cause. CMF and CCF are often incorrectly used interchangeably. However, CCF only addresses the cause of the failure, while CMF addresses both the cause and the manner.<br>In data provided to quantify CCF or CMF events, the failure mode is usually presented (i.e., FTS, FTR), and the cause is not always provided about why the failure mode occurs. There could be multiple causes lumped into the data presentation for a given failure mode. Thus, the available failure data dictate if the QRVA model is modeling CCF or CMF.<br>Consider the figure displayed in the discussion section for CCF. Potential failure modes for emergency diesel generators are FTS and FTR. Potential failure causes include a plugged radiator, a failed load sequencer, bad fuel oil, or faulty bearings. As indicated in the figure for CCF, each of these causes can result in failure of multiple diesel generators in either the same failure mode or in different failure modes. Examples of CMF are shown in the comment column under the term "Common-Cause Failure."<br>The definition provided was based on the definition in the IAEA Safety Glossary. |
| **Complementary Cumulative Distribution Function** | |
| *(see Cumulative Distribution Function)* | The term complementary cumulative distribution function is a type of cumulative distribution function and is defined under "Cumulative Distribution Function." |
| **Completeness Uncertainty** | |
| *(see Uncertainty)* | The term completeness uncertainty is related to epistemic uncertainty and defined under "Uncertainty." |
| **Component** | |
| A part of a system in a facility. *(see Basic Event)* | In a QRVA, the facility is usually modeled at the component level. The ASME/ANS PRA Standard defines a component as "an item in a nuclear power plant, such as a vessel, pump, valve, or circuit breaker."<br>Basic events are associated with individual components, such that different basic events will be associated with different failure modes of a particular component. |
| **Conditional Acute Fuel Release Probability** | |
| *(see Conditional Probability)* | The term conditional acute fuel release probability is a type of conditional probability and is defined under "Conditional Probability." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Conditional Containment Failure Probability** | |
| *(see Conditional Probability)* | The term conditional containment failure probability is a type of conditional probability and is defined under "Conditional Probability." |
| **Conditional Probability (Acute Fuel Release)** | |
| Probability of occurrence of an event, given that a prior event has occurred. *(see Probability)* | In a QRVA, a conditional probability can be calculated for containment failure, and acute fuel release given the knowledge of a variety of prior events has occurred. Examples include:<br>• Conditional containment failure probability can be calculated given that a particular accident type has occurred.<br>• Conditional acute fuel release probability can be calculated given that an internal loss of fuel inventory control event has occurred, or given that a bypass sequence has occurred.<br>Conditional probability exists in other contexts. For example, seismic fragility is the conditional probability of a component, structure, or system failure given a seismic motion of a certain magnitude. |
| **Confidence Interval** | |
| A range of values that has a specified likelihood of including the true value of a random variable. *(see Uncertainty Interval)* | In a QRVA, a confidence interval is sometimes used to describe the uncertainty of a parameter input. However, confidence intervals cannot be propagated through the QRVA model. A confidence interval with a confidence level *p* is defined such that the probability that the true value of a random variable contained within that interval *p* can be stated with a specified likelihood. The confidence level can take a specified value, with the most common being 95% or 99%. The following figure shows a 95% confidence interval. In this case, 2.5% of the probability distribution is greater than the 95% confidence interval (shaded area under the probability distribution function curve), while 2.5% of the probability distribution is less than the 95% confidence interval.<br>  <br> |
| **Configuration Risk Profile** | |
| *(see QRVA Configuration Control)* | The configuration risk profile is related to configuration control and is defined under "QRVA Configuration Control." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Consequence** | |
| *(see Accident Consequence)* | In the context of a QRVA, the term consequence has the same meaning as accident consequence, which is defined under "Accident Consequence." |
| **Consequence Analysis** | |
| *(see Accident Consequence Analysis)* | In the context of a QRVA, the term consequence analysis has the same meaning as accident consequence analysis, which is defined under "Accident Consequence Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Conservative Analysis (Demonstrably)** | |
| An analysis that uses assumptions such that the assessed outcome is meant to be less favorable than the expected outcome. *(see Bounding Analysis)* | In a QRVA, conservative analysis may be performed to show that a certain contributor is not significant to risk, and thus, resources do not need to be spent on more accurate modeling. A conservative analysis provides a result that may not be the worst result of a set of outcomes, but produces a quantified estimate of a risk metric that is significantly greater than the risk metric estimate obtained by using the most realistic information obtainable (i.e., a realistic analysis). Therefore, in a QRVA, if there is not much change in risk with the contributor in question set at an unfavorable value (as opposed to its most favorable value), then the contributor can be omitted from the analysis. For example, a facility operator's request for change in technical specifications may show that the requested change will result in acceptable risk increases, even with pessimistic assumptions associated with the proposed change. If that is the case, then it may be acceptable not to perform a realistic assessment of the proposed change since it may involve detailed and time-consuming modeling. Conservative analysis also may be used to demonstrate that an item that is not modeled in the QRVA has negligible impact on risk and therefore can be justifiably neglected. A conservative analysis provides a result that may not be the worst result of a set of outcomes, but produces a quantified estimate of a risk metric that is significantly greater than the risk metric estimate obtained by using a best-estimate evaluation.<br><br>A conservative analysis should be distinguished from a bounding analysis in which assumptions and parameters are chosen such that the impact on risk is as detrimental as possible; therefore, bounding analysis is a special case of conservative analysis. For example, for a conservative analysis a human error probability event can be set to a value that is unlikely to be exceeded, whereas for a bounding analysis, the error probability would be set to 1.0. Conservative analyses, then, include a spectrum of assessments with results less favorable than those of realistic analysis all the way to bounding assessments with the most unfavorable results.<br><br>Examples of areas in which conservative analyses can be used in Level 1 risk assessments are initiating events, success criteria, thermal-hydraulics, and human error probabilities.<br><br>The terms conservative and demonstrably conservative are used interchangeably.<br><br>The definition is based on the ASME/ANS PRA Standard, which defines demonstrably conservative analysis as one "that uses assumptions such that the assessed outcome will be conservative relative to the expected outcome." |
| **Containment Building** | |
| *(see Containment)* | The term containment building has the same meaning as containment and is defined under "Containment." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Containment Bypass** | |
| A flow path that allows the unintended release of fuel directly to the environment, bypassing the containment. (see Containment Failure, Containment Isolation Failure, Interfacing Systems Loss-of-Fuel-Inventory-Control Accident) | In a QRVA, the potential for containment bypass is modeled and such a bypass often is determined to be a significant risk contributor. A containment bypass circumvents the containment's design function, which is to confine and reduce a release of fuel. Therefore, a containment bypass can lead to a significant release of fuel chemicals in the event of a loss of fuel inventory control accident. A containment bypass can result from the failure of various containment components so that a direct path to the environment is opened.<br>Containment bypass is distinct from containment isolation failure in which the containment is not acceptably leak-tight.<br>The definition provided is based on the definition found in the ASME/ANS PRA Standard. |
| **Containment Capacity** | |
| The ability of the containment to withstand the challenges that result from accidents. *(see Containment, Containment Capacity Analysis, Containment Pressure Boundary)* | In a Level 2 QRVA, the containment capacity is evaluated so that it can be compared against the postulated challenges to the containment that could result from a severe accident, both pre- and post-loss of fuel inventory control. As such, the containment performance in response to severe accident conditions can be assessed.<br>The containment capacity is the ability of the structures, systems, and components that make up the containment pressure boundary to withstand postulated loads and challenges. |
| **Containment Capacity Analysis** | |
| A calculation that estimates the ability of the containment to withstand the challenges that result from accidents. *(see Containment Capacity)* | In a Level 2 QRVA, the containment capacity analysis involves selecting a method or methods to evaluate the structural capacity to withstand challenges (e.g., high pressure, temperature, etc.) of the SSC that make up the containment pressure boundary. A facility-specific containment capacity analysis usually involves developing and solving a computer model of the relevant SSCs using finite element analysis or similar techniques. In the simplest case, the containment capacity can be inferred from that of a previously analyzed similar containment of a reference facility. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Containment Event Tree** | |
| A logic diagram that graphically represents the status of the containment and containment equipment when subjected to severe accident loads. *(see Accident Progression Event Tree, Event Tree)* | In a QRVA, a CET begins with the onset of loss of fuel inventory control and progresses through a limited number of branches that depict the various scenarios of the containment and containment equipment performance when subjected to severe accident loads (e.g., high temperatures, pressures).<br>As noted in NUREG-1150, an APET is a more detailed representation of the containment response to severe accident loads. The APET includes the interaction of phenomena, the availability of equipment, and the performance of operators.<br>The end states of both the CET and the APET are: no containment failure, various containment failure modes, or containment bypass. |
| **Containment Failure Mode** | |
| The various ways in which the ability of the containment to prevent fuel release is compromised. *(see Containment Failure, Containment Bypass, Containment Isolation Failure)* | In a QRVA, the modes of containment failure define the manner in which containment integrity is lost (i.e., the way a fuel release pathway from inside the containment to the environment is created). Containment failure mode encompasses both structural failures of containment induced by containment challenges when they exceed containment capability, as well as the failure modes of containment induced by human failure events, isolation failures, or bypass events.<br>The definition provided is based on the definition in the ASME/ANS PRA Standard. |
| **Containment Failure Probability** | |
| *(see Probability)* | The term containment failure probability is a type of failure probability that is computed based on the likelihood of containment failure and is discussed under the discussion for the term "Probability." |
| **Containment Failure (Early, Late)** | |
| Loss of integrity of the containment from a fuel release accident that is expected to result in an unacceptable release of fuel chemicals. *(see Containment, Containment Bypass,* Containment Pressure Boundary) | In a QRVA, determining when and if the containment fails or is bypassed during a severe accident is very important from a risk perspective. If the containment pressure boundary remains leak-tight, the offsite consequence will be low. Conversely, if the containment fails or is bypassed, then the consequence to the surrounding population and environment can be potentially high. For specific containments there can be selected severe accident scenarios in which the containment fails before fuel products have penetrated the primary system. If the accident is successfully arrested at this point, no release will occur. However, usually containment failure represents the failure of the final barrier preventing a fuel release.<br>Containment bypass failures (e.g., interfacing-system loss-of-fuel accidents) occur in the early timeframe but usually are categorized separately from early structural failures of the containment.<br>The definition is derived from the ASME/ANS PRA Standard. |

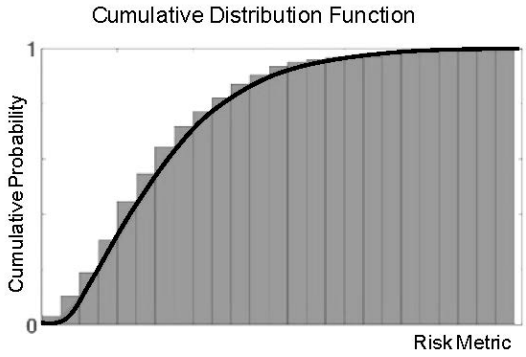
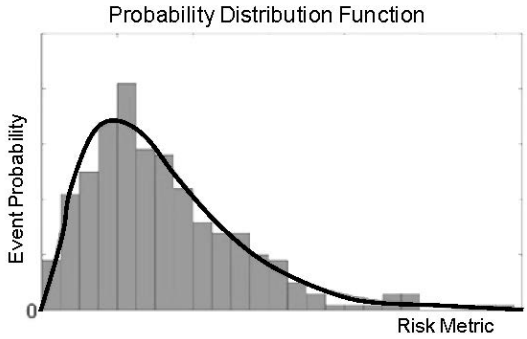
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Containment Integrity** | |
| The ability of the containment to function as a barrier to prevent release of fuel chemicals as a result of an accident. *(see Containment Failure Mode)* | In a Level 2 QRVA, an important concern is the potential loss of containment integrity. Containment integrity depends on the structures, systems, and components of the facility containment pressure boundary that perform the containment function. Maintaining containment integrity largely depends on the individual containment design and the particular phenomena or load that challenges the integrity of the containment. Examples of particular severe accident challenges to the containment integrity include overpressure, internal missiles, external missiles, burn-through, and bypass. |
| **Containment Isolation Failure** | |
| A failure in the piping, valves, or actuators that isolate the containment. *(see Containment Bypass, Containment Failure Mode)* | In a QRVA, containment isolation failures are one of the containment failure modes considered in a Level 2 analysis. Containment isolation is provided to prevent or limit the escape of fuel products that may result from postulated accidents. In a containment isolation failure, fuel chemicals can pass to the environment through the containment because the containment is not properly isolated (i.e., not acceptably leak-tight). |
| **Containment Pressure Boundary** | |
| Those parts of the facility containment that sustain loading and provide a pressure boundary in the performance of the containment function. *(see Containment)* | In a Level 2 QRVA, the evaluation of containment integrity is an evaluation of the structures, systems, and components of the facility containment pressure boundary that perform the containment function; i.e., that form the containment system. As stated in NUREG-0800, the facility containment system design must include the functional capability of enclosing the facility system and of providing a final barrier (boundary) against the release of radioactive fuel chemicals in case of postulated accidents.<br>Leak-tightness of the containment is ensured by a continuous pressure boundary consisting of nonmetallic seals and gaskets and metallic components that are either welded or bolted together. Each containment also includes numerous access and process penetrations that complete the pressure boundary.<br>The definition provided is derived from Chapter 6 of NUREG-0800. |
| **Containment Structure** | |
| *(see Containment)* | The term containment structure has the same meaning as containment and is defined under “Containment.” |

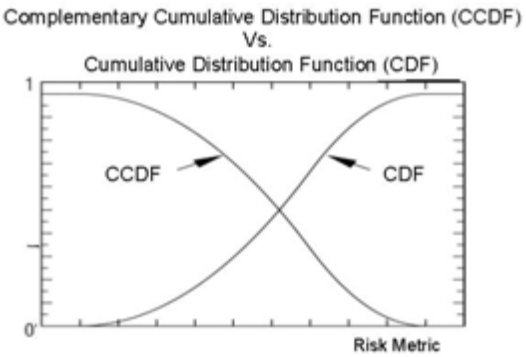
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Containment, Containment Building, Containment Structure** | |
| A physical structure surrounding a facility that is designed to prevent or control the release of fuel. *(see Containment Capacity, Containment Failure, Containment Failure Mode, Containment Integrity, Containment Pressure Boundary)* | In a Level 2 QRVA, the ability of the containment (containment building or containment structure) to contain fuel chemicals that have escaped from a fuel tank or associated piping is analyzed to estimate the limits of the containment's capacity.<br>A containment, containment building, or containment structure, in its most common usage, is a steel or reinforced concrete structure enclosing a facility designed to contain the escape of fuel to the environment. The containment is the final barrier to fuel release.<br>Containments are designed to remain intact when subject to the pressure and temperature loads from DBA. Moreover, because of safety factors built into containment designs, they are predicted to fail at pressures and temperatures (from loss of fuel inventory control accidents) that are significantly higher than those of DBAs. |
| **Cumulative Distribution Function (Complementary)** | |
| A function that provides the probability that a parameter is less than or equal to a given value. *(see Probability Distribution)* | In a QRVA, the cumulative distribution function is often used to present the results of the analysis.<br>The cumulative distribution function gives the probability that the random variable does not exceed a specified value. The cumulative distribution function is the integral of the probability distribution functions. The cumulative distribution function adds up the probabilities of occurrence of all possible parameter values less than the specified value, as represented by the probability distribution function of the parameter. The following graphs illustrate the cumulative distribution function and the probability distribution function. |

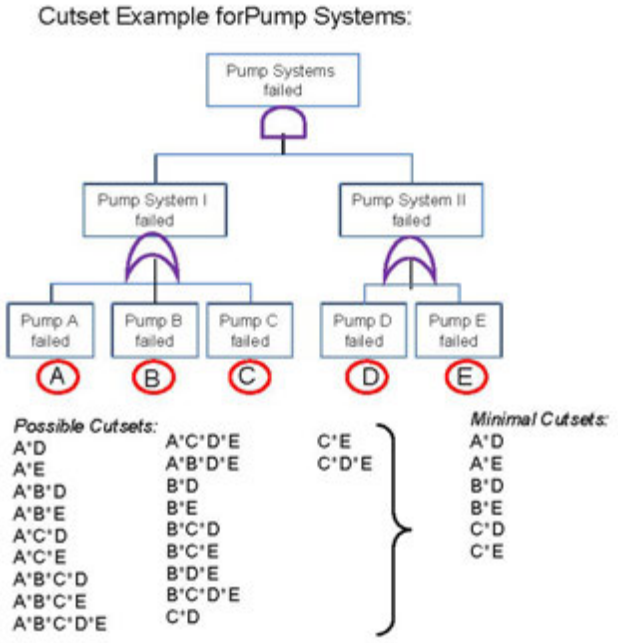
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| |  <br>  <br>The cumulative distribution function may be used to calculate the quantiles or the probability of not exceeding the mean of a risk metric.<br>Other examples of using the cumulative distribution function are calculation of the seismic fragility of a component, or the calculation of probability of recovery of offsite power within a certain time period.<br>NUREG/CR-6823 defines cumulative distribution function as one that "gives the probability that the random variable does not exceed a given value."<br>The complementary cumulative distribution function is the complement of the cumulative distribution function (i.e., the result of subtracting the cumulative distribution function from unity). Therefore, the complementary cumulative distribution function can be defined as a function that provides the probability that a parameter value is greater than a given value. The following graphs illustrate the complementary cumulative distribution function and its corresponding cumulative distribution function. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| |  <br>Some examples of using the complementary cumulative distribution function are calculating the probability of exceeding a certain release fraction of fuel release accidents, calculating the frequency of exceeding a certain intensity of external hazard occurrence, calculating the frequency of loss of offsite power events exceeding a certain duration, or calculating the probability of emergency diesel generator repair lasting longer than a certain time period.<br>The definition provided was based on the definition in NUREG/CR-6823. |
| **Cut Set (Minimal Cut Set)** | |
| A combination of failures that result in a particular outcome. *(see Truncation Limit)* | In a QRVA, a cut set (sometimes also written as "cut set") is the product (i.e., result) of the analysis and identifies a combination of failures that would result in loss of fuel inventory control or fuel release. However, the cut sets produced by the QRVA are minimal cut sets in which each minimal cut set is the smallest combination of failures needed to cause loss of fuel inventory control or fuel release.<br>Cut sets are expressed in the form of combinations of basic events. Basic events represent elements of the QRVA model for which no further decomposition is performed because they are at the limit of resolution consistent with available failure data. Basic events can represent equipment unavailability, human errors, and initiating events.<br>NUREG-1560 defines cut set as a "combination of a set of events (e.g., initiating event and component failures) that, if they occur, will result in an undesirable condition (such as the onset of fuel release)." In addition, NUREG-1560 defines the term "minimal cut set" as "the minimum combination of the set of events that would result in the undesirable condition."<br>The Fault Tree Handbook defines minimal cut set in the context of a fault tree as "a smallest combination of component failures which, if they all occur, will cause the top event to occur."<br>To illustrate the concept of a minimal cut set, consider an accident involving the combination of loss of offsite power, EDG failure, and electrically-driven emergency cooling pump failure: |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | • For this postulated accident, a "cut set" may include separate events that represent (1) failure of offsite power, (2) failure of all EDGs, and (3) independent failure of the electrically-driven emergency cooling pumps; however, this would represent a nonminimal cut set because the electrically-driven emergency cooling pumps rely on the EDGs. If the EDGs fail, the electrically-driven emergency cooling pumps will not function, regardless if they independently fail.<br>• For this accident, a "minimal cut set" would represent (1) failure of offsite power and (2) failure of all EDGs. These are the minimal failures required to cause failure of emergency cooling regardless if the electrically-driven emergency cooling pumps fail.<br>  |
| **Demonstrably Conservative Analysis** | |
| *(see Conservative Analysis)* | A demonstrably conservative analysis has the same meaning as a conservative analysis and is defined under "Conservative Analysis." |
| **Dependency** | |
| Reliance of a function, system, component, or human action on another part of the system or another human action to accomplish its function. | Dependency is significant to the fidelity of a QRVA model to capture the interrelationship between the modeled systems and human actions.<br>Dependency has also been defined as:<br>• "Requirement external to an item and upon which its function depends and is associated with dependent events that are determined by, influenced by, or correlated to other events or occurrences."<br>• "Requirement external to a SSC, and upon which the SSC's function depends." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Design-Basis Accident** | |
| A postulated accident that a facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety. (see Beyond-Design-Basis Accident, Severe Accident, Design-Basis Event) | In a QRVA, the accidents traditionally modeled are not DBA. Instead, the QRVA typically models accidents that are more severe than DBAs, which are referred to as BDBA or severe accidents. It is important, though, to distinguish that the term "severe accident" indicates that fuel release occurred; however, the term "beyond-design-basis accident" merely indicates that the accident exceeded the design limits of the facility.<br>When developing a facility, DBAs are selected to bound credible accident conditions and to ensure that the facility can withstand and recover from these accidents. An example of a DBA is a major rupture of a pipe containing fuel up to and including the double-ended rupture of the largest pipe containing fuel.<br>Another term, design-basis event (DBE), is used to broadly describe any event, internal or external to the facility, which could challenge safety functions. Therefore, DBAs are a subset of DBEs, and other examples of DBEs are anticipated transients, external events, and natural phenomena.<br>NUREG-0800, Standard Review Plan 15.0, defines design-basis accidents as "postulated accidents that are used to set design criteria and limits for the design and sizing of safety-related systems and components." |
| **Design-Basis Event** | |
| Any of the events specified in the facility's safety analysis that are used to establish acceptable performance for safety-related functions. (*see Design-Basis Accident, Severe Accident*) | In a QRVA, the outcome of concern is whether or not a particular accident leads to fuel release. Therefore, BDBA that exceed the design envelope and lead to fuel release are typically modeled. In this instance, these BDBAs that lead to fuel release are referred to as severe accidents. Because a facility is designed and engineered to contend with DBA they typically are not the focus of current QRVAs. However, DBAs represent only a portion of a broader category, DBE. DBEs represent conditions within the facility design envelope and include anticipated transients, AOO, DBAs, external events, and natural phenomena.<br>AOOs, an example of a DBE mentioned above, are a type of DBE described in NUREG-0800, Standard Review Plan 15.0, as "conditions of normal operation that are expected to occur one or more times during the life of the facility"; e.g., example loss of all offsite power.<br>DBAs are a subset of DBEs, as noted above. An example of a DBA is a major rupture of a pipe containing fuel up to and including the double--ended rupture of the largest pipe containing fuel.<br>The definition provided was based on the definition in NUREG-1560. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Deterministic (Analysis, Approach, Regulation)** | |
| A characteristic of decision-making in which results from engineering analyses, not involving probabilistic considerations, are used to support a decision. *(see Risk-Informed, Probabilistic)* | A QRVA represents an approach for assessing the likelihood of accidents and their potential consequences. However, the QRVA model cannot be separated from and depends on deterministic analyses. For example, success criteria for various systems used in QRVA to prevent and mitigate fuel release are based on deterministic analyses.<br>As discussed in SECY-98-144, a deterministic regulation assumes that adverse conditions can exist and establishes a specific set of design-basis events (i.e., what can go wrong?). The deterministic approach involves implied, but unquantified, elements of probability in the selection of the specific accidents to be analyzed as design-basis events. It then requires that the design include safety systems capable of preventing or mitigating the consequences (i.e., what are the consequences?) of those design-basis events to protect public health and safety.<br>The NRC Website Glossary defines the term deterministic as "consistent with the principles of 'determinism,' which hold that specific causes completely and certainly determine effects of all sorts. A deterministic approach or regulation is the opposite of a risk-informed approach or regulation in which the likelihood of potential accidents is integrated. Deterministic approaches or regulations do not account for likelihood, and thus do not incorporate risk results obtained from a QRVA. |
| **Deterministic Analysis** | |
| *(see Deterministic)* | The term deterministic analysis is defined under "Deterministic." |
| **Deterministic Approach** | |
| *(see Deterministic)* | The term deterministic approach is defined under "Deterministic." |
| **Deterministic Regulation** | |
| *(see Deterministic)* | The term deterministic regulation is defined under "Deterministic." |

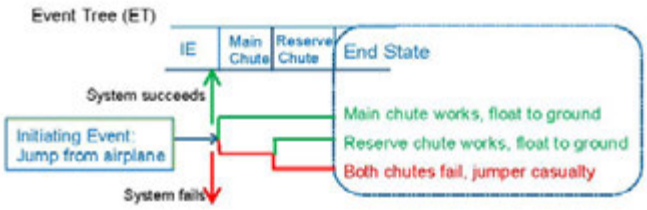
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Dynamic QRVA** | |
| A QRVA that accounts for time-dependent effects by integrating them directly into the computer model. *(see QRVA, Living QRVA)* | In a traditional QRVA, the coupling of deterministic analyses into the QRVA model is achieved by manually constructing the linkage between the probabilistic and deterministic models. Thus, the manner in which an accident evolves with time (i.e., time-dependent effects) is based on a set of system and operator response characteristics that are manually entered into the QRVA model. This is done by constructing event sequences in a discrete way such that they bound the contribution from all the scenarios that differ in the timing of the contributing events.<br>In contrast, a dynamic QRVA models accident sequences by automatically constructing the linkage between the probabilistic and deterministic models such that system and operator response characteristics are automatically accounted for in the QRVA model.<br>A dynamic QRVA is not the same as a living QRVA. In a living QRVA, the QRVA is updated as necessary to reflect changes in facility characteristics (e.g., design, operations) so that it continuously represents the as-built as-operated facility. |
| **Early Containment Failure** | |
| *(see Containment Failure)* | The term early containment failure is discussed under the discussion for the term “Containment Failure.” |
| **Early Fatality** | |
| *(see Fatality)* | The term early fatality is discussed under the discussion for the term “Fatality.” |
| **Early Fatality Risk** | |
| *(see Fatality)* | The term early fatality risk is a type of risk-involved fatality caused by exposure to fuel chemicals and is defined under “Fatality.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Economic Factors** | |
| The considerations taken into account when assessing costs related to a release of fuel chemicals to the environment. *(see Economic Impact)* | The Level 3 (or 4) portion of a QRVA assesses the injuries and economic losses that might result if fuel escaped from containment. The economic factors in assessing risk include the costs of various actions taken to protect the public from short-term and long-term exposure through different exposure pathways (e.g., evacuation, relocation, decontamination), the costs of health effects and health care following exposure, and secondary economic effects.<br>An illustrative list of required cost inputs from NUREG/CR-2300 includes:<br>• evacuation cost per person<br>• value of residential, business, and public areas per person<br>• relocation cost per person<br>• decontamination cost per acre for farm areas<br>• decontamination cost per person for residential, business, and public areas<br>• compensation rate per year for residential, business, and public areas (i.e., fraction of value)<br>• average value of farmland per acre for state, county, or smaller areas<br>• average annual value of farm sales per acre for state, county, or smaller areas<br>• miscellaneous information, such as seeding and harvesting month, fraction of land devoted to farming, and fraction of farm sales due to dairy production. |
| **Economic Impact** | |
| The incurred costs of evacuation and relocation of the population, the costs of land condemnation, and the cost of condemned crops and other farm products as a result of an accident. *(see Economic Factors)* | In a Level 3 (or 4) QRVA, in addition to the health effects on the surrounding population, the impact of the severe accident on the surrounding economy is often estimated. Therefore, the economic impact risk is one of the risk categories calculated in a Level 3 (or 4) QRVA.<br>The economic model in a Level 3 (or 4) QRVA includes the direct costs associated with protective actions taken after the accident, such as evacuation and relocation of the population, temporary or permanent interdiction of contaminated land and property, destruction of crops and foodstuffs. The model also may include other direct costs of actions, such as decontamination. Therefore, costs are a function of the stringency of post-accident fuel chemical protection measures. Other direct costs may include costs of treatment of individuals exposed to fuel. Some models may include indirect economic impacts (e.g., litigation costs, government spending for disaster relief, regional economic activity impacts). |

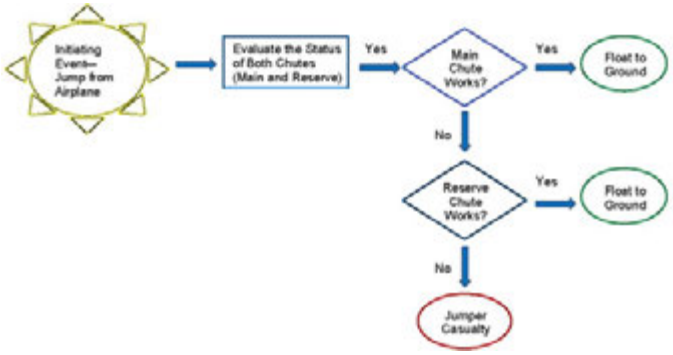
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Economic Impact Risk** | |
| *(see Economic Impact)* | The economic impact risk is the risk resulting from the economic impact of the accident and is defined in the discussion under "Economic Impact." |
| **Emergency Preparedness** | |
| The actions put into place to prepare personnel to rapidly identify, evaluate, and react to emergencies. *(see Emergency Response, Accident Mitigation)* | In a Level 3 or 4 QRVA, to credit an effective emergency response when calculating the consequences of postulated accidents, adequate emergency preparedness (EP) is assumed. EP includes the programs, plans, training, exercises, and resources necessary to prepare emergency personnel to respond to emergencies, including those arising from terrorism or natural events such as hurricanes. EP strives to ensure that facility operators can implement measures to protect public health and safety in the event of a fuel release emergency.<br>The definition provided is based on the definition in the NRC Website Glossary. |
| **Emergency Response** | |
| The actions initiated by the facility to mitigate the consequences of an accident that could potentially result in fuel chemicals release. *(see Emergency Preparedness, Accident Mitigation, Cohort)* | In a Level 3 or 4 QRVA, the emergency response is taken into account when calculating the consequences of the postulated accidents.<br>The emergency response encompasses the actions used to mitigate the consequences of an emergency to human health and safety, quality of life, property, and the environment. The feasibility of some emergency actions may be limited by the hazard type; e.g., seismic events.<br>The definition provided is based on the definition in the IAEA Safety Glossary. |
| **End State** | |
| A set of conditions selected to characterize the facility states at the end of a chain of events. *(see Accident Sequence)* | In most QRVAs, end states associated with Level 1 accident sequences typically include: success states (i.e., those states with negligible impact), and fuel release or facility damage states. End states associated with Level 2 sequences usually are containment failure modes or release categories.<br>The following figure illustrates different end states of an event tree:<br>  <br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |

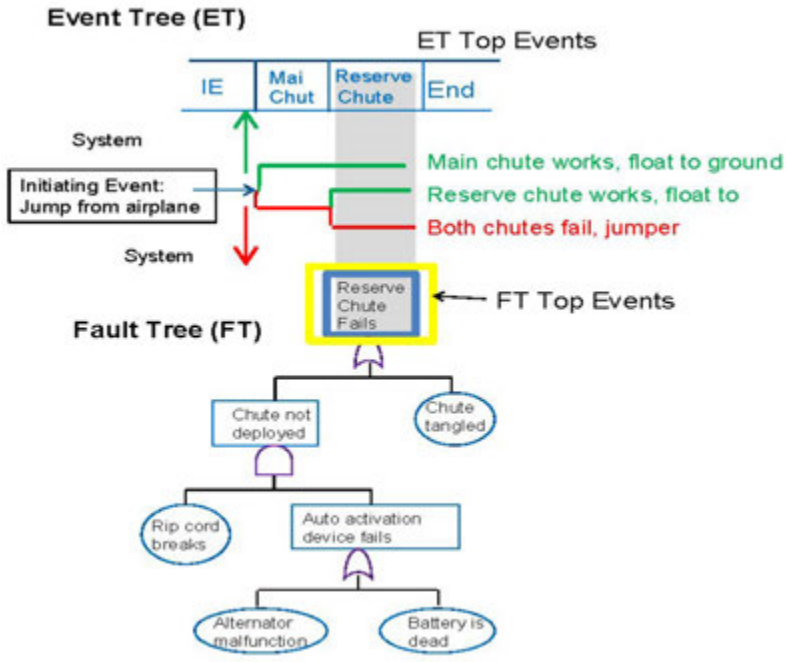
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Environmental Qualification** | |
| A process for demonstrating that equipment will be capable of withstanding the accident ambient conditions that could exist when functionality is required. | In most QRVAs, the focus is on severe accidents. The environment during a severe accident can be quite harsh and affect equipment performance. Safety equipment may experience high temperatures, pressures, humidity, and aerosol and particulate levels. The equipment may or may not be credited in the QRVA as continuing to function under these conditions for many hours. One issue is that the environmental qualification carried out for equipment in currently operating facilities is carried out for the ambient conditions expected for design-basis accidents, and these conditions are likely to differ from those encountered in a severe accident. 10 CFR 50.49 establishes requirements for environmental qualification for safety electric equipment important to safety for facilities.<br>The definition provided was based on the definition in the NRC Website Glossary. |
| **Epistemic Uncertainty** | |
| *(see Uncertainty)* | Epistemic uncertainty is a type of uncertainty and is defined under "Uncertainty." |
| **Error Factor (Human)** | |
| A measure of uncertainty associated with probability estimates. | In a QRVA, error factors are used to account for the uncertainty of the various parameters in the QRVA model, such as the probability associated with a component failure or human error event. The error factor is a measure of the spread of the distribution of a parameter in the calculation of these types of failure.<br>The term human error factor refers to the uncertainty in the probability of a human error. The probability of a human error event is often referred to as the human error probability.<br>From a mathematical perspective, when the uncertainty distribution for an event failure probability is characterized by the log-normal distribution, uncertainties on these probability estimates are expressed as error factors. The lognormal error factor is defined as the 95$^{th}$ percentile divided by the median (i.e., the 50$^{th}$ percentile). |
| **Event Scenario** | |
| *(see Accident Sequence)* | The term event scenario has the same meaning as accident sequence and is defined under "Accident Sequence." |
| **Event Sequence** | |
| *(see Accident Sequence)* | The term event sequence has the same meaning as accident sequence and is defined under "Accident Sequence." |
| **Event Sequence Analysis** | |
| *(see Accident Sequence Analysis)* | The term event sequence analysis is another way of describing an accident sequence and is defined under "Accident Sequence Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Event Sequence Class** | |
| *(see Accident Sequence Class)* | The term event sequence class has the same meaning as accident sequence class and is defined under "Accident Sequence Class." |
| **Event Sequence Diagram (ESD)** | |
| A flowchart that represents various accident scenarios that can occur as a result of a facility upset condition. *(see Event Tree, Top Event)* | In a QRVA, event sequence diagrams sometimes have been used to represent the progression of an initiating event by asking questions about successes and failures of facility responses to that initiating event. Each leg of the ESD ends with a successful or undesired end state for individual sequences. Once an ESD is developed, it can be mapped into an event tree, which relates more directly to a practical quantification of accident scenarios in a QRVA. However, in comparison to event trees, ESDs tend to include additional supporting details on facility design and operational information that illustrates why a branch in the event tree proceeds down a particular success path. In this regard, ESDs are related to event trees in that they can help document the assumptions used in constructing an event tree.<br>The following figure illustrates a simple ESD. The oval to the left corresponds to top events in the "jump from airplane" event tree.<br>  |
| **Event Sequence Group** | |
| *(see Accident Sequence Class)* | The term event sequence group has the same meaning as accident sequence group and is defined under "Accident Sequence Class." |
| **Event Sequence Type** | |
| *(see Accident Sequence Class)* | The term event sequence type has the same meaning as accident sequence type and is defined under "Accident Sequence Class." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Event Tree** | |
| A logic diagram that graphically represents the various scenarios that can occur as a result of an upset condition. (*see Accident Sequence, Containment Event Tree, Top Event, Accident Progression Event Tree, Bridge Tree)* | In a QRVA, event trees are used in various parts of the analysis:<br>• Level 1 event trees provide the facility response logic from the initiating event to the successful prevention of fuel release or fuel release end states.<br>• Bridge event trees often are used as the interface between the Level 1 event trees and Level 2 event trees, in that they define the initial conditions for the Level 2 analysis (i.e., facility damage states), based on the facility conditions when fuel release occurs.<br>• Level 2 event trees provide the facility response logic from the facility damage states to the successful prevention of containment failure or containment failure and release end states. In Level 2, these event trees are referred to as a containment event tree or accident progression event tree.<br>Event trees start with an initiating event and progress through questions about successes and failures of facility responses to that initiating event, ending with a successful or undesired end state for individual sequences. Individual sequences are pathways through the event tree.<br>An example of a simple event tree is shown below:<br>  <br><br>An event tree has also been defined as:<br>• "A logic diagram that begins with an initiating event or condition and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails. The progression arrives at either a successful or failed end state." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | • "An event tree graphically represents the various accident scenarios that can occur as a result of an initiating event; i.e., a challenge to facility operation. Toward that end, an event tree starts with an initiating event and develops scenarios, or sequences, based on whether a facility system succeeds or fails in performing its function. The event tree then considers all of the related systems that could respond to an initiating event, until the sequence ends in either a safe recovery or fuel release." |
| **Event Tree Sequence** | |
| *(see Accident Sequence)* | The term event tree sequence is a specific description of an accident sequence and is defined under "Accident Sequence." |
| **Event Tree Top Event** | |
| *(see Top Event)* | The term event tree top event is discussed under the discussion for the term "Top Event." An illustration of an event tree top event is shown under the discussion for the term "Event Tree." |
| **Exclusion Area Boundary** | |
| The boundary of the area surrounding the facility where the facility owner has the authority to determine all activities, including exclusion or removal of personnel and property. | QRVA consequence calculations usually are concerned with the consequences outside of the exclusion area boundary. The exclusion area is that area around the facility where public residence is not normally permitted. The exclusion area boundary is the inner edge of the low population zone. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Expert Elicitation** | |
| A formal, structured, and documented process in which judgments from expert(s) are obtained. *(see Expert Judgment*) | In a QRVA, expert elicitation may be used to obtain information from technical experts on topics that are uncertain. An expert elicitation is a process in which experts are assembled and their judgment is sought and aggregated in a formal way.<br>NUREG-1563 states, "Typically an elicitation is conducted to evaluate uncertainty. The uncertainty could be associated with: the value of a parameter to be used in a model; the likelihood and frequency of various future events; or the relative merits of alternative conceptual models. In each of these cases, the information regarding uncertainty would be represented by encoding the subjective probabilities from each subject-matter expert."<br>An expert elicitation is a more formal process than expert judgment. Expert judgment may be the opinion of one or more experts, whereas expert elicitation is a highly structured process in which the opinions of several experts are sought, collected, and aggregated in a very formal way.<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |
| **Expert Judgment** | |
| Information (or opinion) provided by one or more technical experts that is based on their experience and knowledge. *(see Expert Elicitation)* | In a QRVA, expert judgment is used when there is a lack of information. For example, if certain parameter values are unknown, or there are questions about phenomenology in accident progression, then expert judgment may be used. Expert judgment may be part of a structured approach, such as expert elicitation.<br>Obtaining expert judgment is not necessarily as formal as invoking an expert elicitation process. Expert judgment may be the opinion of one or more experts, whereas expert elicitation is a highly structured process in which the opinions of several experts are sought, collected, and aggregated in a very formal way.<br>NUREG-1563 states, "expert judgments may also be opinions that can be analyzed and interpreted, and used in subsequent technical assessments. Expert judgments can be either qualitative or quantitative. Expert judgments also can be judgments about uncertain quantities or judgments about value preferences."<br>The ASME/ANS PRA Standard defines expert judgment as "information provided by a technical expert, in the expert's area of expertise, based on opinion, or on an interpretation based on reasoning that includes evaluations of theories, models, or experiments." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Exposure** | |
| The state of being subjected to fuel chemicals. *(see Exposure Time, Inhalation, Ingestion, Skin Deposition, Health Effects)* | In a Level 3 or 4 QRVA, the offsite health effects resulting from exposure to fuel chemicals are considered. As stated in the NRC Website Glossary, exposure occurs through absorption of fuel chemicals because of an external source or an internal exposure caused by inhalation or ingestion of a fuel chemical. Acute exposure is a large exposure received over a short period of time. Chronic exposure is exposure received over a long period of time, such as during a lifetime. |
| **Exposure Pathways** | |
| The various means by which exposure to fuel chemicals occurs. *(See Inhalation, Ingestion, Skin Deposition, Health Effects)* | In a Level 3 or 4 QRVA, exposure pathways to an individual are assumed for the consequence calculations. Water immersion is a pathway by which external exposure is given to an individual immersed in contaminated water (e.g., by bathing or swimming); inhalation is the pathway by which internal exposure is given by breathing in contaminated air (resuspension inhalation is the pathway by which internal exposure is given to an individual from breathing resuspended fuel chemicals previously deposited on the ground); ingestion is the pathway by which internal exposure is given from consuming fuel-contaminated food or water; and skin deposition is exposure resulting from fuel chemicals deposited directly onto the surface of the body. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **External Event** | |
| The term external event is no longer used and has been replaced by the term external hazard. *(see Hazard)* | A full scope QRVA includes accidents resulting from both internal and external hazards. Internal hazards could include internal events, internal floods, and internal fires. External hazards could include seismic events, high winds, external floods, and other external hazards.<br>The no-longer-used term, external event, is defined in the ASME/ANS PRA Standard as "an event originating outside a facility that directly or indirectly causes an initiating event and may cause safety system failures or operator errors that may lead to loss of fuel inventory control or acute fuel release. Events such as earthquakes, tornadoes, and floods from sources outside the facility and fires from sources inside or outside the facility are considered external events. By historical convention, loss of offsite power not caused by another external event is considered to be an internal event."<br>Historically, the difference between an internal event and an external event was the equipment boundary. The internal event represented something that occurred "internal" to the boundary of the piece of equipment. Conversely, occurrences external to the equipment boundary but within the facility boundary were classified as external events. With time, the definition for internal hazards has come to encompass all the hazards within the facility boundary, not just within the equipment. Thus, the external events have changed to currently represent events that occur outside the facility boundary but can cause undesired outcomes or conditions leading to facility equipment damage. Loss of offsite power is still considered an internal event.<br>The term external event and external hazard have been used incorrectly interchangeably. The term external event is no longer used and has been subsumed by the term external hazard. |
| **External Flood** | |
| A flood initiated outside the facility boundary that can affect the operability of the facility. *(see Hazard, External Flood Analysis, Internal Flood)* | In a QRVA, external floods are a specific hazard group in which the flood occurs outside the facility boundary. The QRVA considers floods because they have the potential to cause equipment failure by the intrusion of water into facility equipment through submergence, spray, dripping, or splashing.<br>The definition provided was based on the definition in NUREG-1742. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **External Flood Analysis** | |
| A process used to assess potential risk from external floods. *(see Hazard Analysis, External Flood)* | In a QRVA, an external flood analysis quantifies the risk contribution as a result of an external flood. The analysis models the potential failures of facility systems and components from external floods, as well as random failures. Floods have the potential to cause equipment failure by the intrusion of water into facility equipment through submergence, spray, dripping, or splashing. The likelihood of an external flood is determined through an external flood hazard analysis, which evaluates the frequency of occurrence of different external flood severities. The frequency of the external flood is used as input to the model used to assess external flood risk. |
| **External Flood Fragility Analysis** | |
| *(see Fragility Analysis)* | The term external flood fragility analysis is a type of fragility analysis and is included in the discussion to the term "Fragility Analysis." |
| **External Flood Hazard Analysis** | |
| *(see Hazard Analysis)* | The term external flood hazard analysis is a specific type of hazard analysis and is defined under "Hazard Analysis." |
| **External Flood Facility Response Analysis/Model** | |
| *(see Facility Response Analysis/Model)* | The term external flood facility response analysis is a type of facility response analysis and is included under "Facility Response Analysis/Model." |
| **External Hazard** | |
| *(see Hazard)* | The term external hazard is related to the term hazard and is defined under "Hazard." |
| **External Hazard Analysis** | |
| *(see Hazard Analysis)* | The term external hazard analysis is a type of hazard analysis and is defined under "Hazard Analysis." |
| **Facility Configuration Control** | |
| The process of maintaining consistency between the physical condition of a facility and its associated design and engineering records. | A QRVA relies on facility configuration control to ensure that the as-built as-operated facility is accurately modeled. Without facility configuration control, uncertainty can be introduced about the extent to which the QRVA accurately reflects important characteristics of the facility; e.g., the design of facility SSCs.<br>Facility configuration control represents the process of identifying and documenting the characteristics (e.g., design or operating conditions) of facility SSCs, and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded, and incorporated into the facility documentation. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Facility Damage State** | |
| A group of accident sequence end states that share similar characteristics with accident progression, and containment or engineered safety feature operability. *(see Bin)* | In a Level 2 QRVA, the critical first step is developing a structured process for defining the specific accident conditions to be examined. Attributes have to be determined for binning the large number of accident sequences developed for Level 1 QRVA analysis into a practical number for detailed Level 2 analysis. Combinations of attributes of similar accident conditions define the facility damage states.<br>The definition provided is based on the definition in the ASME/ANS PRA Standard. |
| **Facility Hazard** | |
| (*see Hazard)* | The term facility hazard has the same meaning as hazard and is defined under "Hazard." |
| **Facility-Operating-State-Year** | |
| *(see Reactor-Year)* | The term reactor-operating-state-year is related to the term facility-year and is defined under "Facility-Year." |
| **Facility Operational Mode** | |
| *(see Facility Operational State)* | The term facility operational mode has the same meaning as facility operational state and is defined with "Facility Operational State." |
| **Facility Operational State, Facility Operational Mode** | |
| A particular facility configuration with specified operational characteristics. | The scope of the QRVA determines the various individual facility operating states that the QRVA model must include for the risk estimation results. The term facility operational state has the same meaning as facility operational mode. |
| **Facility Partitioning** | |
| The defining of the facility physical boundary affected by the flood and fire hazard and the segmenting of the physical boundary into smaller spatial units. | In a QRVA, facility partitioning is used in flood and fire evaluations to define the physical analysis units in terms of flood or fire areas and flood or fire compartments. In the ASME/ANS PRA Standard, the objective of facility partitioning for internal floods (referred to as internal flood facility partitioning) is to account for facility-specific physical layouts and separations in such a way as to identify in the QRVA facility areas where internal floods could lead to loss of fuel inventory control. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Facility Response Analysis, Facility Response Model (External Floods, Internal Fire, High Winds, Other External Hazard, Seismic)** | |
| The logic framework for identification and analysis of accident scenarios resulting from the effects of a hazard on the facility. | In a QRVA conducted to evaluate the effect of an external hazard group on the facility, or the effect of internal fires on the facility, facility response analysis usually involves modification of the internal events QRVA model. This modification includes the event trees and fault trees and the initiating event set. It involves identifying and selecting important initiating events, deleting unlikely events from event trees, deleting unimportant internal failures and human errors (from fault trees or event trees), modifying event tree logic to conform to event-specific procedures, and adding hazard event induced failure events and human errors (to fault trees and event trees). These modifications are performed when the facility response model is used in conducting an external flood, internal fire, high wind, seismic, or other external hazards analysis.<br>For example, in a seismic analysis, the initiating event is assumed to be a loss of offsite power. Recovery of offsite power is trimmed from the event trees. Seismic failures of structures and equipment are added and comparatively unimportant internal failures are trimmed. Human errors and their probabilities are adjusted. Mission time is extended, usually to 72 hours.<br>A simplified facility response model also can be constructed "from scratch" (ad hoc model), without starting with the internal events model.<br>Note that in an internal flood QRVA the facility response also is determined in a manner similar to that described above. The ASME/ANS PRA Standard states that the expected facility response(s) to the selected set of flood scenarios is determined, and an accident sequence, from the internal events at power QRVA that is reasonably representative of this response is selected for each scenario. |
| **Facility Response Model** | |
| *(see Facility Response Analysis)* | The term facility response model has the same meaning as facility response analysis and is defined under "Facility Response Analysis." |
| **Facility Risk Profile** | |
| *(see Risk Profile)* | The term facility risk profile has the same meaning as risk profile and is defined under "Risk Profile." |

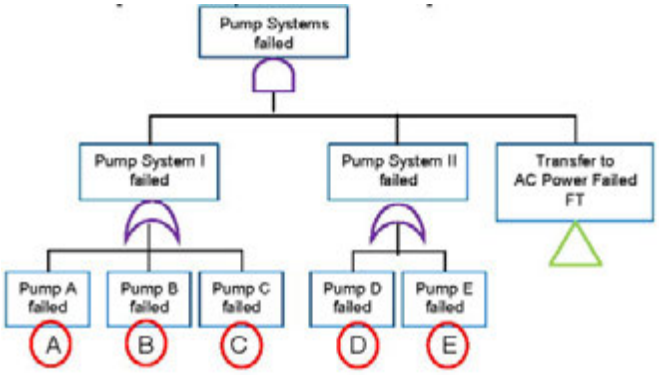
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Facility-Year (Facility-Operating-State-Year)** | |
| A unit of time by which risk parameters are measured in a QRVA. *(see Facility Operational State)* | In a QRVA, the terms facility-year and reactor-operating-state-year refer to units of time by which risk parameters (e.g., LOFICF, AFRF) are measured. The term facility-year assumes that more than one facility can operate during a year (e.g., a calendar year during which five facilities operated would be the experience equivalent of 5 facility-years).<br>For some applications, such as configuration risk management or analyses that compare specific risks during different modes of operation, it may be appropriate to develop risk metrics that consider the time period associated with a given facility operational state. On a more general basis, it could be considered to be per facility-operating-state-year. |
| **Failure Mechanism** | |
| The fault associated with a component that causes it to malfunction. *(see Failure Mode)* | In a QRVA, the concept of failure mechanism is used to explain the immediate cause of component failure. The fault that causes failure could be electrical, mechanical, chemical, physical, thermal, or human error. An example of a failure mechanism would be an electrical short in the electric motor winding that causes failure of a pump to start.<br>The ASME/ANS PRA Standard defines failure mechanism as "any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error."<br>While failure mechanism is a cause of failure, failure mode is the functional manifestation of failure; e.g., failure to start, failure to run. |
| **Failure Mode** | |
| The manner in which a component fails to perform its function. *(see Failure Mechanism, Failure Modes and Effects Analysis)* | In a QRVA, the failure modes of a component are represented as basic events, and while it is a visible manifestation of failure, it is distinguished from failure mechanism, which is a cause of failure. Failure of a component is distinguished by its failure mode. Each failure mode is modeled separately, with its own failure probability. Failure mode is failure in a distinct functionality of a component that is necessary for it to successfully operate (e.g., failure modes of a valve might be failure to open, failure to close, or inadvertent opening). Failure of a pump may be distinguished into two separate failure modes, namely failure to run or failure to start.<br>In a fire QRVA, spurious (unintended) operation is also defined as a failure mode.<br>The ASME/ANS PRA Standard defines failure mode as "a specific functional manifestation of a failure (i.e., the means by which an observer can determine that a failure has occurred) by precluding the successful operation of a piece of equipment, a component, or a system (e.g., fails to start, fails to run, leaks)."<br>A failure modes and effects analysis can be used to identify component failure modes and evaluate their effects on other components, subsystems, and systems. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Failure Modes and Effects Analysis** | |
| A process for identifying failure modes of specific components and evaluating their effects on other components, subsystems, and systems. *(see Failure Mode)* | In a QRVA, a failure modes and effects analysis generally is not used except to identify initiating events for a new facility design with no operational history or failure data. A FMEA is aimed at analyzing the effects of a single component or function failure on other components, systems, and subsystems. A FMEA can be useful in identifying initiating events that involve support system failures and the expected effects on the facility (especially on mitigating systems).<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |
| **Failure Probability** | |
| *(see Probability)* | The term failure probability is a specific type of probability and is defined under "Probability." |
| **Fatality (Early, Latent, Prompt, Latent Cancer)** | |
| Death occurring as a result of exposure to fuel chemicals. *(see Exposure, Quantitative Health Objectives)* | Depending on the amount of fuel chemical exposure and the duration over which it is received, early and latent fatalities can occur. The risk of incurring fatalities, both early and latent fatalities, is one of the most important outputs of a Level 3 or 4 QRVA.<br>Early fatalities, synonymous with prompt fatalities, are defined as deaths from the acute effects of fuel chemicals that may occur within a few months of the exposure. Latent cancer fatalities are defined as deaths from cancer caused by chronic effects of fuel chemical exposure; latent cancer fatalities may occur years after the exposure.<br>Prompt or early fatalities are usually the result of acute exposures (large exposure received over a short period of time). Latent fatalities resulting from cancer that became active after a latent period can result from exposure from early pathways (e.g., skin deposition), as well as long-term pathways; e.g., resuspension inhalation and ingestion. |
| **Fatality Risk (Early, Latent, Prompt)** | |
| *(see Fatality)* | The fatality risk (early or prompt fatality risk, latent fatality risk) is the risk involving fatalities caused by exposure to fuel chemicals and is defined in the discussion under "Fatality." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Fault Tree** | |
| A deductive logic diagram that graphically represents the various failures that can lead to a predefined undesired event. *(see Top Event, Event Tree)* | In a QRVA, fault trees are used to depict the various pathways that lead to a system failure.<br>Fault trees describe how failures of top events occur because of various failure modes of components, human errors, initiator effects, and failures of support systems that combine to cause a failure of a top event in the event trees.<br>A fault tree also has been defined as:<br>• "A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events."<br>• "A fault tree identifies all of the pathways that lead to a system failure. Toward that end, the fault tree starts with the top event, as defined by the event tree, and identifies …what equipment and operator actions, if failed, would prevent successful operation of the system. All components and operator actions that are necessary for system function are considered. Thus, the fault tree is developed to a point where data are available for the failure rate of the modeled component or operator action."<br>The following is an example of a fault tree diagram:<br>  |
| **Fault Tree Top Event** | |
| *(see Top Event)* | The term fault tree top event is a type of top event in a QRVA model and is defined under "Top Event." An illustration of a fault tree top event is shown under the discussion for the term "Event Tree." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Fire QRVA Facility Response Model (Analysis)** | |
| *(see Facility Response Analysis)* | The term fire QRVA facility response analysis is a type of facility response analysis and is defined under "Facility Response Analysis/Model."<br>The term fire QRVA facility response model is also a technical element for internal fires in the ASME/ANS PRA Standard whose objective is to identify the initiating events that can be caused by a fire event and develop a related accident sequence model, and to depict the logical relationships among equipment failures (both random and fire induced) and human failure events for LOFICF and AFRF assessment when combined with the initiating event frequencies. |
| **Fragility** | |
| The likelihood that a component, system, or structure will cease to function given the occurrence of a hazard event of a certain intensity. *(see Fragility Analysis, High Confidence of Low Probability of Failure, Fragility Curve)* | In a QRVA, fragility is a concept used in the evaluation of external hazards. The fragility of a component, system, or structure is generally calculated for seismic events, high wind events, and external flood events.<br>Since a given component may fail because of various mechanisms (e.g., seismic motion may cause anchor failure, structural failure, systems interactions), fragility can be calculated for each of these failure mechanisms, or the results can be presented for the dominant mechanism.<br>The ASME/ANS PRA Standard states, "fragility of a SSC is the conditional probability of its failure at a given hazard input level. The input could be earthquake motion, wind speed, or flood level." |
| **Fragility Analysis (External Flood, High Winds, Other External Hazards, Seismic)** | |
| Estimation of the likelihood that a given component, system, or structure will cease to function given the occurrence of a hazard event of a certain intensity. (see Fragility, Fragility Curve) | In a QRVA, fragility analysis identifies the components, systems, and structures susceptible to the effects of an external hazard and estimates their fragility parameters. Those parameters are then used to calculate fragility (conditional probability of failure) of the component, system, or structure at a certain intensity level of the hazard event. Fragility analysis considers all failure mechanisms due to the occurrence of an external hazard event and calculates fragility parameters for each mechanism. This is true whether the fragility analysis is used for an external flood hazard, fire hazard, high wind hazard, seismic hazard, or other external hazards. For example, for seismic events, anchor failure, structural failure, and systems interactions are some of the failure mechanisms that would be considered. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Fragility Curve** | |
| A graph that plots the likelihood that a structure, system or component will fail versus the increasing intensity of a hazard event. *(see Fragility, Fragility Analysis)* | In a QRVA, fragility curves generally are used in seismic analyses and provide the conditional frequency of failure for structures, systems, or components as a function of an earthquake-intensity parameter, such as peak ground acceleration. Fragility curves also can be used in QRVAs examining other hazards, such as high winds or external floods. |
| **Frequency (Accident Sequence, Initiating Event, Acute Fuel Release, Large Fuel Release, Fuel Chemicals Release)** | |
| The expected number of occurrences of an event or accident condition expressed per unit of time. (*see Probability)* | In a QRVA, a frequency is calculated for various events. For a Level 1 QRVA, frequencies are calculated for the initiating events and for the loss of fuel inventory control accident sequences; the latter frequencies are summed to provide an overall LOFICF. For a Level 2 QRVA, frequencies are calculated for the facility damage states and for the release of fuel chemicals; e.g., AFRF, large fuel release frequency, and the overall fuel chemicals release frequency. For a Level 3 or 4 QRVA, frequencies are calculated for accident consequences (i.e.; early and latent fatalities) and, sometimes, economic consequences.<br>Frequency is normally expressed in events per facility operating year or events per facility calendar year.<br>The subset terms of frequency can be defined as follows:<br>• Accident Sequence Frequency: The frequency associated with a series of events that follow from a particular initiating event, through system and operator responses, and ultimately to a well-defined end state, such as loss of fuel inventory control. *(see Accident Sequence)*<br>• Loss of Fuel Inventory Control Frequency: The sum of the accident sequence frequencies of those accident sequences whose end state is loss of fuel inventory control.<br>• Initiating Event Frequency: The frequency of an event originating from an internal or external hazard that both challenges normal facility operation and requires successful mitigation.<br>• Acute Fuel Release Frequency: The frequency of a rapid, unmitigated release of fuel chemicals from the containment to the environment that occurs before effective implementation of offsite emergency response, and protective actions, such that there is a potential for early health effects.<br>• Large Fuel Release Frequency: One informal definition for large fuel release frequency is the frequency of an unmitigated release of fuel chemicals from the containment to the environment that is of sufficient magnitude to cause severe health effects, regardless of its timing. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | • Fuel Chemicals Release Frequency: The frequency of the release of fuel chemicals from the containment to the environment. This may refer to the total frequency of all releases regardless of size or timing. The fuel chemicals release frequency may also be subdivided depending on the size and timing of the release. AFRF and large fuel release frequency are defined above. A small early fuel release frequency can be defined as the frequency of early releases of low enough magnitude to have minimum potential for early health effects. A small late release frequency can be defined as the frequency of late releases of low enough magnitude and with a long enough delay to have minimum potential for early health effects. A large late release frequency can be defined as the frequency of late releases that have sufficient magnitude to cause severe health effects, but which occur in a timeframe that allows effective emergency response and protective actions so that the offsite health effects will be significantly reduced compared to those of an acute fuel release.<br>In some instances, the terms frequency and probability are used interchangeably, but incorrectly. Unlike frequency, probability represents a unitless quantity. |
| **Frequentist Analysis, Frequentist Estimation, Frequentist Statistics** | |
| A type of data analysis that relies solely on actual occurrences of the event under consideration. *(see Bayesian Analysis)* | In a QRVA, frequentist analysis is only used when occurrences of an event are sufficiently abundant such that a reliable estimate of event probability can be expressed as the ratio of number of event occurrences to total number of occurrences in which the event could occur. In frequentist statistics, error probability can be calculated as the number of errors experienced over some number of tries divided by the number of tries.<br>In the frequentist approach, the probability of a random event is interpreted as the fraction of times that the event would occur, in a large number of trials.<br>In risk analysis, both frequentist and Bayesian analysis may be used, depending on whether occurrence data is sufficiently abundant.<br>The terms frequentist analysis, frequentist estimation, and frequentist statistics are used interchangeably. |
| **Frequentist Estimation** | |
| *(see Frequentist Analysis)* | The term frequentist estimation has the same meaning as frequentist analysis and is defined the same as the term “Frequentist Analysis.” |
| **Frequentist Statistics** | |
| *(see Frequentist Analysis)* | The term frequentist statistics has the same meaning as frequentist analysis and is defined the same as the term “Frequentist Analysis.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Frontline System** | |
| A system used to directly provide a safety function. *(see Support System)* | In a QRVA, frontline systems are modeled to help represent the ways in which a facility can prevent loss of fuel inventory control or prevent containment failure. The ASME/ANS PRA Standard defines a frontline system as "a system (safety or non-safety) that is capable of directly performing one of the accident mitigating functions modeled in the PRA."<br>In some references, the definition of a frontline system only includes safety-related systems. However, other definitions are more generalized to include the possibility that a frontline system can be a nonsafety system, such as the ASME/ANS PRA Standard definition cited above. |
| **Full-Scope QRVA** | |
| A QRVA that considers all the various challenges that could contribute to the risk posed by the facility to the health and safety of the public. (*see QRVA, Risk Metric*) | A full-scope QRVA generally only considers the reactor and associated systems and is comprised of three distinct parts, referred to as Levels. The full-scope QRVA includes a Level 1 (loss of fuel inventory control), Level 2 (fuel chemicals release) and Level 3 or 4 (consequences, generally to public health and safety, but can also include economic) QRVA.<br>Offsite risk metrics in the Level 3 or 4 portion may include both health effects and economic considerations brought about by the release of fuel chemicals. |
| **Fussell-Vesely Importance** | |
| *(see Importance Measure)* | The term Fussell-Vesely importance is one type of importance measure and is defined under "Importance Measure." |
| **General Transient** | |
| *(see Transient)* | The term general transient has the same meaning as transient and is defined under "Transient." |

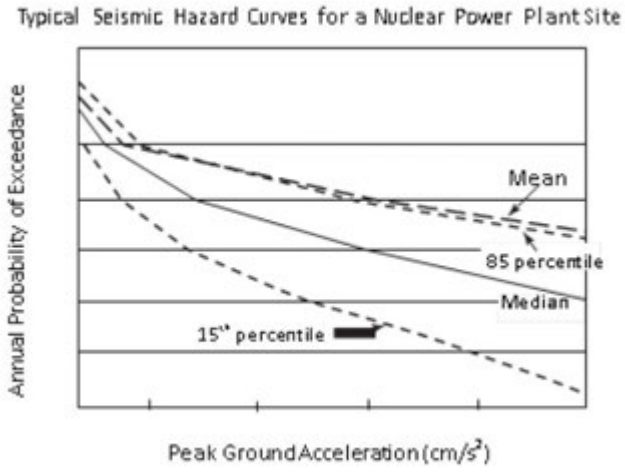
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Hazard (Type (Internal, External), Group, Event)** | |
| Anything that has the potential to cause an undesired event or condition that leads to equipment damage. *(see Hazard Analysis, Initiating Event)* | In a QRVA, there are three different uses of the term hazard as an adjective (the terms hazard and facility hazard tend to be correctly used interchangeably): types, groups, and events. The first, hazard type, classifies hazards as either internal or external to the facility. Within each hazard type, internal and external, there are subcategories, which are referred to as hazard groups. For internal hazards, this hazard group includes internal events, internal floods, and internal fires. For external hazards, this includes seismic events, high winds, external floods, and other external hazards. Finally, a hazard event represents the events brought about by the occurrence of the specified hazard. For example, those of interest in a QRVA are ones that directly or indirectly cause an initiating event and may further cause safety system failures or operator errors that may lead to loss of fuel inventory control or fuel chemicals release.<br>As defined in Regulatory Guide 1.200, a hazard group "is a group of similar causes of initiating events that are assessed in a PRA using a common approach, methods, and likelihood data for characterizing the effect on the plant."<br>A hazard event is described in terms of the specific levels of severity of impact that a hazard can have on the facility. The hazard event is an occurrence of the phenomenon that can result in a facility precursor to loss of fuel inventory control and result in the loss of a key safety function. The ASME/ANS PRA Standard states that there "is a range of hazard events associated with any given hazard, and, for analysis purposes, the range can be divided into bins characterized by their severity." An example of the overall concept of hazard, hazard event, and initiating event is as follows:<br>• Earthquakes are a hazard;<br>• 0.1g, 0.3g, 0.5g earthquakes and their associated spectral shapes and time histories may be defined as hazard events.<br>The ASME/ANS PRA Standard defines a hazard as an event or a natural phenomenon that poses some risk to a facility. Internal hazards include events such as equipment failures, human failures, and flooding and fires internal to the facility. External hazards include events such as flooding and fires external to the facility, tornadoes, earthquakes, and aircraft crashes. |
| **Hazard Analysis (External, External Flood, High Wind, (Probabilistic) Seismic, Other Hazards)** | |
| A process used to assess potential facility challenges, including natural phenomena, and to assess their likelihood, typically | In a QRVA, it is important to identify and characterize the nature and causes of specific types of hazards. A hazard represents an event or a natural phenomenon that poses some challenge to a facility. Examples of external hazards typically evaluated in a QRVA include external floods, high winds, seismic events, and external fires. A hazard analysis is used to evaluate the frequency of occurrence of different severities for the hazard being analyzed. Results from the |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| as a function of severity. | hazard analysis are used as input to the QRVA, which subsequently examines the hazards with respect to risk.<br>Listed below are specific types of hazard analyses:<br>• External hazard analysis: The objective is to evaluate the frequency of occurrence of different severities or intensities of external events or natural phenomena (e.g., external floods or high winds).<br>• External flood hazard analysis: The objective is to evaluate the frequency of occurrence of different external flood severities.<br>• High wind hazard analysis: The objective is to evaluate the frequency of occurrence of different intensities of high winds.<br>• (Probabilistic) seismic hazard analysis: A seismic hazard analysis expresses "the seismic hazard in terms of the frequency of exceedance for selected ground motion parameters during a specified time interval. The analysis involves identification of earthquake sources, evaluation of the regional earthquake history, and an estimate of the intensity of the earthquake-induced ground motion at the site. As stated in Regulatory Guide 1.200: "at most sites, the objective is to estimate the probability or frequency of exceeding different levels of vibratory ground motion" The term probabilistic seismic hazard analysis is similar in meaning to the definition of seismic hazard analysis as stated above.<br>• Other hazards analysis: Evaluates the frequency of occurrence of different intensities of other internal or external hazards (e.g., external fires).<br>The ASME/ANS PRA Standard defines hazard analysis as "the process to determine an estimate of the expected frequency of exceedance (over some specified time interval) of various levels of some characteristic measure of the intensity of a hazard (e.g., peak ground acceleration to characterize ground shaking from an earthquake). The time period of interest is often taken as 1 year, in which case the estimate is called the annual frequency of exceedance."<br>An example of a hazard curve is shown below. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| |  |
| **Hazard Event** | |
| *(see Hazard)* | The term hazard event is related to the term hazard and is defined under "Hazard." |
| **Hazard Group** | |
| *(see Hazard)* | The term hazard group is related to the term hazard and is defined under "Hazard." |
| **Hazard Type** | |
| *(see Hazard)* | The term hazard type is related to the term hazard and is defined under "Hazard." |
| **Health Effects** | |
| The effects of fuel chemicals on the health and safety of exposed individuals. *(see Quantitative Health Objectives, Accident Consequence, Exposure Time, Land Contamination)* | In a Level 3 or 4 QRVA, the health effects represent the main component of the calculated risk. Health effects from fuel chemicals usually are distinguished as acute or latent.<br>Acute health effects are adverse health symptoms (e.g., fatalities) occurring within a short time (days or months rather than years) of an exposure to large fuel releases. Acute fatalities and injuries are expected to occur within 1 year of an accident or sooner.<br>Latent health effects refer to cancer deaths that may occur with a considerable latency period, from approximately 2 to 25 years, depending on the type of cancer involved.<br>Public health effects refer to illnesses or fatalities to the population beyond the site boundary resulting from the release of fuel chemicals. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **High Confidence of Low Probability of Failure** | |
| A measure of seismic capacity of a structure, system, or component, expressed in terms of a threshold earthquake intensity, below which failure of the structure, system, or component is highly unlikely. *(see Seismic Margin, Fragility)* | In a seismic QRVA, the high confidence in low probability of failure measure is generally not used, but it is a key parameter primarily in a seismic margin analysis.<br>The HCLPF capacity is a measure of the seismic capacity of a SSC or of the whole facility. It indicates an earthquake intensity level at which there is high (95%) confidence the conditional probability of failure of the SSC is low (5% or less). At the facility level, HCLPF can refer to the peak ground acceleration level at which there is a high (95%) confidence of low (5%) conditional probability of loss of fuel inventory control. It is used extensively in a seismic margin analysis.<br>The ASME/ANS PRA Standard states that "HCLPF capacity: refers to the High Confidence of Low Probability of Failure capacity, which is a measure of seismic margin." |
| **High-Level Requirements** | |
| The minimum requirements for a technically acceptable baseline QRVA, independent of application. *(see Supporting Requirements)* | For a base QRVA, NRC Regulatory Guide 1.200 defines a set of technical characteristics and associated attributes that make it technically acceptable. One approach to demonstrate a QRVA is acceptable is to use a national consensus QRVA standard, supplemented to account for the NRC staff's regulatory positions. The ASME/ANS PRA Standard is one example of a national consensus QRVA standard. The ASME/ANS PRA Standard uses high-level requirements and supporting requirements.<br>Regulatory Guide 1.200 states, "Technical requirements may be defined at two different levels: (1) high-level requirements and (2) supporting requirements. High-level requirements are defined for each technical element and capture the objective of the technical element. These high-level requirements are defined in general terms, need to be met regardless of the level of analysis resolution and specificity (capability category), and accommodate different approaches. Supporting requirements are defined for each high-level requirement. These supporting requirements are those minimal requirements needed to satisfy the high-level requirement."<br>The ASME/ANS PRA Standard states, "The high level requirements are defined in general terms and present the top level logic for the derivation of more detailed supporting requirements. The high level requirements reflect not only the diversity of approaches that have been used to develop the existing PRAs, but also the need to accommodate future technological innovations."<br>The definition provided was based on the definition in the introduction section of ASME/ANS PRA Standard. |
| **High-Wind Fragility Analysis** | |
| *(see Fragility Analysis)* | High-wind fragility analysis is a type of fragility analysis and is included in the discussion under "Fragility Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **High-Wind Hazard Analysis** | |
| *(see Hazard Analysis)* | The term high-wind hazard analysis is a specific type of hazard analysis and is defined under "Hazard Analysis." |
| **High-Wind Facility Response Analysis/Model** | |
| *(see Facility Response Analysis/Model)* | The high-wind facility response analysis is a type of facility response analysis and is included in the discussion under "Facility Response Analysis/Model." |
| **High Winds** | |
| Winds of a certain size that could potentially damage or affect the operability of a facility. *(see Hazard)* | In a QRVA, the typical high winds analyzed as a hazard include the following: tornadoes, hurricanes (or cyclones or typhoons as they are known outside of the United States), extratropical (thunderstorm) winds, and other wind phenomena depending on the site location. High winds are a hazard group and, more specifically, a type of external hazard. |
| **Human Action (Operator Action)** | |
| An action performed by facility personnel. *(see Human Failure Event*, *Human Reliability Analysis)* | In a QRVA, the human actions that are modeled include those actions that facility personnel might fail to perform or might fail to perform correctly. Facility personnel interact with the facility in a number of ways. For example, maintenance personnel perform surveillance tests, calibrate equipment, and repair failed equipment. Control room operators control the facility and, after an initiating event, bring the facility to a safe stable state using as guidance written or memorized procedures. These actions are of concern for the QRVA because failure to perform any of the actions correctly can lead to a reduced capability of responding to a transient or accident. For example, failure to restore a system following maintenance can lead to its unavailability to perform its function when called upon. Failure of the control room crew to correctly follow their procedures might lead to a loss of a critical safety function.<br>A human action and an operator action do not necessarily mean the same thing. A human action can be performed by different types of facility personnel, while an operator action is an action performed by a formally qualified individual in the control room.<br>Human actions are an important component in conducting an HRA. HRA is used to support the development of a QRVA by identifying relevant human actions and the associated human errors that might occur. Human errors modeled in the QRVA are referred to as human failure events. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Human Error (Operator Error)** | |
| Any human action, including inaction, which exceeds some limit of acceptability, excluding malevolent behavior. (see Human Failure Event, Human Reliability Analysis) | In a QRVA, human (operator) errors are modeled in the QRVA as human failure events if they are unrecovered and lead to the failure or unavailability of a component, system, or function. Human errors of interest are those that result in the unavailability of a component, system, or function, or a failure to initiate, terminate, or control a system or function that can affect an accident sequence.<br>A human error and an operator error do not necessarily mean the same thing. A human error can be attributed to different types of facility personnel, while an operator error is specifically attributed to a formally qualified individual (i.e., operator) in the control room.<br>Human reliability analysis is used to identify the possible human errors that might occur. The term human failure event is synonymous with and has replaced the term human error in the QRVA lexicon.<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |
| **Human Error Event** | |
| *(see Human Failure Event)* | A human error event is a type of human error modeled in a QRVA and is defined under "Human Failure Event." |
| **Human Error Factor** | |
| *(see Error Factor)* | A human error factor is a specific type of error factor applicable to human reliability analysis and is defined under "Error Factor." |
| **Human Error Probability** | |
| *(see Probability)* | A human error probability is a specific type of probability applicable to human reliability analysis and is defined under "Probability." |
| **Human Failure Event, Human Error Event** | |
| A basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action. *(see Human Action, Human Error)* | In a QRVA, potential human errors (i.e., human actions or inappropriate human actions) are modeled as basic events. The term human failure event is synonymous with and has replaced the term human error in the QRVA lexicon.<br>Human failure events can be classified as either errors of omission or errors of commission. An error of omission would be failure to perform a system-required task or action. An error of commission would be incorrectly performing a system-required task or action, or performing an extraneous task that is not required and could contribute to component, system, or function failure or unavailability. In the QRVA, failures to restore a function, referred to as recovery, are also modeled as human failure events.<br>The terms human failure event and human error event have the same meaning in a QRVA context and it is correct and appropriate to use them interchangeably.<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Human Reliability Analysis** | |
| A structured approach used to identify potential human failure events and to systematically estimate the probability of those events using data, models, or expert judgment. *(see Human Action, Human Error)* | In a QRVA, a human reliability analysis is used to identify relevant human actions and possible human errors that might occur. Human actions considered in the human reliability analysis include those actions that facility personnel might fail to perform or might fail to perform correctly. Failure to correctly perform certain human actions can lead to a reduced capability of responding to a transient or accident, including the loss of one or more critical safety functions. The failure to correctly perform a human action is referred to as a human error.<br>The definition provided was based on the definition in the ASME/ANS PRA Standard. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Importance Measure (Risk Reduction Worth, Risk Achievement Worth, Fussell-Vesely, Birnbaum Importance, Uncertainty Importance)** | |
| A metric that provides either the absolute or relative contribution of a component, system, structure, or human action to the defined risk. | In a QRVA, importance measures are used to determine the contribution of the basic events to a number of risk metrics, such as LOFICF. By using importance measures, the QRVA analyst can determine the risk-significance of SSCs or human actions. Different importance measures provide different perspectives. For example, importance measures can evaluate the risk-reduction potential of improving SSC performance or human action, or they can show the significance of an SSC or human failure event for maintaining the current risk level. There are five importance measures typically used in a QRVA:<br>• Risk Reduction Worth: As defined in NUREG/CR-3385, risk reduction worth is: "The decrease in risk if a plant feature (e.g., system or component) were assumed to be optimized or were assumed to be made perfectly reliable. Depending on how the decrease in risk is measured, the risk reduction worth can either be defined as a ratio or an interval."<br>• Risk Achievement Worth: The increase in risk if a plant feature (e.g., system or component) was assumed to be failed or was assumed to be always unavailable. Depending on how the increase in risk is measured, the risk achievement worth can either be defined as a ratio or an interval. Sometimes risk achievement worth is referred to as "risk increase."<br>• Fussell-Vesely: For a specified basic event, Fussell-Vesely importance is the relative contribution of a basic event to the calculated risk. This relative or fractional contribution is obtained by determining the reduction of the risk if the probability of the basic event to zero.<br>• Birnbaum Importance (Bi): NUREG-1489 defines Birnbaum importance as: "An indication of the sensitivity of the accident sequence frequency to a particular basic event." Bi measures the change in total risk as a result of changes to the probability of an individual basic event.<br>• Uncertainty Importance: The uncertainty in each input parameter, as expressed through its probability distribution, contributes to the uncertainty in the output parameter of interest (e.g., LOFICF). The uncertainty importance measure attempts to quantify the contribution of each individual basic event's uncertainty to this total output uncertainty. The uncertainty importance is the Birnbaum importance multiplied by the standard deviation of the input probability distribution. |
| **Important to Safety** | |
| *(see Safety Significant)* | The term important to safety has a safety connotation and is defined under "Safety Significant." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Incremental Conditional Probability (Loss of Fuel Inventory Control, Acute Fuel Release)** | |
| A measure of the impact of a temporary facility modification on the probability of an undesired end state. *(see Conditional Probability,* Instantaneous Conditional Probability). | As applied to QRVA and facility risk evaluations, the term incremental conditional probability refers to the change in the probability of an undesired facility end state attributable to (conditional on) a temporary modification in facility configuration or operations, over the time that the modification is in place. Usually, this incremental change in conditional probability is reflected as an increase in the probability of an undesired end state such as loss of fuel inventory control when compared to the baseline loss of fuel inventory control probability. Because the probability of loss of fuel inventory control depends on the temporary modification or change at the facility, it is therefore a conditional probability.<br>Incremental conditional probability also is calculated in a QRVA for acute fuel release. Incremental conditional probability differs from instantaneous conditional probability in that instantaneous conditional probability represents the probability that an undesired facility end state is reached given an initiating event and the actual (instantaneous) facility configuration. The incremental conditional probability is integrated over the duration of the temporary condition, while the instantaneous conditional probability represents a point-in-time measure. |
| **Ingestion** | |
| Exposure from intake of food and water contaminated with fuel chemicals. *(see Exposure Pathways, Exposure, Exposure Time, Cloudshine, Water Immersion, Groundshine, Inhalation, Skin Deposition, Health Effects)* | In a Level 3 or 4 QRVA, for the consequence calculation ingestion is one of the assumed pathways by which an individual can receive chemical exposures. The pathways of exposure include:<br>• direct exposure from fuel chemicals in contaminated water given to an individual immersed in the water,<br>• exposure from inhalation of fuel chemicals in a cloud and resuspended material deposited on the ground,<br>• exposure to fuel chemicals deposited on the ground<br>• fuel chemicals deposited onto the body surfaces (skin deposition), and<br>• ingestion from deposited fuel chemicals that make their way into the food and water pathway. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Inhalation** | |
| Exposure from breathing fuel chemicals. *(see Exposure Pathways, Water Immersion, Ingestion, Skin Deposition)* | In a Level 3 or 4 QRVA, for the consequence calculation inhalation is one of the assumed pathways by which an individual can receive chemical exposures. The pathways of exposure include:<br>• direct exposure from fuel chemicals in contaminated water given to an individual immersed in the water,<br>• exposure from inhalation of fuel chemicals in a cloud and resuspended material deposited on the ground,<br>• exposure to fuel chemicals deposited on the ground,<br>• fuel chemicals deposited onto the body surfaces (skin deposition), and ingestion from deposited fuel chemicals that make their way into the food and water pathway. |
| **Initiating Event, Initiator** | |
| An event that perturbs the steady-state operation of the facility and could lead to an undesired facility condition. | In a QRVA, an initiating event is an event originating from an internal or external hazard that both challenges normal facility operation and requires successful mitigation. As such, these events represent the beginning of accident sequences modeled in the QRVA. Having a reasonably complete set of initiating events is crucial in determining what events could propagate to loss of fuel inventory control.<br>Initiating events can arise from the following:<br>• Internal Hazards, which include:<br>- Internal event (*see Internal Event*)<br>- Floods (see Internal Flood)<br>- Fires (see Appendix A for fire terms)<br>• External Hazards, which include:<br>- Floods (see External Flood)<br>- High winds (see High Winds)<br>- Seismic events (see Hazard Analysis)<br>- Other external hazards<br>These hazards result in different types of initiating events. Examples of initiating events are transients and fuel containment system leaks or ruptures.<br>The terms initiating event and initiator are both used in a QRVA context and generally have the same meaning. In some cases, the term initiator may refer to a class of initiators (e.g., transient), while the term initiating event may refer to the actual event. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Initiating Event Analysis** | |
| The process used to identify events that perturb the steady-state operation of the facility and could lead to an undesired facility condition. *(see Initiating Event, Master Logic Diagram [MLD])* | In a QRVA, the initiating event analysis considers how accidents can start by identifying and quantifying those events that challenge facility operation and require successful mitigation to prevent loss of fuel inventory control from occurring. To facilitate the efficient modeling of potential accidents, initiating events typically are identified using a systematic process (e.g., master logic diagram) and grouped according to their mitigation requirements. The frequencies of these initiating event groups are then quantified. |
| **Initiating Event Frequency** | |
| *(see Frequency)* | The term initiating event frequency is a type of frequency that is defined under "Frequency." |
| **Initiator** | |
| *(see Initiating Event)* | The term initiator is similar in meaning to initiating event and is defined under "Initiating Event." |
| **Instantaneous Conditional Probability (Loss of Fuel Inventory Control, Acute Fuel Release)** | |
| Event probability at the specific time the facility is analyzed, given that a prior event has occurred. (see Conditional Probability, Incremental Conditional Probability) | Using a QRVA, instantaneous conditional probability can be calculated for loss of fuel inventory control and acute fuel release. The probability of either of those undesired outcomes occurring depends on the occurrence of an initiating event while the facility is in a given configuration. Thus, loss of fuel inventory control or acute fuel release is "conditional" on the probability of a prior event occurring.<br>The following are other definitions that could describe instantaneous conditional probability:<br>• The probability that an undesired facility end state is reached given an initiating event and the actual (instantaneous) facility configuration.<br>• The average probability that an undesired facility end state is reached, weighted over all credible initiating events, for the actual (instantaneous) facility configuration.<br>Instantaneous conditional probability differs from incremental conditional probability in that incremental conditional probability represents the impact of a temporary facility modification on the probability of an undesired end state. The incremental conditional probability is integrated over the duration of the temporary condition, while the instantaneous conditional probability represents a point-in-time measure. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Internal Event** | |
| Failure of equipment as a result of either an internal random cause or a human event which perturbs the steady-state operation of the facility and could lead to an undesired facility condition. *(see Hazard)* | In a QRVA, internal events result from or involve random mechanical, electrical, structural, or human failures within the facility boundary and are a specific hazard group. The ASME/ANS PRA Standard has been revised and internal flood and internal fire are not considered internal events. |
| **Internal Fire** | |
| A fire initiated within the facility that can affect the operability of the facility. *(see Hazard and Appendix A)* | In a QRVA, internal fires are a specific hazard group in which the fire occurs within the facility boundary. The QRVA considers fires because they have the potential to cause equipment failure by direct flame impact or high thermal radiation. |
| **Internal Flood, Internal Flooding Event** | |
| A flood initiated within the facility that can affect the operability of the facility. *(see Hazard, External Flood)* | In a QRVA, internal floods are a specific hazard group in which the flood occurs within the facility boundary. The QRVA considers floods because they have the potential to cause equipment failure by the intrusion of water into facility equipment through submergence, spray, dripping, or splashing.<br>The term internal flooding event represents the occurrence of an internal flood. |
| **Internal Flooding Event** | |
| *(see Internal Flood)* | The term internal flooding event is the occurrence of an internal flood and is defined under “Internal Flood.” |
| **Internal Hazard** | |
| *(see Hazard)* | The term internal hazard is a specific type of hazard and is defined under “Hazard.” |
| **Key Assumption** | |
| *(see Assumption)* | The term key assumption is a specific type of assumption and is defined under “Assumption.” |
| **Key Model Uncertainty** | |
| *(see Uncertainty)* | The term key model uncertainty is a type of uncertainty and is defined under “Uncertainty.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Key Source of Model Uncertainty** | |
| *(see Uncertainty)* | The term key source of model uncertainty is defined under "Uncertainty." |
| **Key Source of Uncertainty** | |
| *(see Uncertainty)* | The term key source of uncertainty is defined under "Uncertainty." |
| **Land Contamination** | |
| Contamination of land outside of the facility site boundary with fuel chemicals released in an accident. *(see Health Effects)* | In a Level 3 or 4 QRVA, land contamination often is evaluated along with health effects.<br>Land contamination refers to the fuel chemicals deposited on the ground.<br>Land contamination risk involves the frequency and amount of land contamination and its associated cost. |
| **Land Contamination Risk** | |
| *(see Land Contamination)* | Land contamination risk is sometimes calculated in a Level 3 or 4 QRVA and is defined in the discussion under "Land Contamination." |
| **Large Late Release** | |
| *(see Fuel Chemicals Release)* | The term large late release is a type of fuel chemicals release and is defined in the discussion under "Fuel Chemicals Release." |
| **Large Late Release Frequency** | |
| *(see Frequency)* | The term large late release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency." |
| **Large Late Release Frequency Analysis** | |
| *(see Fuel Chemicals Release Frequency Analysis)* | The term large late release frequency analysis is a type of fuel chemicals release frequency analysis and is defined under "Fuel chemicals Release Frequency Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Large Release** | |
| *(see Fuel Chemicals Release)* | The notion of a large release implies that in the range of possible releases there exists a threshold value that distinguishes large releases from not large releases. Many QRVAs include their own specific definitions of a large release, but no universally accepted definition has been established. Attempts have been made to define a large release magnitude based on offsite health effects. There is an inherent arbitrariness in definitions since offsite health effects depend not only on release magnitude but also on site-specific parameters, such as population. Therefore, what would be a large release at one site would not necessarily be one at another site. Weather and wind variability are other site-specific factors.<br>In the past, regulators have considered several alternate definitions of a large release. These include:<br>• A release that would result in one or more early fatalities;<br>• A release that has the potential to result in one early offsite fatality within 1 mile of the facility boundary;<br>• A definition of a large release source term in the traditional form of a fractional release of the fuel inventory.<br>• Any release from an event that involves severe loss of fuel inventory control, primary system pressure boundary failure, and early containment failure. |
| **Large Release Frequency** | |
| *(see Frequency)* | The term large release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under “Frequency.” |
| **Late Containment Failure** | |
| *(see Containment Failure)* | The term late containment failure is a type of containment failure and is defined under “Containment Failure.” |
| **Latent Cancer Fatality** | |
| *(see Fatality)* | The term latent cancer fatality is a type of fatality caused by exposure to fuel chemicals and is defined under “Fatality.” |
| **Latent Fatality** | |
| *(see Fatality)* | The term latent fatality is a type of fatality caused by exposure to fuel chemicals and is defined under “Fatality.” |
| **Latent Fatality Risk** | |
| *(see Fatality)* | The term latent fatality risk is a type of risk-involved fatality caused by exposure to fuel chemicals and is defined under “Fatality.” |
| **Latent Health Effects** | |
| *(see Health Effects)* | The term latent health effect refers to a type of health effect and is defined in the discussion under “Health Effects.” |

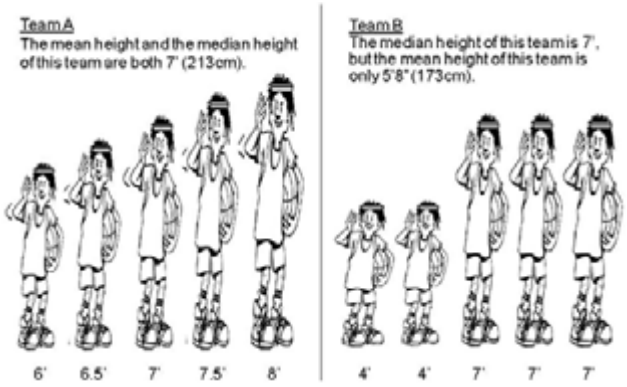
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Level 1, 2, 3 or 4 QRVA** | |
| A characterization of the scope of a QRVA in terms of increasing specification of consequences. *(see QRVA)* | The three types of QRVA are distinguished by the risk metric calculated, and when all three are calculated for a particular facility, it is referred to as a full-scope QRVA. Level 1 refers to LOFICF as the risk measure, Level 2 refers to fuel chemical releases as the risk measure, and Level 3 or 4 refers to offsite consequences as the risk measure.<br>A Level 2 QRVA takes the results of the Level 1 QRVA (accident sequences resulting in loss of fuel inventory control) as input and produces frequencies of radioactivity releases as output. A Level 3 or 4 QRVA takes the results of the Level 2 QRVA as input and produces offsite consequences (health effects, economic consequences) as output. In some usages, a Level 2 QRVA includes the Level 1 analysis, and the Level 3 or 4 QRVA includes both the Level 1 and Level 2 analyses. |
| **Level of Detail** | |
| The degree of resolution or specificity in the analyses performed in the QRVA. *(see Model, Capability Categories)* | In a QRVA, the level of detail generally refers to the level to which a system is modeled (e.g., function level, train level, component level), the extent to which systems are included in the success criteria (e.g., safety systems and nonsafety systems), the extent to which phenomena are included in the challenges to the facility in the Level 2 analysis, and the extent to which operator actions are considered (e.g., accident management strategies).<br>Level of detail generally is dictated by four factors: (1) the level of detail to which information is available, (2) the level of detail required so that dependencies are included, (3) the level of detail so that the risk contributors are included, and (4) the level of detail sufficient to support the application.<br>In the ASME/ANS PRA Standard, the degree to which the level of detail (and scope) of the facility design, operation, and maintenance are modeled forms one of the bases for the capability categories defined in the Standard. |
| **Living QRVA** | |
| A QRVA that is maintained so that it reflects the current facility design and operational features. (*see Dynamic QRVA, QRVA Configuration Control, As-Built As-Operated)* | The term living QRVA designates a QRVA that is updated as necessary to reflect any changes in the facility (e.g., design, operating procedures, data) to continue to represent the as-built as-operated facility. Therefore, the living QRVA can be used in risk-informed decision-making processes. QRVA configuration control is part of the process used to support a living QRVA.<br>A living QRVA is not the same as a dynamic QRVA. A dynamic QRVA refers to a QRVA that accounts for time-dependent effects by integrating these effects directly into the computer model. |
| **Loss of Fuel Inventory Control Frequency** | |
| *(see Frequency)* | The term loss of fuel inventory control frequency is a type of frequency used in QRVA and is defined under “Frequency.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Loss of Offsite Power** | |
| The loss of all AC power from the electrical grid to the facility. *(see Transient)* | In a QRVA, LOOP is referred to as both an initiating event and an accident sequence class. As an initiating event, LOOP to the facility can be a result of a weather-related fault, a grid-centered fault, or a facility-centered fault. During an accident sequence, LOOP can be a random failure. Generally, LOOP is considered to be a transient initiating event. |
| **Master Logic Diagram** | |
| A graphical model that can be constructed to guide the selection of initiating events. *(see Fault Tree)* | In a QRVA, a master logic diagram is often used to identify the specific events that are potential initiating events and to group them according to the challenges they pose to facility safety. An MLD is developed using fault tree logic to show general categories of initiating events proceeding to increasingly detailed information at lower levels, with specific initiating events presented at the bottom level. In a more general sense, an MLD is a fault tree identifying all the hazards that affect a system or mission.<br>An MLD generally uses a fault tree logic approach to identify the logic or relationship between events. However, the difference between an MLD and a fault tree is that a fault tree focuses on accounting for the specific causes leading to failure of a system or group of systems, whereas the MLD focuses on listing the hazards that can affect a top event. The ASME/ANS PRA Standard defines an MLD as a "summary fault tree constructed to guide the identification and grouping of initiating events and their associated sequences to ensure completeness." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Mean** | |
| The expected value of a random variable. *(see Median, Best Estimate, Point Estimate, Probability Distribution)* | In a QRVA, the metrics (e.g., LOFICF, AFRF) generally are evaluated and presented as mean values to reflect the uncertainties in the parameter values used as input to the evaluation of the metrics. The mean values and the distributions from which they are calculated can be used to address the parameter uncertainties.<br>The mean is the average value from a probability distribution. It is the expected value one would get from many samples taken of the random variable. The random variable in question could be a risk parameter, such as a component failure probability, or a risk measure, such as LOFICF.<br>The mean and median provide different information and cannot be used interchangeably. An illustration of the difference between mean and median is shown below.<br>  |
| **Mechanistic Source Term** | |
| A source term that is calculated considering the characteristics of specific accidents. (*see Source Term)* | In a Level 2 QRVA, the source term calculated is usually a mechanistic source term. A mechanistic source term is calculated using validated models and supporting scientific data that simulate the physical and chemical processes that describe the fuel chemicals inventories and the time-dependent fuel chemicals transport mechanisms necessary and sufficient to predict the source term.<br>For licensing calculations not involving a QRVA, current LWR use a deterministic predetermined source term into containment for different accidents, instead of a mechanistic source term, to analyze the effectiveness of the containment and site suitability for regulator approval purposes. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Median** | |
| That value of a random variable for which the occurrence of larger values is just as likely as occurrence of smaller values. *(see Mean, Probability Distribution)* | In a QRVA, median values are not usually calculated. In some cases, median values of the risk metric are calculated in addition to the mean to provide a perspective on the distribution of the risk metric. Conclusions can be made about the spread and shape of a probability distribution of a risk metric or a parameter by comparing the median to the mean and to the other quantiles.<br>The median is the middle value in a probability distribution. It is a reference point in which half the data values in a probability distribution (e.g., uncertainty distribution) lie below it and half lie above it. For example, if the median of a failure rate of a particular type of electric motor is $2x10^{-4}$/hr then half of all electric motors of that type would have failure rates below $2x10^{-4}$/hr and half would have failure rates above $2x10^{-4}$/hr.<br>An illustration of the difference between mean and median is under the discussion of the term "Mean." |
| **Minimal Cut Set** | |
| *(see Cut Set)* | The term minimal cut set is a type of cut set used in QRVA and is defined under "Cut set." |
| **Mission Time** | |
| The time period that a system or component is required to operate to successfully perform its function. | In a QRVA, the failure probability of a component to operate is directly related to its mission time. By convention, in a Level 1 internal events QRVA, mission time usually is specified as 24 hours. After that initial time period, multiple options for dealing with the accident would become available so that the residual risk results, beyond the 24-hour timeframe, would be negligibly small. For Level 1 QRVAs that examine external hazards, the mission times usually are longer (e.g., 72 hours) because of area wide effects of such events.<br>The definition provided is based on the definition in the ASME/ANS PRA Standard. |
| **Mitigating System** | |
| A facility system designed to minimize the effects of initiating events. *(see Initiating Event, Frontline System, Support System)* | In a QRVA, the accident mitigating functions and mitigating systems modeled are based on the initiating event(s) being analyzed. Mitigating systems can prevent an accident or reduce the consequences of a potential accident by directly performing or supporting one or more accident mitigating functions.<br>Frontline systems are mitigating systems that directly perform an accident mitigating function. Typically, support systems (e.g., electric power, control power, or cooling) are required to enable the operation of systems that directly perform an accident mitigating function. In this regard, support systems also may be considered mitigating systems. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Model (QRVA)** | |
| A representation of a physical process or system that allows one to predict the system's behavior. *(see Uncertainty)* | The term "model" is used in a variety of ways in a QRVA:<br>• The entire QRVA is sometimes referred to as a QRVA model or risk model.<br>• Different submodels are used inside the QRVA in the performance of the various technical elements (system model, human reliability analysis model).<br>• Other submodels may be phenomenological models.<br>All of these types of models may be sources of model uncertainty in the QRVA. |
| **Model Uncertainty** | |
| *(see Uncertainty)* | The term model uncertainty is related to epistemic uncertainty and is defined under "Uncertainty." |
| **Nonsafety Related** | |
| *(see Safety Significant)* | The term nonsafety related indicates the safety category of a structure, system, or component and is defined under "Safety Significant." |
| **Operator Action** | |
| *(see Human Action)* | The term operator action is a specific type of human action that is defined under the term "Human Action." |
| **Operator Error** | |
| *(see Human Error)* | The term operator error is a specific type of human error that is defined under the term "Human Error." |
| **Other External Hazard Fragility Evaluation/ Analysis** | |
| *(see Fragility Analysis)* | The term other external hazard fragility analysis is a type of fragility analysis and is included in the discussion under "Fragility Analysis." |
| **Other External Hazard Facility Response Analysis/Model** | |
| *(see Facility Response Analysis)* | The term other external hazard facility response analysis is a type of facility response analysis and is included the discussion under "Facility Response Analysis/Model." |
| **Other Hazards Analysis** | |
| *(see Hazard Analysis)* | The term other hazards analysis is a specific type of hazard analysis and is defined under the term "Hazard Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Parameter** | |
| The variables used to calculate and describe frequencies and probabilities. (*see Uncertainty, Point Estimate)* | In a QRVA, parameters are used directly in supporting QRVA models. Initiating event frequencies, component failure rates and probabilities, and human error probabilities are several parameters used in quantifying the accident sequence frequencies.<br>Generally accepted probability models exist for many of the basic events modeled in the QRVA model. These "basic event" models typically are simple mathematical models with only one or two parameters. An example is the simple constant failure rate reliability model, which assumes that the failures of components in a standby state occur at a constant rate. The parameter(s) of such models may be estimated using appropriate data, which, in the example above, may come from the number of failures observed in a population of like components in a given period of time. Statistical uncertainties are associated with the estimates of the model's parameters. Because most of the events that constitute the building blocks of the risk model (e.g., some initiating events, operator errors, and equipment failures) are relatively rare, the data are scarce and the uncertainties can be relatively significant. |
| **Parameter Uncertainty** | |
| *(see Uncertainty)* | The term parameter uncertainty is related to epistemic uncertainty and is defined under "Uncertainty." |
| **Passive Component** | |
| A component whose operation or function does not depend on an external source of motive power. (*see Active Component)* | In a QRVA, both passive and active components are modeled. A passive component has no moving parts, and it can experience changes in pressure, temperature, or fluid flow in performing its functions. Some examples of passive components include heat exchangers, pipes, vessels, and electrical cables and structures.<br>The IAEA Safety Glossary defines passive components as "a component whose functioning does not depend on an external input such as actuation, mechanical movement, or supply of power." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Performance-Based (Approach, Regulation, Regulatory Action)** | |
| Focusing on measurable outcomes, rather than prescriptive processes, techniques, or procedures. *(see Risk-Based)* | In a QRVA, a quantitative evaluation is made about the performance of the facility in response to potential accident conditions. The results of this evaluation can be used to support a performance-based approach to facility operations in which measureable outcomes are used to show compliance with regulation.<br>NUREG/BR-0318 defines the term performance-based as an approach to regulatory practice that establishes performance and results as the primary bases for decision-making. Performance-based regulations have four common attributes: (1) Measurable, calculable, or objectively observable parameters exist or can be developed to monitor performance. (2) Objective criteria exist or can be developed to assess performance. (3) Facility operators have flexibility to determine how to meet the established performance criteria in ways that encourage and reward improved outcomes. (4) A framework exists or can be developed in which the failure to meet a performance criterion, while undesirable, will not constitute or result in an immediate safety concern. |
| **Performance-Based Approach** | |
| *(see Performance-Based)* | The term performance-based approach indicates an evaluation that is based on measureable outcomes and is defined under "Performance-Based." |
| **Point Estimate** | |
| An estimate of a parameter in the form of a single value. *(see Mean)* | In a QRVA, the preferred parameter point estimate is the mean of the value obtained from a probability distribution for the parameter.<br>NUREG-1855 states, "a point estimate is a single value estimate for a parameter population. For example, the mean of a sample of values of a random variable X (i.e., expected value) is a commonly used point estimate of the mean of the distribution. When parameter distributions are not available, a maximum likelihood estimate or a value obtained from expert elicitation can serve as a point estimate."<br>For a point estimate of a risk metric (e.g., LOFICF) mean values of various parameters are used. The mean value of the risk metric usually is very close to this point estimate.<br>The definition provided was based on the definition in NUREG/CR-6823. |
| **Precursor Event** | |
| *(see Accident Precursor)* | The term precursor event is the same as accident precursor and is defined under "Accident Precursor." |

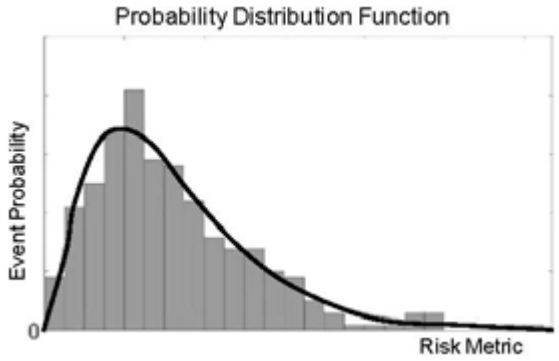
## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Probabilistic (Analysis, Approach)** | |
| A characteristic of an evaluation that includes consideration of events with regard to their likelihood. *(see Deterministic, QRVA, Risk-Based, Risk-Informed)* | A QRVA is an example of a probabilistic analysis, which can be defined as a mathematical evaluation of random (stochastic) events or processes and their consequences. While a QRVA uses probabilistic analysis, a QRVA also depends on deterministic analyses. For example, success criteria for various systems modeled in a QRVA to prevent and mitigate loss of fuel inventory control are based on deterministic analyses.<br>A probabilistic approach can be defined as a method that accounts for the likelihood of possible states that a physical entity or system can assume and predictions of models describing the entity or system.<br>Both risk-based and risk-informed approaches to decision-making and regulation rely upon probabilistic analysis. A risk-based approach to decision-making or regulation means that the decision or regulation is based only on risk information generated from a probabilistic analysis (e.g., from a QRVA), whereas a risk-informed approach combines risk information generated from a probabilistic analysis with other factors to arrive at a decision or develop regulations.<br>The NRC Website Glossary states the following: "The term 'probabilistic' is associated with an evaluation that explicitly accounts for the likelihood and consequences of possible accident sequences in an integrated fashion." Therefore, a probabilistic analysis or approach is unlike a deterministic analysis or approach, which does not include consideration of events with regard to their likelihood. |
| **Probabilistic Analysis** | |
| *(see Probabilistic)* | The term probabilistic analysis is defined under "Probabilistic." |
| **Probabilistic Approach** | |
| *(see Probabilistic)* | The term probabilistic approach is defined under "Probabilistic." |
| **Probabilistic Safety Assessment** | |
| *(see QRVA)* | The term probabilistic safety assessment is another term for QRVA and is defined under "QRVA." |
| **Probabilistic Seismic Hazard Analysis** | |
| *(see Hazard Analysis)* | The term probabilistic seismic hazard analysis is a specific type of hazard analysis and is defined under "Hazard Analysis." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Probability (Basic Event Failure, Containment Failure, Loss of Fuel Inventory Control, Failure, Human Error)** | |
| The likelihood that an event will occur as expressed by the ratio of the number of actual occurrences to the total number of possible occurrences. *(see Frequency)* | In a QRVA, probability is calculated for various types of QRVA input and output parameters (e.g., failures of equipment associated with basic events, loss of fuel inventory control, and containment failure).<br>The probability assigned to a basic event is often referred to as the basic event failure probability. A basic event is an element of the QRVA model for which no further decomposition is performed because it is at the limit of resolution consistent with available data. A failure probability is calculated for each failure mode of a component (e.g., failure to start and failure to run for a pump). In addition, a failure probability may be calculated for a system failing to perform its function or a structure failing (e.g., given a seismic event). For example, containment failure probability is the likelihood that the containment structure fails to perform its function of retaining fuel chemicals.<br>The ASME/ANS PRA Standard defines failure probability as "the likelihood that a system or component will fail to operate upon demand or fail to operate for a specific mission time."<br>Failure probability is also calculated for human actions and is then called human error probability. The ASME/ANS Standard defines human error probability as a measure of the likelihood that facility personnel will fail to initiate the correct, required, or specified action or response in a given situation, or by commission performs the wrong action.<br>Some QRVA studies also calculate the probability of loss of fuel inventory control, also referred to as loss of fuel inventory control probability, given a particular initiating event or set of initiating events.<br>There is a tendency in risk communication to use frequency and probability synonymously, but incorrectly. Probability only conveys the likelihood of an event; frequency conveys that likelihood per unit time.<br>The definition provided was based on the definition in NUREG/CR-6823. |
| **Probability Density Function** | |
| *(see Probability Distribution)* | The term probability density function is an equivalent term for probability distribution and is defined under "Probability Distribution." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Probability Distribution (Probability Density Function)** | |
| A curve that shows all the values that a random variable can take and the likelihood that each will occur. *(see Cumulative Distribution Function, Mean, Median, Uncertainty Interval)* | In a QRVA, probability distributions are used to express uncertainties associated with the state-of-knowledge about the parameter values and models used in constructing the QRVA. A probability distribution can represent either a discrete or continuous set of values for a random variable. It is usually represented as a probability density function. The probability density function is a function of a continuous random variable whose integral over an interval gives the probability that its value will fall within the interval.<br>In comparison, the cumulative distribution function adds up the probabilities of occurrence of all possible parameter values in a probability distribution function that are less than a specified value. An illustration of a probability distribution function and its corresponding cumulative distribution function is shown under the discussion for the term "Cumulative Distribution."<br>  |
| **Prompt Fatality** | |
| *(see Fatality)* | The term prompt fatality is a type of fatality caused by exposure to fuel chemicals and is defined under "Fatality." |
| **Prompt Fatality Risk** | |
| *(see Fatality)* | The term prompt fatality risk is a type of fatality caused by exposure to fuel chemicals and is defined under "Fatality." |
| **Public Health Effects** | |
| *(see Health Effects)* | The term public health effect refers to a type of health effect and is defined in the discussion under "Health Effects." |
| **Qualitative Risk Assessment** | |
| *(see Risk)* | A qualitative risk assessment is one type of risk assessment and is defined under "Risk." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Quantitative Risk and Vulnerability Assessment, Probabilistic Safety Assessment (Base, Baseline)** | |
| A systematic method for assessing the likelihood of accidents and their potential consequences. *(see Probability, Dynamic QRVA, Full-Scope QRVA, Level 1, 2, 3, or 4 QRVA)* | The term quantitative risk and vulnerability assessment has numerous, similar definitions. Some of the formal definitions used are presented below:<br>• "A qualitative and quantitative assessment of the risk associated with facility operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as loss of fuel inventory control or a fuel chemicals release and its effects on the health of the public (also referred to as a probabilistic safety assessment (PSA))."<br>• "For a method or approach to be considered a QRVA, the method or approach provides (1) a quantitative assessment of the identified risk in terms of scenarios that result in undesired consequence (e.g., loss of fuel inventory control or large early release) and their frequencies, and (2) is comprised of specific technical elements in performing the quantification."<br>• "A systematic method for assessing three questions used to define "risk." These questions consider (1) what can go wrong, (2) how likely is it, and (3) what are its consequences. These questions allow understanding of likely outcomes, sensitivities, areas of importance, system interactions, and areas of uncertainty, which can identify risk-significant scenarios. The QRVA determines a numeric estimate of risk to provide insights into the strengths and weaknesses of the design and operation of a nuclear power plant."<br>A specific type of QRVA is the base or baseline QRVA, which represents the as-built as-operated facility to the extent needed to support the application. For a facility at the design stage, where the facility is not built or operated, the base(line) QRVA model reflects the as-designed facility. This type of QRVA is also used as a benchmark to estimate the change in risk from a proposed design change. A dynamic QRVA is a special type of QRVA that automatically accounts for time-dependent effects by integrating these effects directly into the computer model. In a traditional QRVA, time-dependent effects are accounted for manually. A full-scope QRVA addresses three specific levels of analysis; namely, Level 1 (loss of fuel inventory control), Level 2 (fuel chemicals release), and Level 3 or 4+ (consequences).<br>The term probabilistic safety assessment is another term that is sometimes used interchangeably with QRVA. Typically, the term probabilistic safety assessment is used outside of the U.S. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **QRVA Configuration Control (Maintenance, Upgrade)** | |
| A process that maintains and updates the quantitative risk and vulnerability assessment so that it reflects the as-built as-operated facility. *(see Living QRVA, Risk Management)* | In a QRVA, updates to the model may be needed to ensure that the QRVA reflects the as-built as-operated facility. As described in the ASME/ANS PRA Standard, a "PRA configuration control program shall include a process to monitor changes in the design, operation, maintenance, and industry-wide operational history that could affect the PRA. These changes shall include inputs that impact operating procedures, design configuration, initiating event frequencies, system or subsystem unavailability, and component failure rates. The program should include monitoring of changes to the PRA technology and industry experience that could change the results of the PRA model."<br>As further described in the ASME/ANS PRA Standard, QRVA maintenance involves "update of the PRA models to reflect plant changes such as modifications, procedure changes, or plant performance (data)."<br>Additionally, the ASME/ANS PRA Standard states that a QRVA upgrade involves "the incorporation into a PRA model of a new methodology or changes in scope or capability that impact the significant accident sequences or the significant accident progression sequences. This could include items such as new human error analysis methodology, new data update methods, new approaches to quantification or truncation, or new treatment of common cause failure."<br>QRVA configuration control is part of the process used to support a living QRVA (i.e., a QRVA that is continuously updated to reflect current facility design, configuration, operating procedures, and facility-specific data).<br>Listed below are definitions of related terms:<br>• Configuration risk management: The term configuration risk management is the same as risk management and is defined under "Risk Management."<br>• Configuration risk profile: A change in the overall facility risk metric value as a result of a change from the initial facility configuration. Results from a QRVA can be used as the basis for developing configuration risk profiles using various risk metrics (e.g., LOFICF, AFRF). |
| **QRVA Maintenance** | |
| *(see QRVA Configuration Control)* | The term QRVA maintenance is part of QRVA configuration control and is defined under "QRVA Configuration Control." |
| **QRVA Model** | |
| *(see Model)* | The term QRVA model is a specific type of model and is defined under the term "Model." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **QRVA Technical Acceptability** | |
| *(see Technical Acceptability)* | The term QRVA technical acceptability is discussed in the discussion for the term "Technical Acceptability." |
| **QRVA Technical Adequacy** | |
| *(see Technical Adequacy)* | The term QRVA technical adequacy is discussed in the discussion for the term "Technical Adequacy." |
| **QRVA Technical Elements** | |
| The basic pieces (or analyses) required to produce the QRVA model. (*see Appendix B*) | The individual analyses used in the development of a QRVA model are organized according to a set of QRVA technical elements. As described in the ASME/ANS PRA Standard, a number of specific QRVA technical elements are used to support the evaluation of contributors to risk (e.g., the evaluation of hazard groups). Examples of QRVA technical elements include the following: initiating events analysis, accident sequence analysis, and high wind hazard analysis. |
| **QRVA Upgrade** | |
| *(see QRVA Configuration Control)* | The term QRVA upgrade is part of QRVA configuration control and is defined under "QRVA Configuration Control." |
| **Qualitative Screening** | |
| *(see Screening)* | A qualitative screening is one type of screening performed and is defined under "Screening." |
| **Quantitative Health Objectives** | |
| Numerical criteria for the acceptable levels of risk to public health and safety in the population surrounding a facility that satisfy regulator safety goals. *(see Fatality, Risk to Average individual)* | In some risk-informed decisions, the results of a QRVA are used to compare the risk from the facility with the quantitative health objectives (QHO) that support regulator safety goals.<br>Regulator safety goals are often expressed by two QHOs: (1) the annual average individual probability of prompt fatality in the population within 1 mile of the site boundary of a facility should not exceed one-tenth of 1 percent of the risk of prompt fatality due to all other risks that the U.S. population is generally exposed to, and (2) the annual average individual probability of latent cancer fatality in the population within 10 miles of the site boundary of a facility should not exceed one-tenth of 1 percent of the U.S. cancer fatality rate due to all other causes. |
| **Quantitative Screening** | |
| *(see Screening)* | A quantitative screening is one type of screening and is defined under "Screening." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Random Failure** | |
| A failure not anticipated to occur at a certain time (i.e., occurring with no specific pattern). | In a QRVA, potential failures of the modeled SSCs are treated as random events. This treatment is necessary because it is not possible to predict when an SSC will possibly fail. Instead, it is only possible to predict the likelihood that an SSC will fail. The likelihood that an SSC will fail is based on failure rate data, which represents the expected number of failures of the SSC per unit time. Failure rate data are developed for each SSC modeled in a QRVA. |
| **Random Uncertainty** | |
| *(see Uncertainty)* | The term random uncertainty is related to aleatory uncertainty and defined under "Uncertainty." |
| **Rare Initiator** | |
| An initiating event that is extremely unlikely and not expected to occur in facilities. *(see Initiating Event)* | In a QRVA, rare initiators generally are screened because of their low frequencies. Examples of rare initiators include aircraft impact, meteor strikes, and very large earthquakes. These occurrences are also correctly referred to as rare events. |
| **Rationalist** | |
| An approach to defense-in-depth that uses probabilistic information to evaluate the uncertainties and to determine what steps should be taken to compensate for those uncertainties. *(see Structuralist, Defense-in-Depth)* | When used in a QRVA context, the term rationalist is a relatively new term associated with defense-in-depth. The rationalist approach is made practical by the ability to quantify risk and estimate uncertainties using QRVA techniques. In this approach, results from a QRVA or other probabilistic analysis are used to assess the strengths and weaknesses of defense-in-depth, while accounting for analysis uncertainties. Ultimately, the rationalist approach provides a way to increase the degree of confidence in the conclusion that the defense-in-depth is sufficiently robust to achieve adequate safety.<br>In contrast, the fundamental principle of the structuralist approach is that if a system is designed to withstand all the worst-case credible accidents, then it is by definition protected against any credible accident. It is a deterministic method of establishing how precautions can be placed into a system, just in case an existing barrier or system fails.<br>Competent regulators describe that the rationalist will (1) establish quantitative acceptance criteria, such as the quantitative health objectives, loss of fuel inventory control frequency and large early release frequency, (2) analyze the system using PRA methods to establish that the acceptance criteria are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for those uncertainties. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Realistic Analysis** | |
| *(see Conservative Analysis)* | The term realistic analysis is discussed in the discussion for "Conservative Analysis" and is defined there. |
| **Recovery** | |
| Restoration of a failed function. *(see Repair)* | In a QRVA, the term recovery usually refers to an action or series of actions performed by an operator or other facility personnel to restore a function in response to a failed component or system. This term is sometimes used incorrectly as a synonym for repair. However, repair is restoring a failed function by fixing the actual cause of the failure while recovery is restoring the function in some other way.<br>The ASME/ANS PRA Standard defines the term recovery as "restoration of a function lost as a result of a failed structure, system or component (SSC) by overcoming or compensating for its failure. Generally modeled by using human reliability analysis (HRA) techniques." |
| **Release** | |
| *(see Radioactive Material Release)* | For purposes of a Level 2 and Level 3 or 4 QRVA, the term release is used interchangeably with "Fuel Chemical Release." |
| **Release Category** | |
| A group of fuel chemical releases expected to result in similar consequences. *(see Source Term)* | In a Level 2 QRVA, a release category is a grouping of accident sequences into an accident sequence class or family based on a common potential for release of fuel chemicals.<br>The release categories are characterized by a bounding mechanistic source term. This grouping is based on the following common attributes: common initiating events, combination of successful and failed safety functions, release magnitude, release timing and location, and specific fuel chemicals released from the facility as a result of an accident. |
| **Release Fraction** | |
| The amount of fuel chemicals released from the facility expressed as a fraction of the original inventory of the fuel chemicals. *(see Source Term)* | In a Level 2 QRVA, the release fraction specifies the amount of fuel chemicals released to the environment and provides the basis for the subsequent chemical exposure calculations to the affected population.<br>fuel chemical |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Release Timing and Duration** | |
| The time of release and the timeframe over which the fuel chemicals are released to the environment during an accident. *(see Source Term)* | In a Level 3 or 4 QRVA, the time of release and its duration are used to calculate the health consequences to the affected population. Both the timing and duration of the release also form the basis for potential offsite protective action strategies. |
| **Reliability (Unreliability)** | |
| The likelihood that a system, structure, or component performs its required function(s) for a specified period of time. *(see Availability)* | In a QRVA, the unreliability of systems, structures and components, as well as human actions, are used as input to the QRVA model, as opposed to the reliability. Unreliability is the complement of reliability and is the likelihood that an SSC does not operate for its mission time when required.<br>The term reliability is often inappropriately used interchangeably with the term availability. Availability only represents the degree to which a SSC is operational and accessible when required for use, with no reference to a mission time. Availability is the likelihood that the SSC is in a state to perform its required function at a given moment in time.<br>In the ASME/ANS PRA Standard, unreliability is defined as "the probability that a system or component will not perform its specified function under given conditions upon demand or for a prescribed time." |
| **Repair** | |
| The restoration of a failed function by correcting the cause of failure. *(see Recovery)* | In a QRVA, the term repair usually refers to an action or series of actions performed by an operator or other facility personnel to restore the function of a failed SSC by correcting the cause of failure and returning the failed SSC to service so that it can perform its intended function(s).<br>This term is sometimes used incorrectly as a synonym for the term recovery. However, repair is restoring a failed function by fixing the actual cause of the failure while recovery is restoring the function in some other way.<br>The ASME/ANS PRA Standard defines the term repair as "restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality. Generally modeled by using actuarial data." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Response Time** | |
| The period of time something takes to react to a given input. | In a QRVA, the term response time has different connotations, depending on the situation. Some of these connotations are as follows:<br>• When referring to facility components, response time is "the period of time necessary for a component to achieve a specified output state from the time that it receives a signal requiring it to assume that output state."<br>• When referring to human reliability analysis, response time is the time required for "the actions carried out after the operator has received and processed information related to his tasks. These responses constitute the human outputs in a man-machine system and serve as inputs to the man-machine interfaces."<br>• When referring to a Level 3 or 4 QRVA emergency response, response time is the time required for offsite responders to arrive at a facility site during an emergency (as related to accident response and accident preparedness). |
| **Risk (Assessment, Analysis)** | |
| The combined answer to three questions that consider (1) what can go wrong, (2) how likely is it, and (3) what are its consequences. *(see QRVA, Level 1, 2, 3 or 4 QRVA, Risk Metric)* | Risk assessment or risk analysis and QRVA are often incorrectly used as synonyms. A QRVA is one type of risk assessment or risk analysis. The QRVA has a structured format and quantifies the ultimate consequences. A risk assessment or risk analysis does not necessarily reflect all the technical elements. For example, a seismic margin risk analysis is not a QRVA. A qualitative risk assessment or analysis is a risk evaluation that uses descriptions or distinctions based on some characteristic rather than on some quantity or measured value.<br>In comparison to a risk assessment or analysis, a QRVA generates different ways to measure risk, called risk metrics, which satisfy specified safety objectives or goals. The consequences are manifested in the onset of loss of fuel inventory control and each level of the QRVA uses different risk metrics, which can be found in the discussion of Level 1, 2, 3 or 4+ QRVA.<br>The ASME/ANS PRA Standard defines the term risk as the "probability and consequences of an event, as expressed by the "risk triplet" that is the answer to the following three questions: *(a)* What can go wrong? *(b)* How likely is it? *(c)* What are the consequences if it occurs?"<br>The definition provided was based on the definition in the NRC Website Glossary. |
| **Risk Achievement Worth** | |
| *(see Importance Measure)* | The term risk achievement worth is one type of importance measure and is defined under "Importance Measure." |
| **Risk Characterization** | |
| *(see Risk Metric)* | The term risk characterization is a process that uses risk metrics to determine risk and is defined under "Risk Metric." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk Insights** | |
| The understanding about a facility's response to postulated accidents. *(see Risk, Risk-Based, Risk-Informed)* | One of the main objectives of a QRVA is to gain insights about a facility's response to initiating events and accident progression, including the expected interactions among facility SSCs, and between the facility and its operating staff. Risk insights are derived by investigating in a systematic manner: (1) what can go wrong, (2) how likely it is, and (3) what the consequences are. A risk assessment is a systematic method for addressing these questions as they relate to understanding issues like: important hazards and initiators, important accident sequences and their associated SSC failures and human errors, system interactions, vulnerable facility areas, likely outcomes, sensitivities, and areas of uncertainty.<br>Risk insights can be obtained via both quantitative and qualitative investigations. Quantitative risk results from QRVA calculations are typically the most useful and complete characterization of risk, but they are generally supplemented by qualitative risk insights and traditional engineering analysis. Qualitative risk insights include generic results, i.e., results that have been learned from numerous QRVAs that have been performed in the past, and from operational experience, and that are applicable to a group of similar facilities.<br>Risk insights are an important part of risk-informed regulation, in which regulatory decisions are made by integrating risk insights with considerations of defense-in-depth and safety margins. |
| **Risk Management** | |
| A process used at a facility to keep the risk at acceptable levels. | A QRVA is a tool used to evaluate a facility from a risk management perspective. The QRVA quantifies the facility risk and also quantifies changes in facility risk because of modifications of the facility design or operation. For example:<br>• A QRVA represents an important risk management tool that ensures that other potentially lower probability, but nonetheless risk-significant, configurations resulting from facility maintenance and other operational activities are identified and compensated for.<br>Risk Management may be used in a broader context to refer to an approach for achieving a more comprehensive, holistic, risk-informed, performance-based regulation for facilities that would continue to ensure the safe and secure use of fuel chemicals. The objective of such an approach is described NUREG-2150 as managing the risks from the use of byproduct, source and special materials through appropriate performance based regulatory controls and oversight. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk Metric** | |
| A measure that is used to express the risk quantity of interest. *(see Risk, Level 1, 2, 3 QRVA, Risk Profile, Full-Scope QRVA)* | In a QRVA, several risk metrics are evaluated. Examples of risk metrics are LOFICF, developed as part of a Level 1 QRVA and AFRF, developed as part of a Level 2 QRVA. Health effects developed in a Level 3 or 4 QRVA also can be used as a risk metric. In this instance, limiting to a threshold value the annual average individual probability of death due to acute fuel chemical within 1 mile of the site boundary would be an example of a risk metric. A full-scope QRVA develops risk metrics associated with Levels 1, 2, and 3. Risk metrics are used among other things, to illustrate compliance with safety goals. Risk metrics focus attention on those areas where risk is most likely (such as events that cause loss of fuel inventory control) and how the risk metric value for that area is achieving the desired safety objective. Risk metrics can be used in performing risk characterization. Risk characterization combines the major components of risk (hazards, consequences, frequency, and probability), along with quantitative estimates of risk, to give a combined and integrated risk perspective (i.e., a risk profile). Additionally, it shows the key assumptions and rationale, expert elicitation, uncertainties associated with the analysis, and sensitivity analysis. |
| **Risk Monitor** | |
| A facility-specific analysis tool used to determine the risk in real-time based on the current facility configuration. *(see Living QRVA)* | The model the risk monitor uses is based on, and is consistent with, the living QRVA for the facility. At any given time, the risk monitor reflects the current facility configuration in terms of the known status of the various systems or components (e.g., if any components are out of service for maintenance or tests). The risk monitor assists facility personnel in making decisions about facility configuration changes. |
| **Risk Profile (Facility)** | |
| The major results generated by a QRVA that characterize facility risk. | A facility risk profile presents a concise synopsis of the major QRVA results. This synopsis may consist of numerous characterizations of risk, including:<br>• LOFICF and AFRF for internally and externally initiated events during various modes of operation.<br>• Percentage contributions to LOFICF and AFRF by initiating event and accident sequence type.<br>• Ranking of the contribution of individual basic events and cut sets to LOFICF and AFRF, based on various importance measures.<br>• Comparison of QRVA results to QRVAs for other facilities.<br>• Qualitative risk insights on facility design features. |
| **Risk Reduction Worth** | |
| *(see Importance Measure)* | The term risk reduction worth is one type of importance measure and is defined under “Importance Measure.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk Significant** | |
| A level of risk associated with a facility's system, structure, component, human action or modeled accident sequence that exceeds a predetermined level. *(see Safety Significant, Significant)* | A principal focus of a QRVA is to determine the risk significance of the various "features"; i.e., the SSC, human actions or the accident sequences involving those SSCs, of the facility being analyzed. Usually, an item is considered risk significant when the risk associated with it exceeds a predetermined limit for contributing to the risk associated with the facility. Since the overall risk of a facility can be calculated in terms of LOFICF (Level 1 QRVA), or releases (Level 2 QRVA), or health effects (Level 3 or 4 QRVA), risk significance can also be determined as related to these various risk measures. Note that risk significant does not have the same meaning as safety significant (defined elsewhere in this glossary) and safety significance is not evaluated in a QRVA.<br>The term also describes a level of risk exceeding a predetermined "significance" level. |
| **Risk Significant Equipment** | |
| *(see Significant)* | The term risk significant equipment is related to the term significant and is defined under "Significant." |
| **Risk to Average Individual** | |
| A measure of the risk to an individual that represents an average over the parameters characterizing the population at risk *(see Fatality, Quantitative Health Objectives)* | In a Level 3 or 4 QRVA, the risk to an average individual is calculated as the total fatalities in the surrounding population as a result of an accident divided by the total population. For example, the risk of prompt fatality to an average individual within 1 mile of the facility boundary can be calculated as the number of prompt fatalities per year to the total population within 1 mile of the facility boundary because of each accident sequence, summed over all accident sequences weighted by their frequency of concurrence, divided by the population within 1 mile. The average individual in the vicinity of the facility is defined as the average individual biologically (in terms of age and other risk factors) and who resides within 1 mile of the facility site boundary. |
| **Risk-Based Approach** | |
| *(see Risk-Based)* | The term risk-based approach is related to the term risk-based and is defined under "Risk-Based." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk-Based (Approach, Decision-Making, Regulation)** | |
| A characteristic of decision-making in which a decision is solely based on the results of a risk assessment. *(see Risk-Informed)* | The modifying term "risk-based" is applied to decision-making and regulation activities that rely solely on the use of risk information from QRVA results. The terms risk-based approach, risk-based decision-making, and risk-based regulation are often used interchangeably and somewhat correctly to describe the same concept; therefore, these terms are grouped under the same definition. However, as indicated below, each of these terms has its own distinct meaning:<br>• Risk-Based Approach: A philosophy on decision-making "in which a safety decision is solely based on the numerical results of a risk assessment."<br>• Risk-Based Decision-Making: "An approach to regulatory decision-making that considers only the results of a probabilistic risk assessment."<br>• Risk-Based Regulation: An approach to regulation that uses the results of a risk assessment to develop applicable regulations.<br>Risk-informed is a term that is often used incorrectly in place of risk-based. These terms are not synonyms. Unlike a risk-based approach, a risk-informed approach to decision-making or regulation combines risk information with other factors (e.g., engineering design features) to arrive at a decision or develop regulations.<br>Since risk-based approaches, decision-making, and regulation put a greater emphasis on risk assessment results than is currently practical because of uncertainties in QRVA, such as completeness, the Commission does not endorse a solely "risk-based" approach. |
| **Risk-Based Decision-Making** | |
| *(see Risk-Based)* | The term risk-based decision-making is related to the term risk-based and is defined under "Risk-Based." |
| **Risk-Based Regulation** | |
| *(see Risk-Based)* | The term risk-based regulation is related to the term risk-based and is defined under "Risk-Based." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk-Informed (Approach, Decision-making, Regulation)** | |
| A characteristic of decision-making in which risk results or insights are used together with other factors to support a decision. *(see Risk-Based, Deterministic, Probabilistic)* | The modifying term "risk-informed" is applied to decision-making and regulation activities that combine risk information (e.g., QRVA results) with other factors (e.g., engineering design features) to arrive at a decision. The terms risk-informed approach, risk-informed decision-making, and risk-informed regulation are often used interchangeably and somewhat correctly to describe the same concept; therefore, these terms are grouped under the same definition. However, as indicated below, each of these terms has its own distinct meaning:<br>• Risk-Informed Approach: "A 'risk-informed' approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus facility operator and regulatory attention on design and operational issues commensurate with their importance to health and safety. A 'risk-informed' approach enhances the traditional approach by: (a) allowing explicit consideration of a broader set of potential challenges to safety, (b) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment, (c) facilitating consideration of a broader set of resources to defend against these challenges, (d) explicitly identifying and quantifying sources of uncertainty in the analysis, and (e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions. Where appropriate, a risk-informed regulatory approach can also be used to reduce unnecessary conservatism in deterministic approaches, or can be used to identify areas with insufficient conservatism and provide the bases for additional requirements or regulatory actions."<br>• Risk-Informed Decision-Making: "An approach to regulatory decision making, in which insights from probabilistic risk assessment are considered with other engineering insights."<br>• Risk-Informed Regulation: "An approach to regulation taken by the NRC, which incorporates an assessment of safety significance or relative risk. This approach ensures that the regulatory burden imposed by an individual regulation or process is appropriate to its importance in protecting the health and safety of the public and the environment."<br>A term often used incorrectly in place of risk-informed is risk-based; these terms are not synonyms. A risk-based approach to decision-making or regulation means that the decision or regulation is based only on risk information (e.g., risk results obtained from a QRVA), whereas a risk-informed approach combines risk information with other factors to arrive at a decision or develop regulations. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Risk-Informed Approach** | |
| *(see Risk- Informed)* | The term risk-informed approach is related to the term risk-informed and is defined under "Risk- Informed." |
| **Risk-Informed Decision-Making** | |
| *(see Risk- Informed)* | The term risk-informed decision-making is related to the term risk-informed and is defined under "Risk-Informed." |
| **Risk-Informed Regulation** | |
| *(see Risk- Informed)* | The term risk-informed regulation is related to the term risk-informed and is defined under "Risk-Informed." |
| **Safe Stable State** | |
| Condition of the facility in which the necessary safety functions are achieved. | In a QRVA, safe stable states are represented by success paths in modeling of accident sequences. A safe stable state implies that the facility conditions are controllable within the success criteria for maintenance of safety functions. |
| **Safety Margin** | |
| The extra capacity factored into the design of a structure, system, or component so that it can cope with conditions beyond the expected to compensate for uncertainty. *(see Defense-in-Depth, Uncertainty)* | In a QRVA, the extra capacity of SSC provided by the safety margin is used in calculating the facility response to an accident. A safety margin is used to provide capacity for emergency situations, unexpected loads, misuse, or attrition.<br>Many engineering codes and standards provide quantitative guidance on appropriate safety margin for a particular design application. However, the term safety margin also is often found in regulatory documents that contain phrases such as "maintain adequate safety margin," or "provide sufficient safety margin," without specification of a particular quantitative margin.<br>Safety margins can be considered a part of, or complementary to, defense-in-depth in that they provide extra (redundant) capacity. Incorporation of safety margins is one of the ways designers deal with the uncertainty of the challenges that the designed SSCs face.<br>The figure below illustrates several concepts on safety margins. A regulator may impose the requirement that a margin is maintained between a component's allowable limit of operation, the regulatory limit, and the component's ultimate capacity. The component designer may want to design or select the component so that during normal operation it operates below, rather than right at, the regulatory limit (i.e., he or she may want to add an additional margin). The total safety margin then encompasses both the designer and regulatory margins. |
| **Safety-Related** | |
| *(see Safety Significant)* | The term safety-related indicates the safety significance of a structure, system, or component and is defined under "Safety Significant." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Safety Significant (Important to Safety, Safety-Related, Nonsafety-Related)** | |
| A qualifying term that indicates if something does not meet some predetermined criterion, it has the potential to affect safety. | In a QRVA, the risk significance of SSC are determined, not the safety significance. This risk significance is then used in a risk- informed regulatory framework to determine the safety significance of SSCs. The term safety significant is generally used to categorize facility SSCs using the process outlined in 10 CFR 50.69. In this application, a facility-specific QRVA is used to delineate and quantify severe accident scenarios resulting from internal initiating events at normal operation. In 10 CFR 50.36, Technical Specifications, Criterion 4 requires that "a structure, system, or component which operating experience or probabilistic risk assessment has shown to be significant to public health and safety" must have a technical specification limiting condition for operation established for it. |
| **Screening (Analysis, Criteria, Qualitative, Quantitative)** | |
| A process that distinguishes items that should be included or excluded from an analysis based on defined criteria. | In a QRVA, screening may be applied in a variety of ways (e.g., screening out (eliminating) component failure events from the QRVA based on a low probability or frequency). Another form of screening is to identify the more significant events that should be analyzed in a detailed manner. Insignificant events may be addressed using less detailed and usually conservative methods. Screening is an integral step in most QRVAs to reduce the complexity of the QRVA model using sound judgment. The terms screening and screening analysis are similar in meaning and often used interchangeably.<br>The definitions of the grouped terms are presented below as they apply to screening:<br>• Screening criteria: "The values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences."<br>• Qualitative screening: The objective is to identify portions of the analysis whose potential risk contribution can be judged negligible without quantitative analysis.<br>• Quantitative screening: The objective is to eliminate portions of the analysis from further consideration based on preliminary estimates of risk contribution through the use of established quantitative screening criteria.<br>The ASME/ANS PRA Standard defines screening as "a process that eliminates items from further consideration based on their negligible contribution to the probability of an accident or its consequences." |
| **Screening Analysis** | |
| *(see Screening)* | The term screening analysis is similar in meaning to screening and is discussed under "Screening." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Screening Criteria** | |
| *(see Screening)* | The term screening criteria is defined under "Screening." |
| **Seismic Fragility Analysis** | |
| *(see Fragility Analysis)* | Seismic fragility analysis is a type of fragility analysis and is included in the discussion under "Fragility Analysis." |
| **Seismic Hazard Analysis** | |
| *(see Hazard Analysis)* | The term seismic hazard analysis is a type of hazard analysis and is defined under "Hazard Analysis." |
| **Seismic Margin** | |
| A measure of the capacity of the facility to withstand an earthquake more severe than the design-basis earthquake. *(see High Confidence of Low Probability of Failure, Stable Safe Operation Earthquake, Seismic Margin Analysis)* | For some applications, seismic margin, rather than a QRVA risk metric, has been used to estimate the ability of a facility to safely withstand seismic events. The ASME/ANS PRA Standard states that seismic margin is expressed in terms of the earthquake motion level that compromises facility safety, specifically leading to severe loss of fuel inventory control. The margin concept also can be extended to any particular structure, function, system, equipment item, or component for which 'compromising safety' means sufficient loss of safety function to contribute to loss of fuel inventory control either independently or in combination with other failures.<br>NUREG-1742 defines seismic margin as the ability of a facility, system, component or structure to safely withstand seismic demands or input ground-motion levels beyond those imposed by the design basis earthquake. |
| **Seismic Margin Analysis** | |
| The process to estimate the seismic margin of the facility and to identify any seismic vulnerabilities in the facility. *(see High Confidence of Low Probability of Failure, Seismic Margin, Safe-Shutdown Earthquake)* | For some applications, seismic margin analysis is an alternative to a seismic QRVA for identifying seismic vulnerabilities at a facility. The earthquake specified for assessing the seismic margin can depend on a number of factors, usually the facility's location. Some facilities have been assessed against a review-level earthquake whose intensity was higher than the design-basis earthquake and varied according to the facility location.<br>Seismic margin analysis is performed to show HCLPF at a certain earthquake level (peak ground acceleration) above the design-basis (safe-shutdown) earthquake.<br>A number of methods can be used to calculate seismic margin. |
| **Seismic Facility Response Analysis/Model** | |
| *(see Facility Response Analysis/Model)* | The term seismic facility response analysis is a type of facility response analysis and is included in the discussion under "Facility Response Analysis/Model." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Sensitivity Analysis** | |
| An analysis in which one or more input parameters to a model are varied in order to observe their effects on the model results. | In a QRVA, sensitivity analyses often are performed to help assess the results. Sensitivity analyses often involve variations of quantitative parameters (e.g., component failure probabilities, initiating event frequencies, human error rates).<br>The definition provided was based on the definition in NUREG-1560. |
| **Significant (Accident Sequence, Accident Progression Sequence, Basic Event, Containment Challenge, Contributor, Cut Set, Equipment)** | |
| A factor that can have a major or notable influence on the results of a risk analysis. | In a QRVA, the modifying term significant is applied to factors that have an important influence on causing a measurement of risk to exceed a predetermined level or limit. The terms significant and risk significant have the same meaning in a QRVA context and are often used interchangeably, which is correct and appropriate in this context.<br>As discussed in NRC Regulatory Guide 1.200, the determination of significance is a function of how the QRVA is being, or is intended to be, used. When a QRVA is being used to support an application, the significance of an accident sequence or contributor is measured with respect to whether its consideration has an effect on the decision being made. Quantitative thresholds (criteria) often are used to determine if a basic event, cut set, accident sequence, or accident progression sequence is considered significant from a risk perspective (e.g., based on importance measures, percentage contribution). The previously mentioned items (e.g., basic event, cut set) represent the different types of significant risk contributors that could influence the results of a risk analysis. These quantitative criteria may vary, depending on the source of the guidance. The following terms (excluding risk significant) and the subsequent definitions are based on the ASME/ANS PRA Standard:<br>a. Significant Accident Sequence: "One of the sets of accident sequences resulting from the analysis of a specific hazard group, defined at the functional or systematic level, which, when rank-ordered by decreasing frequency, sum to a specified percentage of the loss of fuel inventory control frequency for that hazard group, or that individually contribute more than a specified percentage of loss of fuel inventory control frequency. For this version of the Standard [RA-Sa-2009], the summed percentage is 95% and the individual percentage is 1% of the applicable hazard."<br>b. Significant Accident Progression Sequence: "One of the sets of accident sequences contributing to large early release frequency resulting from the analysis of a specific hazard group that, when rank-ordered by decreasing frequency, sum to a specified percentage of the large early release frequency, or that individually contribute more than a specified percentage of large early release frequency for that hazard group. For this version of the Standard [RA-Sa-2009], the summed percentage is 95% and the individual percentage is 1% of the applicable hazard." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | c. Significant Basic Event: "A basic event that contributes significantly to the computed risks for a specific hazard group. For internal events, this includes any basic event that has an FV importance greater than 0.005 or a RAW importance greater than 2."<br>d. Significant Containment Challenge: "A containment challenge that results in a containment failure mode that is represented in a significant accident progression sequence."<br>e. Significant Cut Set: "One of the sets of cut sets resulting from the analysis of a specific hazard group that, when rank-ordered by decreasing frequency, sum to a specified percentage of the loss of fuel inventory control frequency (or large early release frequency) for that hazard group, or that individually contribute more than a specified percentage of loss of fuel inventory control frequency (or large early release frequency). For this version of the Standard [RA-Sa-2009], the summed percentage is 95% and the individual percentage is 1% of the applicable hazard."<br>f. Risk Significant Equipment: "Equipment associated with a significant basic event."<br>A significant contributor can refer to an important factor associated with a significant accident sequence, such as a particular accident sequence cut set, a significant basic event, or an initiating event. As stated in the ASME/ANS PRA Standard, a significant contributor also can be "an essential characteristic of a significant accident progression sequence, and if not modeled would lead to the omission of the sequence." |
| **Significant Accident Progression Sequence** | |
| *(see Significant)* | The term significant accident progression sequence is related to the term significant and is defined under "Significant." |
| **Significant Accident Sequence** | |
| *(see Significant)* | The term significant accident sequence is related to the term significant and is defined under "Significant." |
| **Significant Basic Event** | |
| *(see Significant)* | The term significant basic event is related to the term significant and is defined under "Significant." |
| **Significant Containment Challenge** | |
| *(see Significant)* | The term significant containment challenge is related to the term significant and is defined under "Significant." |
| **Significant Contributor** | |
| *(see Significant)* | The term significant contributor is related to the term significant and is defined under "Significant." |
| **Significant Cut Set** | |
| *(see Significant)* | The term significant cut set is related to the term significant and is defined under "Significant." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Small Early Release** | |
| *(see Fuel Chemical Release)* | The term small early release is a type of fuel chemical release and is defined in the discussion under "Fuel Chemical Release." |
| **Small Early Release Frequency** | |
| *(see Frequency)* | The term small early release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency." |
| **Small Early Release Frequency Analysis** | |
| *(see Radioactive Material Release Frequency Analysis)* | The term small early release frequency analysis is a type of fuel chemical release frequency analysis and is defined under "Fuel Chemical Release Frequency Analysis." |
| **Small Late Release** | |
| *(see Fuel chemical Release)* | The term small late release is a type of fuel chemical release and is defined in the discussion under "Fuel chemical Release." |
| **Small Late Release Frequency** | |
| *(see Frequency)* | The term small late release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency." |
| **Small Late Release Frequency Analysis** | |
| *(see Fuel chemical Release Frequency Analysis)* | The term large late release frequency analysis is a type of fuel chemical release frequency analysis and is defined under "Fuel chemical Release Frequency Analysis." |
| **Source of Risk** | |
| A substance that can pose danger or threat to public health. *(see Hazard, Initiating Event)* | In a QRVA, sources of risk at facilities include, for example, the fuel contained within the facility. These sources of risk could be affected by hazards which directly or indirectly cause initiating events and may further cause safety system failures or operator errors leading to loss of fuel inventory control or fuel chemical release.<br>The terms source of risk and hazard are sometimes incorrectly used as synonyms. A hazard is anything that has the potential to cause an undesired event. Intrinsically, a source of risk does not cause an event, but a hazard can cause an initiating event leading to loss of fuel inventory control. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Source Term** | |
| Types and amounts of fuel chemicals released to the environment following an accident. *(see Release Category, Mechanistic Source Term, Chemical Element Group, Release Fraction, Release Timing and Duration, Source Term Analysis)* | In a Level 2 QRVA, the source term is one of the end products of the analysis and involves the characterization of the release from containment to the environment.<br>This characterization involves a description of the fuel release at a particular location, including the physical and chemical properties of released material, release magnitude, heat content (or energy) of the carrier fluid, location relative to local obstacles that would affect transport away from the release point, and the temporal variations in these parameters; e.g., time of release duration.<br>The information used to define a source term can vary, depending on the objective and intended application of the QRVA. For instance, if the Level 2 QRVA results will be used in a Level 3 or 4 consequence assessment, it may be necessary to provide more detailed source term information than if no Level 3 or 4 assessment will be performed. For a Level 3 or 4 assessment, the source term information needs to be sufficient to estimate offsite consequences such as land contamination. |
| **Source Term Analysis** | |
| An analysis to determine the characteristics of the fuel chemical released to the environment following an accident. *(see Source Term)* | In a Level 2 QRVA, the source term analysis determines the release of fuel chemicals from the fuel and the transport of this material through the primary system and containment to the environment. |
| **Split Fraction** | |
| The likelihood that one specific outcome from a set of possible outcomes will be observed. *(see Event Tree, Probability)* | A split fraction is a unitless parameter (i.e., probability). This term typically is used with regard to the quantification of an event tree of a QRVA model. It represents the fraction with which each possible outcome, or branch, of a particular top event in an event tree may be expected to occur. Split fractions are, in general, conditional on prior events. At any event tree branch point, the sum of all the split fractions representing the possible outcomes should be unity.<br>The ASME/ANS PRA Standard defines the term split fraction as “a unitless quantity that represents the conditional (on preceding events) probability of choosing one direction rather than the other through a branch point of an event tree.” |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **State-of-Knowledge Correlation** | |
| A type of dependency that arises when the same data is used to quantify the individual probabilities of two or more basic events. *(see Uncertainty)* | In a QRVA, when the basic event mean values and uncertainty distributions are propagated without accounting for the state-of-knowledge correlation (SOKC), the calculated mean value of the relevant risk metric and the uncertainty about this mean value will be underestimated.<br>When the same data is used to quantify the individual probabilities of two or more basic events, the uncertainty associated with such basic event probabilities must be correlated to correctly propagate the parameter uncertainty through the risk calculation. The SOKC arises because, for identical or similar components, the state-of-knowledge about their failure parameters is the same. In other words, the data used to obtain mean values and uncertainties of the parameters in the basic event models of these components may come from a common source and, therefore, are not independent, but are correlated.<br>The ASME/ANS PRA Standard defines the term SOKC as "the correlation that arises between sample values when performing uncertainty analysis for cut sets consisting of basic events using a sampling approach (such as the Monte Carlo method); when taken into account, this results, for each sample, in the same value being used for all basic event probabilities to which the same data applies." |
| **State-of-Knowledge Uncertainty** | |
| *(see Uncertainty)* | The term state-of-knowledge uncertainty is related to epistemic uncertainty and defined under "Uncertainty." |
| **Stochastic Uncertainty** | |
| *(see Uncertainty)* | The term stochastic uncertainty is related to aleatory uncertainty and defined under "Uncertainty." |
| **Structuralist** | |
| An approach to defense-in-depth that relies on multiple strategies in the design and operation of a facility to compensate for both known and unknown uncertainties. *(see Rationalist, Deterministic, Defense-in-Depth)* | A QRVA is not used in the structuralist approach to defense-in-depth, unlike the rationalist approach. Instead, the structuralist approach asserts that safety margins associated with defense-in-depth are embodied within the regulations and in the design of a facility built to comply with those regulations.<br>The fundamental principle of the structuralist approach is that if a system is designed to withstand all the worst-case credible accidents, then it is by definition protected against any credible accident. It is a method that is solely based on deterministic analyses and principles to establish how precautions can be placed into a system, just in case an existing barrier or protective system fails. By comparison, a rationalist approach uses QRVA methods to quantify and reduce system uncertainties, as opposed to relying on potentially overly conservative safety margins. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Success Criteria** | |
| The minimum combination of systems and components needed to carry out the safety functions given an initiating event. | In a QRVA, success criteria are used at different places or levels in the analysis. At a high level, the success criteria define the safety functions that must be performed following an initiating event. Success criteria are then defined for each safety function, which are expressed in terms of requirements for the systems needed to support that function. Success criteria also are developed for the components within these systems. The success criteria specify how the systems and components must function, when they must begin to function, and how long they must function. Success criteria for QRVA studies typically are developed through the use of deterministic analyses that represent the design and operation of the facility being evaluated.<br>Success criteria may be defined in a number of ways, including the following:<br>a. In terms of the equipment required (e.g., one out of two service water pumps).<br>b. In terms of equipment performance (e.g., at least 50 percent of the maximum system flow rate).<br>c. In terms of the timing (e.g., system must be initiated within 30 minutes and operate for 24 hours).<br>The ASME/ANS PRA Standard defines the term success criteria as "criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied." |
| **Success Path** | |
| A sequence of events (responding to an upset condition) that result in a successful state of a system or the facility. *(see Event Tree, Safe Stable State)* | In a QRVA, the term success path often is used in the context of describing an event tree path that leads to a safe stable state of the facility. Alternatively, a fault tree model can be transformed into its logical complement, a success tree that shows the specific ways (success paths) in which an undesired event (e.g., system failure) can be prevented from occurring.<br>A successful state of a system occurs when the system is able to perform its intended function. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Supplementary Analysis** | |
| Any evaluation that is performed to support another study or evaluation. | In a QRVA context, the term supplementary analysis often is used to denote an evaluation made to facilitate the development or review of a QRVA consistent with the ASME/ANS PRA Standard. An example of a supplementary analysis would be an evaluation of facility-specific component failure data to support derivation of facility-specific component failure rates for use in a QRVA.<br>Sometimes the supplementary analysis is performed instead of following the specific requirements in the ASME/ANS PRA Standard. In this situation, the supplementary analysis is performed to meet the Standard's intent, but it is outside the scope of the Standard. Therefore, performing a supplementary analysis does not meet all the Standard's criteria. |
| **Support System** | |
| A system that enables the operation of one or more systems. *(see Frontline System, Support System Initiating Event)* | In a QRVA, support system failures are evaluated to determine the effect of these failures on the operability of other facility systems and components. Often one support system, such as electric power, provides functionality to multiple systems or components, and therefore, needs to be considered in QRVA modeling to assess what happens if that capability is lost to multiple systems.<br>Examples of support systems include electrical power, cooling water, instrument air, and heating, ventilation, and air conditioning. Support systems (e.g., cooling water) can require other support systems for operation (e.g., electric power may be needed to operate the cooling water pumps). Frontline systems typically require one or more support systems. In some instances, a failed support system can lead to an undesired facility condition that requires successful mitigation by facility equipment and personnel to prevent loss of fuel inventory control from occurring. In this situation, the support system failure would be characterized as a support system initiating event.<br>The ASME/ANS PRA Standard defines the term support system as "a system that provides a support function (e.g., electric power, control power, or cooling) for one or more other systems." |
| **Support System Initiating Event** | |
| A support system failure that perturbs the steady-state operation of the facility and could lead to an undesired facility condition. *(see Initiating Event, Support System)* | In a QRVA, the failures of support systems are evaluated to determine if they could potentially cause an undesired facility condition. At the same time, this failed support system also may have the potential to disable one or more systems that could be used to mitigate the undesired facility condition. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Supporting Requirements** | |
| Requirements that support the high-level requirements in defining the minimum needed for a technically acceptable baseline QRVA. *(see High-Level Requirements, Capability Categories)* | For a base QRVA, NRC Regulatory Guide 1.200 defines a set of technical characteristics and associated attributes that make it technically acceptable. One approach to demonstrate a QRVA is acceptable is to use a national consensus QRVA standard, supplemented to account for the NRC staff's regulatory positions. The ASME/ANS PRA Standard is one example of such a national consensus QRVA standard. The ASME/ANS PRA Standard uses high-level requirements and supporting requirements.<br>Regulatory Guide 1.200 states, "Technical requirements may be defined at two different levels: (1) high-level requirements and (2) supporting requirements. High-level requirements are defined for each technical element and capture the objective of the technical element. These high-level requirements are defined in general terms, need to be met regardless of the level of analysis resolution and specificity (capability category), and accommodate different approaches. Supporting requirements are defined for each high-level requirement. These supporting requirements are those minimal requirements needed to satisfy the high-level requirement."<br>To use a QRVA for a risk-informed application, it is recognized that not every QRVA item will be, or needs to be, developed to the same level of detail, same degree of facility-specificity, or the same degree of realism. The ASME/ANS PRA Standard uses three capability categories to distinguish levels of detail, facility specificity, and realism. Furthermore, the supporting requirements are developed commensurate with each capability category. Therefore, while the high-level requirements are the same across all three capability categories, their supporting requirements reflect the differences in levels of detail, facility specificity, and realism across the three categories. |
| **Systems Analysis** | |
| The evaluation of the reliability and availability of a system. *(see Availability, Reliability)* | In a QRVA, the term systems analysis can refer to a qualitative or quantitative evaluation of the failure modes of an individual system or group of systems (e.g., a fault tree analysis of a cooling water system or an electrical distribution system). |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Technical Acceptability, Technical Quality (QRVA)** | |
| Refers to a set of characteristics and related attributes that provide the minimum qualities a base QRVA must satisfy to be used in risk-informed decision-making. *(see Technical Adequacy)* | For a QRVA to be technically acceptable, it must satisfy a set of technical characteristics and associated attributes.<br>Technical acceptability and technical quality mean the same thing and are used interchangeably. |
| **Technical Adequacy (QRVA)** | |
| Refers to the fact that the QRVA has the scope and level of detail necessary to support the application for which it is being used and is also technically acceptable. *(see Technical Acceptability)* | The scope of a QRVA (i.e., risk characterization, level of detail, facility specificity and realism) needs to be commensurate with the scope of the specific risk-informed application that it is supporting. Some applications may only use a portion of the base QRVA, whereas other applications (e.g., safety significance categorization of structures, systems, and components) may require the complete model. Regulatory Guide 1.200 provides guidance on an acceptable approach for demonstrating the technical adequacy of a QRVA used to support a regulatory application. Central to this approach is the concept that the QRVA needs to only have the scope and level of detail necessary to support the application for which it is being used, but it always needs to be technically acceptable. |
| **Technical Elements** | |
| *(see QRVA Technical Elements)* | The term technical elements has the same meaning as QRVA technical elements in the context of QRVA and is defined under "QRVA Technical Elements." |
| **Technical Quality** | |
| *(see Technical Acceptability)* | The term technical quality has the same meaning as technical acceptability and is defined the same as the term "Technical Acceptability." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Top Event (Event Tree Top Event)** | |
| The events across the top of an event tree needed to mitigate an accident. *(see Event Tree, Fault Tree)* | Top events are the events across the top of the event tree, which graphically represent the systems needed to keep the facility in a safe state following an initiating event; i.e., a challenge to facility operation. A top event is the starting point of the fault tree, which identifies all of the pathways that lead to a system failure. The fault tree starts with the top event, as defined by the event tree, and identifies what equipment and operator actions, if failed, would prevent successful operation of the system.<br>The ASME/ANS PRA Standard includes two terms: event tree top event and top event. Event tree top event is defined as "the conditions (i.e., system behavior or operability, human actions, or phenomenological events) that are considered at each branch point in an event tree." Top event is defined as the "undesired state of a system in the fault tree model (e.g., the failure of the system to accomplish its function) that is the starting point (at the top) of the fault tree."<br>An illustration of a top event is shown under the discussion for the term "Event Tree." |
| **Truncation Limit** | |
| The minimum value of contributors retained in the QRVA quantification process. *(see Accident Sequence, Cut set)* | In a QRVA, a truncation limit is a numerical criterion that defines the boundaries, in terms of frequencies or probabilities, of what is retained and what is screened out. The truncation limit determines what accident sequences or cut sets are retained for or excluded from further analysis.<br>Since truncation limit affects QRVA quantification, Regulatory Guide 1.200 notes that truncation values should be set relative to the total facility LOFICF such that the LOFICF is stable with respect to further reduction in the truncation value.<br>The ASME/ANS PRA Standard defines truncation limit as "the numerical cutoff value of probability or frequency below which results are not retained in the quantitative QRVA model or used in subsequent calculations (such limits can apply to accident sequences-cut sets, system level cut sets, and sequence-cut set database retention)." |
| **Unavailability** | |
| *(see Availability)* | The term unavailability is the opposite of availability and is defined under "availability." |
| **Uncertainty (Aleatory, Random, Stochastic, Epistemic, State-of-Knowledge, Model, Source of Model, Key Source of Model, Parameter, Completeness)** | |
| Variability in an estimate because of the randomness of the data or the lack of knowledge. | When used in the context of a QRVA, the term uncertainty is associated with the lack of information or knowledge, or the random behavior of a system or model that is taken into account in the QRVA in different ways. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | In defining uncertainty, there are two types: aleatory and epistemic. Aleatory uncertainty is based on the randomness of the nature of the events or phenomena and cannot be reduced by increasing the analyst's knowledge of the systems being modeled. Therefore, it is also known as random uncertainty or stochastic uncertainty. Epistemic uncertainty is the uncertainty related to the lack of knowledge or confidence about the system or model and is also known as state-of-knowledge uncertainty.<br>The QRVA model itself reflects aleatory uncertainty. The QRVA model contains epistemic uncertainty that includes model uncertainty, parameter uncertainty, or completeness uncertainty.<br>In the ASME/ANS PRA Standard, uncertainty is defined as "a representation of the confidence in the state-of-knowledge about the parameter values and models used in constructing the PRA."<br>In the ASME/ANS PRA Standard, aleatory uncertainty is defined as "the uncertainty inherent in a nondeterministic (stochastic, random) phenomenon. Aleatory uncertainty is reflected by modeling the phenomenon in terms of a probabilistic model. In principle, aleatory uncertainty cannot be reduced by the accumulation of more data or additional information. (Aleatory uncertainty is sometimes called 'randomness.')"<br>In the ASME/ANS PRA Standard, epistemic uncertainty is defined as "the uncertainty attributable to incomplete knowledge about a phenomenon that affects our ability to model it. Epistemic uncertainty is reflected in ranges of values for parameters, a range of viable models, the level of model detail, multiple expert interpretations, and statistical confidence. In principle, epistemic uncertainty can be reduced by the accumulation of additional information. (Epistemic uncertainty is sometimes also called 'modeling uncertainty.')"<br>Model uncertainty is discussed in NUREG-1855 as follows:<br>"Model uncertainty is related to an issue for which no consensus approach or model exists and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, and introduction of a new initiating event). A model uncertainty results from a lack of knowledge of how structures, systems and components (SSC) behave under the conditions arising during the development of an accident. A model uncertainty can arise for the following reasons:<br>a. The phenomenon being modeled is itself not completely understood (e.g., behavior of gravity-driven passive systems in new reactors, or crack growth resulting from previously unknown mechanisms). For some phenomena, some data or other information may exist, but it needs to be interpreted to infer behavior under conditions different from those in which the data were collected (e.g., RCP seal LOCA information).<br>b. The nature of the failure modes is not completely understood or is unknown (e.g., digital instrumentation and controls)." |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| | In the ASME/ANS PRA Standard, source of model uncertainty is defined as: "a source that is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event). A source of model uncertainty is labeled "key" when it could impact the PRA results that are being used in a decision, and consequently, may influence the decision being made. Therefore, a key source of model uncertainty is identified in the context of an application. This impact would need to be significant enough that it changes the degree to which the risk acceptance criteria are met, and therefore, could potentially influence the decision."<br><br>NUREG-1855 has additional discussion on key sources of model uncertainty. The terms key model uncertainty and key sources of model uncertainty have the same meaning.<br><br>Parameter uncertainty is the uncertainty in the values of the parameters of a model represented by a probabilistic distribution. Examples of parameters that could be uncertain include initiating event frequencies, component failure rates and probabilities, and human error probabilities that are used in the quantification of the accident sequence frequencies.<br><br>Completeness uncertainty is caused by the limitations in the scope of the model, such as whether all applicable physical phenomena have been adequately represented, and all accident scenarios that could significantly affect the determination of risk have been identified.<br><br>Completeness uncertainty also can be thought of as a type of model uncertainty. However, completeness uncertainty is separated from model uncertainty because it represents a type of uncertainty that cannot be quantified. It also represents those aspects of the system that are, either knowingly or unknowingly, not addressed in the model. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Uncertainty Analysis** | |
| A process for determining the level of imprecision in the results of the QRVA and its parameters. | In a QRVA, the ways in which the uncertainty in the results is presented includes the following:<br>a. A continuous probability distribution on numerical results.<br>b. A discrete probability distribution representing the impact of different models or assumptions.<br>c. Sensitivity studies that provide a discrete set of results that represent the results of making different assumptions or using different models, or that represent the impact of varying key parameters in the model that have significant uncertainty, without providing weights or probabilities to the members of the set.<br>d. Bounds or ranges of results that represent the results of the extreme assumptions.<br>e. An identification of limitations in the scope of the model (e.g., incompleteness) and how they might influence the applicability of the QRVA.<br>The ASME/ANS PRA Standard defines uncertainty analysis as "the process of identifying and characterizing the sources of uncertainty in the analysis, and evaluating their impact on the PRA results and developing a quantitative measure to the extent practical." |
| **Uncertainty Distribution** | |
| *(see Probability Distribution)* | The term uncertainty distribution is related to the term probability distribution and is defined under "Probability Distribution." |
| **Uncertainty Interval, Uncertainty Range** | |
| A range that bounds the uncertainty value(s) of a parameter or analysis result by establishing upper and lower limits. *(see Confidence Interval, Probability Distribution)* | In a QRVA, uncertainty intervals can provide the range of the frequency or probability of the various inputs (e.g., initiating event frequencies, component failure probabilities, human error probabilities), as well as outputs of the analysis; e.g., LOFICF, conditional containment failure probability. However, in most cases, a probability distribution of the uncertainty around a mean value is preferred.<br>NUREG 1855 defines uncertainty interval as a characterization of the uncertainty. This characterization could, in the simplest approach, take the form of an interval; i.e., a range of values within which the value lies. However, it is more usual to characterize the uncertainty in terms of a probability distribution on the value of the quantity of concern, whether it is a parameter, accident sequence frequency, or a loss of fuel inventory control frequency.<br>The NRC Website Glossary defines uncertainty range as "an interval within which a numerical result is expected to lie within a specified level of confidence. The interval often used is the 5–95 percentile of the distribution reporting the uncertainty."<br>The definition provided was based on definitions in the NRC Website Glossary and in NUREG-1855. |

## Table E-1. Terms and Definitions (Continued)

| Term and Definition | Discussion |
|---|---|
| **Uncertainty Range** | |
| *(see Uncertainty Interval)* | The term uncertainty range has the same meaning as uncertainty interval and is defined under "Uncertainty Interval." |
| **Unreliability** | |
| *(see Reliability)* | The term unreliability is the opposite of reliability and is defined under "Reliability." |
| **Up-to-Date** | |
| *(see QRVA Configuration Control*, *As-Built As-Operated)* | The term up-to-date is related to QRVA configuration control and is defined under "QRVA Configuration Control" or "As-Built As-Operated." |
| **Vulnerability** | |
| Weakness in the design or operation of a system, component, or structure that could disable its function. | Results from a QRVA of a facility model can be used to identify facility vulnerabilities (e.g., vulnerabilities related to system design or facility operations). The term vulnerability has been based on the contribution of accident sequence types or individual failure events (e.g., fault tree basic events) to overall facility LOFICF or a percent contribution to LOFICF (e.g., a functional accident sequence with a LOFICF that exceeds 1E-04/yr, or one that contributes more than 50% to the total facility LOFICF). |
| **Water Immersion** | |
| Direct exposure from fuel chemical in contaminated water given to an individual immersed in the water. | In a Level 3 or 4 QRVA, for the consequence calculation, water immersion, is one of the assumed pathways by which an individual can receive fuel chemical exposure. The pathways of exposure include: (1) direct external exposure from fuel chemical in a plume (air immersion ), (2) direct exposure from fuel chemical in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of fuel chemicals in the plume and resuspended material deposited on the ground, (4) exposure to fuel chemical deposited on the ground (groundshine), (5) fuel chemical deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited fuel chemicals that make their way into the food and water pathway. |

## E.2. QRVA Technical Elements

Table E-2 provides the technical elements as adapted from the ASME PRA Standard for Level 1, Level 2 and Level 3 (or 4) QRVA with the associated discussion. The technical elements are listed alphabetically by level of the QRVA and hazard groups.

**Table E-2. QRVA Technical Elements**

| Technical Element | Discussion |
|---|---|
| **Level 1 Internal Events** | |
| **Accident Sequence Analysis** | The term accident sequence analysis is a technical element in the ASME/ANS PRA Standard whose objectives are to ensure that the response of the facility's systems and operators to an initiating event is reflected in the assessment of LOFICF and AFRF. |
| **Data Analysis** | The term data analysis is a Level 1 technical element in the ASME/ANS PRA Standard whose objectives are to provide estimates of the parameters used to determine the probabilities of the basic events representing equipment failures and unavailabilities modeled in the QRVA. |
| **Human Reliability Analysis** | The term human reliability analysis is a Level 1 technical element in the ASME/ANS PRA Standard whose objective is to ensure that the impacts of facility personnel actions are reflected in the risk assessment. |
| **Initiating Event Analysis** | The term initiating event analysis is a technical element in the ASME/ANS PRA Standard whose objective is to identify and quantify events that could lead to loss of fuel inventory control. |
| **AFRF Analysis** | The term acute fuel release frequency analysis is a technical element of Part 2 of the ASME/ANS PRA Standard. The objectives of the AFRF analysis element are to identify and quantify the contributors to acute fuel releases based on the facility-specific loss of fuel inventory control scenarios. |
| **Quantification** | The term quantification is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to provide an estimate of loss of fuel inventory control frequency (and support the quantification of AFRF) based on the facility-specific loss of fuel inventory control scenarios. |
| **Success Criteria** | The term accident success criteria is a technical element in the ASME/ANS PRA Standard whose objectives are to define the facility-specific measures of success and failure that support the other technical elements of the QRVA. |
| **Systems Analysis** | The term systems analysis is also a technical element in the ASME/ANS PRA Standard whose objectives are to identify and quantify the causes of failure for each facility system represented in the initiating event analysis and accident sequence analysis. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Level 1 Internal Flood** | |
| **Internal Flood Accident Sequences and Quantification** | The term internal flood accident sequences and quantification is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to quantify the loss of fuel inventory control frequency and AFRF for the internal flood facility response sequences. |
| **Internal Flood Facility Partitioning** | The term internal flood facility partitioning is a technical element in the ASME/ANS Level 1 PRA Standard whose objectives are to identify facility areas where internal floods could lead to loss of fuel inventory control in such a way that facility-specific physical layouts and separations are accounted for. |
| **Internal Flood Scenarios** | The term internal flood scenarios is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to develop a set of internal flood scenarios relating flood source, propagation path(s), and affected equipment. |
| **Internal Flood Source Identification and Characterization** | The term internal flood source identification and characterization is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to identify the various sources of floods and equipment spray within the facility, along with the mechanisms resulting in flood or spray from the sources, and a characterization of the flood/spray sources is made. |
| **Internal Flood-Induced Initiating Events** | The term internal flood-induced initiating events is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to determine the expected facility response to the selected set of flood scenarios, and an accident sequence from the internal event QRVA that is reasonably representative of this response is selected for each scenario. |
| **Internal Fire** | |
| **Circuit Failure Analysis** | The term circuit failure analysis is a technical element in the ASME/ANS Level 1 PRA Standard whose objectives are to treat fire-induced cable failures and their impact on the facility equipment, systems, and functions, and estimate the relative likelihood of various circuit failure modes. |
| **Fire Ignition Frequency** | The term fire ignition frequency is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objective is to estimate the frequency of fires (expressed as fire ignitions per facility-year). |
| **Fire QRVA Cable Selection** | The term fire QVRA cable selection is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objectives are to identify and locate cables required to support the operation of fire QRVA equipment selected and cables whose failure could adversely affect credited systems and functions. |
| **Fire QRVA Equipment Selection** | The term fire QVRA equipment selection is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objective is to identify the set of facility equipment that will be included in the fire QRVA. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Fire QRVA Facility Response Model** | The term fire QVRA facility response model is a technical element for internal fires in the ASME/ANS PRA Standard whose objective is to identify the initiating events that can be caused by a fire event and develop a related accident sequence model; and to depict the logical relationships among equipment failures (both random and fire-induced) and human failure events for loss of fuel inventory control frequency and AFRF assessment when combined with the initiating event frequencies. |
| **Fire Risk Quantification** | The term fire risk quantification is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objective is to quantify and present fire risk results. |
| **Fire Scenario Selection and Analysis** | The term fire scenario selection and analysis is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objectives are to select a set of fire scenarios for each unscreened physical analysis unit upon which fire risk estimates will be based, characterize the selected fire scenarios, determine the likelihood and extent of risk-relevant fire damage for each select fire scenario, and examine multi-compartment fire scenarios. |
| **Facility Boundary Definition and Partitioning** | The term facility boundary definition and partitioning is a technical element in the ASME/ANS PRA Standard for internal fire whose objective is to define the physical boundaries of the analysis and divide the various volumes within that boundary into physical analysis units. |
| **Post-Fire Human Reliability Analysis** | The term post-fire human reliability analysis is a technical element in the ASME/ANS PRA Standard whose objective is to consider the operator actions as needed for stable safe operation, including those called out in the relevant facility fire response procedures. |
| **Qualitative Screening** | The term fire QVRA cable selection is a technical element in the ASME/ANS Level 1 Internal PRA Standard whose objective is to identify physical analysis units whose potential fire risk contribution can be judged negligible without quantitative analysis |
| **Quantitative Screening** | The term fire ignition frequency is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objective is to screen physical analysis units from further consideration based on preliminary estimates of fire risk contribution and using established quantitative screening criteria. |
| **Seismic/Fire Interactions** | The term seismic/fire interactions is a technical element in the ASME/ANS Level 1 PRA Standard whose objective is to provide a qualitative review of potential interactions between an earthquake and fire that might contribute to facility risk. |
| **Uncertainty and Sensitivity Analyses** | The term uncertainty and sensitivity analysis is a technical element in the ASME/ANS Level 1 Internal Fire PRA Standard whose objectives are the identification and treatment of uncertainties throughout the Fire QRVA process. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Seismic Events** | |
| **Probabilistic Seismic Hazard Analysis** | The term probabilistic seismic hazard analysis is a technical element for seismic QRVA in the ASME/ANS PRA Standard whose objective is to estimate the probability or frequency of exceeding different levels of vibratory ground motion. |
| **Seismic Fragility Analysis** | The term seismic fragility analysis is a technical element for seismic QRVA in the ASME/ANS PRA Standard whose objective is to determine the facility-specific failure probabilities of structures, systems, and components as a function of the seismic event intensity level, usually given in peak ground acceleration. |
| **Seismic Facility Response Analysis** | The term seismic facility response analysis is a technical element in seismic QRVA in the ASME/ANS PRA Standard whose objective is to develop a facility response model that addresses the initiating events and other failures resulting from the effects of the seismic hazard that can lead to loss of fuel inventory control or acute fuel release. The model usually is based on the internal events QRVA model to incorporate those aspects that are different, because of the seismic hazard's effects, from the corresponding aspects of the internal events model. |
| **High Winds** | |
| **High Wind Fragility Analysis** | The term high wind fragility analysis is a technical element for high wind hazards in the ASME/ANS PRA Standard whose objective is to identify those structures, systems, and components susceptible to the effects of high winds and to determine their facility-specific failure probabilities as a function of the wind intensity. |
| **High Wind Facility Response Analysis** | The term high wind facility response analysis is a technical element for high winds QRVA in the ASME/ANS PRA Standard. The objective is: (1) to modify the internal events of the QRVA model to include the effects of high wind events in terms of the initiating events and failures induced, and (2) to exercise the resulting model to obtain quantitative results in terms of loss of fuel inventory control frequency and AFRF. |
| **High Winds Hazard Analysis** | The term high winds hazard analysis is a technical element for high wind hazards in the ASME/ANS PRA Standard whose objective is to assess the frequency of occurrence of high wind as a function of intensity on a site-specific basis. |
| **External Floods** | |
| **External Flood Fragility Analysis** | The term external flood fragility analysis is a technical element for external floods in the ASME/ANS PRA Standard whose objective is to identify those structures, systems, and components susceptible to the effects of external floods and to determine their facility-specific failure probabilities as a function of the severity of the external flood. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **External Flood Hazard Analysis** | The term external flood hazard analysis is a technical element for external floods in the ASME/ANS PRA Standard whose objective is to assess the frequency of occurrence of external floods as a function of severity on a site-specific basis. |
| **External Flood Facility Response Model and Quantification** | The term external flood facility response model and quantification is a technical element for external floods in the ASME/ANS PRA Standard whose objectives are to:<br>• develop an external flood facility response model by modifying the internal events QRVA model to include the effects of the external flood in terms of initiating events and failures caused;<br>• quantify this model to provide the CLOFICP and conditional acute fuel release probability (CAFRP) for each defined external flood facility damage state;<br>• evaluate the unconditional LOFICF and AFRF by integrating the CLOFICP/CAFRP with the frequencies of the facility damage states obtained by combining the external flood hazard analysis and external flood fragility analysis. |
| **Other External Hazards** | |
| **External Hazard Analysis** | The term external hazard analysis is also a technical element for other external hazards in the ASME/ANS PRA Standard whose objective is to assess the frequency of occurrence of the external hazard as a function of intensity on a site-specific basis. |
| **External Hazard Fragility Evaluation/ Analysis** | The term external hazard fragility evaluation is also a technical element for other external hazards in the ASME/ANS PRA Standard whose objective is to identify those structures, systems, and components susceptible to the effects of the other external hazard and to determine their facility-specific failure probabilities as a function of the intensity of the hazard. |
| **External Hazard Facility Response Model/Analysis** | The term external hazard facility response model is a technical element for other external hazards in the ASME/ANS PRA Standard whose objective is to develop a facility response model that addresses the initiating events and other failures resulting from the effects of the external hazard that can lead to loss of fuel inventory control or acute fuel release. The model is based on the internal events QRVA model to incorporate those aspects that are different, because of the external hazard's effects, from the corresponding aspects of the internal events model. |
| **Level 2** | |
| **Containment Capacity Analysis** | The term containment capacity analysis is a technical element of a Level 2 QRVA whose objective is to select an analysis method and calculate the ability of the facility containment characteristics to withstand challenges. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Interface between a Level 2 and Level 3 (or 4) QRVA** | The term interface between Level 2 and Level 3 (or 4) QRVA is a technical element of a Level 2 QRVA whose objectives are to provide clear traceability of the release category quantification back to the Level 2 analysis, to assure that initiating event information that could affect the Level 3 (or 4) analysis is communicated, and to assure that all information required for the Level 3 (or 4) analysis is provided in suitable form. |
| **Level 1–2 Interface** | The term level 1-2 interface is a technical element of a Level 2 QRVA whose objective is to consolidate or group accident sequences (or individual cut sets) from the Level 1 QRVA in a way that reduces the number of unique scenarios for evaluation, but preserves initial and boundary conditions to the analysis of facility response (i.e., facility damage states or equivalent). |
| **Probabilistic Treatment of Event Progression and Source Terms** | The term probabilistic treatment of event progression and source terms is a technical element of a Level 2 QRVA whose objective is to establish a framework to support the systematic quantification of the potential severe accident sequences evolving from each Level 2 loss of fuel inventory control sequence in sufficient detail. |
| **Fuel Chemical Source Term Analysis** | The term source term analysis is a technical element in the draft Level 2 QRVA whose objective is to develop a quantitative basis for associating a unique fuel chemical source term to the environment for each accident progression sequence and release category. The metrics used to define a source term can vary, depending on the objective and intended application of the QRVA. |
| **Severe Accident Progression Analysis** | The term severe accident progression analysis is a technical element of a Level 2 QRVA whose objective is to generate a technical basis, rooted in realistic deterministic analysis for describing the chronology of postulated accident involving significant fuel release, quantitatively characterizing thermal and mechanical challenges to engineered barriers to fuel chemical release to the environment, and generating quantitative estimates of fuel chemical release to the environment for accident sequences identified as contributors to the frequency of release. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Level 3 (or 4) QRVA** | |
| **Fuel Transport and Diffusion** | The term transport and diffusion is a technical element of a Level 3 (or 4) QRVA that refers to the process by which material that has been released from facility containment, moves through and spreads upon release to the environment. The objective of FTD is to model the transport of fuel chemical as it travels for many hours in the atmosphere, above-ground, and underground environment under the meteorological and other environmental conditions prevailing at and beyond the site that can change in both space and time. FTD models range from simple straight-line, steady-state Gaussian dispersion models that calculate ground-level instantaneous and time-integrated airborne concentrations in the plume, to more sophisticated models that allow terrain-dependent effects and temporal variations in wind speed, atmospheric stability, soil or rock conditions, etc.<br>Probabilistic consequence modeling codes typically include sampling of meteorological and monitoring well data from a site-specific annual data base of hourly weather data to determine appropriately weighted scenarios of plume transport under different weather and other environmental conditions to provide probabilistic results, model FTD for accident- and site-specific input parameters, accommodate temporal and spatial changes in meteorological conditions, calculate deposition of chemicals, and document algorithms, assumptions, limitations, and uncertainties. |
| **Economic Factors** | The term economic factor is a technical element in a Level 3 (or 4) QRVA whose objective is to determine the economic impacts of the release on the surrounding land, water tables, and the population. |
| **Meteorological Data** | The term meteorological data is a technical element of a Level 3 (or 4) QRVA whose objective is to provide valid and representative meteorological data that are input into the atmospheric transport and dispersion codes, which provide the basis for consequences analysis calculations. |
| **Protective Action Parameters and Other Site Data** | The term protective action parameters and other site data is a technical element in a Level 3 (or 4) QRVA whose objectives are to model appropriate emergency response actions and protective actions; use appropriate site, local, and regional data; and document site-specific data, emergency response planning modeling, assumptions, limitations, and uncertainties. |
| **Quantification and Reporting** | The term quantification and reporting is a technical element of a Level 3 (or 4) QRVA whose objectives are to ensure that the Level 3 (or 4) model executes properly, proves appropriate results, and is documented in a manner that facilitates risk assessments, QRVA applications, upgrades and peer reviews. |

## Table E-2. QRVA Technical Elements (Continued)

| Technical Element | Discussion |
|---|---|
| **Risk Integration** | The term risk integration is a technical element of a Level 3 (or 4) QRVA whose objective is to combine the Level 3 (or 4) analyses with the results from the Level 1–2 analyses to obtain a characterization of the overall risk, including uncertainty. |
| **Transition from the Fuel (Fuel chemical) Release to Level 3 (or 4)** | The term transition from fuel chemical release to Level 3 (or 4) is a technical element of a Level 3 (or 4) QRVA whose objectives are to provide clear traceability of the release category quantification back to the fuel chemical release analysis, to ensure that initiating event information that could affect the Level 3 (or 4) analysis is communicated, and to ensure that all information required for the Level 3 (or 4) analysis is provided in suitable form. |

# Appendix F. In-Progress Review Feedback Summary

On November 27, 2017, a skeleton draft report for the Phase 1 QRVA, R-3751812-2043 (RHBFSF QRVA Phase 1 Draft Report for IPR [Data Analysis]) (Draft A).pdf, was distributed to the Navy and key stakeholders for review and comment. This draft report and the ensuing QRVA Phase 1 IPR was designed to focus primarily on the data analysis, specifically, the initiating events data analysis and the hardware response events data analysis, for the QRVA. A formal IPR meeting was conducted for the Phase 1 QRVA during the week of December 5–9, 2017, at the ABS Consulting office in Irvine, California. During this review week, ABS Consulting presented a QRVA Methodology Orientation Training Seminar on December 5, 2017, and reviews of the material presented in the skeleton draft report for the Phase 1 QRVA, R-3751812-2043 (RHBFSF QRVA Phase 1 Draft Report for IPR [Data Analysis]) (Draft A).pdf, were performed by the Navy and key stakeholders, including the EPA, Hawaii DOH, and the Honolulu Board of Water Supply and their consultants during and after December 6–7, 2017. Associated review comments were documented and discussed during subsequent conference call meetings in January 2018. The IPR review comments and proposed resolutions are presented in Table F-1.

## Table F-1. IPR Comments and Proposed Resolutions

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 1 | 12/26/2017 | IPR Comments-Takara.docx | Recommend replacing 3rd & 4th sentences with, "This preliminary draft of the Phase 1 QRVA baseline report focuses only on the data analysis section and was submitted to support the in-progress review (IPR) meeting scheduled to be held December 5-7, 2017." [Comment 1; Page 1-1, 2nd ¶, §1] | Agree; will revise text. |
| 2 | 12/26/2017 | IPR Comments-Takara.docx | Recommend changing 2nd sentence to read, "The RHBFSF QRVA team applies probability…" [Comment 2; Page 2-5, 2nd ¶, §2.3] | Agree; will revise text. |
| 3 | 12/26/2017 | IPR Comments-Takara.docx | Recommend changing last sentence to read, "Such information…" [Comment 3; Page 5/18, 4th ¶, §5.2.1.3.1] | Agree; will revise text. |
| 4 | 12/26/2017 | IPR Comments-Takara.docx | Recommend changing last sentence to read, "In addition, each time the component failed the test, …" [Comment 4; Page 5-66, 5th ¶, §5.2.2.1.3.2] | Agree; will revise text. |
| 5 | 12/26/2017 | IPR Comments-Takara.docx | Recommend revising the 1st sentence as it seems like some words may be missing. [Comment 5; Page 5-98, 1st ¶, §5.3.3] | Agree; will revise text. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 6 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | The NUREG/CR-2300 is stated to be published April 1983. The only copy I could find on-line is dated January 1983. Is the April 1983 on the internet? [Item 1; Page 2-2] | January 1983 is correct. We will revise the reference information. |
| 7 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | 2nd line: Change “apples” to “applies” [Item 2; Page 2-5] | Agree; will revise text. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 8 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Also slide 22: Will the QRVA also consider the Security System (if there is a Security System failure, will the first responders be able to access the facility?" [Item 3; Page 3-1] | We are unclear on what the reviewer's "slide numbers" refer to in these comments. The review was to be for the IPR draft QRVA report document distributed for review, and not on any slides presented at the IPR meeting. In addition, this comment does not appear to relate to Item 3 on page 3-1 of the draft report distributed for review. Loss of the Security System is not included as an initiating event, as we are unaware of any scenario that could lead to loss of fuel inventory control directly resulting from loss of the Security System. Loss of the Security System could potentially be associated with various loss of power scenarios, but would only be considered as an influencer to potential human response actions. This would more likely be an issue in an external events analysis for Phase 2-4 work (e.g., flooding, fire, and seismic event scenarios), which are not in the current scope of the Phase 1 internal events analysis. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 9 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Also slide 22: Will the QRVA also consider the telecommunication (telephones throughout the tunnel and system and from the control room to the outside world?) [Item 4; Page 3-1] | We are unclear on what the reviewer's "slide numbers" refer to in these comments. The review was to be for the IPR draft QRVA report document distributed for review, and not on any slides presented at the IPR meeting. In addition, this comment does not appear to relate to Item 4 on page 3-1 of the draft report distributed for review. Loss of the Telecommunication System is not included as an initiating event, as we are unaware of any scenario that could lead to loss of fuel inventory control directly resulting from loss of the Telecommunication System. Loss of the Telecommunication System could potentially be associated with various loss of power scenarios, but would only be considered as an influencer to potential human response actions. This would more likely be an issue in an external events analysis for Phase 2-4 work (e.g., flooding, fire, and seismic event scenarios), which are not in the current scope of the Phase 1 internal events analysis. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 10 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Also slide 22: Will the QRVA also consider the risks associated with the failure of the internet connection? Is it a stand-alone system or is it connected to NMCI that can perform updates to the system without notice? [Item 5; Page 3-1] | We are unclear on what the reviewer's "slide numbers" refer to in these comments. The review was to be for the IPR draft QRVA report document distributed for review, and not on any slides presented at the IPR meeting. In addition, this comment does not appear to relate to Item 5 on page 3-1 of the draft report distributed for review. Loss of the Internet System is not included as an initiating event, as we are unaware of any scenario that could lead to loss of fuel inventory control directly resulting from loss of the Internet System. Loss of the Internet System could potentially be associated with various loss of power scenarios, but would only be considered as an influencer to potential human response actions. This would more likely be an issue in an external events analysis for Phase 2-4 work (e.g., flooding, fire, and seismic event scenarios), which are not in the current scope of the Phase 1 internal events analysis. |
| 11 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Refer to the TIRM Procedure Decision Document, Attachment C for the Planned TIRM schedule for the 18 tanks. [Item 6; Page 4-1] | |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 12 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | 2nd to last line: Change "Stich" to "Such" [Item 7; Page 5-18] | Agree; will revise text. |
| 13 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Are there any references to coating failure, which will affect the risk of a release through a defective weld? The coating system that we are proposing to use is a thick-based system that will cover over weld indications, and will prevent a release if the weld "opens up". Coating failure will increase the risk of a release if the tank is coated.<br>The tanks are currently coated on the lower dome. The TIRM and TUA 1A both consider recoating the lower dome. [Item 8; Slide 98] | We are not aware of any such references; however, we are happy to incorporate information from them if/when identified to the QRVA project team. We do not follow the reviewers comment that "Coating failure will increase the risk of a release if the tank is coated." This is counterintuitive to our team, as a coating failure plus an opening (hole or crack) in the tank would have to exist to result in loss of fuel inventory control. We are aware of the TUA recoating alternative. However, it is important to emphasize that our Phase 1 QRVA is a baseline QRVA and will not be including any evaluations on unfunded alternatives. |
| 14 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | My general question is that there have been prior releases, but then does the failure rate change if the root cause of the failure has been removed, such as the removal of the tell-tails, coating the tank, replacing the sample lines on the outside of the tank, etc. [Item 9; Slide 122] | We intend to investigate alternative failure rates based on removal of certain failure modes/mechanisms. We are considering alternative initiating event frequencies based on removal of the telltales. We do not understand the reviewer's reference to "Slides" here. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 15 | 12/26/2017 | Rev Cmmts Template for Sect 8 QRVA SOW_WP_Regin.doc | Not sure about my notes, but I wrote: "UST vs AST --- corrosion occurs on soil side not matter what type of tank it is." Note that a 50,000 bbl AST has less sq ft exposed to soil than a 50,000 bbl UST. Therefore, the unit used should be sq ft exposed to soil, not size of tank. [Item 10; Slide 117] | We do not understand the reviewer's reference to "Slides" here. We do acknowledge the sq ft relationship to corrosion. |
| 16 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 1. The Regulatory Agencies are interested in the data and other supporting information that the Navy will use to evaluate its ability to detect and respond to initiating events not only for the entire facility, but also for the tanks specifically. The magnitude of any uncontrolled release is highly correlated with the ability to detect and respond to the initiating event(s). Releases that go undetected over long periods of time, or releases that are detected but do not receive an effective response can result in large-scale events that may pose a significant risk to groundwater and drinking water. The Regulatory Agencies believe there is opportunity to reduce risk at the facility by improving release detection and response practices. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. Our planned modeling will account for this issue. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 17 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 2. The Regulatory Agencies recommend that the Navy evaluate the likelihood of initiating events from the tank vessels using various sources of generic data as well as Red Hill specific data, and consider including a discussion on the range of likelihood using these different data sources. As new corrosion and pitting data from scanning the tanks during inspections becomes available, the Navy should determine whether and how this site-specific scanning data could be incorporated to revise the likelihood of an initiating event from the tanks. Considering these recommendations, the Navy and its consultant should ultimately provide their assessment of the likelihood of an initiating event, based on their professional judgment. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. We are investigating use of generic data sources other than NUREG/CR-6828. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 18 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 3. The Regulatory Agencies recommend that the Navy continue to collect data on the human factors related to release detection and response. During our meetings, it did not appear that ABSG Consulting had sufficient relevant information related to the initiation of and response to the January 2014 release. Improvements in these human factors after the January 2014 release should only be credited due to demonstrable actions, such as written operating procedures, training, etc. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. This has an impact on the human reliability analysis that will be performed in the Phase 1 QRVA, but this was not part of the IPR draft report. We have received additional information on the January 2014 event since the IPR meeting. |
| 19 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 4. The Navy should consider quantification of thresholds of detection during static and transient (fuel movement) operations to define range and probable release sizes. This can be achieved by applying the standard tools of the QRVA already under way. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. This issue is being considered within the Event Sequence Analysis of the Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 20 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 5. The Regulatory Agencies suggest segregating the release assessment into two physical areas that contain fuel. The first area would focus on the tank vessels. This would include the tank vessel and nozzle to the point of the first valve. The second area would focus on the mechanical infrastructure attached to the tank vessels, such as the piping, valves and pumps. Estimating the frequency of an initiating event from the second area may have less uncertainty due to the more standard nature of the infrastructure. Understanding nature and magnitude of risk posed by these distinct physical areas is important for risk management decisions. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. The two general areas identified in this comment are being considered in the Event Sequence Analysis of the Phase 1 QRVA along with several other subdivided physical areas. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 21 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 6. Historical data should be incorporated thoughtfully into the QRVA. The Navy should characterize whether data is useful and relevant given the facility's current configuration. For example, many previous initiating events were the result of leaks in the telltale system that was eventually decommissioned in 1984. Additionally, other leaks were the result of faulty repairs, such as what occurred during the January 2014 release from tank 5. The Navy should also consider partitioning the probability of initiating events into those that may occur during different modes of normal operation (static storage, fuel movements, etc.), and those that may occur during other periods, such as recommissioning. | Agree. We are investigating alternative failure rates based on removal of certain failure modes/mechanisms. We are considering alternative initiating event frequencies based on removal of the telltales. We are considering splitting initiating event frequencies to apply to the return-to-service process versus during the normal service period. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 22 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 7. The Navy should review environmental data trends from soil vapor monitoring probes and groundwater monitoring wells and discuss whether any aberrations correspond to historical releases from the facility. | We have agreed to look at these data trends. However, looking forward, we anticipate identifying potential dates or date ranges where aberrations appear to exist, and then questioning the Navy on if these aberrations correspond to any record of actual fuel inventory loss; e.g., based on AFHE, top-gage, and periodic fuel inventory balancing calculations. We would generally only assume fuel loss occurred if these fuel inventory measurement processes clearly indicated the loss. |
| 23 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 8. The Regulatory Agencies suggest revising the categorization of leak magnitude ranges for initiating events. Currently the assessment indicates three general ranges which are:<br>• Chronic or Undetected (below 0.7 gallon per hour or 16.8 gallons per day)<br>• Small (below 72,000 gallons per day)<br>• Large (above 72,000 gallons per day)<br>We suggest further segregating the small category range because 72,000 gallons per day may be much greater than a release caused by corrosion hole or crack. Per our | We are investigating how we can apply RHBFSF-specific information to perform the segregation of the small leak category initiating events. If the reviewer can provide specific references for the corrosion/crack failure research indicated, particularly for the RHBFSF, we are happy to apply that information in more refined segregated initiating event category frequency evaluation for the QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| | | | preliminary calculation, I II 01h of an inch diameter hole could produce a leak of approximately 3,700 gallons per day at the 175-foot fill level assuming no back pressure on the hole. Given that one of the primary initiating events of concern could be caused by a through-hole corrosion or crack that has not been detected during tank inspection, the QRVA should reflect a conservative, but realistic initiating event. We suggest further research on corrosion/crack failures from data in the fuel industry to obtain a more realistic initiating event estimate. | |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 24 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments EPA DOH 2017 12 22.pdf | 9. The Regulatory Agencies encourage the Navy to dedicate resources to risk communication and interpretation. The analysis and outcomes of this QRVA involve sophisticated numerical analysis, and it will be important to convey this information in a manner that is conducive for public consumption. We recommend that the Navy include an executive summary and conclusion that clearly summarize the study. The Navy should also develop other communication materials when the Report is submitted to the Regulatory Agencies, such as a two-page fact sheet. | Agree. However, we see no recommended change to the IPR draft QRVA report based on this comment. We intend to report QRVA results in terms conducive for public consumption. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 25 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | We understand that the first draft of the QRVA Report will be made available after November 2018. Phase 1 is limited to certain internal events such as tank leaks, mechanical failures, and operational errors. Subsequent phases will address other hazards including seismic, fire, sabotage, and flooding. Also, the QRVA addresses only uncontrolled releases of fuel inventory past the boundary of the facility (Phase 2) and does not address the potential paths of the release or explicit aquifer risk. The QRVA Report will quantify the release risks for the facility as it exists today (including improvements currently under contract) but will not compare risks of Tank Upgrade Alternatives (TUAs). As such, the results of this QRVA Report will likely have little or no effect on the TUA decision (AOC Section 3). | In general, we agree with this comment. However, sabotage risk assessment is not planned to be performed for any Phase of the QRVA, as currently structured, as the Navy has removed that class of initiating events from consideration for the QRVA. We disagree, in general, with the final statement that "this QRVA Report will likely have little or no effect on the TUA decision (AOC Section 3)." We will not know that until the analysis is complete and we have fully digested the results. |
| 26 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | The Navy is using a comprehensive QRVA methodology and underlying failure rate data conventionally employed at commercial nuclear power plants. In the ABS implementation, frequencies of leaks in the future are estimated from three sources: past leaks as recorded for the nuclear power plant generic data, leaks recorded at other navy tanks, and records of past leaks at Red Hill. There is currently no | We are investigating application of generic data sources other than NUREG/CR-6928. Next, hypothetical failure rate acceleration over time can be included in the analysis, but only to the extent that we have sufficient information to adequately evaluate, quantitatively, what the failure rate acceleration factors would be over time. We do not have research supporting what those factors would be for the RHBFSF. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| | | | intention to incorporate the actual conditions (e.g., current corrosion depth, corrosion rates, weld defects) as determined from ongoing and upcoming testing. The potential for increased leak rates associated with aging mechanisms specific to these tanks will not be captured. | Our team has significant experience in investigating time-dependent failure rates for equipment. If the reviewer can provide such information, it can be applied in the QRVA. However, we note that, because the RHBFSF tanks are periodically inspected, and associated repairs are implemented prior to placing inspected tanks back into service, there is a natural "renewal" process continuously underway at the facility. If properly applied, these inspections would, therefore, tend to counteract the impacts of failure rate acceleration until and unless this acceleration factor was relatively large. We see no evidence of that based on tank inspection results. In addition, we might expect that tank inspection processes will improve over time, enabling the facility operator to more effectively and efficiently detect and measure flaws in the tanks. These factors support application of a constant failure rate model for this analysis. We agree to provide an example analytical approach in our analysis that could be applied for investigation of time-dependent corrosion rates in a QRVA, in general; however, we do not anticipate being able to apply such an approach without access to significant basic research on such issues at the RHBFSF. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 27 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Furthermore, we are concerned that ABS is relying too heavily on generic leak data (nuclear and other Navy tanks) at the expense of the actual Red Hill leak history which is quite extensive: 1,500 tank years of experience (20 tanks for 75 years). The nuclear power plant generic data (from NUREG/CR-6928, 2007 at Table: A.2.48-3) comprise reports from 671 relatively new (compared to Red Hill) unpressurized tanks in 101 commercial nuclear plants over an 8-year period (1997–2004). These data are predominantly from above ground storage tanks constructed to nuclear quality standards and maintained in a highly regulated environment. This entire database has recorded the sum total of just one small leak and zero large leaks. Likewise, the Navy tank leak data does not appear to have been carefully vetted for relevance to Red Hill tanks by removing tank leaks that are not from very large underground single-wall steel tanks that are not cathodically protected. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 28 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | This questionable choice of data sources introduces a significantly optimistic bias in terms of future leak predictions compared to those already observed and reported. The Red Hill tanks, in terms of size, vintage and environment, bear little resemblance to tanks in the generic databases, and the reported leaks at Red Hill should be weighted more heavily. To demonstrate this problem, the BWS has recalculated estimated future leak rates using the same approach employed by ABS, but in a manner that better recognizes the limits of the generic data. Our analysis yields estimated leak frequencies significantly higher than the preliminary estimates in the QRVA Report. The details of this is presented below. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 29 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Furthermore, the current risk assessment methodology described by ABS assumes the risk of a fuel leak is constant over the projected residual operating life of the facility and does not consider potential effects of aging. These effects may be mitigated by the Navy's non-destructive testing (NOT) and modified API tank inspection and repair methodology intended to assure leak-free operation for the 20-year period between inspections. However, as we have commented previously, the reliability of this methodology as applied at Red Hill has not yet been demonstrated. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 30 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Overall, we disagree with the manner in which preliminary estimates of future leak rates at Red Hill have been developed, and we believe the current approach has produced a biased (and significantly optimistic) projection of future performance. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 31 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | ABS lists three sources of data on leaks from unpressurized storage tanks: (1) a compilation of recent experience at United States (US) commercial nuclear power plants (NUREG/CR-6928, 2007); (2) data gathered from Navy installations other than the Red Hill facility; and, (3) a spreadsheet (referenced in the ABS report but not shared with BWS) that listed leak events that have occurred to date at Red Hill. The data from these three sources are summarized in Table 1.<br>See Table 1. Data sources used by ABS in estimating frequencies of tank leakage at Red Hill (NUREG/CR-6928, 2007); ABS, 2017a at Table 5-12 and Table 5-14) in the BWS comment letter. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 32 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | As shown in Table 1, the NUREG data being used by ABS show a dramatically different operating experience at commercial nuclear plants than has been exhibited historically at the Red Hill facility-specifically , the data cited in the ABS report show that leaks (either small or large) of Red Hill tanks have occurred at a frequency more than 100 times greater than the corresponding frequency of nuclear plant tanks (1 leak in 5368 tank years for nuclear tanks = 0.000186 leaks per tank year vs 37 total leaks in 1,500 operating years for Red Hill tanks = 0.025 leaks per tank year). This discrepancy raises questions about the relevance of the NUREG data and the effect of including those data in the QRVA Report of the Red Hill facility. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 33 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Furthermore, the appendices to NUREG/CR-6928 appear to indicate the single recorded leak shown in Table 1 occurred in a tank classified as “Other” (among 26 listed categories of unpressurized tanks). This “Other” category contains only 19 tanks and may be the only category in the NUREG database containing underground tanks. The system descriptions in Section A.2.48.2 suggest that tanks in the other 25 categories are primarily above ground and store water rather than fuel. No leaks were reported in any of these tanks over the 1997-2004 (8-year) time period. Inclusion in the QRVA analysis of data from tanks of questionable relevance is therefore likely to underestimate leak rates at Red Hill. A separate analysis (reported in Table A.2.48-8) shows the mean leak rate (1 leak every 104 years) for unpressurized tanks in this “Other” category is almost 40 times higher than the mean leak rate (1 leak every 3,565 years , see Table 2 below) for all tanks using all the NUREG data as ABS currently does in the QRVA Report. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 34 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | In the limited results presented so far in the QRVA Report, ABS has effectively merged data from Red Hill with data from other sources to develop estimates of the frequency of small and large leaks from unpressurized storage tanks. The method of combining data used by ABS is called "Bayesian updating". In this approach, before considering the Red Hill data, ABS analysts specify a "prior" distribution, which expresses how frequently small or large leaks are expected based on other sources of information, such as the NUREG data. (For example, one can calculate the probability a small leak will occur at a rate greater than one per 1,000 years). This prior distribution is then "updated" with Red Hill data to obtain a "posterior" distribution, which expresses how frequently small or large leaks are expected based on all sources of information, including the Red Hill data. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |
| 35 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | In the QRVA Report, ABS presents results from two separate analyses: a one-stage analysis incorporating leak data from NUREG/CR-6928 | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| | | | and the Red Hill site and a two-stage analysis also incorporating leak data from other Navy installations. After further evaluation of the data, ABS stated it favored its one-stage analysis, results of which are summarized in the second to fourth columns of Table 2. The reported values are the expected leak frequencies using only the NUREG data (prior mean) and then combining the NUREG data with Red Hill data via Bayesian updating (posterior mean). For purposes of comparison, the last column of Table 2 shows the corresponding expected leak frequencies using only the Red Hill data, obtained via Bayesian updating with a "non-informative" prior distribution—i.e., without relying on the NUREG data of questionable relevance.<br>See Table 2 in the BWS comment letter. Expected frequencies of individual tank leakage at Red Hill from ABS analysis, compared to alternative analysis using all Red Hill data only (ABS, 2017a, Table 5-10 & 5-15). Hours have been converted to years in this table.<br>As shown in Table 2, the expected leak frequencies of individual tanks at Red Hill are one-to-two orders of magnitude greater when only Red Hill data are used, compared to the values obtained by ABS using NUREG data | approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| | | | and the data for individual Red Hill tanks (while excluding data from the other 19 Red Hill tanks).<br>The vast discrepancy between the NUREG data and the recorded experience at Red Hill is underscored further by comparing not only the expected frequencies of small and large leaks (as in Table 2), but also corresponding lower and upper bounds. For the prior distributions based on NUREG data, the first column of Table 3 reports, in addition to the mean, 95% and 5% probability values. For example, the 95% value of the prior distribution based on NUREG data is 1 in 1,000 years. In other words, there is only a 5% prior probability that small leaks will occur more frequently than 1 in 1,000 years. But when we look at the Red Hill data, we find that small leaks have occurred at a rate of almost 1 in 50 years-a factor of 20 greater in frequency. Thus, not only is the mean leak frequency of the NUREG prior optimistic and way too low (as shown in Table 2) , even the 95% value of the NUREG prior does not come close to the frequency of leaks actually recorded at Red Hill. | |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 36 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | See Table 3 in the BWS comment letter. Comparing the estimated frequencies of small and large leaks based on NUREG data versus Red Hill recorded leak data.<br>In addition, as shown in Table 3, the 5% values of the NUREG prior are exceedingly small: one in a million years for small leaks and nearly one in a billion years for large leaks. These extreme time periods exceed any reasonable expectation of storage tank life and provide another indication of the unrealistic optimism of estimates based on the NUREG data. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 37 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Table 4 shows this optimism persists in the ABS estimates of leak frequencies for individual Red Hill tanks. The ABS estimates for Tank 3, in particular, strain credulity since the other 19 Red Hill tanks have collectively had 27 small and 10 large leaks reported in the last 70 years. It is simply not credible to expect that Tank 3 could operate for thousands, let alone millions (or billions) of years, without experiencing a single leak.<br>See Table 4 in the BWS comment letter. Comparing ABS estimates (single-stage update) of leak frequencies for Tanks 1 and 3 with Red Hill recorded leak data. | We acknowledge and understand that, via the concerns raised in BWS comments 27 through 37 in this table, BWS feels that a different approach should be applied to the development of tank leak initiating event frequencies for the QRVA. At the IPR meeting, BWS explained their preferred method of analysis, which discounts all other Navy tank failure data and all sources of generic tank failure data. We find this position interesting, as BWS, during an August 2016 meeting, strongly recommended including other Navy fuel tank data in the Bayesian update process, a position with which we agreed. While we understand the BWS preferred method, which involves consideration of only RHBFSF failure events, we disagree that their preferred method represents conventional accepted QRVA best-estimate practice. Application of the BWS method can be applied in the QRVA as a separate sensitivity case study. The Navy is considering authorizing investigation of this type of sensitivity case study in a follow-on phase of the current Phase 1 QRVA. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 38 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | The November 27, 2017 QVRA draft report proposes a triangular distribution (0, 0.7, and 1.4) gallons per hour (gph) for the chronic leak rate. However, ABS indicated during the 5 & 7 December 2017 meetings that they will revise this assumption and use a uniform distribution (0-0.5) gph for the chronic leak rate. This change reduces by almost a factor of 3 the maximum possible rate of chronic fuel leakage (from 1.4 to 0.5 gph). | We agree with the comment statement here, and we are confident that the change we described at the IPR Meeting is technically justified based on our refined understanding of the RHBFSF. We agree to provide additional discussion in the QRVA report to support this change. |
| 39 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | Additional documentation regarding how this 0.5 gal/hr. detection limit is arrived at should be included. Discussion of the applicability of the leak detection limits equation from Mass Technology Corporation (MTC), and confirmation that the equation can be applied to tanks as large as the Red Hill tanks should also be included. | We agree to provide additional discussion on this topic, to include MTC information, in the final report. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 40 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | We understand that this 0.5 gph leak rate is the largest "undetectable" leak rate if the MTC technology is successfully implemented in the future on a "continuous" basis at the Red Hill tank facility. This detection technology has not yet been implemented or demonstrated at the Red Hill facility and thus should not be the current QRVA evaluation basis as the Phase 1 QRVA freezes the facility design as of July 27, 2017. | We are currently under the understanding that the MTC technology has been approved for implementation as of the design freeze date of our project, July 27, 2017, and, therefore, it is included as a basis of this analysis. We see evidence in inspection reports dated in 2015 that the technology is currently in place at the RHBFSF. If this is incorrect, and is confirmed by the Navy, we agree to revise the analysis based on this change. |

## Table F-1. IPR Comments and Proposed Resolutions (Continued)

| Comment Number | Date Received by ABS Consulting | Source | Comment | Proposed Resolution |
|---|---|---|---|---|
| 41 | 12/26/2017 | Red Hill Sec 8 QRVA IPR comments BWS 2017 12 18.pdf | BWS understands that the installed unscheduled fuel movement (UFM) Alarms system provides the current "continuous" leak detection limit, which is significantly higher. BWS's understanding of the Red Hill leak testing frequency and minimum leak rate detectible is summarized in Table 5 of the BWS comment letter. Table 5 also shows how much would leak from a single tank if a leak were occurring just below the minimum detection limit for one year. It is ABS understanding that there are leak detection methods (inventory control, long term monitoring of fuel levels, inventory control, and the like) that can limit the undetectable amount leaked to levels less than those shown in Table 5 and that the QRVA analysis will be better able to estimate probability of release volumes prior to detection and completion of corrective action.<br>See Table 5 of the BWS comment letter. Red Hill Testing and Leak Detection Limits. | In general, we agree with this comment. We see no need for revision of our analysis based on this comment at this time. |

ABSG CONSULTING INC.
300 Commerce Drive, Suite 200
Irvine, CA 92602
Telephone 714-734-4242
Fax 714-734-4282

ABS Consulting

ABS GROUP OF COMPANIES, INC.
16855 Northchase Drive
Houston, TX 77060
Telephone 281-673-2800
Fax 281-673-2801

## NORTH AMERICA

1525 Wilson Boulevard, Suite 625
Arlington, VA 22209
Telephone 703-682-7373
Fax 703-682-7374

1745 Shea Center Drive, Suite 400
Highland Ranch, CO 80129
Telephone 303-674-2990

10301 Technology Drive
Knoxville, TN 37932
Telephone 865-966-5232
Fax 865-966-5287

1360 Truxtun Avenue, Suite 103
North Charleston, SC 29405
Telephone 843-297-0690

1390 Piccard Drive, Suite 350
Rockville, MD 20850
Telephone 301-907-9100
Fax 301-990-7185

140 Heimer Road, Suite 300
San Antonio, TX 78232
Telephone 210-495-5195
Fax 210-495-5134

55 Westport Plaza, Suite 700
St. Louis, MO 63146
Telephone 314-819-1550
Fax 314-819-1551

## MEXICO

Ciudad del Carmen, Mexico
Telephone 52-938-382-4530

Mexico City, Mexico
Telephone 52-55-5511-4240

Monterrey, Mexico
Telephone 52-81-8319-0290

Reynosa, Mexico
Telephone 52-899-920-2642

Veracruz, Mexico
Telephone 52-229-980-8133

## UNITED KINGDOM

EQE House, The Beacons
Warrington Road
Birchwood, Warrington
Cheshire WA3 6WJ
Telephone 44-1925-287300

## SOUTH AMERICA

Rio de Janeiro, Brazil
Telephone 55-21-3179-3182

Sao Paulo, Brazil
Telephone 55-11-3707-1055

Viña del Mar, Chile
Telephone 56-32-2381780

Lima, Peru
Telephone 51-1-437-7430

Chuao, Venezuela
Telephone 58-212-959-7442

## MIDDLE EAST

Dhahran, Kingdom of Saudi Arabia
Telephone 966-3-868-9999

Ahmadi, Kuwait
Telephone 965-3263886

Doha, State of Qatar
Telephone 974-44-13106

Muscat, Sultanate of Oman
Telephone 968-597950

Istanbul, Turkey
Telephone 90-212-6614127

Abu Dhabi, United Arab Emirates
Telephone 971-2-6912000

Dubai, United Arab Emirates
Telephone 971-4-3306116

## EUROPE

Sofia, Bulgaria
Telephone 359-2-9632049

Hamburg, Germany
Telephone 49-40-300-92-22-21

Rotterdam, The Netherlands
Telephone 31-10-206-0778

## ASIA-PACIFIC

Ahmedabad, India
Telephone 079 4000 9595

Navi Mumbai, India
Telephone 91-22-757-8780

New Delhi, India
Telephone 91-11-45634738

Yokohama, Japan
Telephone 81-45-450-1250

Busan, Korea
Telephone 82-51-852-4661

Seoul, Korea
Telephone 82-2-552-4661

Kuala Lumpur, Malaysia
Telephone 608-6212320888

Beijing, PR China
Telephone 86-10-58112921

Shanghai, PR China
Telephone 86-21-6876-9266

Kaohsiung, Taiwan, Republic of China
Telephone 886-7-271-3463

Alexandra Point, Singapore
Telephone 65-6270-8663

Bangkok, Thailand
Telephone 662-399-2420

## INTERNET

Additional office information can be found at www.abs-group.com