

# **U.S. Navy Red Hill Bulk Fuel Storage Facility Quantitative Risk and Vulnerability Assessment Work Plan**

**August 11, 2016**

**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.”**

*Prepared for:*

**Commander, Naval Facilities Engineering  
Command, Pacific**

**DRAFT, PREDECISIONAL FOR DISCUSSION PURPOSES ONLY,  
DO NOT CITE OR QUOTE**

**ABS Consulting**

**R-3709481-2010  
Draft A**

# **U.S. Navy Red Hill Bulk Fuel Storage Facility Quantitative Risk and Vulnerability Assessment Work Plan**

**August 11, 2016**

*Prepared by:*

**James K. Liming**

*Prepared for:*

**Commander, Naval Facilities Engineering  
Command, Pacific  
258 Makalapa Drive, Suite 100  
Joint Base Pearl Harbor-Hickman, HI 96860-3134**

ABSG Consulting Inc. • 300 Commerce Drive, Suite 200 • Irvine, California 92602

**DRAFT, PREDECISIONAL FOR DISCUSSION PURPOSES ONLY,  
DO NOT CITE OR QUOTE**



## Table of Contents

---

	<u>Page</u>
<b>1. Introduction .....</b>	<b>1-1</b>
1.1 Purpose.....	1-1
1.2 Background.....	1-1
1.3 Objectives .....	1-2
1.4 Administrative Order on Consent Statement Work – Section 8 .....	1-2
1.5 Navy Contract QRVA Statement of Work .....	1-3
1.6 QRVA Level and Scope Determination.....	1-6
<b>2. QRVA Proposed Methodology .....</b>	<b>2-1</b>
2.1 Internal Events QRVA for Loss of Fuel Inventory Control (Level 1) .....	2-1
2.1.1 Information Collection.....	2-1
2.1.2 Facility Familiarization and Information Review .....	2-2
2.1.3 Definition of Safety and Fuel Release Protective Functions.....	2-4
2.1.4 QRVA Bases and Assumptions .....	2-5
2.1.5 Initiating Events Analysis .....	2-5
2.1.5.1 Engineering Evaluation.....	2-5
2.1.5.2 Master Logic Diagram (MLD) Development .....	2-6
2.1.5.3 Initiating Event Category Definition.....	2-7
2.1.5.4 Initiating Event Frequency Determination (see Data Analysis).....	2-7
2.1.6 Event Sequence Analysis.....	2-7
2.1.6.1 Event Sequence Diagram (ESD) Development .....	2-8
2.1.6.2 Event Tree Development.....	2-10
2.1.7 Systems Analysis .....	2-21
2.1.7.1 Specification of Analysis Ground Rules and Model Resolution.....	2-22
2.1.7.2 System Dependency Matrix Development.....	2-25
2.1.7.3 Boolean Logic Model (e.g., fault tree) Top Event Definition.....	2-25
2.1.7.4 System Failure Modes and Effects Analysis.....	2-26
2.1.7.5 Boolean Logic Model (e.g., fault tree) Development.....	2-26
2.1.8 Human Reliability Analysis.....	2-33
2.1.8.1 Human Failure Event (HFE) Definition and Evaluation.....	2-33
2.1.8.2 Human Error Probability Evaluation and Analysis.....	2-41
2.1.8.3 Human Action Dependency Analysis.....	2-41
2.1.9 Data Analysis .....	2-48



---

2.1.9.1	Generic Data Analysis .....	2-51
2.1.9.2	Common Cause Failure Analysis .....	2-79
2.1.9.3	Data Uncertainty Analysis.....	2-117
2.1.9.4	QRVA Database Development.....	2-118
2.1.10	Event Sequence Quantification.....	2-122
2.1.10.1	Event Tree Split Fraction Quantification .....	2-124
2.1.10.2	Event Tree Quantification.....	2-128
2.1.10.3	Event Sequence Uncertainty Analysis .....	2-129
2.2	RHFSF Fuel Release from Internal Events QRVA (Level 2) .....	2-133
2.2.1	RHFSF Unplanned Fuel Movement Data Analysis.....	2-133
2.2.2	Acute Releases from Accident/Incident Event Sequences.....	2-133
2.2.2.1	Probable Release Path Evaluation .....	2-133
2.2.2.2	Event-Caused Structural Failure Evaluation.....	2-134
2.2.2.3	Integration with Level 1 Risk Results.....	2-134
2.3	Risk Results Presentation and Interpretation .....	2-134
2.4	QRVA Vulnerability Assessment .....	2-136
2.4.1	Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences) .....	2-136
2.4.2	Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events .....	2-136
2.4.2.1	Fractional Importance.....	2-137
2.4.2.2	Risk Achievement Worth.....	2-137
2.4.2.3	Risk Reduction Worth .....	2-138
2.4.2.4	Fussell-Vesely Importance (risk participation index) .....	2-139
2.4.2.5	Birnbaum Importance (risk derivative) .....	2-139
2.4.3	Risk Contribution Sensitivity Analysis .....	2-140
2.4.4	Vulnerability Assessment Results Presentation and Interpretation ....	2-140
2.5	Internal Flooding QRVA.....	2-141
2.5.1	Internal Flood Events Scope Determination.....	2-141
2.5.2	Internal Flood Facility Partitioning.....	2-141
2.5.3	Internal Flood Source Identification and Characterization .....	2-141
2.5.4	Internal Flood-Induced Initiating Event Analysis .....	2-142
2.5.5	Internal Flood Scenario Development.....	2-142
2.5.6	Internal Flood Human Reliability Analysis.....	2-142
2.5.7	Internal Flood Accident Sequence Analysis .....	2-142
2.5.8	Internal Flood Data Analysis .....	2-143
2.5.9	Internal Flood Risk Quantification .....	2-143
2.5.10	Internal Flood Risk Uncertainty Analysis.....	2-143
2.5.11	Risk Results Presentation and Interpretation.....	2-143
2.5.12	QRVA Vulnerability Assessment.....	2-143



---

2.5.12.1	Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences).....	2-143
2.5.12.2	Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events ..	2-143
2.5.12.3	Risk Contribution Sensitivity Analysis.....	2-144
2.5.12.4	Vulnerability Assessment Results Presentation and Interpretation.....	2-144
2.6	Internal Fire QRVA (FQRVA).....	2-144
2.6.1	Internal Fire Events Scope Determination.....	2-147
2.6.2	Facility Walkdowns.....	2-147
2.6.3	FQRVA Database Development.....	2-150
2.6.4	Internal Fire Facility Partitioning.....	2-151
2.6.5	FQRVA Component Selection.....	2-153
2.6.6	FQRVA Cable Selection.....	2-158
2.6.7	Internal Fire-Induced Initiating Event Analysis.....	2-163
2.6.8	Internal Fire Scenario Development.....	2-163
2.6.9	Internal Fire Human Reliability Analysis.....	2-165
2.6.10	Internal Fire Accident Sequence Analysis.....	2-169
2.6.11	FQRVA Qualitative Screening.....	2-170
2.6.12	Internal Fire Data Analysis.....	2-171
2.6.12.1	Fire-Ignition Frequencies Development.....	2-171
2.6.12.2	Equipment Fire Fragility Evaluation.....	2-178
2.6.12.3	Fire Scenario Propagation Conditional Probability Development.....	2-178
2.6.12.4	Fire Scenario Human Error Probability Evaluation.....	2-178
2.6.13	Internal Fire Risk Quantification.....	2-178
2.6.13.1	Quantitative Screening Phase 1.....	2-179
2.6.13.2	Scoping Fire Modeling.....	2-181
2.6.13.3	Quantitative Screening Phase 2.....	2-190
2.6.13.4	Detailed Circuit Failure Analysis.....	2-190
2.6.13.5	Circuit Failure Mode and Likelihood Analysis.....	2-194
2.6.13.6	Detailed Fire Scenario Modeling (including fire phenomenology).....	2-197
2.6.13.7	Final Fire Risk Quantification.....	2-211
2.6.14	Internal Fire Risk Uncertainty Analysis.....	2-212
2.6.15	Risk Results Presentation and Interpretation.....	2-214
2.6.16	QRVA Vulnerability Assessment.....	2-214
2.6.16.1	Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences).....	2-215
2.6.16.2	Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events ..	2-215



---

2.6.16.3 Risk Contribution Sensitivity Analysis .....	2-215
2.6.17 Vulnerability Assessment Results Presentation and Interpretation ....	2-215
2.7 Seismic QRVA .....	2-215
2.7.1 Develop Facility-Specific Risk Hazard Curves .....	2-218
2.7.2 Review Facility Safety Systems and Perform Initial Modification to Facility Internal Events QRVA System Models .....	2-218
2.7.3 Develop QRVA Seismic Equipment List.....	2-218
2.7.4 Conduct Facility Soil Failures Evaluation.....	2-219
2.7.5 Perform Seismic Response Analysis (including developing floor spectra and structural response analyses) .....	2-219
2.7.6 Perform Facility Walkdowns for Seismic QRVA .....	2-219
2.7.7 Screen Components from Internal Events QRVA Equipment List .....	2-220
2.7.8 Perform Relay Chatter Evaluation .....	2-220
2.7.9 Develop Seismic Fragility Parameters for Screened-In Equipment .....	2-220
2.7.10 Modify Internal Events QRVA Boolean Logic Models .....	2-221
2.7.11 Seismic Events Human Reliability Analysis.....	2-221
2.7.12 Seismic Events Accident Sequence Analysis.....	2-222
2.7.13 Seismic Events QRVA Data Analysis .....	2-222
2.7.14 Seismic Events Risk Quantification .....	2-222
2.7.15 Seismic Events Risk Uncertainty Analysis.....	2-222
2.7.16 Risk Results Presentation and Interpretation.....	2-222
2.7.17 QRVA Vulnerability Assessment.....	2-222
2.7.17.1 Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences) .....	2-222
2.7.17.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events ..	2-223
2.7.17.3 Risk Contribution Sensitivity Analysis .....	2-223
2.7.18 Vulnerability Assessment Results Presentation and Interpretation ....	2-223
2.8 External Flooding QRVA (including tsunamis and heavy precipitation).....	2-223
2.9 External Fire QRVA.....	2-223
2.10 Other External Events QRVA.....	2-223
2.10.1 High Winds and Storms (e.g., tornados, hurricanes, etc.) .....	2-223
2.10.2 Landslides (including mudslides, sinkholes, etc.) .....	2-224
2.10.3 Proximity Transportation Accidents (e.g., aircraft crash, external hazardous material spill or release, etc.) .....	2-224
2.10.4 Extreme Weather (e.g., high temperature, etc.).....	2-224
2.10.5 Other Facility-Specific Hazards.....	2-224
2.11 Environmental Transport and Consequence Analysis for Levels 3+ QRVA (optional) .....	2-225
2.12 Risk Management Decision Support Metric Development and Analysis (optional).....	2-225



---

<b>3. QRVA Proposed Work Breakdown Structure (WBS)</b> .....	<b>3-1</b>
3.1 Proposed Project Phases .....	3-1
3.1.1 Level 1 QRVA for Internal Events.....	3-1
3.1.2 Level 2 QRVA for Internal Events.....	3-1
3.1.3 Level 2 QRVA for Flooding and Fire.....	3-1
3.1.4 Level 2 QRVA for Seismic Events .....	3-1
3.1.5 Level 2 QRVA for Other External Events .....	3-1
3.2 Proposed Task WBS.....	3-1
<b>4. QRVA Project Management Considerations</b> .....	<b>4-1</b>
<b>5. QRVA Quality Assurance Considerations</b> .....	<b>5-1</b>
5.1 ISO 9001 Quality Assurance.....	5-1
5.2 ASME/American Nuclear Society (ANS) Standard RA-S-2008 (with current addenda) Capability Categories .....	5-1
<b>6. QRVA Software Considerations</b> .....	<b>6-1</b>
<b>7. References</b> .....	<b>7-1</b>

### List of Tables

Table 2-1. Example of Format for a Cause Table for Double Failures (buses available).....	2-19
Table 2-2. Conditional Probability Equations.....	2-42
Table 2-3. Sources of Facility Data .....	2-64
Table 2-4. Effect of Two Types of Common Causes on Fault-Tree Quantification <sup>a</sup> .....	2-83
Table 2-5. Generic Causes of Dependent Failures.....	2-87
Table 2-6. Special Conditions.....	2-88
Table 2-7. Dependent Failures Involving Subtle Dependences .....	2-88
Table 2-8. Key Characteristics of some Popular Parametric Models.....	2-92
Table 2-9. MOL to Alpha Factor Conversion Formulae for Staggered Testing.....	2-100
Table 2-10. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing.....	2-102
Table 2-11. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing.....	2-105
Table 2-12. Contributors to Uncertainty in Estimates of Accident-Sequence Frequency .....	2-130
Table 2-13. RHFSF Total Aggregate Mean Risk Results .....	2-135
Table 2-14. Fire Frequency Bins and Generic Frequencies .....	2-173
Table 2-15. Zone of Influence and Severity Factor Recommendations.....	2-185
Table 2-16. Recommended Severity Factors and Suppression Curves for Ignition Sources in the Frequency Model .....	2-206
Table 3-1. Phase 2 Preliminary WBS.....	3-2



---

## List of Figures

Figure 2-1. Excerpt from an Event-Sequence Diagram .....	2-9
Figure 2-2. Simplified Facility Event Tree .....	2-11
Figure 2-3. Example of Format for a System-Interaction FMEA.....	2-24
Figure 2-4. Fault Tree for Overrun of Motor 2 (relay logic only).....	2-27
Figure 2-5. Fault-Tree Symbols.....	2-28
Figure 2-6. Type A Pre-Initiator HFE Questionnaire.....	2-35
Figure 2-7. Type C Post-Initiator HFE Questionnaire .....	2-37
Figure 2-8. Level of Dependence as a Function of Time .....	2-41
Figure 2-9. HRA Dependency Rules for Post-Initiator HFEs .....	2-47
Figure 2-10. Inputs, Outputs, and Steps in Database Development .....	2-50
Figure 2-11. Test Intervals for Sample System .....	2-54
Figure 2-12. Interface Schematic .....	2-54
Figure 2-13. Modeling of Mutually Exclusive Events .....	2-57
Figure 2-14. Fault Tree for a Three-Component System with Independent and Common Causes .....	2-82
Figure 2-15. Example of Data Table for Hardware.....	2-120
Figure 2-16. Example of Data Table for Test or Maintenance Acts .....	2-121
Figure 2-17. Sample Event Tree .....	2-123
Figure 2-18. Example of Format for a Cause Table for Double Failures (buses available).....	2-126
Figure 2-19. FQRVA Task Flow Chart.....	2-145
Figure 2-20. Fire QRVA Cable Selection Process .....	2-160
Figure 2-21. Detailed Circuit Failure Analysis Work Flow .....	2-192
Figure 2-22. Circuit Failure Mode Likelihood Analysis Work Flow .....	2-195
Figure 2-23. General Analysis Flow Chart for Task 11 – Detailed Fire Modeling.....	2-203
Figure 2-24. SQRVA Task Flowchart.....	2-217

## List of Appendices

- A. RHFSF Initial Information Item Request
- B. RHFSF QRVA – Requested Navy Support Interfaces and Activities
- C. Bibliography
- D. Glossary
- E. List of Acronyms



**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.”**

## **1. Introduction**

---

This work plan is the primary deliverable of Phase 1 project work authorized to ABSG Consulting Inc. (ABS Consulting) via HDR Engineering, Inc. and Element Environmental, LLC under Navy contract N62742-14-D-1884, Task Order 0028 (Reference 1).

Phase 2 of the project, when authorized, is intended to complete the Red Hill Bulk Fuel Storage Facility (RHFSF) Quantitative Risk and Vulnerability Assessment (QRVA) in compliance with the RHFSF Administrative Order on Consent (AOC) (Reference 2) and following the general approach and guidance presented in this work plan.

### **1.1 Purpose**

The purpose of this work plan is to clearly communicate the approach and methodology for effective and efficient development of the RHFSF QRVA. The RHFSF QRVA will be designed to serve as a support tool to help facilitate prudent decisions for future RHFSF risk and safety management.

### **1.2 Background**

The Red Hill Bulk Fuel Storage Facility 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 (msl).

The facility consists of 20 12.5-million-gallon underground storage tanks (UST) constructed in the early 1940s. Currently three USTs are out of service (T-1, T-5, and T-19). 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 (ND), F-76, aviation gas, motor gas, JP-5, and JP-8.



There have been several prior petroleum, oil, and lubrication releases at the site and numerous environmental activities/studies performed for various reasons including: pipe and tank testing, release response, tank monitoring, long-term monitoring, and removal actions.

In January 2014, up to 27,000 gallons of JP-8 was released from T-5, which was being re-filled after having undergone inspections and repair. Tank T-5 is currently out of service undergoing inspection, repair, maintenance, and testing. The Navy plans to eventually bring T-5 back into service. As a result of the fuel release from Tank 5 at the RHFSF in January 2014, the U.S. Environmental Protection Agency and the Hawaii Department of Health brought an enforcement action against the Navy and the Defense Logistics Agency (DLA) to address past fuel releases 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 solve complex environmental problems since it allows for flexible and innovative solutions. The Administrative Order on Consent goes beyond the scope of merely complying with the current regulations. To address past fuel releases and prevent future releases, we are collecting the necessary data and evaluating optimal technical solutions.

### **1.3 Objectives**

The objectives of this work plan are:

- Clearly communicate a comprehensive technical approach and methodology to effectively and efficiently support development of the RHFSF QRVA in Phase 2 of the project.
- Provide a foundation for the Naval Facilities Engineering Command (NAVFAC) to implement effective project management for the Phase 2 RHFSF QRVA.
- Provide guidance, references, and a bibliography of information sources supporting implementation of the RHFSF QRVA, and supporting a basis for a clear understanding of the RHFSF QRVA results to NAVFAC and others outside the QRVA team who will be required to review and apply QRVA results to facilitate prudent decision-making for RHFSF management, operation, maintenance, inspection, testing, and associated facility activities.

### **1.4 Administrative Order on Consent Statement Work – Section 8**

The following text excerpt, associated with the RHFSF QRVA, is quoted directly from the RHFSF AOC (Reference 2) Statement of Work:

#### **“8. Risk/Vulnerability Assessment**

The purpose of the deliverables to be developed and work to be performed under this Section is to assess the level of risk the Facility may pose to the



groundwater and drinking water aquifers and to inform the Parties in subsequent development of BAPT decisions.

The Risk/Vulnerability Assessment Report may include:

- a. A risk matrix;
- b. Probability of catastrophic events (seismic events, leaks);
- c. Completed hydrology studies;
- d. Probability of mechanical and human errors;
- e. Effectiveness of risk mitigation and protective measures; and
- f. A comparison of risks and benefits between the current Facility and alternative fuel storage facilities.

### **8.1 Scoping Meeting(s) for Risk/Vulnerability Assessment**

Within thirty (30) days from the Effective Date of the AOC, Navy and DLA shall schedule and hold an initial Scoping Meeting to be attended by the Parties. The purpose of the Scoping Meeting is to detail the contents of the draft Scope of Work for Risk/Vulnerability Assessment, and a decision will be made as to whether additional Scoping Meetings are needed.

### **8.2 Risk/Vulnerability Assessment Scope of Work**

Within ninety (90) days from the final Scoping Meeting, Navy and DLA shall submit the Risk/Vulnerability Assessment Scope of Work to the Regulatory Agencies for approval.

### **8.3 Risk/Vulnerability Assessment Report**

Within eighteen (18) months from the Regulatory Agencies' approval of the Risk/Vulnerability Assessment Scope of Work, Navy and DLA shall submit a Risk/Vulnerability Assessment Report to the Regulatory Agencies for approval. The Risk/Vulnerability Assessment Report may be revised as new information becomes available. All revisions to the Risk/Vulnerability Assessment Report shall be submitted to the Regulatory Agencies for approval."

## **1.5 Navy Contract QRVA Statement of Work**

The following text, associated with the RHFSF QRVA, is quoted directly from the Navy Contract N62742-14-D-1884, Amendment 34, Task Order 0028, Statement of Work (Reference 1):

### **"4.0 SCOPE OF WORK**



The project will be performed in phases. The first phase is to design, with collaboration from the Navy and Stakeholders, the specific methodology to perform the RHFSF RVA. Initially, the Contractor will submit a cost proposal for Phase 1 which includes Tasks 1, 2, 3, and 4 listed below. After receiving Navy and Stakeholder concurrence on the methodology, Phase 2 will be to perform and document the RVA, Task 5. The Contractor will submit a proposal for contract modification to include this second phase after completion of the first phase.

The RVA will assess the level of risk the RHFSF may pose to the groundwater and drinking water aquifers to inform the Government in subsequent development of best available practicable technology (BAPT) decisions. At a minimum, the quantitative RVA will be designed to:

- perform an internal system risk/reliability analysis (e.g. equipment failures, fires, human error etc.)
- evaluate the risk of penetration by ongoing corrosion-fatigue and associated potential leak rates
- evaluate the ability to quantify the reliability of leak detections
- evaluate seismic risk (including geotechnical hazards)
- perform formal Failure Modes and Effect Analysis of releases due to weld defects, corrosion, fatigue, equipment failure, fire, and human error etc.
- evaluate of structure, system and component fragilities (condition damage probabilities), and
- calculate annual probability of damage (or release)

#### 4.1. Task 1 – Project Management

- a. The Contractor shall provide project oversight and coordination, provide budget control/tracking/reports, attend meetings to discuss special concerns, provide periodic progress reports, and project completion/close-out efforts. Assume a project duration of five months for Phase 1 and there will be periods of less activity.
- b. The Contractor shall prepare and maintain a detailed project schedule. The project schedule is critical since the AOC has stipulated penalties for missed milestones.
- c. All Contractor personnel (including subcontractors) anticipated to work on this project will be required to sign a Navy non-disclosure agreement prior to handling any project information.



4.2. Task 2 – Meetings

- d. The Contractor shall have weekly progress meetings (telecoms) during development of the in- progress Proposal (assume 12 meetings). The weekly progress meetings discussion will include the scope of the proposed work including scheduling, channels of communication, coordination and points of contact.
- e. The Contractor shall be responsible for providing meeting support including but not limited to supplying draft meeting agendas and all other relevant and pertinent meeting materials.
- f. The Contractor shall have a multiday (5-day) scoping meeting with Navy and Regulators to present the draft proposal to all parties. The Contractor will supply all material needed to hold the meeting, including all prep work, meeting exhibits, and presentations. The Contractor shall also provide a facilitator for this meeting.
- g. The Contractor shall be responsible for documenting the minutes of all meetings and provide a draft within seven calendar days of the meeting.

4.3. Task 3 – Evaluate Methodology

- h. The Contractor shall review existing information pertaining to the RHFSF.
- i. The Contractor shall perform a site visit to the RHFSF to become familiar them with the facility.
- j. The Contractor shall determine methodology and approach for the quantitative RVA.
- k. The Contractor shall determine the data needed for the methodology and approach and identify data gaps.
- l. The Contractor shall identify how the other AOC sections fit into the methodology and approach and the impact of the other sections and data gaps on the schedule.

4.4 Task 4 – Prepare Proposal on RVA Methodology

- m. The Contractor shall prepare an internal Navy Revision 0 on the RVA methodology for review. The Revision 0 version will contain sufficient level of detail to adequately describe the quantitative RVA data collection efforts, types of analysis to be performed, data evolution steps, and final reporting/deliverable requirements. (Assume 2 rounds of review).
- n. The Contractor shall prepare a draft Proposal on the RVA methodology for review that incorporates the comments received on the Revision 0. (Assume 2 rounds of review).



- o. The Contractor shall prepare a final Proposal on the RVA methodology that incorporates the comments received from the Navy and Stakeholders on the draft Proposal.

#### 4.5 Task 5 – Perform RVA and Prepare Report

- p. After obtaining Navy and Stakeholder concurrence on the Final Proposal, the Contractor shall perform and document the RVA.
- q. An internal Navy in-progress draft RVA report shall be submitted to the Navy 12 months after being given the notice to proceed on the Phase 2 of the project.
- r. The Contractor shall prepare a draft RVA report for review that incorporates the comments received on the in-progress draft RVA report. (Assume 2 rounds of review).
- a. The Contractor shall prepare a final RVA report for review that incorporates the comments received on the draft RVA report. (Assume 2 rounds of review)."

### **1.6 QRVA Level and Scope Determination**

Prior to initiating technical work on a facility QRVA, it is necessary to clearly establish the desired level and scope of the assessment. "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. For example, for any facility containing hazardous material, at least three levels of risk assessment are commonly conceptually defined and applied in QRVA, as follows: Level 1 – Loss of Control of the Target Hazardous Material Within the Facility; Level 2 – Release of the Hazardous Material Outside Owner/Operator Controlled Boundaries; and Level 3 – Impact of the Hazardous Material Release on the Public (often including consideration of public health effects, effects on the environment, and effects on public and/or private property outside the control of the facility owner/operator). 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 RHFSF QRVA:

- Level 1 – Frequency (and Annual Probability) of Loss of Fuel Inventory Control (by Volume Range) Within the RHFSF Property Boundaries
- Level 2 – Frequency (and Annual Probability) of Uncontrolled Release of Fuel Inventory (by Volume Range) Outside the RHFSF 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 RHFSF 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 RHFSF 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 work plan focuses on a Level 2 risk assessment, as defined above. The intent of this risk assessment is to provide evaluation information and results metrics to the AOC Task 7 team that 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. Other QRVA levels can, of course, be defined through modification or supplementation of the risk metrics outlined above.

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 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; e.g., documentation associated with the information item request presented in Appendix A of this work plan.

Closely related to analysis boundaries is the issue of the physical and functional basis or starting point for the QRVA. An effective design freeze date must be established to ensure a stable design basis for the QRVA. Regarding determination of the RHFSF design basis for the QRVA, the following design basis has been selected by the Navy:

- Freeze the facility design as of the date of notification to proceed (NTP) for Phase 2 of the QRVA project. The design basis will be the as-built, as-operated facility as of the NTP date, to include design, operation, maintenance, and testing changes that have been approved and funded as of the NTP date, but with no additional modification options.

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 following hazard sources, which are recommended to characterize the scope of hazards to be addressed in the RHFSF QRVA:

- Internal Events (equipment or structural failures in both frontline and support systems, human errors, etc.)



- Internal Flooding
- Internal Fires
- Internal Sabotage (not included within the scope of this analysis for security reasons)
- External Flooding (including tsunami and heavy precipitation)
- External Fires
- Seismic Events (earthquakes)
- Other 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)

A comparison of risks and benefits between the current facility and alternative fuel storage facilities is not included within the scope of this QRVA work plan.

It is very important that the desired QRVA level and scope (including analysis boundaries) issues are resolved during Phase 1 or very early in Phase 2 of the project to best facilitate an effective and efficient RHFSF QRVA.



## **2. QRVA Proposed Methodology**

---

The proposed methodology recommended for application in Phase 2 of the RHFSF QRVA is presented in this section. Much of the general information presented in this section is an adaptation of the basic methodology presented in NUREG/CR-2300 (Reference 3).

### **2.1 Internal Events QRVA for Loss of Fuel Inventory Control (Level 1)**

This section presents the proposed methodology for the Level 1 QRVA focusing on loss of fuel inventory control within the RHFSF due to internal events. If not determined in the Phase 1 QRVA activities, then the analysis scope and boundaries determination tasks outlined in Section 1.6 must be performed prior to other Phase 2 QRVA activities.

#### **2.1.1 Information Collection**

Quantitative risk and vulnerability assessments are broad, integrated studies requiring large amounts of information. The information that is required depends on the scope of the analysis and falls into three broad categories:

1. Facility design, site, operation, maintenance, and testing information.
2. Generic and facility-specific data.
3. Documents on QRVA methods.

A Level 1 analysis requires available safety analysis reports, piping, electrical, and instrumentation drawings; descriptive information about the systems of interest, and test, maintenance, operating, and administrative procedures. This information is needed to give the analyst a set of documents on facility design and operation that is as complete as possible. Other studies performed on the facility may also prove useful. Most important are discussions with design engineers and facility personnel, which should be held throughout the QRVA to ensure that the information used in the analysis is accurate based on the as-built, as-operated facility. In addition to design information, analysts need both generic and facility-specific data on the occurrence of initiating events, component failures, and human errors. The analysts should refer to this work plan for guidance on the performance of the analysis.

The additional information needed for a Level 2 analysis includes more detailed design information on facility containment systems and structures. The information on the structural design of the containment systems and structures should include dimensions, masses, and materials.

If external events are to be analyzed, considerably more information will be needed, depending on the external events to be included. For example, detailed structural information as well as data on the seismic design of the facility and the seismicity of the site are needed for a seismic risk analysis. Information about the compartmentalization of the facility is necessary to analyze susceptibility to fires and floods.



### **2.1.2 Facility Familiarization and Information Review**

Before the detailed analytical work can begin, it is necessary for the QRVA team to become familiar with the design, operation, and maintenance of the facility. All team members should become as familiar as possible with all aspects of the facility to help ensure that function and system dependences are appropriately considered throughout the QRVA activity.

A large amount of facility information must be collected and organized for a risk assessment. To facilitate this task, a formalized system for data acquisition and tracking should be established. It is preferable to assign data management to one team member who has overall responsibility for cataloging data, controlling the information within the QRVA project team, as well as documenting all requests for additional information and correlating responses.

A focal point for coordinating information on facility operation should also be designated. This should preferably be a person who is a senior employee of the operating facility and is located at the facility site. This person will coordinate all data requests with cognizant onsite personnel and assist in expediting the collection of operational and maintenance information.

Much of the detailed information is needed for review only it is reduced or reformatted for specific uses during the analysis. Information on overall facility functions and performance that is synthesized from the overall data set should be collected in a single information source supporting event-tree development and the integrated assessment. Information on individual systems should be organized, updated, and retained in the system-analysis notebooks.

Specific types of facility documentation that are necessary for the analysis can be defined at the outset. This information is supplemented by detailed data requests formulated as the study progresses. An important part of the information is obtained from facility visits and interviews with operations and maintenance personnel. These visits should be coordinated to optimize the flow of information to the QRVA study team and its use in specific study activities.

A partial list of the sources of information needed to support the task of accident-sequence definition is given in Appendix A of NUREG/CR-2300. An attempt was made to relate the data to three major study activities, even though many of the data sources have a general application. The safety analysis report for the facility may contain a significant amount of information pertinent to a QRVA. However, the use of this information must be carefully considered, particularly in those areas where minimum requirements for equipment configurations or criteria for meeting functional requirements are derived. Requirements reflecting building code criteria may be overly conservative for a realistic QRVA. Conversely, in important activities like defining success criteria, care must be exercised not to use information that cannot be properly documented and justified.

Additional sources of valuable information are documented risk assessments of similar facilities. An attempt should be made to obtain available documentation of applicable



QRVAs. Care should be exercised, however, in reviewing and applying such information because the specific objectives, analytical assumptions, or analytical approaches of another study may have been different.

The information sources in Appendix A provide a foundation for study and initial facility-modeling activities. All team members should become familiar with the basic safety functions necessary to prevent facility damage or to mitigate its consequences and the systems that perform these functions. They must also know the events that initiate potential accident sequences as well as the success criteria for functions and systems. During the facility-familiarization process, the QRVA team investigates those facility-level characteristics to become thoroughly familiar with the key elements (i.e., safety functions, initiating events, function and system success criteria) that are fundamental to all subsequent study activities.

As already mentioned, a QRVA entails a substantial effort in information collection and management. The appointment of a data manager and an organized method for cataloging and controlling information will greatly enhance the efficiency and orderly conduct of the study.

The facility-familiarization process cannot be strictly specified, as it consists of numerous activities all aimed at gaining an understanding of the facility and its operation. However, some generalized tasks and documentation activities can be pointed out.

An early task in any QRVA is the identification and listing of the frontline systems (i.e., the systems that directly perform the safety functions and thereby have a direct impact on the course of a potential accident) and the support, or auxiliary, systems that are associated with each frontline system. Since an understanding of the interactions between systems and the dependence of one system on another is vitally important to any QRVA activity, an overview of system operations should be performed to identify dependences between frontline and support systems.

Initial information on accident-initiating events can be obtained from generic lists and the operating history of the facility. The operational responses of the facility, as documented in safety analysis reports and available transient analyses, should be carefully reviewed. All of the information can be brought together in the facility and systems notebook, which will be updated as the study progresses.

In addition, it may be desirable to systematically perform a preliminary qualitative analysis of each system that might either initiate or affect accident sequences. A comprehensive list of facility systems is drawn up, and a partial analysis is performed for each system on the list.

A detailed analysis should be made later only for selected systems found to be important through further analysis. Some systems that are not important to mitigation can initiate accident sequences. A preliminary systems analysis can thus be a vital step in the search for initiators, helping to ensure completeness in the definition of accident sequences.



If this approach, a preliminary qualitative analysis, is taken, a partial system description (PSD) is written for each system. These PSDs document the information on which the importance of the system (i.e., its role in the initiation and mitigation of sequences) is based. The PSDs for systems found to be not important need not be developed any further. The PSDs for systems that are analyzed in detail will become part of a complete system-description notebook.

Facility familiarization provides baseline information for starting the definition of accident sequences and the modeling of facility systems. Initial requirements for the types and number of event trees should be developed and documented, key systems should be identified, and their success criteria should be defined. The team of analysts will be loosely divided into two groups, one concerned with sequence definition and the other with system modeling. These activities can begin concurrently, with maximum attention given to interaction and communication between the two groups. Although the two activities are distinct, an analyst may be involved in both of them, further enhancing his overall understanding of the assessment.

It is during the facility-familiarization process that the QRVA team becomes familiar not only with the facility but also with the different analytical tasks to be performed and the role that each team member will play. It is important that team members understand the basic methods associated with their portion of the assessment and how their activity is integrated into the overall QRVA process.

### **2.1.3 Definition of Safety and Fuel Release Protective Functions**

The functions that must be performed to control the sources of energy in the facility and the fuel release hazard are called "safety functions". The concept of safety functions forms the basis for selecting accident initiating events and delineating potential facility responses. Generally, safety functions are defined by a group of actions that prevent loss of fuel inventory control, prevent fuel containment failure, or minimize fuel releases. Such actions can result from the automatic or manual actuation of a system, from passive system performance, or from the natural feedback inherent in the design of the facility.

Safety functions can be defined in many different ways, depending on the facility type, the system design, the timing of system responses, and the preference of the analyst. Typically, safety functions can be considered within a certain hierarchical framework. This kind of logic illustrates the logic used in structuring the basic safety functions for the facility under evaluation.

Definition of the necessary safety functions forms the preliminary basis for grouping accident-initiating events. It also provides the structure for defining and grouping systems in order to define a complete set of system responses and interactions for each class of accident-initiating events.

Additional distinction may be needed in the definition of safety functions to differentiate between classes of initiating events.



#### **2.1.4 QRVA Bases and Assumptions**

Throughout the analysis, it is important to apply and document realistic bases, assumptions, and criteria. When information is lacking or controversy exists, it may be necessary to introduce conservatisms or evaluate bounds, but the goal of the QRVA should be to produce as realistic an analysis as possible, as this approach best supports realistic and accurate prioritization of resources regarding risk management.

#### **2.1.5 Initiating Events Analysis**

The objective of event tree development is to define a comprehensive set of accident sequences that encompasses the effects of all realistic and physically possible potential accidents involving loss of fuel inventory control at the facility. By definition, an initiating event is the beginning point in the sequence. Hence, a comprehensive list of accident-initiating events must be compiled to ensure that the event trees properly depict all important sequences.

The selection of initiating events for inclusion in event trees consists of two steps:

1. Definition of possible events.
2. Grouping of identified initiating events by the safety function to be performed or combinations of system (including human action) responses.

A clear understanding of the general safety functions and features incorporated into the facility design, supplemented by the preliminary system reviews, will provide the initial information necessary to select and group the initiating events.

Two approaches can be taken in identifying the accident-initiating events. One is a comprehensive engineering evaluation, taking into consideration information from previous risk assessments, documentation reflecting operating histories, and facility-specific design data. The information is evaluated and a list of initiating events is compiled, based on the engineering judgment derived from the evaluation. Another approach is to more formally organize the search for initiating events by constructing a top level logic model and then deducing the appropriate set of initiating events. Portions of each approach can be effectively used as appropriate to define and display the accident-initiating events. The two approaches are described below in Sections 2.1.5.1 and 2.1.5.2.

##### **2.1.5.1 Engineering Evaluation**

The focus of a QRVA for an underground storage tank facility is the loss of UST inventory control and associated release of UST contents outside the facility boundaries; e.g., outside the facility property. There are two major types of accidents with the potential for loss of inventory control: transient events and direct loss of inventory accidents (LOIA). The identification of accident-initiating events can be done by making a list of potential facility-specific events for each of the two types of potential accidents.



Although each type of accident can be treated separately in developing a list of initiating events, it must be recognized that certain transient sequences can result in the loss of UST inventory.

The fuel storage and transfer system and its interfaces with other systems should be surveyed to determine all possible breaks (ruptures) that could result in a loss of UST inventory. A complete spectrum of LOIA sizes, or breaks, in the UST and interfacing systems should be considered. Typically the number of LOIA types can be reduced to three or four break sizes, grouped by mitigation requirements, each requiring a separate event tree. The size and the location of the break are the two important parameters to be considered in selecting LOIA-initiating events.

In addition to the search for tank and pipe breaks, it is also important to survey the UST interfacing systems for the potential of inventory loss by other means. A systematic search of the fuel pressure boundary should be performed to identify any active elements that could fail or be operated in such a manner as to result in an uncontrolled loss of fuel inventory. Particular attention should be paid to elements, such as safety relief valves, whose failure to reclose could result in a loss of UST or piping inventory that might be induced by a transient.

Transient initiators are more complex events and thus more difficult to characterize for event-tree development. Some generic lists exist that provide general guidance on what types of transient events should be considered in formulating potential UST loss of inventory control event sequences. However, in using such lists, care must be taken to ensure that the events chosen are properly defined for the grouping and modeling of potential accident sequences. Any such generic list must be checked for applicability to a specific facility before it is used and should not be regarded as a complete or exhaustive set of potential initiating events. If the facility under consideration has a history of operation, as does the RHFSF, all available information on the occurrence of transient events should be used to supplement the generic data.

The accident-initiating events must be grouped by safety function or system response. This reduces the number of event trees needed to represent all initiating events. All initiating events in a given group would require the same set of system actions. The groups of events can be further refined by examining specific system responses and associated temporal considerations. Event-tree development is very much an iterative process. The identification and grouping of initiating events will be modified and updated as information from subsequent task elements is refined.

#### **2.1.5.2 Master Logic Diagram (MLD) Development**

A summary fault tree, or master logic diagram, can be constructed to guide the selection and grouping of accident-initiating events and to ensure completeness.

The event “excessive offsite release” of UST contents can be the top event. The events in the MLD are identified by the level they appear in the tree, with the top being Level 1. The use of levels is an ordering technique to assist in locating events by approach to an offsite release. The strategy is to achieve completeness of events by level.



When the diagram proceeds downward in levels, equipment failures or misoperations that could threaten each safety function are identified. A comprehensive listing of such events should define all important accident-initiating events.

The initiating events defined by the MLD are already grouped by the safety function they most threaten. However, “safety function most threatened” is usually not sufficiently descriptive to serve as the sole means for grouping initiators. Usually, a further breakdown according to more specific mitigating-system requirements is necessary.

### **2.1.5.3 *Initiating Event Category Definition***

In general, there are two fundamental high-level categories or groups of initiating events considered for an UST QRVA. These are direct “loss of inventory accident” events that occur from tank or pipe ruptures or breaches or from isolation valve failures directly associated with containment of UST contents (fuel, in this case), and “transient” events that can lead to loss of inventory control. An example of a transient event could be a loss of electric power event or a control circuit hot short event that can lead to one or more isolation valves failing in the open position. Experience has shown that, in QRVA, it is prudent to group or categorize initiating events in accordance with how they would likely be addressed, controlled, or mitigated via facility or system automatic response actions and/or via human (operator) response actions to the initiating event. This approach supports consistent, logical accident sequence analysis for the QRVA.

### **2.1.5.4 *Initiating Event Frequency Determination (see Data Analysis)***

After the initiating event categories have been determined, the frequencies of individual initiating events and initiating event groups to be quantified must be determined. The first step in this process is generally accomplished via selection of generic initiating event frequency values from a generic data source for initiating events, such as the OREDA 2015 Handbook (Reference 4) or NUREG/CR-6928 (Reference 5). These generic initiating event frequency values, presented in the form of probability density distributions, are then updated using facility-specific experience data, via application of a Bayesian updating technique (see Data Analysis for additional information). The final updated probability distributions for the initiating event frequency values are then applied during the event sequence quantification process of the QRVA.

### **2.1.6 *Event Sequence Analysis***

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.

#### **2.1.6.1 Event Sequence Diagram (ESD) 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 safe-shutdown 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 2-1 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 2-1 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.



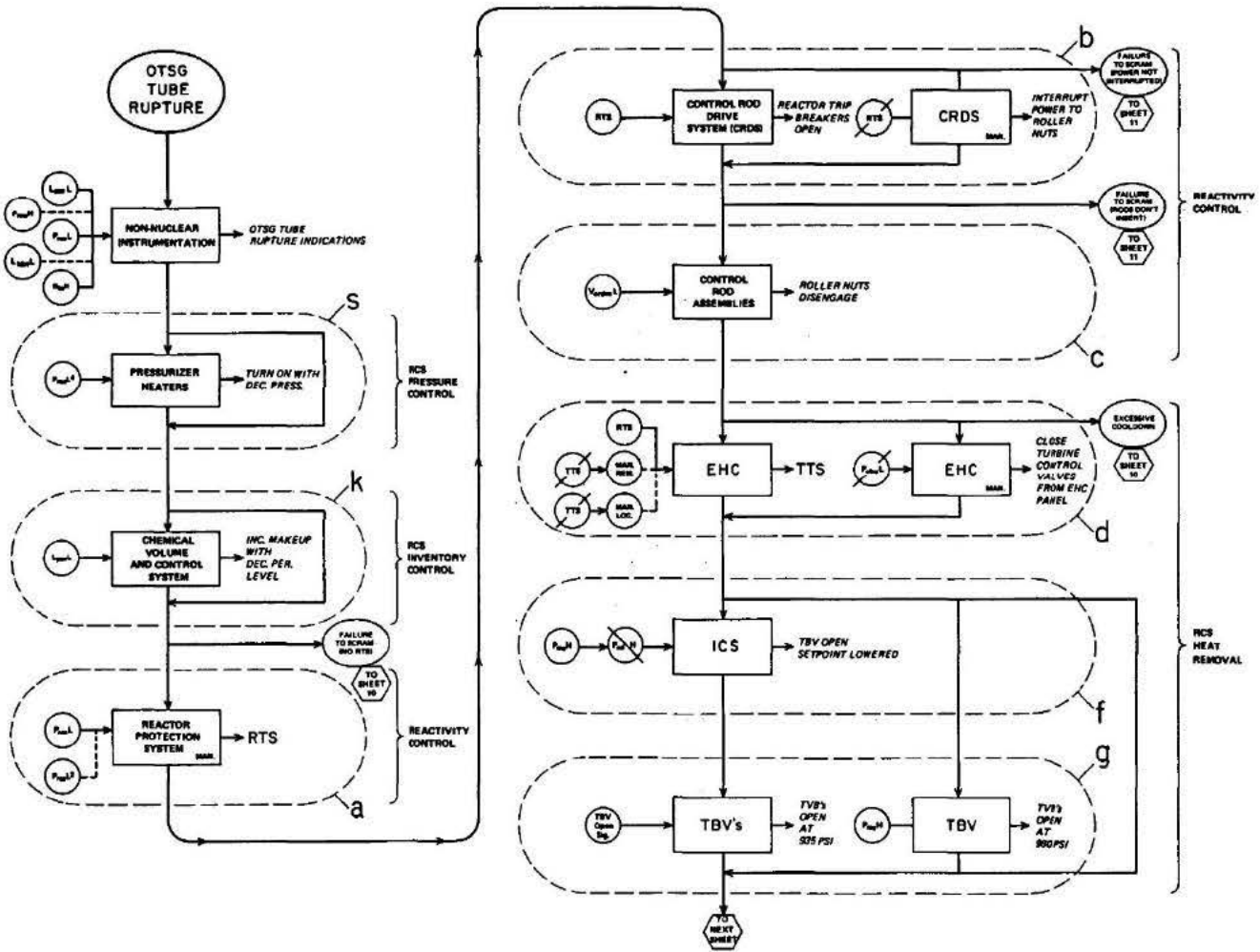


Figure 2-1. Excerpt from an Event-Sequence Diagram



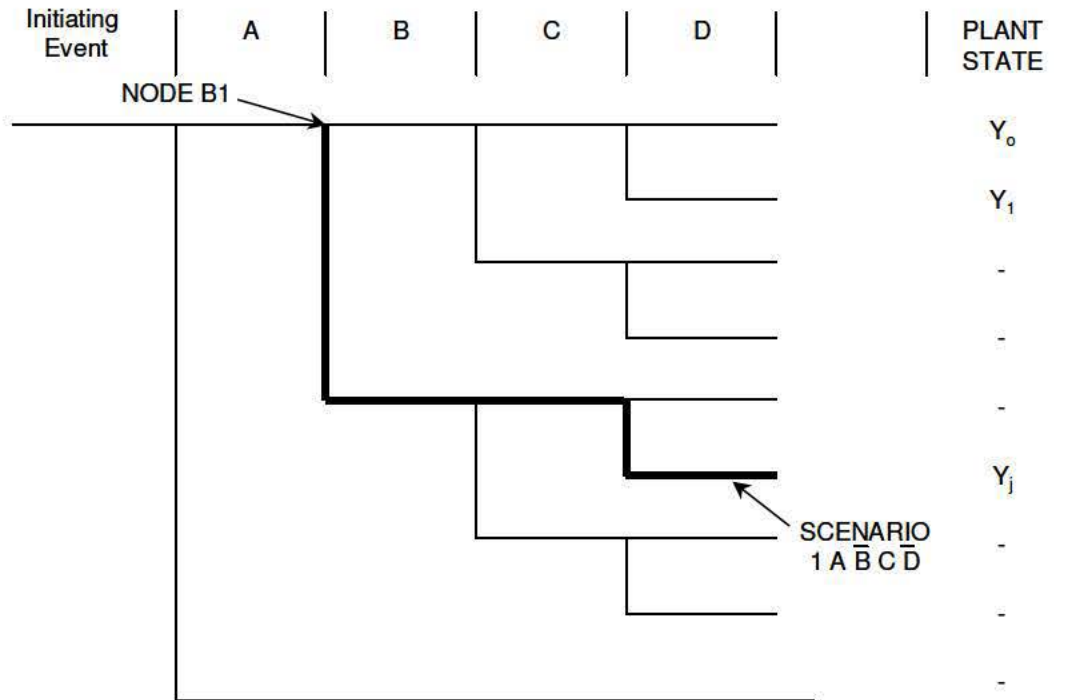
In addition to documenting the agreement on the expected facility response to each initiating event, event-sequence analysis delineates the required operator/system interactions for the human-factors evaluation. The ESDs also help disseminate information to all project participants about how the facility 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.

#### **2.1.6.2 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 RHFSF QRVA, it is anticipated that the event sequences will be quantified applying the method of event trees with boundary conditions.

Figure 2-2 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 2-2. 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 2-1, the scenario

$$S = I A \bar{B} C \bar{D}$$

(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 B.

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.

#### 2.1.6.2.1 *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.

*2.1.6.2.2 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.

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; e.g., excessive reactor coolant system (RCS) heat removal. 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, before the development of the event tree, to trace out each sequence on a system level, 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.

#### 2.1.6.2.3 *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. For example, the power-conversion system could contribute to the RCS heat-removal function for transients and very small loss of coolant accidents (LOCA) and therefore would be included among the systems that perform this safety function.

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.

#### 2.1.6.2.4 *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.

#### 2.1.6.2.5 *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, and 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.

#### 2.1.6.2.6 *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 plant damage bin (PDB) 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 arrived at. 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 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 (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

---

\* This recognition can also be thought of as boundary conditions on the system fault tree—hence the term “event trees with boundary conditions”.



table (see Table 2-1 for an abbreviated example). In this table, all possible causes (“candidate” causes) are listed in the left column.

DRAFT



**Table 2-1. 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 x 10 <sup>-6</sup>	Mainly Pumps	Fails	No Effect	No Effect
Testing	1.0 x 10 <sup>-10</sup>	Pumps	No Effect	No Effect	No Effect
Maintenance and Hardware Failure	2.0 x 10 <sup>-4</sup>	Pumps or MV-8700A, B	Fails	No Effect	No Effect
Human Error and Hardware Failure	8.2 x 10 <sup>-9</sup>	MOV-8809A, B Closed Failure on Other Side	Fails	No Effect	No Effect
Other	4.6 x 10 <sup>-5</sup>	Valves or Pumps	Fails	No Effect	No Effect
Total	3.0 x 10 <sup>-4</sup>				

*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.

#### 2.1.6.2.7 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 PDB can contain one accident sequence (in which case the PDB 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.

Most event tree codes apply a “binning” procedure that eliminates the need to store and sort all of the sample (Monte Carlo trial) values generated for an output function. They also use a very efficient algorithm for calculating normally distributed random variables. In the binning procedure the complete range of output-function variability, from the 0<sup>th</sup> to the 100<sup>th</sup> percentile, is partitioned into user-defined intervals called bins. The programmed default is 20 bins with intervals concentrated around the 50<sup>th</sup> and 95<sup>th</sup> percentiles. Event tree codes internally calculate bin boundaries in terms of the output-function values corresponding to the preselected percentiles. A counter is established for each bin. As each random-sample value of the output function is generated, it is compared with the bin boundaries, the bin within which it belongs is identified, and the corresponding counter is incremented by one.

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.

#### 2.1.7 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.

#### **2.1.7.1 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 2-3. 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



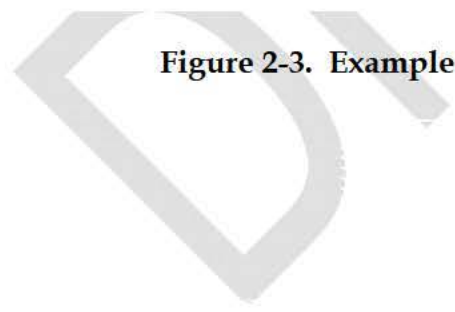
of interface and support required for system operation are thoroughly defined and evaluated.

DRAFT



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 Possible motor burnout	Prompt Prompt	Control room monitors ESG E/F 11 voltage, alarmed	Partial failure noted for future reference
	B	MDP-1B	AC power	B	Bus F12					
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 2-3. Example of Format for a System-Interaction FMEA





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.

### **2.1.7.2 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 RHFSF, 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.

### **2.1.7.3 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 6) 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.”

#### **2.1.7.4 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-STD-1629A (Reference 7).

#### **2.1.7.5 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 2-4 illustrates a typical fault tree. Figure 2-5 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.

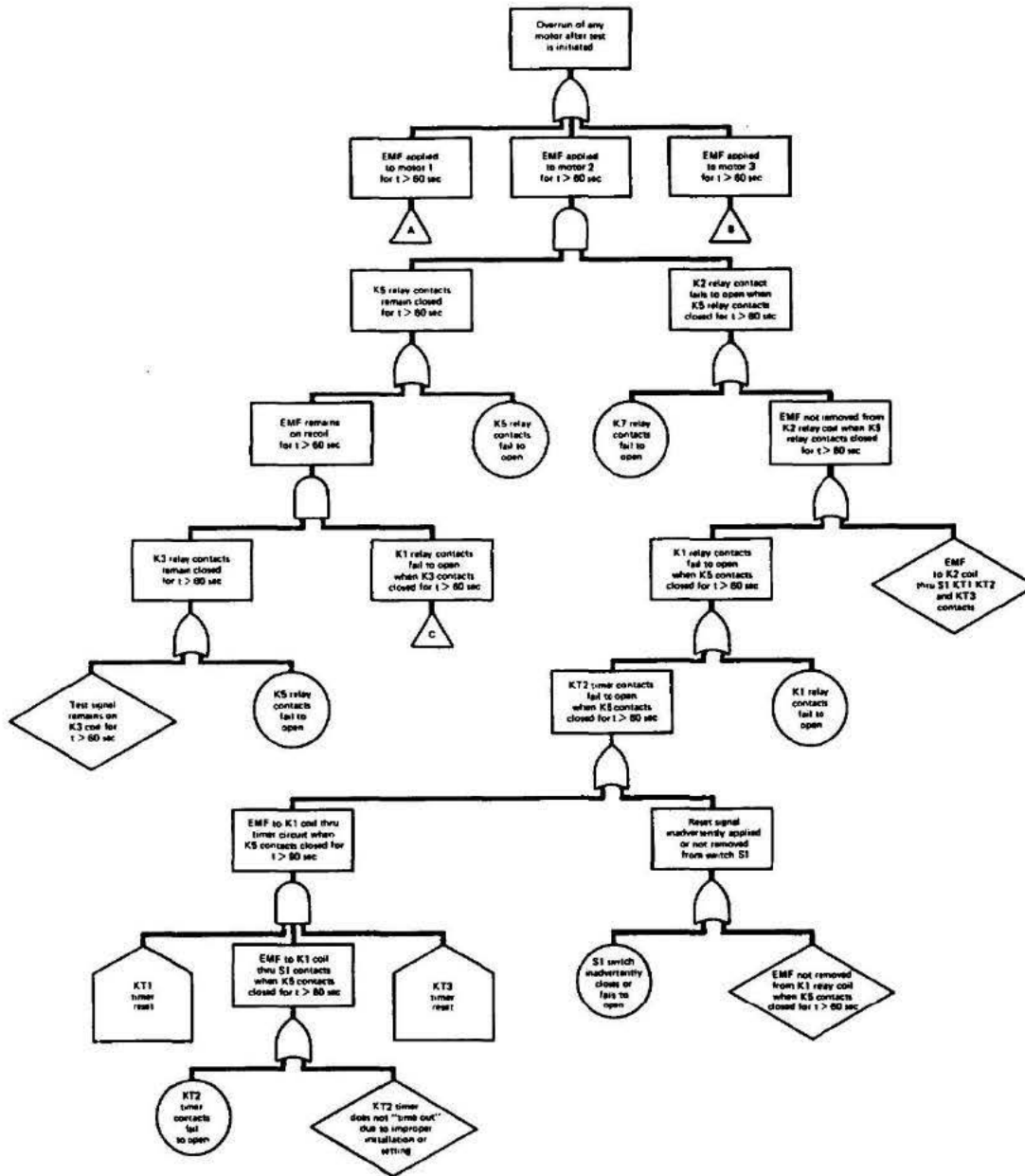


Figure 2-4. Fault Tree for Overrun of Motor 2 (relay logic only)



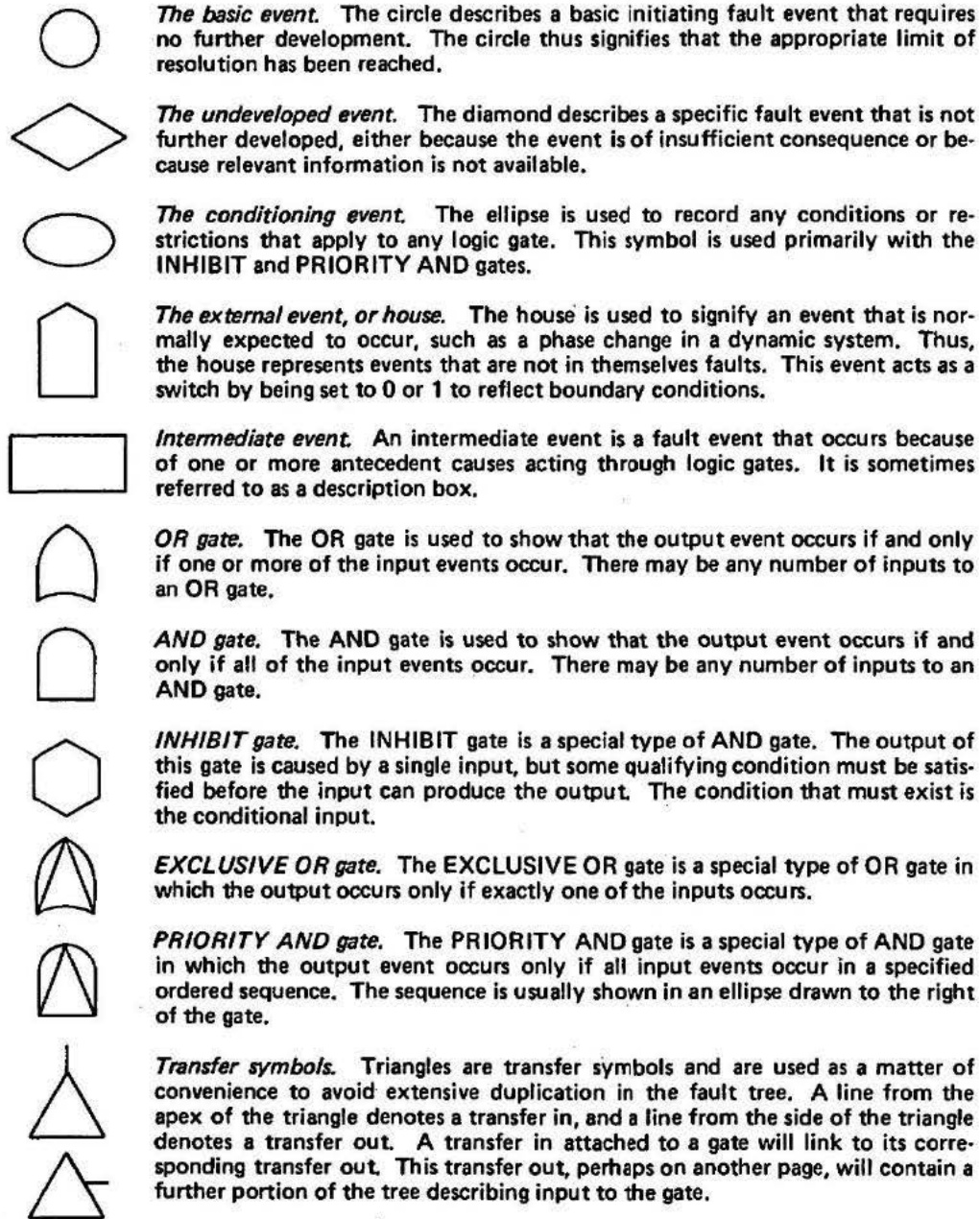


Figure 2-5. Fault-Tree Symbols†

† 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 and, perhaps, what the corresponding likelihoods of occurrence might be. In this fashion, failure mechanisms produce failure 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.

#### 2.1.7.5.1 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.

#### 2.1.7.5.2 *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.

#### 2.1.7.5.3 *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 (HRA) 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.

#### 2.1.7.5.4 *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 this 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.



### 2.1.8 Human Reliability Analysis

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). Other common HRA methods include those described in References 9 through 13.

#### 2.1.8.1 Human Failure Event (HFE) 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 through 13, 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.

#### 2.1.8.1.1 *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.

#### 2.1.8.1.2 *Operator Interviews and Scenario Walk-Throughs*

Determination of human error probability (HEP) 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 through 13. 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 2-6. Similarly, an example of a generic questionnaire for Type C post-initiator HFEs is shown in Figure 2-7.



Facility QRVA HRA Pre-Initiator HFE Operator Interview Questionnaire	
<b>Date:</b>	<b>Interviewer(s):</b>
<b>Human Action Designator:</b>	
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... Display - similar to others? digital or analog? Controls - similar to others? two position or multi position controller? breaker? Valves - similar to others? position indication? Recovery of checker errors - written materials? position indication? 2 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?	
13. What checks are performed after completing the task to verify that it has been left in its intended state?	

**Figure 2-6. Type A Pre-Initiator HFE Questionnaire**



Facility QRVA HRA Pre-Initiator HFE Operator Interview Questionnaire	
Date:	Interviewer(s):
Human Action Designator:	
Description of Action:	
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 2-6. Type A Pre-Initiator HFE Questionnaire (Continued)**

DRAFT



Facility QRVA HRA Post-Initiator Operator Interview Questionnaire	
Date:	Interviewer(s):
Interviewee(s):	
Human Action Designator:	
Description of Action:	
1. <b>What procedure(s) are used to address this situation?</b>	
2. Do the operators receive training on this type of scenario? If so, <b>what type of training</b> (classroom, simulator, other)? If training is received, <b>how often</b> is it conducted? <b>What is your experience specifically to this evolution or set of initial conditions?</b>	
3. <b>What cues and indications</b> are available for this condition in the facility? Where can they be observed by operators?	
4. <b>How much time is needed</b> for the operator to see the cue and then diagnose the cue?	
5. <b>What is the degree of clarity of the cues and indications</b> (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. <b>Confirm that failure to conduct the modeled step would lead to failure of the top event.</b>	
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)? <b>How much time do you perceive having to perform this action before this point of no return</b> (low, best estimate, high)? What's the basis for this perception or knowledge?	
10. After deciding to perform this action, <b>how much time</b> (low, best estimate, high) <b>would it take the crew to perform all parts of the action</b> (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	
Best estimate – [X] seconds/minutes/hours	
High – [X] seconds/minutes/hours	
11. <b>What facility equipment and/or man-machine interfaces are required to perform this action? Where are they located in the facility?</b> [Execution Performance Shaping Factors (PSFs) – Equipment Accessibility – Location(s)?]	

**Figure 2-7. 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:	
12. How would you describe the <b>complexity of diagnosing the need for this action</b> (complex, simple)?	
13. How would you describe the <b>complexity of performing this action</b> after it is diagnosed (complex, simple)?	
14. Are the <b>cues/indications</b> required for diagnosing this action all located in the <b>control room</b> ? Are the indications required for diagnosis available on the <b>front panels of the main control room</b> , or does the operator have to leave the main control area to read these indications?	
15. Are the <b>indications</b> available <b>accurate</b> (consider facility local sensing environment)?	
16. Has the crew received <b>training</b> in interpreting or obtaining the required information under conditions similar to those prevailing in <b>this scenario</b> ?	
17. Recovery – Which, if any, of the following recovery factors apply: <b>Self Review, Extra Crew, STA Review, Shift Change, ERF Review</b> ?	
18. Do the cues/indications for this human action occur at a time of <b>high workload</b> or distraction?	
19. Does this action require a one-time <b>check</b> of a parameter or does it require <b>monitoring</b> 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 <b>annunciator</b> (alarm)?	
21. Is the layout, demarcation, and labeling of the control boards such that it is <b>easy to locate</b> the required indicator(s)?	
22. Does the required <b>indicator</b> have <b>human engineering deficiencies</b> that are conducive to errors in reading the display?	

**Figure 2-7. 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:	
23. Are cue states or <b>parameter values as stated in the procedure</b> ? For example, if high steamline radiation is given as one of the criteria for decision or action, the steamline radiation indicators will read high, rather than normal. The "no" response is to be applied if an indicator is not obviously failed but would not give the value stated in the procedure (as, for example, if the steamline were isolated).	
24. Is the relevant instruction a <b>separate, stand-alone, numbered step</b> 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?	
26. Is the step governing this human action in some way <b>more conspicuous</b> than surrounding steps? For example, steps preceded 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 <b>unfamiliar nomenclature</b> 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 <b>all information</b> required to identify the actions directed and their objects?	
29. Does the step <b>contain the word "not?"</b>	
30. Does the procedure step present diagnostic logic in which more than one condition is combined to determine the outcome? ( <b>AND or OR or BOTH</b> )	
31. Has the crew <b>practiced</b> executing this step in a scenario similar to this one in a <b>simulator</b> ?	
32. Does the crew <b>believe</b> that the <b>instructions</b> presented are <b>appropriate</b> 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 2-7. 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:	
<p>33. Execution Performance Shaping Factors (PSFs) –</p> <p style="padding-left: 40px;"><b>Environment – Lighting</b> (<u>Normal</u>, Emergency Only, Portable Only)?</p> <p style="padding-left: 40px;"><b>Heat/Humidity</b> (<u>Normal</u>, Hot/Humid, Cold)?</p> <p style="padding-left: 40px;"><b>Radiation</b> (<u>Background</u>, Green, Yellow, Red)?</p> <p style="padding-left: 40px;"><b>Atmosphere</b> (<u>Normal</u>, Steam, Smoke, Respirator Required)?</p> <p style="padding-left: 40px;"><b>Tools</b> (Required, Adequate, Available)? No</p> <p style="padding-left: 40px;"><b>Parts</b> (Required, Adequate, Available)? No</p> <p style="padding-left: 40px;"><b>Clothing</b> (Required, Adequate, Available)? No</p> <p style="padding-left: 40px;"><b>Complexity of Execution</b> (<u>Simple</u>, Complex)?</p> <p style="padding-left: 40px;"><b>Equipment Accessibility</b> (<u>Easily Accessible</u>, Accessible with Difficulty, Inaccessible)?</p> <p style="padding-left: 40px;"><b>Facility Response as Expected</b> (<u>Yes/No</u>)?</p> <p style="padding-left: 40px;"><b>Workload</b> (Low/<u>High</u>)?</p> <p style="padding-left: 40px;"><b>PSFs Overall</b> (<u>Optimal</u>/Negative)?</p>	
(normal)	
34. How would you characterize the <b>overall execution stress</b> (Low, Moderate, High)?	
35. Are there any “ <b>recovery</b> ” 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 <b>interdependence</b> 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 <b>other human actions that would likely be associated with this scenario</b> ? 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 2-7. Type C Post-Initiator HFE Questionnaire (Continued)**

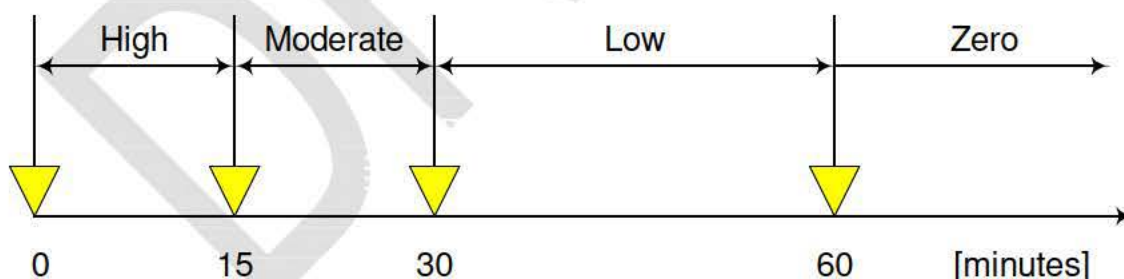


### 2.1.8.2 Human Error Probability Evaluation and Analysis

HFE HEP values can be evaluated and determined following guidance presented in References 8 through 13. However, experience has shown that HFE HEP evaluation is most effectively and efficiently implemented via HRA software, such as the Electric Power Research Institute (EPRI) HRA Calculator® software. Such software packages are designed, to the greatest degree feasible, to implement the guidance provided in HRA procedures, such as References 8 through 13, 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.

### 2.1.8.3 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) applied in the widely-used EPRI HRA software (the EPRI HRA Calculator), 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 2-8.



**Figure 2-8. 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) Table 20-17 that are reproduced below in Table 2-2. 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 2-2. Conditional Probability Equations**

<b>Level of Dependence</b>	<b>Conditional Probability Equation (<math>N = \text{HEP}</math>)</b>	<b>Approximate Value for Small <math>N</math></b>
<b>Zero Dependence (ZD)</b>	$N$	$N$
<b>Low Dependence (LD)</b>	$\frac{1 + 19N}{20}$	0.05
<b>Medium Dependence (MD)</b>	$\frac{1 + 6N}{7}$	0.14
<b>High Dependence (HD)</b>	$\frac{1 + N}{2}$	0.5
<b>Complete Dependence (CD)</b>	1.0	1.0

The steps of the HADA procedure applied via Reference 8 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  $P(A)*P(B|A)*P(C|B)$ .



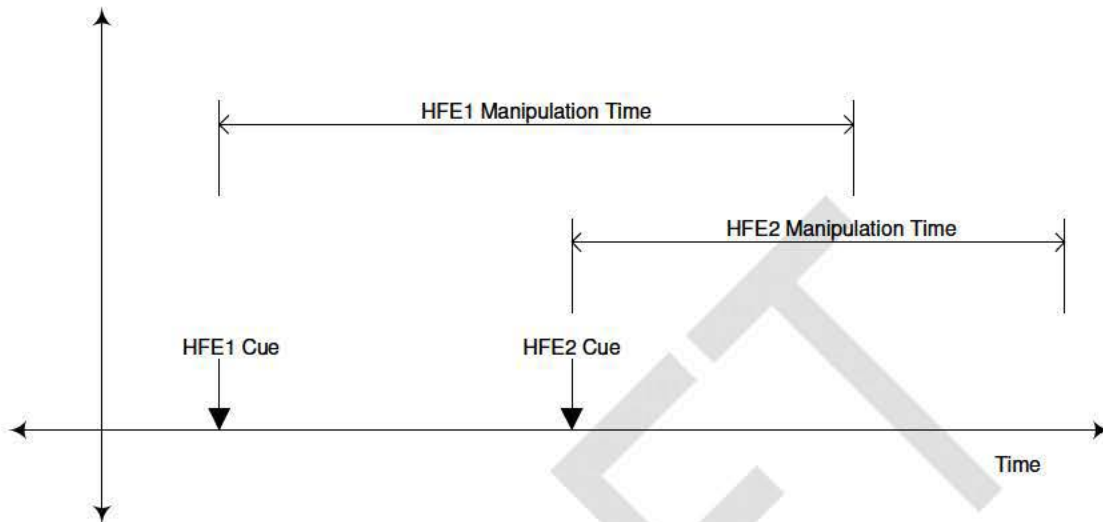
The criteria for applying Table 20-17 of NUREG/CR-1278 to assign the level of dependence between post-initiator HFEs are listed below and summarized in Figure 2-9.

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 2-9 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<sup>‡</sup> situations (Sequence Case 18 (S18) in Figure 2-9). 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 2-9 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 2-9 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 2-9 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 2-9 is also selected, as the required actions would have to be performed either simultaneously or the crew may select to do either

<sup>‡</sup> 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, atmosphere, and radiation), 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).



**DRAFT, PREDECISIONAL FOR DISCUSSION PURPOSES ONLY,  
DO NOT CITE OR QUOTE**

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 2-9 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 2-8 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 2-9 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.



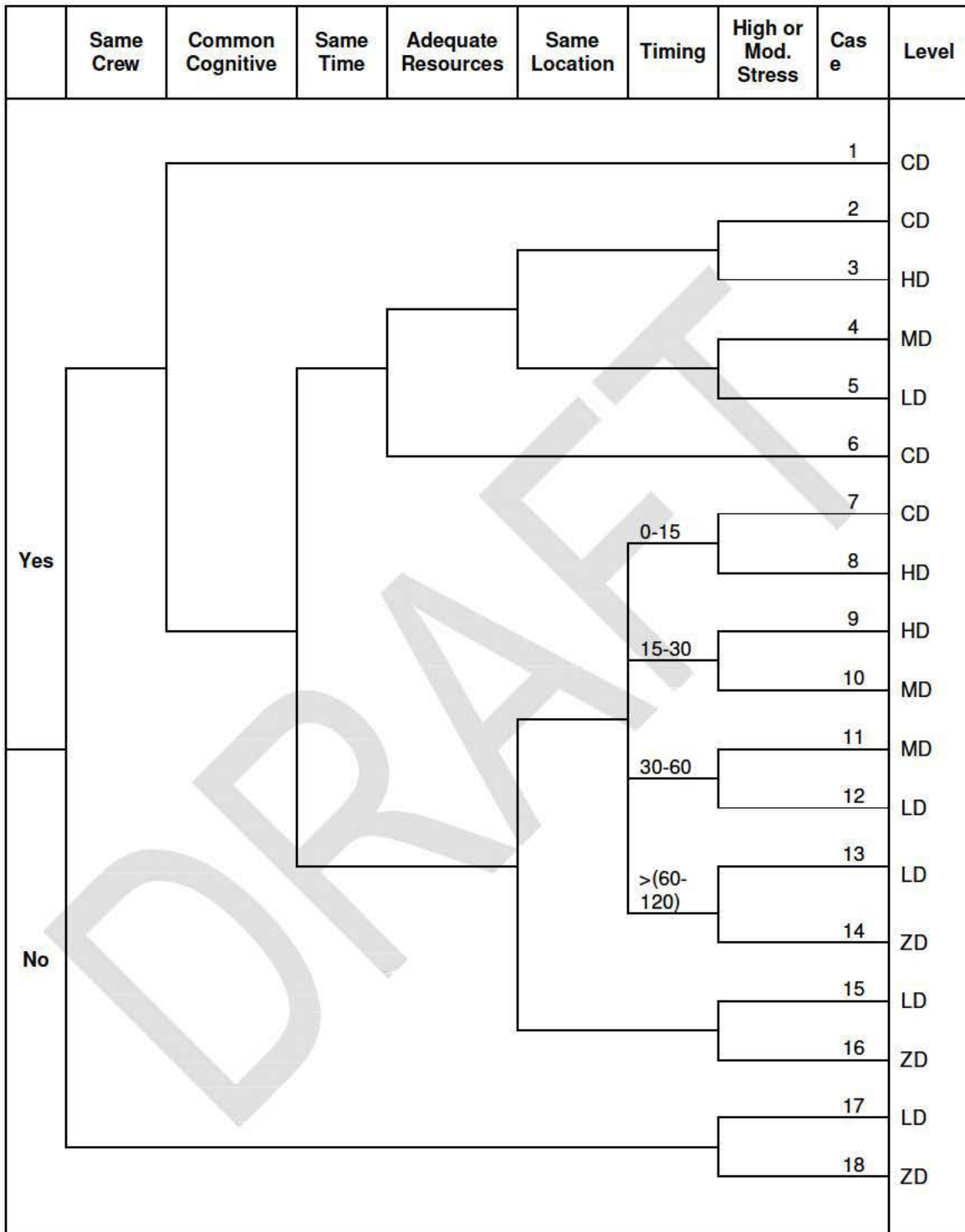


Figure 2-9. HRA Dependency Rules for Post-Initiator HFEs



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.

### 2.1.9 Data Analysis

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.<sup>§</sup>

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 raw 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 here 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 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

<sup>§</sup> 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.



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 raw 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 2-10 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 QVRA 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.

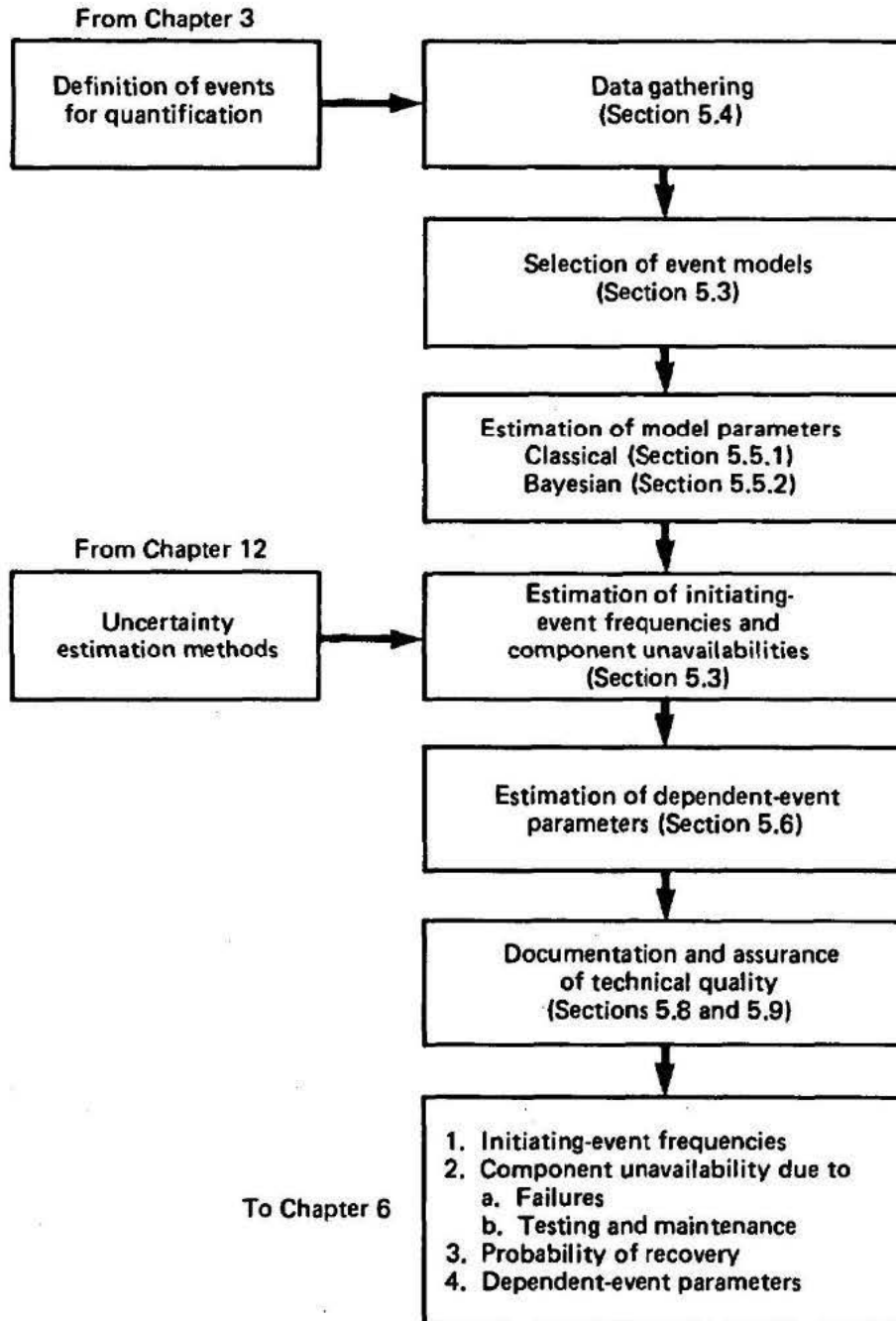


Figure 2-10. Inputs, Outputs, and Steps in Database Development



### 2.1.9.1 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 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 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 raw 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 raw (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 4) and NUREG/CR-6928 (Reference 5).

Another method of using raw generic data for determining a prior distribution is described by Kaplan (Reference 14); it uses Bayes' theorem to determine the prior distribution.

#### 2.1.9.1.1 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).

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.

#### 2.1.9.1.2 *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.

##### 2.1.9.1.2.1 **Time-Related Models**

###### 2.1.9.1.2.1.1 *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 15).

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 16) and the analytical methods described by Mann et al. (Reference 17) 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

$$U(t) = 1 - e^{-\lambda t} \quad (2-1)$$

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

#### 2.1.9.1.2.1.2 Use of Time-Related Models

##### Failure in Time: Standby

Many components in a complex facility are in a standby mode<sup>1</sup> 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  $\tau$ . The fault-exposure time  $\tau$  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 2-11. This system is tested in various pieces, that is, the logic is tested once a month, as are the spray pumps.



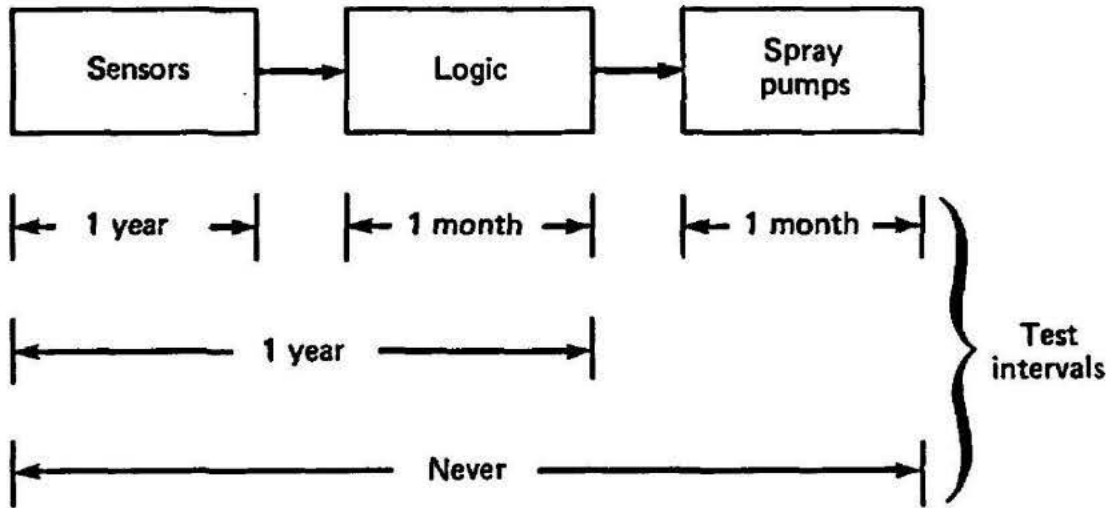


Figure 2-11. Test Intervals for Sample System

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 2-12 focuses on this situation.

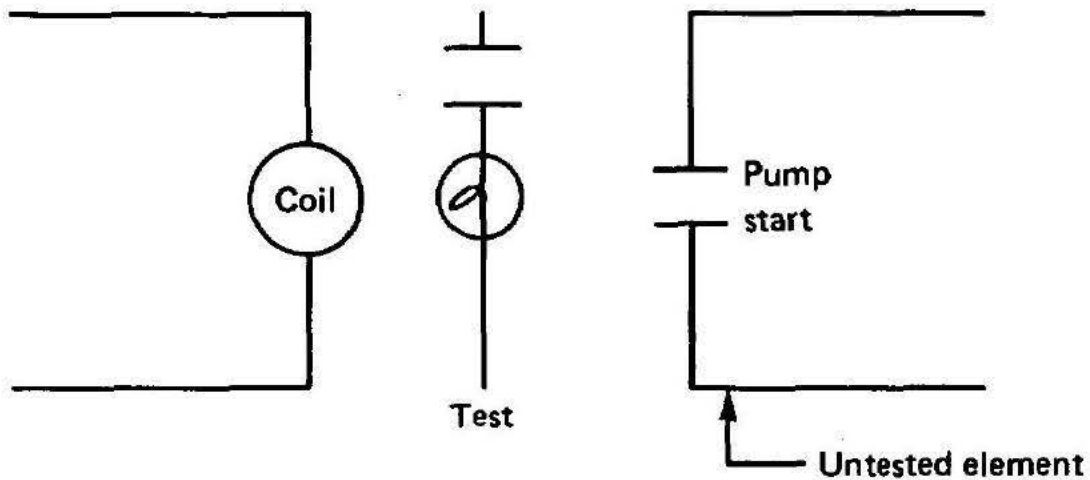


Figure 2-12. Interface Schematic

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. 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<sup>1</sup> 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.,  $f(t) = \lambda e^{-\lambda t}$ ), 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<sup>2</sup> over the time period  $\tau$ . Thus,

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

or, for the exponential considered above,

$$\begin{aligned} \bar{U} &= \frac{1}{\tau} \int_0^{\tau} (1 - e^{-\lambda t}) dt \\ &= 1 + \frac{1}{\lambda \tau} (e^{-\lambda \tau} - 1) \\ &= \frac{\lambda \tau}{2!} - \frac{(\lambda \tau)^2}{3!} + \frac{(\lambda \tau)^3}{4!} - \dots \\ &\approx \frac{\lambda \tau}{2} \end{aligned}$$

<sup>1</sup> 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 18), for the definition and use of the term "average availability".



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:

$$U \approx \lambda T$$

#### 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  $\lambda$  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  $\tau^*$  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 2-13).



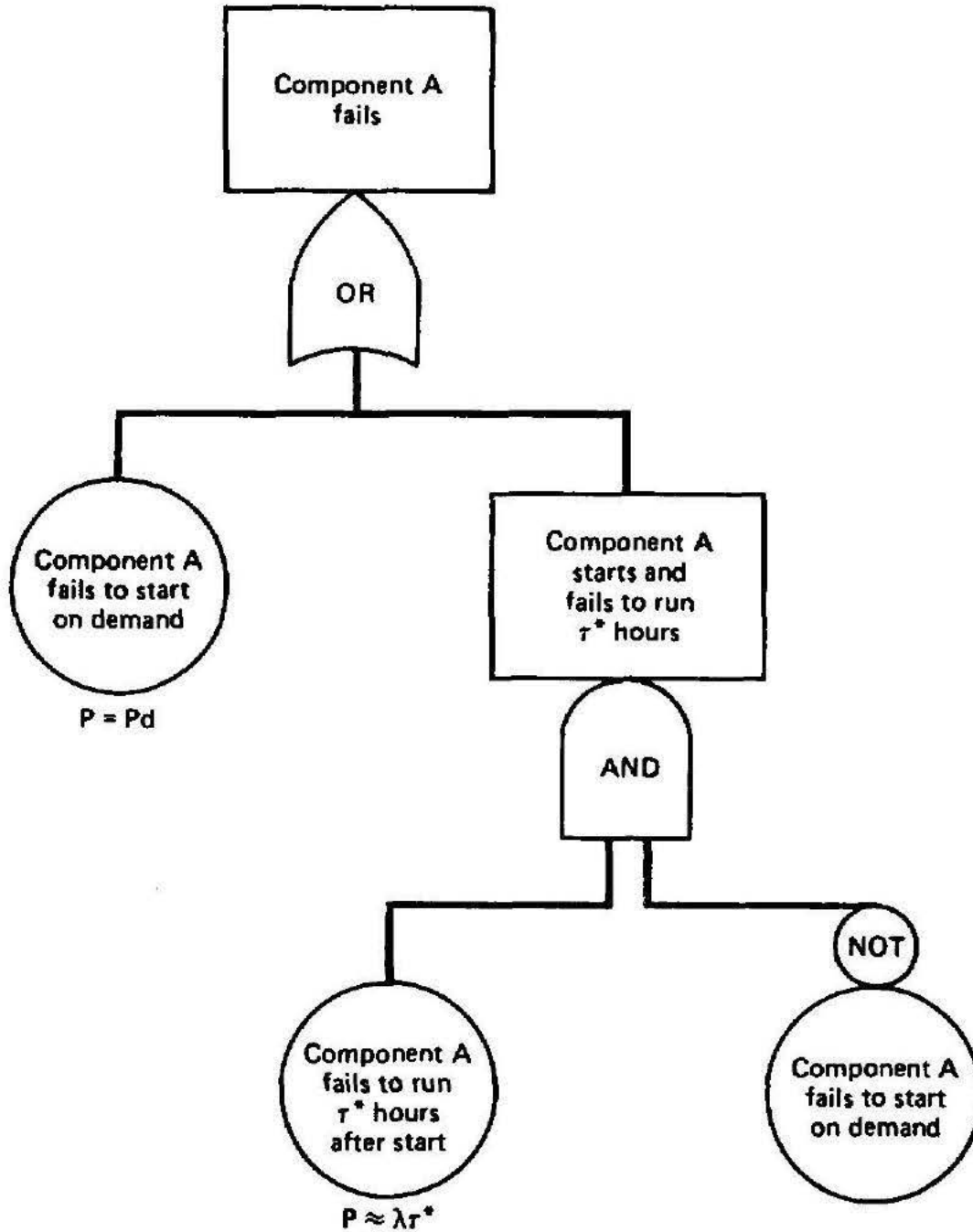


Figure 2-13. Modeling of Mutually Exclusive Events

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 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.

<u>Duration (hours)</u>	<u>Percentage of Events</u>
<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,

$$\begin{aligned} P(D > t|S) &= P(L > t \text{ AND } G > t|S) \\ &= P(L > t|S) P(G > t|S) \text{ (assuming independence)} \end{aligned}$$

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:

$$\begin{aligned} P(S \text{ and } D > t) &= (.30) (.66) (4.9 \times 10^{-4}) \\ &= 9.7 \times 10^{-5} \text{ yr}^{-1} \end{aligned}$$

For t = 4 hours:

$$\begin{aligned} P(S \text{ and } D > t) &= (.27) (.47) (4.9 \times 10^{-4}) \\ &= 6.2 \times 10^{-5} \text{ yr}^{-1} \end{aligned}$$



For  $t = 8$  hours:

$$\begin{aligned} P(S \text{ and } D > t) &= (.12) (.23) (4.9 \times 10^{-4}) \\ &= 1.3 \times 10^{-5} \text{ yr}^{-1} \end{aligned}$$

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:

$$\Pr(X \leq r) = \sum_{x=0}^r \binom{n}{x} p^x (1-p)^{n-x} \quad (2-2)$$

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.

#### 2.1.9.1.2.2 Demand Model vs. Time-to-Failure Model

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  $1 - e^{-\lambda\tau}$ . The maximum-likelihood estimate (MLE) of  $1 - e^{-\lambda\tau}$  is  $x/N$ , and thus the MLE of  $\lambda$  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

$$\begin{aligned} \hat{P}_1 &= 1 - \exp(-\hat{\lambda}\tau_1) \\ &= 1 - \exp\left[-\frac{\tau_1}{\tau} \ln(1 - P)\right] \\ &= 1 - (1 - P)^{\tau_1/\tau} \end{aligned}$$

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

$$\hat{P} = 1 - [1 - (1 \times 10^{-2})]^{12} = 1.14 \times 10^{-1}$$

### **2.1.9.1.2.3 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 19 through 21).

The equation for the lognormal distribution is

$$C(t) = \frac{1}{\sigma\sqrt{(2\pi)}} \int_{-\infty}^{\ln t} \exp\left[-\frac{(y-\mu)^2}{2\sigma^2}\right] dy \sigma^2 \quad (2-3)$$

This equation represents the cumulative probability that the event has been completed by time  $t$ . The parameters  $\sigma$  and  $\mu$  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 percent 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.

#### **2.1.9.1.2.4 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 20), for example, found that the time of maintenance for all components could be modeled by a lognormal distribution with 5<sup>th</sup> and 95<sup>th</sup> 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 [2-3]) 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).

#### 2.1.9.1.3 Facility-Specific Data Collection, Review, and Interpretation

At present, no complex facility keeps 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 2-3 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 2-3. 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 <sup>a</sup>	a. Number of failures	See 1a above
	b. Time in standby	Control-room log
3. Operating failure rate <sup>a</sup>	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
6. Recovery	Length of time to recover	Maintenance reports, control-room log
7. Human errors <sup>b</sup>	a. Number of errors	Maintenance reports, control-room log, periodic test procedures, operating procedures
	b. Opportunities	

<sup>a</sup> See Section 2.1.9.1.2.1.

<sup>b</sup> 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.

### 2.1.9.1.3.1 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.



### 2.1.9.1.3.2 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.

Unfortunately, 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 guesswork 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.



### **2.1.9.1.3.3 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 startup or shutdown, 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.

### **2.1.9.1.3.4 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 has records of demands made (e.g., pumps and diesel generators) at times other than periodic tests. It notes the starting and stopping times for these components, thus supplying operating-time data. The log also notes the initiation of various operating procedures, thus adding to the information about demand. Furthermore, it records periods when certain components and systems are out of service, and in 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.

#### *2.1.9.1.4 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 opinion. 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. The data analyst should be aware that this may be difficult to do, and it will be even more difficult to convince the community at large to adopt his degree of belief as their own.

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, thus allowing the reader of a QRVA to separate the data and the belief components of the results.

#### **2.1.9.1.4.1 Classical Estimation**

##### *2.1.9.1.4.1.1 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:  $\lambda$ , 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,  $x_1, x_2, \dots, x_n$ , such as repair times, whose logarithms are modeled as being normally distributed.

Parameters:  $\mu$ , 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 17), 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  $\lambda$ .

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.

#### 2.1.9.1.4.1.2 *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.

#### 2.1.9.1.4.1.3 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  $\lambda$  besides  $\lambda^* = f/T$  can give rise to this particular outcome. Some values of  $\lambda$ , 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-percent limit on  $\lambda$  is found to be  $\lambda_{95} = 10^{-4}$  failures per hour. This means that, for  $\lambda$  values greater than  $10^{-4}$ , the observed data are in the extreme 5 percent of possible outcomes; such  $\lambda$  values are not very consistent with the data. Values of  $\lambda$  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 -  $\alpha$ )% 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 -  $\alpha$ )% 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, slide rules, and computer programs are available for solving these equations (References 22 and 23). 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 -  $\alpha$ )% confidence limits, respectively, and  $\chi^2(m, \gamma)$  denotes the 100  $\gamma$ -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 - 2 $\alpha$ )% confidence interval.

*Poisson Distribution*

The upper and the lower 100(1 -  $\alpha$ )% confidence limits on  $\lambda$  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  $\lambda$  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 -  $\alpha$ )% confidence limits on  $\mu$ . are obtained from

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



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

For the upper and the lower  $100(1 - \alpha)\%$  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 databased 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 QVRAs 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.

#### **2.1.9.1.4.2 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 24) 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 25).

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<sup>th</sup>-century work of the Rev. Thomas Bayes (Reference 26). Bayes’ theorem (see Section 2.1.9.1.4.2.1.1) 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 24). 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.

#### *2.1.9.1.4.2.1 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.

#### 2.1.9.1.4.2.1.1 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  $\lambda$  (number of failures per unit time), Bayes' theorem states that

$$f(\lambda|E) = \frac{f(\lambda) L(E|\lambda)}{\int_0^{\infty} f(\lambda) L(E|\lambda) d\lambda} \quad (2-4)$$

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

If the parameter of interest is the probability of failure on demand,  $p$ , rather than a failure rate  $\lambda$  per unit time, then  $\lambda$  is simply replaced by  $p$  in Equation (2-4). 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 (2-4) 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 2.1.9.1.4.2.2.3 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 24).

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  $\lambda$  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 2.1.9.1.4.2.2.3), 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

$$f(\lambda|E) = \frac{f(\lambda_i)L(E|\lambda_i)}{\sum_{i=1}^m f(\lambda_i)L(E|\lambda_i)} \quad (2-5)$$

where  $\lambda_i$  ( $i = 1, 2, \dots, m$ ) 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 (2-4) when the denominator in Equation (2-4) 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 24, 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 (2-4). A better approximation is to use Equation (2-4) 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 27).

The denominator of either Equation (2-4) or Equation (2-5) 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.

#### 2.1.9.1.4.2.1.2 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<sup>th</sup> 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 28). The mean or the median would be found by conventional statistical procedures: using the prior distribution, the mean of a failure rate  $\lambda$  is given by

$$\mu_{\lambda} = \int_0^{\infty} \lambda f(\lambda) d\lambda \quad (2-6)$$

while the median is the solution to

$$F(\lambda) = \int_0^{\lambda} f(t) dt = .5 \quad (2-7)$$

$F(\lambda)$  denoting the cumulative distribution function. Using the posterior distribution, the prior  $f(\lambda)$  would be replaced by the posterior  $f(\lambda|E)$  in Equations (2-6) and (2-7).

Now consider the problem of obtaining an interval estimate for  $\lambda$ , 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  $(1 - \gamma)$  that the interval estimate really includes the unknown failure rate. (For example,  $\gamma = .05$  for .95 probability.) We can obtain a  $100(1 - \gamma)\%$  two-sided Bayes probability interval estimate of  $\lambda$  by solving the two equations

$$\int_0^{\lambda_L} f(\lambda) d\lambda = \frac{\gamma}{2} \quad (2-8)$$

and

$$\int_{\lambda_U}^{\infty} f(\lambda) d\lambda = \frac{\gamma}{2} \quad (2-9)$$

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 (2-8) and (2-9). The interval estimate  $(\lambda_L, \lambda_U)$  would then be such that  $P(\lambda_L < \lambda < \lambda_U | E) = 1 - \gamma$ .

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



---

2.1.9.1.4.2.1.3 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 2.1.9.1.4.2.2.1).
2. Select a prior-distribution family if none has been specified as part of the generic information (see Sections 2.1.9.1.4.2.2.2 and 2.1.9.1.4.2.2.3).
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 2.1.9.1.4.2.1.2.
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.

*2.1.9.1.4.2.2 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.

#### 2.1.9.1.4.2.2.1 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.

#### 2.1.9.1.4.2.2.2 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 28), 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 29), and a summary of the relevant literature on this subject has been presented by Parry and Winter (Reference 25).

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.

#### 2.1.9.1.4.2.2.3 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 will 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 will also be 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 28). Finally, there are well-developed methods for fitting natural conjugate priors to generic prior data. Some of these will be 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 QRVA's (see, for example, Reference 30). Their use is recommended (see, for example, Reference 27) 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.

### 2.1.9.2 *Common Cause Failure Analysis*

Several terms have been used to describe specific types of dependent failures. Common-mode failures<sup>††</sup> 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.

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 31).

#### 2.1.9.2.1 *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 32). The purpose here,

---

<sup>††</sup> In the Reactor Safety Study (Reference 20), 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.



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—an event that happened during the Three Mile Island accident when an operator turned off the emergency core-cooling system.

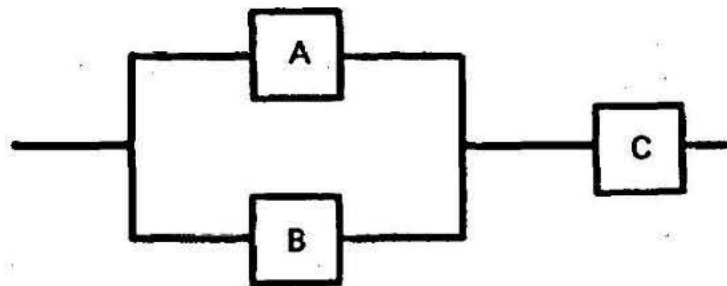
**Type 3. Intercomponent Dependences:** events or failure causes that result in a dependence among the probabilities of failure for multiple components or subsystems. The multiple failures of interest in risk analysis are usually within the same system or the same minimal cut set that has been identified 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.

#### **2.1.9.2.1.1 Analysis of Intercomponent Dependences (common cause failures)**

Once the intersystem dependences are accounted for 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

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

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

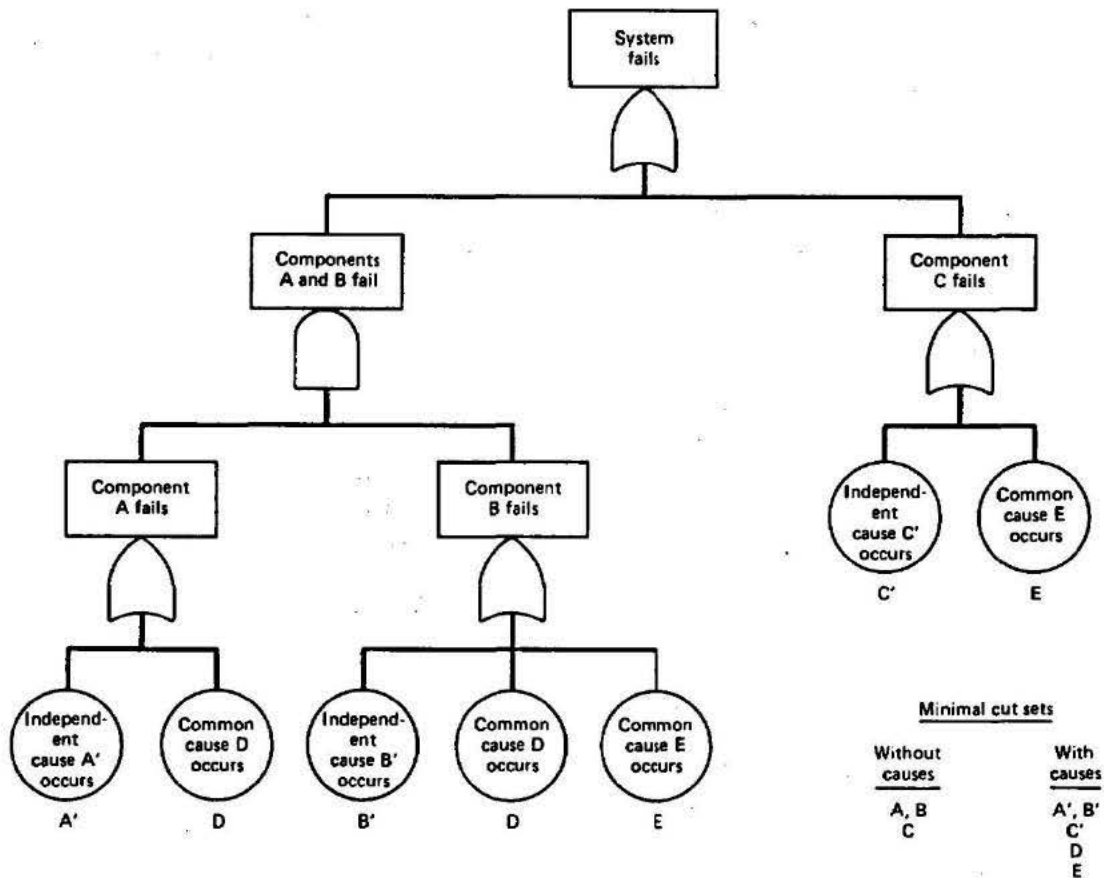
The significance of common-cause failures in this example is as follows: any cause of failure that affects any pair or all three components at the same time (or, in general, any multiple set of components in the system) will have an effect on system unavailability. When Equation 3-2 of NUREG/CR-2300 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,  $P(B|A) \gg P(B)$ . 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 2-14) where the causes appear at the level below the basic component-failure modes.



**Figure 2-14. 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 2-4 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 2-14.

**Table 2-4. Effect of Two Types of Common Causes on Fault-Tree Quantification<sup>a</sup>**

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')	$1.0 \times 10^{-3}$	$9.9 \times 10^{-4}$	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')	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	$1.0 \times 10^{-6}$	$1.1 \times 10^{-5}$	$2.0 \times 10^{-3}$	$1.5 \times 10^{-3}$

<sup>a</sup> see Figure 2-14 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 B. 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 10. 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 percent 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 2.) 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 or 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 percent (i.e., as the beta factor increases from 0 to 0.50), the system unavailability decreases by 30 percent. In most cases the common cause fraction would be expected to be less than 50 percent, 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.

#### **2.1.9.2.1.2 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 2.1.9.2.1.1, 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. Tables 2-5 and 2-6 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.

For example, failure data for auxiliary feedwater systems in pressurized water reactors (see the example 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 2-7 lists just a few.



**Table 2-5. 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
Radiation Damage	Neutron sources, charged-particle radiation
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 fission products
Biological Hazards	Poisonous gases, explosions, missiles



**Table 2-6. 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

**Table 2-7. Dependent Failures Involving Subtle Dependences**

Facility	Description
Rancho Seco	Dropped lightbulb led to shorted instrument bus, leading to a scram and a severe transient
Three Mile Island Unit 2	Maintenance error: valves in auxiliary feedwater system left closed
Brunswick	Gasket rupture on service-water liner resulting spray failed a pressure switch
Vermont Yankee	Improper installation of insulation led to failure of three ADS valves through overheating
Trojan	Maintenance error: lifted electrical lead prevented automatic pump start
Cooper	Mechanic maintaining one service-water pump accidentally broke an adjacent pump



### 2.1.9.2.1.3 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

$$A_I = \sum_i A_I^{(i)} + \sum_j A_{C_1}^{(j)} \quad (2-10)$$

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

$$C_{AB} = \sum_i C_{AB(C_2)}^{(i)} \quad (2-11)$$



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<sub>2</sub>) indicates that the common cause event involved two components only. Similar expansions can be developed for B<sub>1</sub> and C<sub>BC</sub>.

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

$$A_I \cdot B_I = \sum_i A_I^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_I^{(i)} \cdot \sum_j B_{C_1}^{(j)} + \sum_i A_{C_1}^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_{C_1}^{(i)} \cdot \sum_j B_{C_1}^{(j)} \quad (2-12)$$

$$C_{AB} \cdot C_{BC} = \sum_i C_{AB(C_2)}^{(i)} \cdot \sum_j C_{BC(C_2)}^{(j)} \quad (2-13)$$

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  $C_{AB} \cdot C_{AC}$  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  $A_I C_{BC}$ ,  $A_I B_I C_I$ ,  $C_{ABC}$ , and other permutations, but excluding  $C_{AB} \cdot C_{BC}$ . 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, 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

$$\begin{aligned} P(A_1) &= P(B_1) = P(C_1) = Q_1 \\ P(C_{AB}) &= P(C_{AC}) = P(C_{BC}) = Q_2 \\ P(C_{ABC}) &= Q_3 \end{aligned} \tag{2-14}$$

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:

$$Q_k^{(m)} = \text{probability of a basic event involving } k \text{ specific components} \\ (\text{ } 1 \leq k \leq m) \text{ in a common cause component group of size } m \tag{2-15}$$

And, the general,

$$Q_k^{(m)} \neq Q_k^{(l)} \quad l \neq m \tag{2-16}$$

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.

#### 2.1.9.2.1.3.1 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 this appendix and also in Section 5 of

---

# 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).



NUREG/CR-5485, cover a wide range of such models. The main characteristics of these models are summarized in Table 2-8.

**Table 2-8. Key Characteristics of some Popular Parametric Models**

Estimation Approach	Model	Model Parameters*	General Form for Multiple Component Failure Frequency**
NONSHOCK MODELS	Direct	Basic Parameter	$Q_k^{(m)} = Q_k^{(m)} \quad k = 1, 2, \dots, m$
	S I N G L E P A R A M E T E R	Beta Factor	$Q_k^{(m)} = \begin{cases} (1 - \beta) Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$
	I N D I R E C T M U L T I P A R A M E T E R	Multiple Greek Letters	$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \binom{k}{i=1} \rho_i (1 - \rho_{k+1}) Q_t$ $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \dots, \rho_{m+1} = 0$
	M U L T I P A R A M E T E R	Alpha Factor	Non-staggered testing $Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \dots, m$ $\alpha_t = \sum_{k=1}^m k \alpha_k$
S M O O D C E K S	Binomial Failure Rate	$Q_k^{(m)} = \begin{cases} Q_1 + \mu \rho (1 - \rho)^{m-1} & k = 1 \\ \mu \rho^k (1 - \rho)^{m-k} & 2 \leq k < m \\ \mu \rho^m + \omega & k = m \end{cases}$	

\* 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).

Table 2-8 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 like the OREDA Handbook may be used to estimate ratios of multiple to single components failure events.

#### Basic Parameter Model

The basic parameter model (Reference 33) refers to the straightforward definition of the probabilities of the basic events as given by Equation (2-15). 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 (2-15), the total failure probability,  $Q_t$ , of a component in a common cause group of  $m$  components is

$$Q_t = \sum_{k=1}^m \binom{m-1}{k-1} Q_k^{(m)} \quad (2-17)$$

where the binomial term

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(m-k)!(k-1)!} \quad (2-18)$$

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 (2-17) is still valid under the rare event approximation.

### Beta Factor Model

The beta factor model (Reference 34) 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 ( $\beta$ ) 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 (2-15) are zero except  $Q_1^{(m)}$  and  $Q_m^{(m)}$ . The last two quantities are written as (dropping the superscript  $m$ )

$$\begin{aligned} Q_1^{(m)} &= (1 - \beta)Q_t \\ Q_m^{(m)} &= \beta Q_t \end{aligned} \tag{2-19}$$

This implies that

$$\beta = \frac{Q_m^{(m)}}{Q_1^{(m)} + Q_m^{(m)}} \tag{2-20}$$

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

$$Q_t = Q_1^{(m)} + Q_m^{(m)} \tag{2-21}$$

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

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

$$Q_k^{(m)} = \begin{cases} (1 - \beta)Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases} \tag{2-22}$$

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. As will be shown later in this appendix, 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 appendix. 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 35) 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 around specific contributions from third or higher order trains, more general parametric models are recommended.

#### Multiple Greek Letter Model

The MGL model (Reference 36) 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 37). 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

$$Q_t = Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)} \quad (2-23)$$

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

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2Q_2^{(3)} + Q_3^{(3)}} \quad (2-24)$$

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

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

$$Q_t = Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)} \quad (2-25)$$

$$\delta^{(4)} = \frac{Q_4^{(4)}}{3Q_3^{(4)} + Q_4^{(4)}} \quad (2-26)$$

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,  $m \neq l$ . 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:

$$\begin{aligned} Q_1^{(3)} &= (1 - \beta)Q_t \\ Q_2^{(3)} &= \frac{1}{2}\beta(1 - \gamma)Q_t \\ Q_3^{(3)} &= \gamma\beta Q_t \end{aligned} \quad (2-27)$$

For a four-component group, the equations are

$$\begin{aligned} \beta^{(4)} &= \frac{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}} \\ \gamma^{(4)} &= \frac{3Q_3^{(4)} + Q_4^{(4)}}{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}} \end{aligned} \quad (2-28)$$



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

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

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

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

The generalization of this is given by

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^k \rho_i (1 - \rho_{k+1}) Q_t \quad (k = 1, \dots, \rho_{m+1} = 0) \quad (2-29)$$

where

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

#### 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 38). A rigorous approach to estimating beta factors is presented in Reference 39 by introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference 40 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



$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^m \binom{m}{k} Q_k^{(m)}} \quad (2-30)$$

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

$$\begin{aligned} \alpha_1^{(3)} &= \frac{3Q_1^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} \\ \alpha_2^{(3)} &= \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} \\ \alpha_3^{(3)} &= \frac{Q_3^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} \end{aligned} \quad (2-31)$$

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

Using Equations (2-30) and (2-17), we can see that the basic event probabilities can be written as a function of  $Q_t$  and the alpha factors as follows:

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} Q_t \quad (2-32)$$

where

$$\alpha_t \equiv \sum_{k=1}^m k \alpha_k^{(m)} \quad (2-33)$$



To see how Equation (2-32) is obtained from Equations (2-17) and (2-30), note that Equation (2-30) 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 (2-17) and (2-33). By using the above equation in Equation (2-30) and solving for  $Q_k^{(m)}$  we get Equation (2-32).

The parameters of the  $\alpha$ -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 parameters are

$$\begin{aligned} \beta^{(3)} &= \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \\ \gamma^{(3)} &= \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3} \end{aligned} \tag{2-34}$$

Similarly, the alpha factor model parameters for the same group are written as

$$\begin{aligned} \alpha_1^{(3)} &= 3(1 - \beta) \\ \alpha_2^{(3)} &= \frac{3}{2}\beta(1 - \gamma) \\ \alpha_3^{(3)} &= \beta\gamma \end{aligned} \tag{2-35}$$

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 2.1.9.2.1.3.2. Tables 2-9, 2-10, and 2-11 list such conversion equations for common cause component groups of up to size  $m = 8$ , under both staggered and non-staggered testing schemes.

**Table 2-9. MOL to Alpha Factor Conversion Formulae for Staggered Testing**

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



**Table 2-9. MOL to Alpha Factor Conversion Formulae for Staggered Testing  
(Continued)**

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





Table 2-10. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing

m	Alpha Factor to MGL
2	$\beta = 1 - \alpha_1 = \alpha_2$
3	$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$ $\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3}$
4	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4}{2\alpha_2 + 3\alpha_3 + 4\alpha_4}$ $\delta = \frac{4\alpha_4}{3\alpha_3 + 4\alpha_4}$
5	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\delta = \frac{4\alpha_4 + 5\alpha_5}{3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\epsilon = \frac{5\alpha_5}{4\alpha_4 + 5\alpha_5}$



Table 2-10. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing (Continued)

m	Alpha Factor to MGL
6	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\delta = \frac{4\alpha_4 + 5\alpha_5 + 6\alpha_6}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\epsilon = \frac{5\alpha_5 + 6\alpha_6}{4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\mu = \frac{6\alpha_6}{5\alpha_5 + 6\alpha_6}$
7	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\delta = \frac{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\epsilon = \frac{5\alpha_5 + 6\alpha_6 + 7\alpha_7}{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\mu = \frac{6\alpha_6 + 7\alpha_7}{5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $v = \frac{7\alpha_7}{6\alpha_6 + 7\alpha_7}$



Table 2-10. Alpha Factor to MGL Conversion Formulae for Non-Staggered Testing (Continued)

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



**Table 2-11. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing**

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



Table 2-11. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing (Continued)

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



**Table 2-11. MGL to Alpha Factor Conversion Formulae for Non-Staggered Testing (Continued)**

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

Binomial Failure Rate (BFR) Model

The Binomial Failure Rate model (Reference 41) 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.

$\mu$  = frequency of occurrence of nonlethal shocks.

$\rho$  = conditional probability of failure of each component, given a nonlethal shock.

$\omega$  = frequency of occurrence of lethal shocks.

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

$$Q_k^{(m)} = \begin{cases} Q_I + \mu\rho(1 - \rho)^{m-1} & k = 1 \\ \mu(\rho)^k(1 - \rho)^{m-k} & 2 \leq k < m \\ \mu\rho^m + \omega & k = m \end{cases} \quad (2-36)$$

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.

#### 2.1.9.2.1.3.1.1 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 the effects of various assumptions including alternative strategies is given in Section 2.1.9.2.1.3.2.



### Estimators for Basic Parameters

The maximum likelihood estimator for  $Q_k$  is given as

$$\hat{Q}_k = \frac{n_k}{N_k} \quad (2-37)$$

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

$$N_k = \binom{m}{k} N_D \quad (2-38)$$

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

$$\hat{Q}_k^{(m)} = \frac{n_k}{\binom{m}{k} N_D} \quad (2-39)$$

Thus, Equation (2-39) 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 (2-39). 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 (2-17) with the corresponding estimator yields the following estimator for the total failure probability for a specific component:

$$\hat{Q}_t = \frac{1}{m N_D} \sum_{k=1}^m k n_k \quad (2-40)$$

### Estimator for the $\beta$ -Factor Model Parameter

Although the  $\beta$ -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  $\beta$ -factor estimator can be defined for a system of  $m$  redundant components.

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



$$\beta = \frac{1}{Q_t} \sum_{k=2}^m \frac{(m-1)!}{(m-k)!(k-1)!} Q_k \quad (2-41)$$

Using the estimator of  $Q_k^{(m)}$ , given by Equation (2-39), and  $Q_t$ , given by Equation (2-40), in the above equation results in the following estimator for  $\beta$ .

$$\beta = \frac{\sum_{k=2}^m kn_k}{\sum_{k=1}^m kn_k} \quad (2-42)$$

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

$$\beta = \frac{2n_2}{n_1 + 2n_2} \quad (2-43)$$

Note that the estimator  $\beta$  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 (2-41). Additional discussion of this is in Appendix D of this report.

### 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,

$$\beta = \frac{1}{Q_t} \sum_{k=2}^m \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \quad (2-44)$$

$$\gamma = \frac{1}{\beta Q_t} \sum_{k=3}^m \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \quad (2-45)$$

$$\delta = \frac{1}{\beta \gamma Q_t} \sum_{k=4}^m \frac{(m-1)!}{(m-k)!(k-1)!} Q_k^{(m)} \quad (2-46)$$

Therefore, by using Equations (2-39) and (2-40) in the above expressions, the following estimators are obtained:



$$\hat{\beta} = \frac{\sum_{k=2}^m kn_k}{\sum_{k=1}^m kn_k} \quad (2-47)$$

$$\hat{\gamma} = \frac{\sum_{k=3}^m kn_k}{\sum_{k=2}^m kn_k} \quad (2-48)$$

$$\hat{\delta} = \frac{\sum_{k=4}^m kn_k}{\sum_{k=3}^m kn_k} \quad (2-49)$$

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

$$\hat{\beta} = \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \quad (2-50)$$

Similarly,

$$\hat{\gamma} = \frac{3n_3}{2n_2 + 3n_3} \quad (2-51)$$

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 (2-51), 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  $\alpha$ -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 $\alpha$ -factor Model Parameters**

An estimator for each of the  $\alpha$ -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,

$$\hat{\alpha}_k = \frac{n_k}{\sum_{k=1}^m n_k} \quad (2-52)$$



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  $Q_i$ ,  $\mu$ ,  $\omega$ , and  $\rho$ . To develop estimators for these parameters, several other quantities are defined as:

$\Lambda_t \equiv$  rate of nonlethal shocks that cause at least one component failure

$n_t \equiv$  total number of common cause failure events

$$n_t \equiv \sum_{k=1}^m n_k \quad (2-53)$$

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  $Q_i$ ,  $\lambda_t$ ,  $\omega$ , and  $\rho$ , as presented in Appendix D of NUREG/CR 5485, are

$$\hat{Q}_i = \frac{n_i}{mN_D} \quad (2-54)$$

$$\hat{\lambda}_t = \frac{n_t}{N_D} \quad (2-55)$$

$$\hat{\omega} = \frac{n_L}{N_D} \quad (2-56)$$

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

$$\hat{s} = \hat{\rho} \frac{mn_t}{1 - (1 - \rho)^m} \quad (2-57)$$

where

$$\hat{s} = \sum_{k=1}^m kn_k \quad (2-58)$$



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

$$\lambda_t = \mu[1 - (1 - \rho)^m] \quad (2-59)$$

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

$$\hat{\mu} = \frac{\hat{\lambda}_t}{1 - (1 - \hat{\rho})^m} \quad (2-60)$$

#### 2.1.9.2.1.3.2 *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 Tables 2-9 through 2-11.

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:

$$N_{k=} \binom{m}{k} N_D \quad (2-61)$$

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:

$$N_D = N_{TS}$$

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  $N_D^*$  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.<sup>§§</sup>

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

$$\begin{aligned} N_k &= \left( N_D^* - \sum_{j=1}^m n_j \right) \binom{m-1}{k-1} + \left( \sum_{j=1}^m n_j \right) \binom{m-1}{k-1} \\ &= N_D^* \binom{m-1}{k-1} = m N_{TS} \binom{m-1}{k-1} \end{aligned} \quad (2-62)$$

The number of single component demands is given by

$$N_D^* + \sum_{j=1}^m n_j \cdot (m-1) \quad (2-63)$$

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 (2-61),

$$Q_k^{NS} = \frac{n_k}{\binom{m}{k} N_{TS}} \quad (2-64)$$

For a staggered testing scheme, using Equation (2-62),

$$Q_k^S = \frac{n_k}{m \binom{m-1}{k-1} N_{TS}} \quad (2-65)$$

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

$$\frac{Q_k^S}{Q_k^{NS}} = \frac{1}{k} \quad (2-66)$$

<sup>§§</sup> 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  $Q_i \cdot Q_k$  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.



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,

$$\beta = \frac{Q_2}{Q_1 + Q_2} \quad (2-67)$$

Therefore,

$$\beta^S = \frac{Q_2^S}{Q_1^S + Q_2^S} \quad (2-68)$$

and,

$$\beta^{NS} = \frac{Q_2^{NS}}{Q_1^{NS} + Q_2^{NS}} \quad (2-69)$$

thus,

$$\beta^{NS} = \frac{2Q_2^S}{Q_1^S + 2Q_2^S} \cong 2 \frac{Q_2^S}{Q_1^S + Q_2^S} = 2\beta^S \quad (2-70)$$

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 (2-68) is similar in form to the estimator of a single parameter model called the C-factor model (Reference 35). In this respect, C-factor is another estimator of the  $\beta$ -factor under the assumptions leading to Equation (2-68). It should be mentioned, however, that the C-factor method was developed to try to use the licensee 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).

#### **2.1.9.2.1.4 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 42 through 44). 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 45). 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 46), Putney (Reference 47), and Worrell and Stack (Reference 44). 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.



### 2.1.9.3 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.

#### 2.1.9.3.1 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.

#### 2.1.9.3.2 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.

#### 2.1.9.3.3 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



licensee 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.

#### 2.1.9.4 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.

##### 2.1.9.4.1 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.

##### 2.1.9.4.2 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 Figures 2-15 and 2-16 should be used to tie the specific events to the general database.

Figure 2-15 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 2-16. 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).

DRAFT











#### 2.1.9.4.3 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.

#### 2.1.10 Event Sequence Quantification

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”.

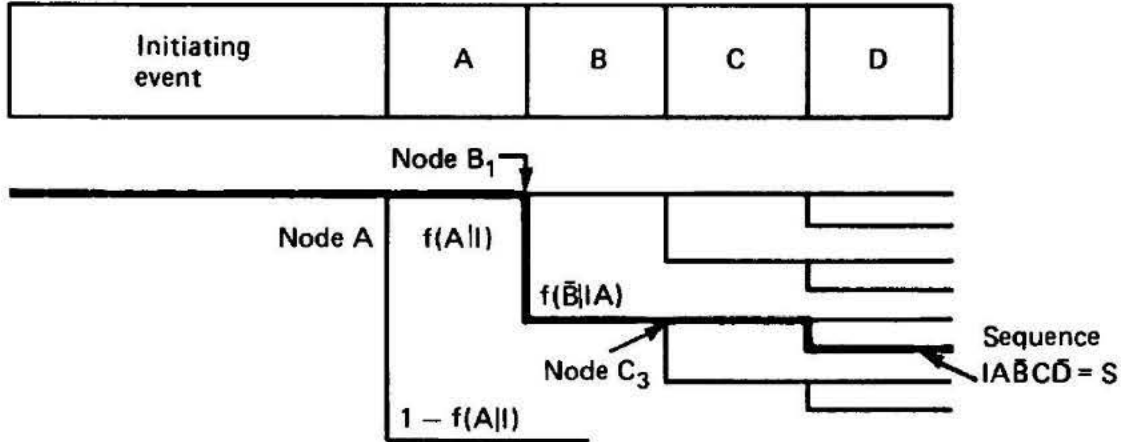
Since we have not, in fact, done this experiment, we cannot, of course, say what this sequence frequency is with complete certainty. However, we can logically infer some things about this frequency from the frequencies of the “elemental” events that make up the sequence; i.e., the split fractions.

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 2-17. 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 2-17. 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<sub>1</sub>. Out of all those sequences, let  $f(\bar{B}|IA)$  be the fraction that emerges from B<sub>1</sub> along the lower branch. The term is  $f(\bar{B}|IA)$  then the split fraction at Node B<sub>1</sub>.

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,

$$\phi(S) = \phi(I) f(A|I) f(\bar{B}|IA) f(C|IAB) f(\bar{D}|IABC)$$

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 B<sub>1</sub>)

$f(C|IAB)$  = the frequency of success for System C, given that I has happened, A has succeeded, and B has failed

$f(\bar{D}|IABC)$  = 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  $f(C|IA\bar{B})$ , 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.<sup>\*\*\*</sup>

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 2-17 and discuss the calculation of PDB frequencies.

### 2.1.10.1 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

---

<sup>\*\*\*</sup> 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.



table (see Figure 2-18 for an abbreviated example). In this table, all possible causes (“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<sup>†††</sup> 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.

---

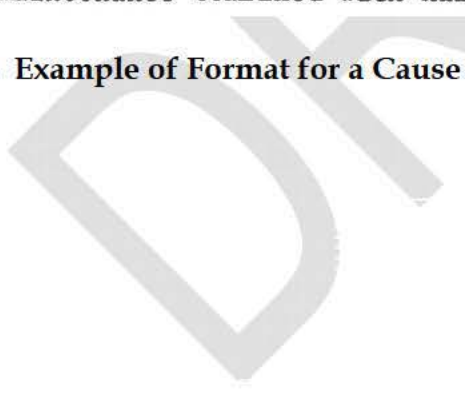
<sup>†††</sup> These, along with the  $\phi(I)$ , are examples of elemental frequencies.



Cause	Failure frequency	Components	Effect		Initiating events
			System	Other systems	
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.

Figure 2-18. Example of Format for a Cause Table for Double Failures (buses available)





2.1.10.1.1 Computation of PDB Frequencies

Event trees are not limited as in Figure 2-17 to nodes with two branches. Therefore, to generalize the notation, let  $f_{nb}$  denote the split fraction at Node  $n$  that goes with Branch  $b$ . With these quantities established for each branch point, one can calculate the frequency of each accident-sequence path as

$$\begin{aligned}\phi(S) &= \phi(I)f_{1b,1}f_{2b,2}\dots f_{nb,n}\dots \\ &= \phi(I) f(S)\end{aligned}\tag{2-71}$$

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

$$m_{ij} = \sum_h f(s_{ih})\tag{2-72}$$

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

$$\phi(I_i)m_{ij}\tag{2-73}$$

is the frequency of occurrence of Exit State  $y_j$  as a result of Initiating Event  $I_i$ . Moreover,

$$\sum_i \phi(I_i)m_{ij}\tag{2-74}$$

is the frequency of occurrence of Exit State  $y_j$  as a result of all initiating events.

Equation (2-72) 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

$$\phi^Y = \phi^I M\tag{2-75}$$

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 (2-71) through (2-75) 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 PDB 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 (2-71) through (2-75). 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.

#### 2.1.10.2 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.

### 2.1.10.3 Event Sequence Uncertainty Analysis

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:

1. 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.
2. 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.
3. 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.

#### 2.1.10.3.1 Sources of Uncertainty

Table 2-12 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 2-12. 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

2.1.10.3.2 *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 PDB 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 18), the Fussell-Vesely (Reference 48), and the Birnbaum (Reference 49) measures; they have been defined and described by Lambert and Gilman (Reference 50). 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 51).

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 51), 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 52) 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 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 assumed to be 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

$$\begin{aligned} P(\text{top}) = & P(\text{pump A}) * P(\text{pump B}) \\ & + P(\text{pump A}) * P(\text{control B}) \\ & + P(\text{pump B}) * P(\text{control A}) \\ & + P(\text{control A}) * P(\text{control B}) \end{aligned}$$

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

$$P(\text{top}) = [P(\text{pump})]^2 + 2[P(\text{pump}) P(\text{control})] + [P(\text{control})]^2$$

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 53). 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.

## **2.2 RHFSF Fuel Release from Internal Events QRVA (Level 2)**

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 RHFSF 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.

### **2.2.1 RHFSF Unplanned Fuel Movement Data Analysis**

Chronic releases can be addressed via analysis of RHFSF unplanned fuel movement (UFM) reports. At the RHFSF, 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 RHFSF 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.

### **2.2.2 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 RHFSF. In general, these models characterize the relatively low-frequency high-consequence event sequences applied in assessing facility risk from acute hazard sources.

#### **2.2.2.1 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.

#### 2.2.2.2 *Event-Caused Structural Failure Evaluation*

It is conceivable that, for event sequences involving large-capacity release from one or more RHFSF 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.

#### 2.2.2.3 *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.

### 2.3 Risk Results Presentation and Interpretation

When completed, the QRVA total aggregated risk results can be expressed via table and via probability distribution graphs. For example, a hypothetical risk results table for the RHFSF mean or best-estimate risk results could be expressed as shown in Table 2-13.

The consequence bins shown in Table 2-13 are hypothetical (for example only) at this stage. In this case, a hypothetical bin boundary of 13,000 gallons was selected, because AOC Sections 6 and 7 preliminary task results have indicated that this potential fuel release volume may be critical in predicting important fuel contamination levels for the Red Hill Water Shaft. The consequence bin values are selected based on hypothetical fuel releases based on analysis, and they do not conform to any historical release volumes. These consequence bins will be firmly established during the QRVA Phase 2 project. For each row consequence bin in Table 2-13, a probability density function graph can be developed and presented, showing the entire probability density curve and highlighting the associated characteristic values, such as the distribution mode, median, mean, 5<sup>th</sup> percentile, and 95<sup>th</sup> percentile values. Also, the results table can be expanded to present the probability density function characteristic values in tabular format, in addition to showing the probability density curves for each row of the table.



**DRAFT, PREDECISIONAL FOR DISCUSSION PURPOSES ONLY,  
DO NOT CITE OR QUOTE**

**Table 2-13. RHFSF Total Aggregate Mean Risk Results**

<b>Fuel Type</b>	<b>Mean Frequency</b>	<b>Annual Mean Probability</b>	<b>Consequence Bin (gal/yr released to the Red Hill Water Shaft)</b>	<b>Remarks</b>
1	To Be Determined (TBD)	TBD	0-999	TBD
2	TBD	TBD	0-999	TBD
3	TBD	TBD	0-999	TBD
1	TBD	TBD	1000-9999	TBD
2	TBD	TBD	1000-9999	TBD
3	TBD	TBD	1000-9999	TBD
1	TBD	TBD	10000-12999	TBD
2	TBD	TBD	10000-12999	TBD
3	TBD	TBD	10000-12999	TBD
1	TBD	TBD	13000-99999	TBD
2	TBD	TBD	13000-99999	TBD
3	TBD	TBD	13000-99999	TBD
1	TBD	TBD	100000-999999	TBD
2	TBD	TBD	100000-999999	TBD
3	TBD	TBD	100000-999999	TBD
1	TBD	TBD	1000000-12499999	TBD
2	TBD	TBD	1000000-12499999	TBD
3	TBD	TBD	1000000-12499999	TBD
1	TBD	TBD	12500000-124999999	TBD
2	TBD	TBD	12500000-124999999	TBD
3	TBD	TBD	12500000-124999999	TBD
1	TBD	TBD	>125000000	TBD
2	TBD	TBD	>125000000	TBD
3	TBD	TBD	>125000000	TBD



## **2.4 QRVA Vulnerability Assessment**

The total aggregate risk results discussed in Section 2.3 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 RHFSF. 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.

### **2.4.1 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 2.4.2.

### **2.4.2 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.

#### 2.4.2.1 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).

#### 2.4.2.2 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

$$R_i^t = \text{the increased risk level without feature } i \text{ or with feature } i \text{ assumed failed,} \quad (2-76)$$

and

$$R_0 = \text{the present risk level,} \quad (2-77)$$

where the risk can be any measure such as core melt frequency, expected dose, etc. Then, on a ratio scale, the risk achievement worth  $A_i$  of feature  $i$  is defined as:

$$A_i = R_i^t / R_0 \quad (2-78)$$

On an interval scale the risk achievement worth  $A_i$  is defined as:

$$A_i = R_i^t - R_0 \quad (2-79)$$



In calculating  $R_i^t$  with feature  $i$  removed, it is important to consider other features which 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 core melt frequency and 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.

### 2.4.2.3 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

$$R_{\bar{1}} = \text{the decreased risk level with the feature optimized or assumed to be perfectly reliable,} \quad (2-80)$$

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:

$$D_i = R_0/R_{\bar{1}} \quad (2-81)$$

On an interval scale the risk reduction worth  $D_i$  is:

$$D_i = R_0 - R_{\bar{1}} \quad (2-82)$$

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.



#### 2.4.2.4 *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 54) measure of importance,  $I_i$ , which can be expressed as:

$$I_i = \frac{R_0 - R_{\bar{i}}}{R_0} \quad (2-83)$$

where the numerator represents the risk due to contributor  $i$ . Equation (2-83) can be expressed as:

$$I_i = 1 - \frac{1}{D_i} \quad (2-84)$$

or

$$I_i = \frac{D_i - 1}{D_i} \quad (2-85)$$

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  $i$ .

#### 2.4.2.5 *Birnbaum Importance (risk derivative)*

If the risk measure is defined to be the system unavailability or unreliability then the more generally applied Birnbaum (Reference 49) importance  $\Delta_i$  of Component  $i$  can be defined as:

$$\Delta_i = R_i^t - R_{\bar{i}} \quad (2-86)$$

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 18) call the  $\Delta_i$  reliability importance of Component  $i$ .

By adding and subtracting the nominal unavailability  $R_0$  to the right side of Equation (2-86) it can be seen that

$$\Delta_i = A_i - D_i \quad (2-87)$$

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.



### 2.4.3 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.

### 2.4.4 Vulnerability Assessment Results Presentation and Interpretation

Key elements of the QRVA Vulnerability Assessment are presentations of the risk element risk importance measures and associated sensitivity case studies in the form of tabular results and via presentation of risk element “tornado charts”. In effect, tornado charts are bar charts of risk element importance measure or sensitivity case study results rotated by 90 degrees and rank ordering the bars from high to low moving downward on the chart, creating, in effect, a tornado-shaped chart of results with the most important elements at the top and the least important elements at the bottom. Experience has shown that there can be significant pitfalls in attempting to interpret risk importance measure and sensitivity case study results directly from tables and charts.

By reviewing all the ranked lists of importance measure results along with the sensitivity case study tornado charts, we can obtain an understanding of facility-specific risk-dominating vulnerabilities. It is also instructive to compare facility-specific component failure rates (i.e., the Bayesian-updated failure rates) and HFE HEP values with their associated generic data values. Those facility-specific values that are significantly greater than (e.g., more than 50% relative difference) their associated generic values can point to potential facility-specific risk vulnerabilities.

These results will be presented in the QRVA report with an accompanying discussion developed by analysts experienced with the RHFSF risk model designed to facilitate meaningful interpretation of vulnerability assessment results.



## **2.5 Internal Flooding QRVA**

The general steps of an internal flooding QRVA are similar to those for other internal events presented above in Sections 2.1 through 2.4; however, internal flooding, internal fire, and effectively all the external events QRVAs differ because the hazards, failure modes, and HFEs are location-dependent throughout the facility. At the RHFSF, internal flooding can most likely result from misdirected fuel or water within the facility. These misdirected liquids can result from actual tank or piping failures or from human errors associated with operations, maintenance, testing, or inspection activities.

### **2.5.1 Internal Flood Events Scope Determination**

In internal flooding QRVAs, it is important to identify all the liquid-containing fixed systems and transient support systems that could be involved in an internal flooding scenario at the facility. As the internal events QRVA described in Sections 2.1 through 2.4 above includes fuel tank or piping rupture scenarios, it may be determined that only water and other non-fuel sources of liquid should be associated with the flooding QRVA for the RHFSF.

Also within the scope determination is the task of selecting those areas or zones of the facility that are truly susceptible to flooding risk. For example, areas within tanks or piping that normally contain liquid would generally not be considered as flood-susceptible. In general, flood-susceptible areas of a facility are those areas where operators may be expected to perform normal or emergency operator actions or any area that contains flood-susceptible equipment or components; e.g., electrical or electronic components or components potentially susceptible to failure or degradation from flood scenario-related liquid jets or sprays.

### **2.5.2 Internal Flood Facility Partitioning**

For internal flooding QRVA, the facility must be partitioned into logical areas or zones for flood scenario development and associated impact assessment. The flood zones for the QRVA are generally determined by identifying and characterizing liquid barriers within the facility, such as the yellow flood protection doors installed in the RHFSF tunnels. All facility areas or zones containing flood-susceptible equipment must be considered in the partitioning task.

### **2.5.3 Internal Flood Source Identification and Characterization**

In internal flooding QRVAs, it is important to identify and characterize all the potential sources of liquid that could be involved in an internal flooding scenario at the facility are to be considered within the scope of the internal flooding QRVA. These sources of liquid include anticipated “transient” sources, such as moveable water trucks or tanks that may occasionally be in the facility to support periodic maintenance or testing activities as well as fixed sources, such as fuel tanks, fuel piping, facility water system tanks and/or facility water system piping. It is important to determine the specific locations and total capacities or volumes associated with each liquid source.



#### **2.5.4 Internal Flood-Induced Initiating Event Analysis**

After the internal flood sources are identified and characterized, internal flooding initiating event analysis can be performed. Similar to the analysis approach outlined in Sections 2.1.5 and 2.1.9 above, the flooding scenario initiating event frequency values must be determined for event sequence quantification. Also, there are generic data sources available to support flooding initiating event determination.

#### **2.5.5 Internal Flood Scenario Development**

After the flood sources, flood zones, and flood initiating events have been determined, the internal flood scenarios can be characterized applying the event sequence analysis approach outlined previously. It is important to identify flood scenarios by flood initiation zone and by potential flood propagation zones included in each scenario. Also, it is necessary to identify the effective impact heights for each flood-susceptible component and potential HFE modeled within each flood zone for a scenario. That is, a determination must be made and documented as to the minimum height a liquid can reach in the zone to effect a failure mode or HFE of interest for each flood-susceptible component in the zone and each human action modeled to be implemented within the zone. Also, an important part of the scenario development involves the analysis of maximum and effective sustained liquid heights in each zone affected by each flood scenario included in the risk model. It is important to note that, in internal flooding scenarios as for other hazard-specific portions of the QRVA, equipment failures and HFEs can be caused directly by the target hazard, internal flooding in this case, or by other independent failure causes. That is, for each scenario, equipment failures and HFEs may be caused by the effects of the flooding or, independently via any other cause included in the internal events QRVA described in Sections 2.1 through 2.4.

#### **2.5.6 Internal Flood Human Reliability Analysis**

HFEs evaluated in the QRVA described in Sections 2.1 through 2.4 will need to be reviewed and reanalyzed to account for flooding scenario impacts on HFE HEP PSFs. There may be cases where certain human actions credited in the other internal events QRVA may be determined to be infeasible due to liquid inundation at the human action location. Additionally, some internal flood specific human actions may be identified associated with preventing or mitigating potential flood scenario impacts on the facility. In such cases, those additional human actions and associated HFEs will be required to be evaluated for incorporation in the internal flooding QRVA event sequence analysis and quantification.

#### **2.5.7 Internal Flood Accident Sequence Analysis**

Internal flood accident sequence analysis is performed applying the approach outlined in Sections 2.1 through 2.4, via the following major process steps:

- Event Sequence Diagram Development
- Event Tree Development
- Conditional Split Fraction Determination



- Systems Analysis (e.g., fault tree analysis)
- Split Fraction Quantification

### **2.5.8 Internal Flood Data Analysis**

Internal flood data analysis is performed applying the approach outlined in Sections 2.1 through 2.4.

### **2.5.9 Internal Flood Risk Quantification**

Internal flood risk quantification is performed applying the approach outlined in Sections 2.1 through 2.4.

### **2.5.10 Internal Flood Risk Uncertainty Analysis**

Internal flood risk uncertainty analysis is performed applying the approach outlined in Sections 2.1 through 2.4.

### **2.5.11 Risk Results Presentation and Interpretation**

Internal flood risk results presentation and interpretation is performed applying the approach outlined in Sections 2.1 through 2.4.

### **2.5.12 QRVA Vulnerability Assessment**

Internal flood vulnerability assessment is performed applying the approach outlined in Sections 2.1 through 2.4.

#### **2.5.12.1 Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences)**

Internal flood risk decomposition is performed applying the approach outlined in Sections 2.1 through 2.4.

#### **2.5.12.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events**

Internal flood risk importance measure determination and evaluation for event tree split fractions and fault tree basic events is performed applying the approach outlined in Sections 2.1 through 2.4.

##### **2.5.12.2.1 Fractional Importance**

Internal flood QRVA element fractional importance determination and assessment is performed applying the approach outlined in Sections 2.1 through 2.4.



2.5.12.2.2 *Risk Achievement Worth*

Internal flood QRVA element risk achievement worth determination and assessment is performed applying the approach outlined in Sections 2.1 through 2.4.

2.5.12.2.3 *Risk Reduction Worth*

Internal flood QRVA element risk reduction worth determination and assessment is performed applying the approach outlined in Sections 2.1 through 2.4.

2.5.12.2.4 *Fussell-Vesely Importance (Risk Participation Index)*

Internal flood QRVA element Fussell-Vesely importance determination and assessment is performed applying the approach outlined in Sections 2.1 through 2.4.

2.5.12.2.5 *Birnbaum Importance (Risk Derivative)*

Internal flood QRVA element Birnbaum importance determination and assessment is performed applying the approach outlined in Sections 2.1 through 2.4.

2.5.12.3 *Risk Contribution Sensitivity Analysis*

Internal flood risk contribution sensitivity analysis is performed applying the approach outlined in Sections 2.1 through 2.4.

2.5.12.4 *Vulnerability Assessment Results Presentation and Interpretation*

Internal flood risk vulnerability assessment results presentation and interpretation is performed applying the approach outlined in Sections 2.1 through 2.4.

## 2.6 Internal Fire QRVA (FQRVA)

The general steps of an internal fire QRVA are similar to those for other internal events presented above in Sections 2.1 through 2.4; however, internal flooding, internal fire, and effectively all the external events QRVAs differ because the hazards, failure modes, and HFEs are location-dependent throughout the facility. Much of the information presented in this subsection is an adaptation of guidance provided in NUREG/CR-6850. A general flow chart for FQRVA tasks is presented in Figure 2-19.



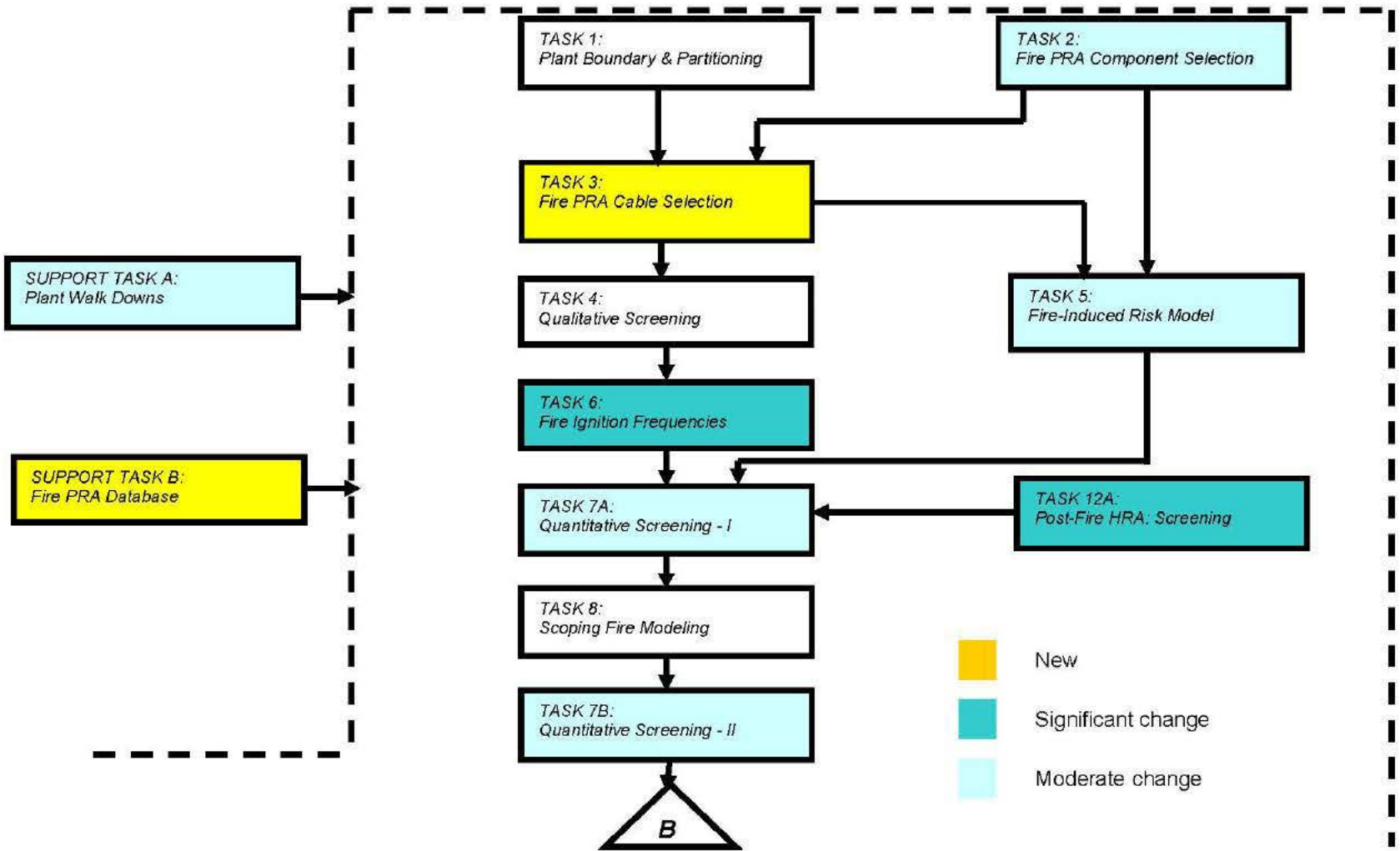


Figure 2-19. FQRVA Task Flow Chart







### **2.6.1 Internal Fire Events Scope Determination**

In internal fire QRVAs, it is important to identify all the fixed and transient fuel sources that could be involved in an internal fire scenario at the facility. Also within the scope determination is the task of selecting those areas or zones of the facility that are truly susceptible to fire risk. For example, areas within tanks or piping that normally contain liquid would generally not be considered as fire-susceptible. In general, fire-susceptible areas of a facility are those areas where operators may be expected to perform normal or emergency operator actions or any area that contains fire-susceptible equipment or components; e.g., electrical or electronic components or components potentially susceptible to failure or degradation from fire scenario-related gases, smoke, or soot.

### **2.6.2 Facility Walkdowns**

Facility walkdown is defined as an inspection of local areas where systems and components are physically located to ensure accuracy of procedures and drawings, equipment location, operating status, and environmental or system interaction effects on equipment during accident conditions. Facility walkdowns also supports facility partitioning under Task 1 by verifying credited partitioning features. It is critically important that several facility walkdowns be conducted as an integral part of fire QRVA. Paper and electronic documents are not sufficient to provide all the information needed for a proper fire QRVA. Subtle features of structural characteristics and equipment installations that may influence the outcome of a fire event are often not explicitly displayed on drawings or other documents. Housekeeping practices and various facility conditions can only be understood by on-site inspection. Also, often a wide range of paper documents need to be reviewed to select those that the analysts may need to use closely and retain as part of project documents. Such a selection process is often best conducted at the site where most up-to-date documents can be found.

Generally, several site walkdowns are conducted in support of a fire QRVA. The first walkdown is typically used for facility familiarization and identification of necessary facility documents. Later walkdowns are typically focused on specific topics. Even though the scope of the walkdowns may vary considerably, all walkdowns involve a common set of steps. In this section, those common steps are discussed first. The various walkdowns are discussed later and cross-referenced with the specific tasks of this fire risk quantification process. The types of analysts that should participate in a walkdown, duration, and schedule are also addressed.

All walkdowns are generally unique and the scope and agenda of a walkdown should be adjusted according to the specific needs of the analyst and the conditions of the facility. However, there are some common elements among the walkdowns that should enhance the efficient use of the analysts' and facility personnel time.

Even though it is obvious, it is important to stress that safe conduct and strict adherence to the safety and security rules of the facility supersedes all other needs and requirements of a walkdown.



All walkdowns consist of the following activities:

- Pre-visit planning and proper communication with facility staff and management to achieve the following:
  - Secure permission to enter the facility (if necessary) and visit various locations
  - Ensure that certain members of facility personnel are available
  - Develop a list of facility locations to be visited
  - Develop a list of documents to be reviewed
  - Develop the walkdown agenda
  - Prepare a list of items to be taken to the facility
- An entrance meeting with facility staff and management to discuss the following:
  - Walkdown objectives
  - Locations the team will visit to identify any relevant requirements pertaining to access, fuel containment, and security controls
  - Securing a convenient work area where the team can review documents and conduct meetings
  - Document retrieval, control, and other relevant topics
  - Work hours
  - Permission to use a camera
- Walkdown activities:
  - Visit planned facility locations and take necessary notes and photographs (if permitted)
  - Interview facility personnel knowledgeable of the topics on the agenda
  - Review facility documents
  - Consolidate and review the notes to ensure that all the necessary information has been collected
- An exit meeting with facility staff and management (if the management so desires) to summarize the objectives of the walkdown, what was done, what was achieved (including any problems encountered), and to identify and clarify additional action items, as appropriate.

The optimal makeup of the walkdown team will depend on the extent to which compartment characterization or other information is desired. In general, it is recommended that the walkdown team include someone knowledgeable of the facility's fire protection program and someone with knowledge of the facility operating and



support systems layout. Fire protection experts can provide enhanced information regarding potential fire sources, the fire barrier qualification status of credited partitions, and fire protection features. Facility systems/layout experts can assist in the identification of facility systems and components located in a given fire compartment. This knowledge will be needed as the analysis progresses. The initial confirmatory walkdown provides a convenient mechanism for gathering this information.

The walkdown team may use a standardized form to record its findings. Using such forms allows some level of standardizing the type of information collected by various analysts when working in parallel on the same task. It also creates a compendium of various key information items for each fire compartment<sup>##</sup> that can facilitate retrieval of specific information items when conducting the detailed fire scenario analysis. The standardized form may include the following topics for the analyst to address during the initial or later walkdown:

- Fire compartment identifier,
- Fire compartment name,
- Characteristics of the boundaries (i.e., fire walls, doors, etc.),
- Access points from other fire compartments and accessibility during power operation,
- Openings into adjacent fire compartments,
- Items typically present in the fire compartment,
- List of fire QRVA components (not including cables),
- Equipment count (per Task 6 instructions),
- Information regarding transient combustibles and transient ignition sources (e.g., possibility of conducting welding during power operation),
- Fire protection features (passive and active), and
- Other special features and characteristics relevant to fire risk analysis (e.g., addressing human performance factors under fire conditions).

The form may be updated every time a member of the analysis team visits the facility or a specific fire compartment.

---

<sup>##</sup> It is convenient to organize information by fire compartment. However, during the first walkdown, the team will need to verify the selection of fire compartments and their boundaries.



During the course of a fire QRVA, it is necessary to visit the facility and walkdown specific locations at different stages of the analysis. In general, the following walkdowns have been found to be necessary:

- An initial walkdown to confirm the definition of fire compartments and establish the characteristics of each fire compartment. In the context of partitioning, the primary walkdown objective is to confirm the existence and integrity of credited partitioning features and elements. The walkdown may also identify secondary partitions that can be credited to further partition an initially identified compartment. A second walkdown objective is to gather information on the dominant features of each compartment. Information of interest includes a description of the credited partitions that define each compartment, identification of (and/or counting of) primary fuel and ignition sources, cataloging of fire protection features (e.g., detection, suppression, raceway fire barriers, etc.), and the identification of adjacent compartments (above, below, and horizontal adjacencies). Such walkdowns can also support mapping of facility components, systems, and cables to and within fire compartments:
- To confirm the location of a specific cable.
- In support of fire frequency estimation process (Task 6), it is necessary to count all the relevant ignition sources within each fire compartment. This can only be completed by visiting each fire compartment and confirming the counts made using paper documents.
- The scoping fire modeling (Task 8) requires direct observations at each fire compartment to confirm that no potential targets are within the zone of influence of a fixed ignition source.
- To verify the detailed fire scenario analysis by direct observations at the affected fire compartments.
- To conduct human reliability analysis interviews with facility operators and direct observations of affected facility fire compartments.
- To verify seismic fire interaction.

### 2.6.3 FQRVA Database Development

A comprehensive fire QRVA project of this type requires an analysis of fire-induced circuit failures beyond that typically conducted during original fire QRVAs. Additional analytical tools are needed to support these refined electrical analyses. The tools of interest generally involve enhancements to an existing database system (e.g., facility cable and raceway system, Appendix R database, QRVA database, etc.) or development of a new database that is structured to support the desired functionality. The purposes of this task are to:

- Identify the database functional capabilities necessary to support a fire QRVA project as outlined in this guide, including analysis, screening, and correlation of data; and



- Establish a framework and process for assessing existing facility database features and functionality, and implementing an enhancement plan to develop the necessary database functional capabilities. A Database Augmentation Plan is developed to ensure enhancements are implemented through a formal and structured process.

The ultimate objective is to develop a relational database that can quickly and accurately assess potential equipment failures for fire scenarios of interest. Scenarios may include, but are not limited to, total failure of all circuits in a fire area or facility compartment, failure of cables within a specific raceway, and failures based on specific equipment failure modes.

#### **2.6.4 Internal Fire Facility Partitioning**

For the purposes of a fire QRVA, the facility is divided into a number of fire compartments. The analysis then considers the impact of fires in a given compartment, and fires that might impact multiple compartments. This procedure establishes the process for defining the global facility analysis boundary and partitioning of the facility into fire compartments. The product of this task will be a list of facility fire compartments in the facility under analysis.

The work package developed to support the facility-partitioning task should address the following issues:

- Basis for and identification of the limits of the selected global facility boundary,
- Basis for and results of partitioning the selected global facility boundary into fire compartments,
- Mapping of fire compartments to facility fire areas defined in regulatory compliance activities, and
- Documentation of the basic features of some or all fire compartments.

The objectives of the partitioning task are to (1) define the global facility analysis boundaries relevant to the fire QRVA, and (2) divide the facility into discrete physical analysis units (fire compartments). The fire compartments form the fundamental basis of the subsequent fire QRVA. That is, the fire QRVA will initially consider fire threats to safe shutdown primarily in the context of the defined fire compartments. The results of the fire QRVA will be presented in terms of the risk contribution for fires confined to a single compartment and for fires that impact multiple adjacent compartments.

A fire compartment is a well-defined enclosed room, not necessarily with fire barriers. Fire compartments generally fall within a fire area, and are bounded by non-combustible barriers where heat and products of combustion from a fire within the enclosure will be substantially confined. Boundaries of a fire compartment may have open equipment hatches, stairways, doorways or unsealed penetrations. The term fire compartment is defined specifically for fire risk analysis and maps facility fire areas and/or zones, defined by the facility and based on fire protection systems design and/or operations



considerations, into compartments defined by fire damage potential. For example, the control room complex or certain areas within the turbine building may be defined as a compartment.

The preceding discussion provides sample criteria for defining fire compartments when partitioning a facility for fire QRVA.

One of the most important effects of the facility partitioning process is in relation to the qualitative and quantitative screening tasks. Qualitative screening (Task 4) assesses each compartment, assuming that fires confined to that single compartment will fail all safe shutdown components and cables in the compartment. Similar assumptions are made in the first quantitative screen (Task 7), and again, compartments are screened as individual contributors. Multi-compartment scenarios are also explicitly screened and/or analyzed based on the compartment definitions, and in particular, postulating failure of the partitioning elements that define each compartment. Hence, the definition of fire compartments is critical to the analysis. It is important that fire compartments be defined in a reasonable manner that appropriately supports the fire QRVA.

The partitioning process involves two competing considerations that should be balanced by the analyst. Partitioning the facility into a greater number of compartments has potential advantages, in that each individual compartment may be easier to analyze as an individual risk contributor. This does, however, increase the burden for the analysis of multi-compartment fire scenarios. Defining a smaller number of larger compartments also has advantages in certain cases, particularly for areas that the analyst expects might screen during qualitative screening (Task 4) or during initial quantitative screening (Task 7).

Ideally, the combination of individual compartment analyses and multi-compartment analyses will reach the same final numerical estimates of the facility-wide fire risk, regardless of how the partitioning was performed. This will be accomplished since identification and analysis of multi-compartment fire scenarios will begin with all fire compartments that are screened, qualitatively or quantitatively. In practice, an ideal consistency may be difficult to achieve and/or demonstrate. Furthermore, the partitioning decisions impact the presentation and interpretation of the fire QRVA results in terms of single and multi-compartment fire scenario contributions. Excessive partitioning, beyond that recommended in Section 1.5.2 of NUREG/CR-6850, may appear to artificially dilute the contribution of a given room to fire risk, and should be avoided. When in doubt, retention of larger and more clearly delineated fire compartments is generally considered the more conservative approach.

The partitioning task assumes that a range of fire protection features will be effective at containing the damaging effects of a fire under most fire conditions. These features include fire-rated barriers, non-fire-rated barriers, active features, such as water curtains, and in some cases spatial separation. The potential failure of a credited partitioning feature is addressed in the multi-compartment fire scenario analysis task (see Task 11).

No input from other activities in the fire QRVA is necessary for the definition of the global facility boundary and partitioning of the facility into fire compartments.



In preparation for the partitioning task, the analyst should possess substantial knowledge of the facility layout, the characteristics of compartment boundary elements, and the general location of facility systems and equipment. For multiunit sites, a general knowledge of the extent to which systems, components, cables, and areas are shared between units is also needed.

Plan and elevation views of different buildings in the facility, as well as walkdowns, may be used to perform this task.

Confirmatory walkdowns will be necessary to complete the partitioning process, although these walkdowns may be deferred pending the identification of walkdown needs associated with other analysis tasks; e.g., fire ignition frequency analysis and fire modeling tasks. Step 3 of this task and Support Task A provide additional information about the recommended walkdown.

The list of fire compartments developed in this task is used throughout the balance of the fire QRVA. The partitioning decisions made in this task define the physical facility analysis units (the fire compartments)—that form the fundamental basis of the fire QRVA.

### **2.6.5 FQRVA Component Selection**

This section provides the procedure for creating the fire QRVA component list. This list serves as the basis for those components modeled in the fire QRVA, and it is the key source of information for which corresponding cables need to be identified and located for the fire QRVA. As such, the fire QRVA component list, fire QRVA model, and corresponding cable identification are iterated upon to ensure an appropriate correspondence among these three items. The product of this task is a list of the equipment to be included in the fire QRVA and for which corresponding cables need to be identified and located for the facility under analysis.

This procedure addresses creating the fire QRVA component list, which needs to span (a) equipment that, if affected by a fire, will cause an initiating event such that the appropriate fire-induced initiators can be defined; (b) all equipment necessary to support those mitigating functions and operator actions that are credited in the analysis in response to any initiator, as well as (c) that equipment which can be a source of undesirable responses adverse to safety during a fire-induced accident sequence, such as a component that can spuriously operate. The terms “equipment” or “components” as used in this procedure are considered synonymous and meant to include facility components such as valves, fans, pumps, etc.; structures; barriers; indicators; alarms; and other devices as appropriate. It is recommended that all the equipment credited in the internal events QRVA (especially equipment in electrically diverse systems) be included in the fire QRVA component list. More specifically, the scope of the fire QRVA component list should include the following major categories of equipment:

- Consideration of equipment whose fire-induced failure will cause an initiating event to be modeled in the fire QRVA model (in this case, the appropriate initiator for a compartment needs to be defined, not that the equipment itself has to be modeled);



- Equipment to support the success of mitigating safety functions credited in the fire QRVA, including equipment implicitly included in internal events QRVA recovery models;
- Equipment to support the success of operator actions credited in the fire QRVA;
- Equipment whose spurious actuation or other fire-induced failure modes could have an adverse effect on the success of the mitigating safety functions credited in the fire QRVA; and
- Equipment whose spurious operation or other fire-induced failure modes could likely induce inappropriate or otherwise unsafe actions by the facility operators during a fire damage sequence.

In many cases, the same equipment might be in several of the five major categories.

Similarly, a limited set of mitigating equipment, as well as instrumentation and diagnostic equipment such as indicators, lights, alarms, and similar devices considered necessary to support successful operator actions (e.g., such as carrying out the emergency operating procedures [EOP], following specific fire emergency procedures [FEP], or to credit certain recovery actions), or the failure of which could cause inappropriate operator actions, should also be added to the fire QRVA component list (more on this in Section 2.5.5 of NUREG/CR-6850). Examples could be remote shutdown panel (or areas) equipment and controls, pump room high temperature alarms, certain facility parameter indications with no or little redundancy in the indication, among others.

Because a key emphasis of the fire QRVA component list is to identify and track relevant cables in Task 3 that could be affected by fires in the facility, the list need not contain passive/mechanical equipment (i.e., non-electrical components) deemed by the analyst to be unaffected by fires. Such equipment may be manual valves, check valves, filters, heat exchangers, tanks, etc. (However, note that temperature, level, or other indications associated with this equipment may need to be on the list for operator action purposes). It is recommended that as part of this procedure, the analyst has identified those types of passive/mechanical equipment that do not need to be on the fire QRVA component list, even though the equipment may be in the fire QRVA model with regard to other mechanical failures, such as random plugging. The facility's existing fire analyses or the internal flooding QRVA will typically have a similar list of component types not considered affected by fires or flooding, and should be good starting points for creating a list of components not vulnerable to fire. In considering components that should not be affected by a fire, any potential damage to valve packing and other valve internals, filter materials, etc., should not be possible or at least not prevent the equipment's operation, should it be necessary. As part of identifying whether non-electrical equipment is or is not vulnerable to fire effects, the analyst should also be sensitive to identifying such situations as instrument air piping/tubing that is copper or has soldered joints that may fail under high heat conditions and thus fail the instrument air function. In such cases, the QRVA model needs to reflect these possible non-electrical equipment failures for applicable compartment fires.



This task's primary purpose is to determine that equipment for which cable identification and location is necessary. This is needed in order to identify what equipment fires in various locations may affect. A fall-out of creating the fire QRVA component list is determining the majority of the equipment scope in the fire QRVA model subject to that equipment which is screened out in subsequent tasks or does not need cabling information.

In order to arrive at the fire QRVA component list, the two most significant inputs available are used to start creating such a list; the internal events QRVA (with knowledge of any unique aspects from any existing fire QRVA) and the fire safe shutdown analysis (e.g., called Appendix R of 10 CFR Part 50 Analysis at some facilities). Together, these two inputs provide much of what is needed for the fire QRVA. However, because these two analyses were performed for different purposes, this procedure calls for a reconciliation to make sure the differences are appropriately considered. Steps 1 and 2 of this procedure address the analysis activities to start the fire QRVA component list from the internal events QRVA and how to perform the reconciliation between the internal events QRVA and the fire safe shutdown analysis. Where options are available to the analyst in carrying out these steps, those options and corresponding considerations are offered.

Steps 3 through 6 address how to build on the product of Steps 1 and 2 and more completely identify the equipment of interest. As in the earlier steps, where options are available to the analyst in carrying out each step, they are noted and briefly discussed.

All the options can be generally considered as tradeoffs between the level of accuracy and completeness of the fire QRVA versus the resources needed to achieve that level. The latter steps in the procedure are largely additions to the fire QRVA component list from Steps 1 and 2 to make the list more complete and to ensure no potentially important equipment has been missed. For instance, Steps 4 and 5 address the potential for spurious equipment operation or malfunctions that could affect system performance and/or operator performance during the response to a fire. Such spurious operations are usually too improbable for consideration in the internal events QRVA, but in the case of a fire, multiple spurious equipment operations or malfunctions may be somewhat likely and cannot easily be dismissed. Step 6 addresses the special subject of equipment whose failure may cause "potentially high-consequence" events to ensure this equipment is included in the list.

Finally, Step 7 covers the documentation of the fire QRVA component list.

The following key assumptions underlie the use of this procedure.

- A good, quality internal events QRVA and fire safe shutdown analysis are available.
- The analysts, collectively, have considerable knowledge and understanding of the facility systems and operator performance, as well as the internal events QRVA and the Fire Safe Shutdown Analysis, and/or have access to other staff that can provide such input.



- The scope and number of spurious equipment operations or malfunctions of concern can easily grow to proportions that are unreasonable to address without unlimited resources. An approach for addressing this subject is found under Steps 4 and 5, with additional considerations provided in Appendix A of NUREG/CR-6850. In carrying out those steps, it is assumed the analysts will:
  - As a minimum –
    - (a) identify cases where the spurious actuation or mal-operation of any single component within each system would affect a safe shutdown function (e.g., spurious actuation of a valve in the auxiliary feedwater (AFW) system which creates a flow diversion path in AFW), and
    - (b) identify cases where a single indicator/alarm associated with a particular operator action of interest would cause an undesirable operator action (e.g., a spuriously operating high-temperature pump motor alarm leading to the operator shutting down the pump);
  - And then as resources allow –

expand the above search within each system or for operator actions of interest to simultaneous “doubles,” “triples,” or even more combinations of spurious operations or failures; e.g., multiple valves, multiple indicators. However, as a practical matter, going beyond “triples” or even “doubles” may prove unwieldy and of little value considering the reasonably low likelihood of three or more affected devices at the same time. For instance, there may be reasons that the likelihood of spurious operation of a component(s) can easily be judged to be low and thus not worthy of consideration; e.g., by looking ahead and implementing criteria in Steps 4 and 5 that address ways to limit the number of coinciding spurious events to be considered.

It is not expected that these searches will cross system boundaries (e.g., a spurious operation of a high pressure injection isolation valve with a spurious operation of an AFW valve) or involve multiple operator activities. Keeping within this framework is analogous to the current state-of-the-art for treating common cause failures in internal events QRVAs (identified within each system boundary), and thus is considered appropriate for the fire QRVA. This is not to say that the procedure specifically precludes examinations across systems or activities. In fact, if the analysts are aware of known vulnerabilities that cross system or activity boundaries or can easily examine for such simultaneous failures, their inclusion is encouraged. Note that when these individual failures are included in the fire QRVA model and the model is “solved” for combinations of events that cause loss of fuel inventory control or a large fuel release, combinations of spurious events across systems will automatically be identified. These can be dealt with during the quantitative screening (Task 7) and subsequent analysis tasks as appropriate.

Given that the initial development of the fire QRVA component list will largely come from the existing internal events QRVA and any existing fire safe shutdown analysis, this task only needs initial assistance from those analysts performing Task 12, Post-Fire Human



Reliability Analysis, to define operator actions and hence related equipment (e.g., specific indicators) of potential significance when carrying out Step 4. However, it is also assumed that two prerequisites have been satisfied. The first is the facility boundary definitions and compartment designations from Task 1, Facility Boundary Definition and Partitioning, so that the fire QRVA component list can include associated location information about each equipment item as well as be useful in defining initiating events for each compartment in Step 3 of this procedure. The second assumed prerequisite, related to Support Task B, Fire QRVA Database System, is that the information needed about each component has been agreed upon and is therefore compatible with the expected input for that database.

The initial development of the fire QRVA component list should be as complete as possible. However, as is the iterative nature of QRVA, the fire QRVA component list may need to be modified by products of other tasks in the fire QRVA process. For example, if Task 12, Post-Fire Human Reliability Analysis, develops new fire-related actions to consider in the analysis, the fire QRVA component list might have to include new instruments that uniquely support these additional actions (with subsequent cable identification, etc.). In some cases, the analysts may decide that it is more efficient to perform portions of other tasks to demonstrate that certain equipment items do not have to be included on the list; e.g., demonstrating that a valve cannot spuriously fail/operate in an undesirable state. While this latter approach should be followed with care since it tends to disrupt the logical flow of first including any potentially important equipment and then finding reasons to later screen items from the analysis, there may be times when the resource tradeoffs may make this the best course of action. Thus, the analysts should be open to adjusting the fire QRVA component list as other task products affect the scope of the fire QRVA model, whether the other tasks are performed after Task 2 (the normal flow expected in carrying out the process) or before or in conjunction with Task 2.

This procedure assumes the availability and use of the following to support the creation of the fire QRVA component list.

- Internal events QRVA (with use of any existing fire QRVA models, insights, etc.),
- Fire safe shutdown analysis,
- Facility piping and instrument diagrams (P&ID) and electrical diagrams,
- Facility procedures (e.g., emergency operating procedures, fire procedures, annunciator response procedures),
- Technical specifications to determine possible limiting conditions of operation requiring forced shutdown of the facility (see Step 3), and
- Other facility drawings and documents, as necessary.



Analysts' knowledge of facility system operation, potential failure modes of equipment, and potential operator responses related to possible conditions of equipment or instrumentation will enhance the use of this procedure and make it more efficient.

Most likely, existing documentation will be adequate to provide all the necessary information produced for the fire QRVA component list as described in Step 5. Thus, walkdowns will generally not be necessary for this task. However, especially for equipment location information, there may be times when a walkdown is needed to determine or verify certain information. In such cases, this need for a walkdown should be planned so as to coincide with other task walkdown needs for efficiency reasons. See Support Task A, Facility Walkdowns.

The primary product of this procedure, the fire QRVA component list, is used to support Fire QRVA Cable Selection (Task 3), to provide the necessary inputs about each equipment item into the Fire QRVA Database System (Support Task B), and to provide a basis for much of what is modeled in the Fire-Induced Risk Model (Task 5), as modified by subsequent screening and other tasks).

### 2.6.6 FQRVA Cable Selection

Conducting a fire QRVA in accordance with this procedure necessitates an analysis of fire-induced circuit failures beyond that typically conducted during original fire QRVAs. The circuit analysis elements of the project are conducted in three distinct phases:

- Fire QRVA cable selection (Task 3),
- Detailed circuit failure analysis (Task 9), and
- Circuit failure mode likelihood analysis (Task 10).

This section provides methods and instructions for conducting the first phase of circuit analysis—selecting fire QRVA cables (Task 3). The purpose of Task 3 is to identify for all fire QRVA components the circuits/cables<sup>§§§</sup> associated with the components and the routing/facility location of the identified circuits/cables. These relationships can then be used to determine the fire QRVA components potentially affected by postulated fires at different facility locations.

In most cases, it is advantageous to perform some or all of Task 9 (detailed circuit failure analysis) coincident with Task 3. The degree to which Task 3 and Task 9 are combined is highly dependent on numerous facility-specific factors. Considerations for combining the two tasks are incorporated in relevant sections of Chapter 3 of NUREG/CR-6850.

---

<sup>§§§</sup> The term “circuit” and “cable” are often used interchangeably for fire-related circuit analyses. A circuit is comprised of electrical components, subcomponents, and cables/connection wire. Within the context of fire-induced equipment failures, it is understood that circuit selection or circuit identification refers to the identification of cables that connect all the related components and subcomponents of a complete circuit.



Chapter 3 of NUREG/CR-6850 provides methods and technical considerations for identifying cables to be included in the fire QRVA cable list. This task contains the following key elements:

- Identify cables associated with fire QRVA equipment,
- Determine facility routing and location for the fire QRVA cables,
- Identify fire QRVA power supplies, and
- Correlate fire QRVA cables to fire QRVA equipment and facility locations (fire compartments and/or fire areas).

Implementation of facility-specific quality assurance and configuration control requirements that might apply to a fire QRVA is not within the scope of this task. Nor does this task address validating the accuracy of facility-specific data extracted from facility drawings, documents, or databases. Each facility should follow appropriate quality assurance, administrative, and configuration control procedures applicable to the work conducted. The need to validate input source documents should be addressed as part of assembling the prerequisite information.

The fire QRVA cable list identifies the circuits/cables needed to support proper operation of equipment contained in the fire QRVA equipment list. Essential electrical power supplies are also identified during this task. The fire QRVA cable list might also include associated circuits. Associated circuits are cables that are not necessarily directly linked to a component, but have the potential to cause improper operation of a component as a result of certain failure modes associated with fire-induced cable damage.

The fire QRVA cable list is not simply a list of cables. It also establishes, for each cable, a link to the associated fire QRVA component and to the cable's routing and location. These relationships provide the basis for identifying potential equipment functional failures at a fire area, fire compartment, or raceway level.

Task 3 is broken down into six distinct steps. Generic step-by-step instructions for completing these steps are provided in this chapter. Figure 2-20 shows a summary of the task work flow.



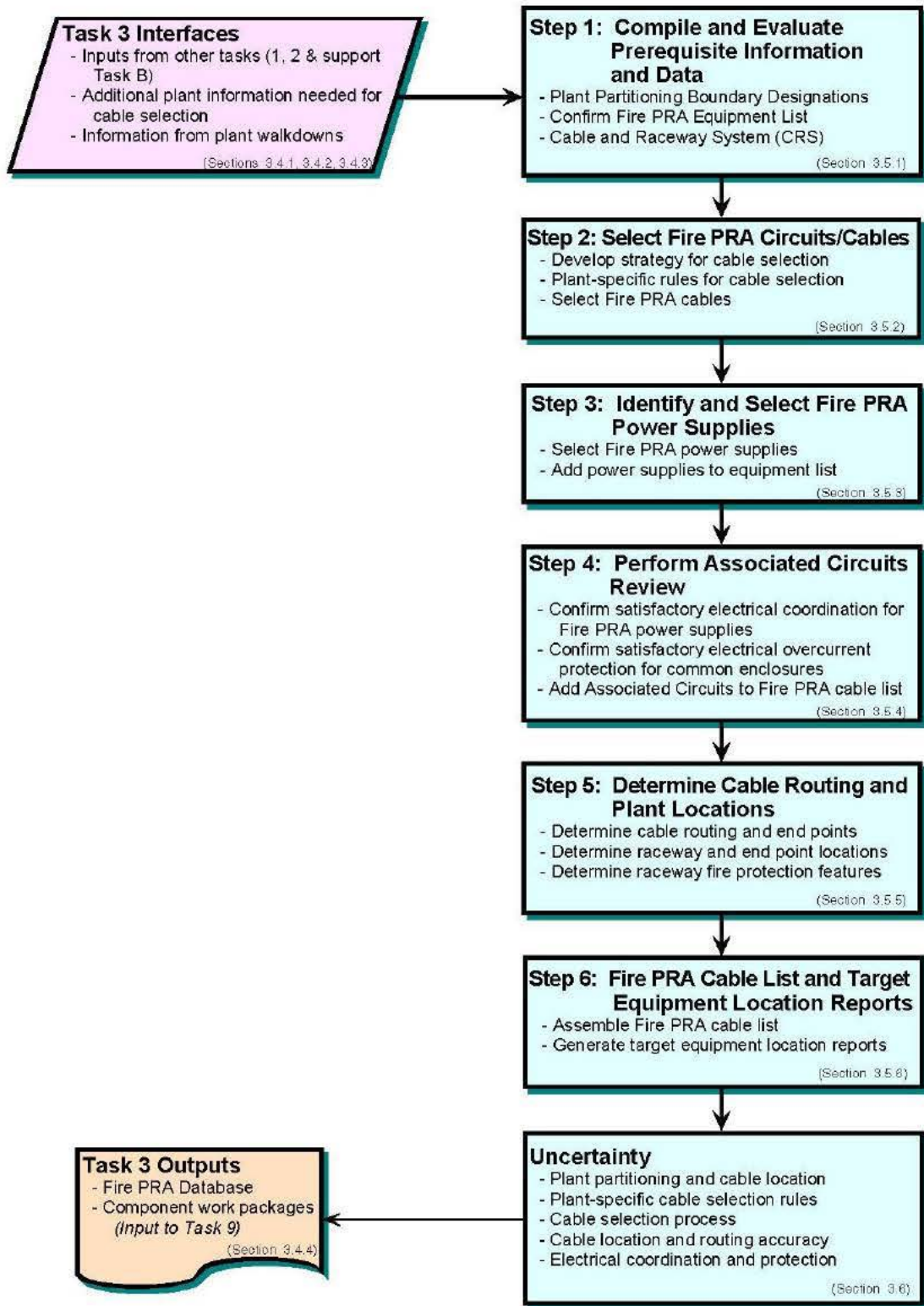


Figure 2-20. Fire QRVA Cable Selection Process



A critical aspect of creating the fire QRVA cable list is preplanning. Experience shows the importance of developing a clear strategy and detailed facility-specific rules for selecting cables. This is true whether cable selection is based on existing analyses (e.g., post-fire safe shutdown analysis, original fire QRVA, etc.) or will be generated from scratch. Also of key importance is assessing up front the degree to which cable and raceway data has been automated and the cables have been correlated against facility locations. The key question is whether or not the existing data allows for easy database retrieval of cable routing and location information. This capability is essential for efficiently conducting a fire QRVA using the methods of this procedure. Facilities without this capability should include in the project resource estimate a realistic projection of the level-of-effort necessary to acquire the desired database sort and query capability, which can be substantial, depending on the actual information available.

The following assumptions form a basis for this task:

- A cable and raceway database system (CRS) is in place and available to identify cable routing and location. The analysis methods presented in this document assume some degree of automated cable-to-location sort and query capability. The ultimate usefulness of the database to support this task will vary depending on the inherent functionality of the database;
- An Appendix R of 10 CFR Part 50 analysis (herein after referred to simply as Appendix R analysis) for the facility has been completed and documented, and is available for helping identify cables associated with fire QRVA equipment. The degree of applicability will vary depending on the facility-specific approach used for the Appendix R circuit analysis;
- Equipment is assumed to be in its normal expected position or condition at the onset of the fire. In cases where the status of a component is indeterminate or could change as a result of expected facility conditions, worst-case initial conditions should be assumed for the purpose of cable selection;
- Properly sized and coordinated electrical protective devices are assumed to function in accordance with their design tripping characteristics, thereby preventing initiation of secondary fires through circuit faults created by the initiating fire; and
- Users of this procedure are knowledgeable in the theory and principles of electrical power and control circuits, and have practical experience with facility circuit schemes, power distribution systems, and cable and raceway routing systems. Work under this procedure is assumed to be conducted by or supervised by personnel familiar with circuit failure analysis methods; i.e., Appendix R safe shutdown analysis or similar.

This task needs, as a prerequisite, the facility partitioning boundary definitions and fire compartment designations from Task 1, Facility Boundary Definition and Partitioning. This information is used to correlate cable routing to specific facility locations. As a minimum, cables should correlate to facility fire areas. Ideally, the cables will correlate to the established fire compartments.



This task needs, as a prerequisite, the list of fire QRVA equipment from Task 2, Fire QRVA Components Selection. The fire QRVA equipment list serves as the starting point for cable selection. The primary objective of Task 3 is to identify circuits/cables associated with the fire QRVA components for the purpose of identifying potential equipment failures on a compartment and fire scenario basis.

The fire QRVA database system (or equivalent database system) is a prerequisite for this task. The database system provides a structured framework for capturing and maintaining fire QRVA data. The database system is populated with the data and information generated by this task, which is then compiled to generate the fire QRVA cable list and accompanying relationships. The data structure and functional relationships established within the database system are specifically designed to maintain data integrity and provide the necessary sort and query capability to conduct compartment and scenario conditional loss of fuel inventory control probability (CLOFICP) and conditional acute fuel release probability (CAFRP) calculations.

This task needs basic cable routing and cable location information from the facility CRS or other sources, as applicable. The availability of readily retrievable cable routing and cable location data will significantly impact the analysis strategy and level of effort needed to complete this task. Manually determining cable routing and locations from facility drawings and/or walkdowns is extremely resource intensive. Facilities that do not have cable routing and location data in an automated database format should, in the planning stage, carefully consider the additional resources needed to obtain this capability. The analysis methods presented in this document assume some degree of automated cable-to-location database sort and query capability. The ultimate effectiveness of the CRS to support the fire QRVA is directly related to the resolution of cable location information; i.e., a CRS that can readily correlate a cable to a specific raceway and facility compartment is more useful than a CRS that can only correlate a cable to fire areas (lower resolution).

Other information required includes:

1. Component Elementary Circuit Diagrams
2. Component Cable Block Diagrams
3. Component Wiring/Connection Diagrams
4. Electrical Distribution System Single-Line Diagrams
5. System Piping and Instrument Diagrams
6. Instrument Loop Diagrams and Block Diagrams
7. Cable Raceway Schedules and routing Drawings
8. Equipment Location and Layout Drawings
9. Electrical Distribution System Protective Device Coordination Studies/Calculations
10. Electrical Distribution System Short Circuit and Equipment Rating Studies

Facility walkdowns are not considered a fundamental part of this task. Rather, facility walkdowns should be considered on a case-by-case basis as a way of obtaining necessary information about cable and/or raceway locations.



The specific products generated by this task are:

- Fire QRVA cable list (input into the fire QRVA database),
- Fire QRVA power supply list (input into the fire QRVA database),
- Associated circuits review, and
- Component analysis work packages (optional).

Developing the fire QRVA cable list is an essential prerequisite for conducting both qualitative and quantitative screening. The cable list, as input into the fire QRVA database, provides the functional and spatial relationships that allow potential equipment failures to be identified on a compartment- and fire-scenario level.

Using the fire QRVA database (which has been populated with the fire QRVA equipment list and fire QRVA cable list), target equipment location reports can be produced for use in compartment-level and scenario-level quantitative screening activities (Task 7). Additionally, Task 3 identifies any essential electrical power supplies not previously identified in Task 2. It is highly recommended that component analysis work packages be generated as part of this task. The electrical analysis work packages are useful later during detailed circuit failure analysis (Task 9) and circuit failure mode likelihood analysis (Task 10).

#### **2.6.7 Internal Fire-Induced Initiating Event Analysis**

Initiating event analysis for fire scenarios follows the general methodology outlined in Sections 2.1 through 2.4. For details on specific fire frequency determination, please refer to Section 2.6.12.1.

#### **2.6.8 Internal Fire Scenario Development**

This section describes the procedure for developing the fire QRVA model to calculate LOFICF, CLOFICP, acute fuel release frequency (AFRF), and CAFRP for fire events. The procedure addresses the process of implementing temporary or permanent changes to the internal events QRVA to quantify fire-induced LOFICF, CLOFICP, AFRF, and CAFRP, and for developing special models to address FEPs. The procedure also addresses the transition from temporary changes to permanent changes to the internal events QRVA model during the development of the fire QRVA model.

This procedure addresses the following major steps for developing the fire QRVA model for calculating LOFICF/CLOFICP and AFRF/CAFRP for fire events.

- Step 1 – Develop the Fire QRVA LOFICF/CLOFICP Model
- Step 2 – Develop the Fire QRVA AFRF/CAFRP Model

The primary objective of this task is to provide an approach that allows the user to configure or modify the internal events QRVA model to quantify fire-induced LOFICF, AFRF, CLOFICP, and CAFRP. There are at least two different QRVA modeling approaches that have evolved in the QRVA field. These two models, in the evolution of QRVA methodology development efforts have come to be known as the “Fault Tree



Linking Approach” and “Event Trees with Boundaries Approach”. There is a number of different QRVA software products available in the industry market designed around these two approaches. The approach described in this procedure is based on standard state-of-the-art QRVA practices, and is intended to be applicable for any QRVA methodology or software product.

This procedure allows the user to quantify LOFICF and AFRF or CLOFICP and CAFRP. The only difference is that the quantified values of the fire scenario frequencies are used for LOFICF and AFRF calculations, while the fire scenario frequencies are set to 1.0 or TRUE<sup>\*\*\*</sup> for CLOFICP and CAFRP calculations.

Most internal events QRVA models are based on the premise that the operators will enter the EOPs. Consequently, the facility response and the operator responses modeled in the QRVA are based on the EOPs. For some facilities, a fire may drive the operators to FEPs that significantly deviate from the EOPs. In some cases, unprotected trains of mitigation systems (i.e., trains not credited in the fire safe shutdown analysis) may be placed out of service to preclude the adverse effects of fire-induced spurious actuations. For these cases, the internal events QRVA model may not be appropriate and special models may have to be developed. For other facilities, the FEPs may not significantly deviate from the EOPs, or the EOPs take precedence over the FEPs. For these cases, the internal events QRVA may be acceptable. The QRVA and HRA analysts should review the EOPs and the FEPs and determine whether a special model for the FEPs is needed.

At many facilities, a combination of approaches is used. For fires that do not necessitate control room evacuation, the EOPs are often used (and thus the internal events QRVA is useable). Even in this case, some fire-specific actions may be taken as the result of the simultaneous use of other fire-specific procedures. For fires that result in control room evacuation (i.e., alternative shutdown), the operators are directed to exit the EOPs and enter the FEPs. Therefore, a dedicated model is often needed. In all cases, unique manual actions may need to be addressed and particularly for control room evacuation cases as well as ex-control room local actions, other equipment including instrumentation not typically addressed in the internal events QRVA may also need to be added to the fire QRVA model (see Task 2 about identifying equipment to be added to the component list and Task 12 about identifying new fire-related human actions).

This procedure assumes that the user is familiar with the QRVA methodology and software employed at the facility. The user should also be familiar with the procedures for quantifying the QRVA model. This procedure assumes that the internal events QRVA has sufficient fidelity to automatically propagate component-level failures through the system and sequence logic models using the QRVA software.

---

<sup>\*\*\*</sup> Care should be taken when configuring the model as to which basic events fail (i.e., failure mode or event set to TRUE or 1.0 failure probability) as a result of the fire. The correct setting (TRUE or 1.0) may need to correspond to the timing of the failure mode (or event) relative to other possible failure modes or events, and/or whether the occurrence of the failure mode or event precludes the other failure modes/events.



This task uses the internal events QRVA sequences and fire-induced initiating event information from Task 2, Fire QRVA Components Selection, a list of unscreened fire compartments from Task 4, Qualitative Screening, the QRVA equipment to be modeled from Task 2 as reflected in the Fire QRVA Database developed in Support Task B, Fire QRVA Database System, and a list of HRA events developed in Task 12, Post-Fire Human Reliability Analysis. Note that in order for the Fire QRVA modeling process to be complete, the model needs to reflect the locations of the cables that will be recorded in the database from Support Task B (information supplied from the Task 3 cable selection process) so that the cable targets are associated with the appropriate compartments when analyzing fires in each compartment. There will be some iteration particularly on the QRVA equipment and HRA events addressed in the fire QRVA model due to more detailed analyses in other tasks as the analysis evolves.

The internal events QRVA model for the facility is needed to support this task. The user should also have access to the software tools necessary to quantify the QRVA model. The EOPs and FEPs and other fire procedures, as necessary, should be accessible to the user.

No walkdown is needed to support this task.

This task provides the steps to configure the internal events QRVA model into becoming the fire QRVA model, and support the quantitative screening task (Task 7) that, along with other task products eventually yields the final loss of fuel inventory control and large fuel release estimates from postulated fire events.

### **2.6.9 Internal Fire Human Reliability Analysis**

FQRVA HRA applies the same general approach outlined for HRA in Sections 2.1 through 2.4; however, the PSFs for specific HFES need to be re-evaluated for the fire scenarios. Additionally, new HFES may be defined for fire scenarios to incorporate human actions to suppress or mitigate fire severity and propagation.

This document describes the procedure for evaluating the impact of fire scenarios on the human actions addressed in the base QRVA study (i.e., the internal events QRVA or original fire individual plant examination of external events [IPEEE] analysis) used to create the fire QRVA model, as well as how to identify and quantify new actions to be performed as part of the facility fire mitigation plans and procedures. Evaluating the reliability for these human actions supports the fire QRVA Model for calculating such metrics as LOFICF, CLOFICP, AFRF, and CAFRP for fire-induced initiating events. The initial quantification of these metrics makes use of screening probabilities for HFES where appropriate. As necessary, more detailed best estimate analyses of some human actions will be needed to obtain more realistic assessments of fire risk.

Task 12 addresses a process for performing both screening and detailed analysis of post-fire human actions identified in accident sequences initiated by a fire. The main focus is to foster the process for assessing the impact of location-specific fires on the human actions taken in response to a fire-induced initiating event, thus preventing loss of fuel inventory control and mitigating releases. This task procedure covers three essential elements of most HRA studies.



- Identification of the HFEs to be included in the fire QRVA.
- The assignment of screening human error probabilities for the identified HFEs to assist in focusing the modeling and fire risk analysis to those scenarios and human actions most important to the overall risk results.
- Considerations for the detailed best-estimate quantification of the more important HFEs to properly consider the fire effects on human performance.

In covering the above scope, it is important to stress that this procedure focuses on those unique fire considerations that need to be included in performing a HRA for the fire QRVA using whatever method (e.g., Accident Sequence Evaluation Program [Reference 55], etc.) is chosen by the analyst. It is therefore equally important to stress what this procedure does not do. This procedure is not a handbook or a similar stand-alone manual for doing a fire HRA, in that it does not attempt to duplicate all the typical activities in carrying out a HRA like that specified by the American Society of Mechanical Engineers (ASME) Standard ASME RA-S-2002 (Reference 56). Nor does this procedure attempt to provide a new or particularly prescriptive method for assessing the HEPs in a fire QRVA, since introducing such a method would be a research project far beyond the intended boundaries and resources for producing these fire procedures. Use of this procedure and the unique fire-related considerations that it covers is expected to be used in concert with already-available HRA techniques and calculation tools by an experienced HRA analyst(s) to perform a defensible and realistic HRA for a fire QRVA.

Notably, the scope of this procedure does not include pre-initiator human failure events specifically related to fire systems, barriers, or programs. Undetected pre-initiator human failures such as improperly restoring fire suppression equipment after test, compromising a fire barrier, or incorrectly storing a transient combustible can all affect the fire risk. Tasks 6, 8, and 11 make use of industry-wide data that within it contains contributions from such human failures. Hence to that extent, these pre-initiator failures are treated within the fire QRVA. Nevertheless, no specific steps are provided here for performing a facility-specific review of the potential for such human failures and thus influencing the use of the industry-wide data. This does not preclude the expectation that pre-initiator human failure events from the internal events QRVA (i.e., not specifically related to fires) should remain in the fire QRVA Model covering their contribution to component unavailability for safe shutdown systems within the QRVA model structure.

This task's primary purpose is to provide a process on how to include and quantify events representing human failures in the development and quantification of the fire QRVA model.

In this task, the internal events HFEs are addressed to incorporate fire location scenario-induced changes in assumptions, modeling structure, and PSFs. In addition, modifications to the models are made to address special actions to maintain acceptable facility configurations and safe shutdown given a fire in specific locations and the need to use procedures that are not modeled in the internal events QRVA.



The procedure for implementing this task is based on three major steps typical of most HRAs:

1. Identifying the human actions and resulting HFEs to include in the fire QRVA, which necessitates the potential modification of existing internal events QRVA HFEs, as well as adding new HFEs related specifically to fire scenarios.
2. Assigning screening HEPs as an aid in simplifying the fire QRVA model and focusing analysis resources on those fire scenarios and associated equipment failures and operator actions most significant to the overall fire risk.
3. Providing detailed best estimate quantification of the more significant HEPs to overall fire risk.

In addition, documenting the HRA is briefly addressed.

The work performed under this procedure inherently assumes the following.

1. In general, a fire anywhere in the facility introduces new accident contextual factors and potential dependencies among the human actions beyond those typically treated in the internal events QRVA that increase (mildly or significantly) the potential for unsafe actions during an accident sequence. These will be addressed in the procedure and include, for instance, potential adverse environments (e.g., heat, smoke), possible accessibility and operability issues, use of fire procedures, potential spurious events associated with both diagnostic and mitigating equipment, and increased demands on staffing and their workload, among others.
2. For all fires modeled in the fire QRVA, the crew is aware of:
  - a. the fire location within a short time (i.e., within the first ~10 minutes of a significant indication of non-normal conditions such as fire alarms, multiple equipment alarms, an automatic trip, etc.),
  - b. the need for a facility trip (if it has not happened automatically),
  - c. the need to implement a fire brigade, and
  - d. the potential for unusual facility behavior as a result of the fire.
3. Even if one or more main control room (MCR) persons are used to assist in ex-control room activities such as aiding the fire brigade, the minimum allowable number of operators remains available in the MCR to manage the safe shutdown of the facility, and the crew makeup is similar to that assumed in the internal events QRVA.

This task provides input to and uses results from many of the other tasks in the fire analysis process. Many of these interactions will be iterative in nature; each iteration



provides insights that will improve the implementation of this and the other tasks. In particular:

- Task 2, Fire QRVA Component Selection, will identify scenario mitigating equipment and diagnostic indications of particular relevance to human actions modeled in the fire QRVA, and this task (Task 12) will identify human actions to include in the model that, in turn, may imply other equipment and indications that need to be added as part of Task 2. Note that these equipment and indications will involve (1) that needed for potential success of actions that are needed per the EOPs, FEPs, or similar fire response instructions, and (2) that whose failure (including spurious events) in a fire can either induce operators to isolate or reposition critical equipment into a less desirable position or add to the crew's workload and potential confusion.
- Task 5, Fire-Induced Risk Model, will provide human actions already in the internal events QRVA for consideration of further treatment, per this task, in the fire QRVA. This task (Task 12) will, in turn, identify new actions to be added to the fire QRVA model (Task 5) because of the implementation of FEPs or other fire response instructions.<sup>†††</sup>
- Task 12 will provide screening HEPs that can be used in performing the quantitative screening per Task 7, Quantitative Screening. Task 7 will provide feedback to Task 12 (based on the accident sequences or cut sets and accompanying CLOFICPs and other results from running the fire QRVA model) as to those HFEs needing a more detailed best estimate analysis to obtain more realistic LOFICFs, etc.
- Knowledge from Tasks 3 (Fire QRVA Cable Selection), 9 (Detailed Circuit Failure Analysis), and 10 (Circuit Failure Mode Likelihood Analysis) associated with cable and circuit analyses will prove useful in determining the potential for equipment failures, as well as spurious operations and indications that the operators may face in various fires. This information will establish which screening HEPs can be used as well as the best-estimate quantification of the more important HEPs. As part of the iterative nature of QRVA, in some cases, it will be desirable to perform some of the more detailed tasks (i.e., Tasks 9 and 10) as input to Task 12 so as to establish the best screening HEPs to carry out Task 7 most efficiently.
- Knowledge from Task 8, Scoping Fire Modeling, and Task 11, Detailed Fire Modeling, will prove useful in determining aspects important to deciding what screening HEPs can be used, as well as the best-estimate quantification of the more important HEPs. For example, the potential for adverse environments and timing information relative to equipment damage comes from insights from these two tasks. As part of the iterative nature of QRVA, in some cases, it will be desirable to perform

<sup>†††</sup> This can be accomplished through interactions between the HRA analyst and the QRVA/systems analysts after studying special fire procedures needed for a location-scenario.



portions of Tasks 8 or 11 as input to Task 12 so as to establish the best screening HEPs to carry out Task 7 most efficiently.

- Ultimately, the final products of Task 12, including the HFEs to be modeled, some screening HEPs, and best-estimate quantification of certain HEPs, are inputs into the final risk quantification performed under Task 14, Fire Risk Quantification.

The following will be useful in performing this task.

1. Facility Procedures (EOPs, alarm response procedures, fire procedures, etc.),
2. Facility training documents and related information (particularly fire-related),
3. Fire QRVA database,
4. Internal events QRVA model and adjustments thereto per other tasks,
5. Facility P&IDs and electrical diagrams as may be necessary to identify the system impacts of human action successes and failures,
6. Other facility drawings and documents, as necessary to resolve location, accessibility, and other issues, and
7. ASME Standard for Probabilistic Risk Assessment (PRA) for Nuclear Power Plant Applications (ASME RA-S-2002) (Reference 56).

Existing documentation will be adequate to perform most of this procedure. However, there may be times when a walkdown is needed to determine or verify certain information relevant to the modeled human actions, such as when addressing the performance-shaping factors like the environmental conditions, the conditions of the man-machine interface and equipment layout, etc. In such cases, this need for a walkdown should be planned to coincide with other task walkdowns for efficiency reasons. See Support Task A, Facility Walkdowns.

Information from Task 12 is used in the following ways:

- As noted above, Task 12 provides information needed in Tasks 2, 5, and 7, as well as final inputs for Task 14.
- Uncertainty information to be propagated or otherwise addressed as part of Task 15, Uncertainty and Sensitivity Analysis, comes from Task 12.
- Elements of the documentation task (Task 16 – Fire QRVA Documentation) will include the assumptions, judgments, analyses, and results from Task 12.

### 2.6.10 Internal Fire Accident Sequence Analysis

FQRVA accident sequence analysis applies the same general approach as outlined in Sections 2.1 through 2.4; however, scenario impact and propagation are now dependent



upon specific aspects of the fire modeling and other detailed FQRVA tasks outlined in the remainder of Section 2.6.

### **2.6.11 FQRVA Qualitative Screening**

This procedure describes the criteria for qualitatively screening the fire compartments defined in Task 1.

This work package addresses the following issues in qualitative screening:

- Definition of screening criteria and basis, including definition of facility trip initiator and controlled manual shutdown;
- Reference to fire QRVA component list used in qualitative screening and criteria for equipment selection.

In most fire IPEEE analyses, the primary containment was qualitatively screened. In this methodology description, the examination of potential risk associated with fires in primary containment will follow steps similar to other locations of the facility.

From Task 1, Facility Partitioning, a set of fire compartments is identified for the fire QRVA. These compartments are subjected to a series of screening analyses that will determine the relative fire risk associated to each. Qualitative screening is the first of such screening analyses. It is not intended to assign risk values to particular fire compartments. It is intended, however, to identify those fire compartments where, according to pre-determined criteria, the fire risk is expected to be relatively low or nonexistent compared to others.

This task assumes that the risk (i.e., LOFICF and/or AFRF) associated with the fire scenarios where a controlled manual facility shutdown may be attempted as a precautionary measure and no other fire QRVA components are affected is low.

This task needs input from the following tasks:

- Task 1: The list of fire compartments in the facility resulting from the partitioning analysis, and
- Tasks 2 and 3: Equipment and cables selected for the fire QRVA.

No additional facility information is needed in support of this task.

A formal walkdown is not necessary to complete this task. A walkdown, however, may be appropriate if the analyst needs to confirm information described in facility documents and drawings.



The results of this task, unscreened fire compartments, are used in:

- Task 6: Fire Ignition Frequency, where fire frequencies are estimated for each of the unscreened fire compartments; and
- Task 7: Quantitative Screening. The unscreened fire compartments are subjected to quantitative screening.

The steps performed under this task should be documented in a work package. The work package should contain the following:

- A list of all fire compartments qualitatively screened and the basis for their screening, and
- A list of all the fire compartments that were not screened and need further analysis.

### **2.6.12 Internal Fire Data Analysis**

Data analysis for the FQRVA is conducted using the same general approach as that outlined in Sections 2.1 through 2.4; however, there are some specific aspects of fire frequency development that are unique to the FQRVA, as described in the following subsection.

#### **2.6.12.1 Fire-Ignition Frequencies Development**

This section describes the procedure for estimating the fire-ignition frequencies associated with fire ignition sources. Generic ignition frequencies that can be specialized to facility conditions in terms of facility characteristics and facility fire event experience are provided. Uncertainties in the generic frequencies are also provided in terms of 5<sup>th</sup>, 50<sup>th</sup>, and 95<sup>th</sup> percentiles.

This work package addresses the following fire-ignition frequency related issues:

- Facility specific fire event data review and generic fire frequency update using Bayesian approach,
- Equipment (ignition source) count by compartment,
- Apportioning of ignition frequencies according to compartment-specific configurations, and
- Uncertainty considerations in the fire frequencies.

This task estimates fire-ignition frequencies and their respective uncertainties for different compartments (e.g., main control room) and ignition sources; e.g., Fuel Pump A and three vertical segments of a motor control center. A generic set of fire-ignition frequencies for various generic equipment types (ignition sources) typically found in certain facility locations was developed as a starting point. It should be noted that when



analyzing historical event data it could not be determined whether or not electrical equipment (e.g., cables and electrical cabinets) employ thermoset or thermoplastic insulation and/or jackets. Therefore, all the events for any given ignition source type were combined and the resulting frequencies should be used for both types of cable insulation and jacket material.

The combination of locations and equipment types (ignition source) are referred to here as ignition frequency bins. Table 2-14 provides the list of these bins and their respective generic mean frequencies (i.e., the mean value of the uncertainty distribution) in terms of number of events per facility year. A description and limitations of the equipment type of each bin is further discussed in Section 6.5.6 of NUREG/CR-6850. The operating mode (i.e., whether or not the facility is in power operation) used for collecting the fire event data for each bin is also noted in that table. Appendix C provides a discussion of the basis of the frequencies and their derivation method. The two-stage Bayesian update method (Reference 57) was used to account for facility-to-facility variability among the facility. The 5<sup>th</sup>, 50<sup>th</sup>, and 95<sup>th</sup> percentiles of the uncertainty distribution are also provided in Appendix C. The underlying fire event data was taken from EPRI's Fire Events Database (FEDB). Single stage Bayesian update method can be used to modify the generic frequencies to reflect the influence of facility-specific fire event experience.

Different fire types can be postulated for some of the ignition sources. For example, the bin "facility-wide components/pumps" can refer to both electric and oil fires. In those cases, Table 2-14 provides a split fraction for each fire type. The split fraction was determined according to fire events in the FEDB. Continuing with the facility-wide-components/pumps example, the pump fire events in the database were reviewed and classified as oil or electrical fires. This classification serves as the basis for the split fraction.







**Table 2-14. Fire Frequency Bins and Generic Frequencies (Continued)**

ID	Location	Ignition Source (Equipment Type)	Mode	Generic Freq (per rx yr)	Split Fractions for Fire Type					
					Electrical	Oil	Transient	Hotwork	Hydrogen	HEAF <sup>1</sup>
15	Plant-Wide Components	Electrical Cabinets	All	4.5E-02	1.0	0	0	0	0	0
16	Plant-Wide Components	High Energy Arcing Faults <sup>1</sup>	All	1.5E-03	0	0	0	0	0	1.0
17	Plant-Wide Components	Hydrogen Tanks	All	1.7E-03	0	0	0	0	1.0	0
18	Plant-Wide Components	Junction Boxes	All	1.9E-03	1.0	0	0	0	0	0
19	Plant-Wide Components	Misc. Hydrogen Fires	All	2.5E-03	0	0	0	0	1.0	0
20	Plant-Wide Components	Off-gas/H <sub>2</sub> Recombiner (BWR)	Power	4.4E-02	0	0	0	0	1.0	0
21	Plant-Wide Components	Pumps	All	2.1E-02	0.54	0.46	0	0	0	0
22	Plant-Wide Components	RPS MG Sets	Power	1.6E-03	1.0	0	0	0	0	0
23a	Plant-Wide Components	Transformers (Oil filled)	All	9.9E-03	0	1.0	0	0	0	0
23b	Plant-Wide Components	Transformers (Dry)			1.0	0	0	0	0	0
24	Plant-Wide Components	Transient fires caused by welding and cutting	Power	4.9E-03	0	0	0	1.0	0	0







The frequencies provided in Table 2-14 apply to all relevant equipment items within a unit. For example, in the case of “batteries”, the mean frequency, 7.5E-04 per facility year, applies to all battery sets of a unit that provides backup power to the DC buses. If there are two battery sets associated with one unit, the fire frequency per battery set would be 3.75E-04 per facility year. If there are four battery sets in another one-unit facility, the mean frequency at that facility would be 1.87E-04 per facility year for each battery set. This is an important feature of the fire frequency model employed in this fire risk methodology and reflects differences in facility design and construction. As the example illustrates, the per-item fire ignition frequency may vary from facility to facility due to the variations in the total population of a given equipment type present in the facility. Such variations are an inherent feature of the methodology presented in this report. The intent of the methodology is to preserve the facility-wide fire frequency for each ignition source type. The facility-wide frequency of, for example battery fires, is assumed to be the same for all units. However, due to variations in the number of battery sets, the fire frequency per battery set at one unit may differ from that of another unit.

In Task 7A, the quantification process needs the fire frequency associated with a compartment. Compartment level frequency is calculated from the sum of all frequencies  $\lambda_{IS,J}$  associated with the ignition sources present in the compartment. The ignition source frequencies  $\lambda_{IS,J}$  are estimated from the following equation:

$$\lambda_{IS,J} = \lambda_{IS} W_L W_{IS,J,L}$$

where:

$\lambda_{IS}$  = Facility-level fire frequency associated with Ignition Source IS.

$W_L$  = Location weighting factor associated with the ignition source.

$W_{IS,J,L}$  = Ignition source weighting factor reflecting the quantity of the ignition source type present in Compartment J of Location L.

Note that where multiple locations (e.g., control building and auxiliary building) are mentioned for the location designator, the bin frequency presented in Table 2-14 applies to all the fire compartments of those locations collectively.

Facility-level fire frequencies (i.e.,  $\lambda_{IS}$ ) are either taken directly from Table 2-14 or after a Bayesian update using facility-specific fire experience. Location weighting factor,  $W_L$ , adjusts the frequencies for those situations where a common location (e.g., turbine building) or set of equipment types are shared between multiple units. For example, if one turbine building serves two units, then 2.0 will be used for location weighting factor.

Ignition source weighting factor, in general terms, is the fraction of an ignition source type found in a specific compartment. As presented earlier, if there are two battery sets associated with a unit and one of them is in Compartment J, 0.5 should be used for the ignition source weighting factor associated with the batteries found in Compartment J. Therefore, to establish the ignition source weighting factors, it is necessary to obtain a count for each compartment of every relevant item; i.e., ignition sources. Also, the



combination of the two factors (i.e.,  $W_L W_{IS,j}$ ) accounts for the fraction of ignition source types in a multiunit site found in a specific compartment of the unit being studied.

Compartment level fire frequency would then be calculated from:

$$\lambda_{j,L} = \sum \lambda_{IS} W_L W_{IS,j,L}$$

(Summed over all Ignition Sources IS in Compartment J of Location L)

In Task 11, the quantification process needs the ignition frequency associated with a fire scenario. Typically, a fire scenario in Task 11 is defined in terms of a fire starting from a specific ignition source and propagating to other combustibles and targets. To establish the ignition frequency associated with a specific ignition source, the equation on page 6-2 can be used.

The estimation of weighting factors for transient fires is treated differently when compared to the method previously used by EPRI in the Fire PRA Implementation Guide (Reference 58). In this procedure, maintenance, storage, and occupancy characteristics are considered in estimating the factors.

The analysis model described in this task is based on the following assumptions.

- Fire ignition frequencies remain constant over time;
- Among the facilities, total ignition frequency is the same for the same equipment type, regardless of differences in the quantity and characteristics of the equipment type that may exist among the facilities;
- Within each facility, the likelihood of fire ignition is the same across an equipment type. For example, pumps are assumed to have the same fire ignition frequency regardless of size, usage level, working environment, etc.

This task needs the list of unscreened fire compartments generated in Task 4, Qualitative Screening.

Fire event records available at the facility may be used to update ignition frequencies using facility-specific data. The events may or may not have been included in EPRI's Fire Events Database (Reference 59). These fire event records may be categorized based on location, ignition source, and facility operating mode; i.e., power or low power.

At least one walkdown of the entire facility or unit is recommended to identify ignition sources in each fire compartment identified in Task 1, map components to the frequency bins of Table 2-14, facilitate the equipment count and identify their locations. The analyst may elect to walkdown only those fire compartments that survive the first qualitative screening (Task 4). This approach may lead to a conservative count of the equipment in the per-component fire frequency context (i.e., an undercount) because components located in the screened out fire compartments would not be included in the equipment counts.



The fire ignition frequencies calculated in this task are used in Tasks 7A, 8, 7B, 11, 14, and 15. Also, ignition source listing by compartment is used in Task 8 for screening the ignition sources and in Task 11 for defining fire frequencies.

### ***2.6.12.2 Equipment Fire Fragility Evaluation***

Prior to determining specific fire scenario impacts, it is necessary to determine susceptibility or “fragility” of facility structures, systems, and components (SSC) to fire, including associated smoke, gases, and soot. An evaluation of which facility SSCs are susceptible to fire damage is conducted by SSC element; e.g., by component type. While it is true that, in the limit of time, effectively all SSCs are susceptible to failure from fire exposure, this task is designed to determine reasonable susceptibility to failure from fire within a time considered to be realistic before we have high confidence that the fires would be extinguished or burn out on their own. For example, it may be reasonable that most fires would be extinguished by competent fire suppression staff resources applied to RHFSF fires, via Navy or public fire department resources, within a certain timeframe (e.g., 24 hours from ignition).

### ***2.6.12.3 Fire Scenario Propagation Conditional Probability Development***

Fire scenarios can be confined to single fire zones, or they can potentially propagate to other adjoining fire zones. In this task, fire propagation characteristics of the fire zone where the initiating event occurs are evaluated to determine the conditional probability of fire propagation to other zones prior to fire suppression. These conditional probability values are then applied in the fire event sequence analysis to determine event sequence impact for analyzed fire scenarios.

### ***2.6.12.4 Fire Scenario Human Error Probability Evaluation***

The general approach described in Sections 2.1 through 2.4 and in Section 2.6.9 is applied in determining specific HFE HEP values to be applied in the FQRVA.

#### ***2.6.12.4.1 Fire Scenario HEP Development***

Fire scenario HFE HEP development is performed following the approach outlined in Sections 2.1 through 2.4, as supplemented by guidance in NUREG-1921.

#### ***2.6.12.4.2 Post-Fire Recovery Action HEP Development***

Post-fire recovery action HFE HEP development is performed following the approach outlined in Sections 2.1 through 2.4, as supplemented by guidance in NUREG-1921.

## **2.6.13 Internal Fire Risk Quantification**

This section describes the procedure for performing fire risk quantification. This procedure provides the user a general method for quantifying the final fire QRVA model to generate the final fire risk results.



### 2.6.13.1 Quantitative Screening Phase 1

This section describes the procedure for performing the following quantitative screening tasks:

- Task 7A–Quantitative Screening I
- Task 7B–Quantitative Screening II
- Task 7C–Quantitative Screening III (optional)
- Task 7D–Quantitative Screening IV (optional)

This procedure provides the user an approach to quantify the fire QRVA model using the procedure provided in Task 5, and to screen out fire compartments based on quantitative criteria. This procedure develops the bases for the quantitative screening criteria and provides specific methods for implementing the screening process.

This procedure addresses the following steps for each of the major quantitative screening tasks.

- Step 1 – Quantify LOFICF Model
- Step 2 – Quantify AFRF Model
- Step 3 – Quantitative Screening

In Tasks 7A and 7B, the fire QRVA model is quantified at the fire compartment level. In Tasks 7C and 7D, the fire QRVA model is quantified at the fire scenario level. Although not recommended, the quantitative screening can be implemented for screening fire scenarios. Therefore, Tasks 7C and 7D are considered optional tasks in this procedure. The basis for the quantitative screening criteria is developed and an approach for implementing the screening process is provided. To address future use of the fire QRVA model for risk-informed applications, quantitative screening criteria also consider the impact of equipment unavailability.

The primary objective of this task is to provide the user an approach to quantify the fire QRVA model developed in Task 5, and to screen out fire compartments based on quantitative screening criteria. It is emphasized that the screening criteria are meant to be applied as part of the fire QRVA model building and quantifying process. The screening criteria are not the same, nor should they be confused with, the acceptance criteria for applications of the fire QRVA model. For example, the screening criteria herein are not directly correlated to the criteria used in Regulatory Guide 1.174 (Reference 60) for the acceptability of making permanent changes to a facility. The screening criteria are intended to complement the Regulatory Guide (RG) 1.174 criteria and to allow for the use of fire QRVA results in risk-informed applications.

There are at least two different QRVA modeling approaches that have evolved in the QRVA field. These two models, in the evolution of QRVA methodology development efforts have come to be known as the “Fault Tree Linking Approach” and “Event Trees with Boundaries Approach”. There is a number of different QRVA software products available in the market designed around these two approaches. The approach



described in this procedure is based on standard state-of-the-art QRVA practices, and is intended to be applicable for any QRVA methodology or software product.

This procedure allows the user to quantify LOFICF and AFRF or CLOFICP and CAFRP. The only difference is that the quantified values of the fire scenario frequencies are used for LOFICF and AFRF calculations, while the fire scenario frequencies are set to 1.0 or TRUE for CLOFICP and CAFRP calculations. The screening criteria also allow for future use of the fire QRVA model for risk-informed applications in that the impact of equipment unavailability can be addressed through an option to calculate incremental loss of fuel inventory control probability (ILOFICP) and incremental acute fuel release probability for components that might be routinely taken out-of-service. Use of this option ensures that sufficient elements of the model are treated in adequate detail to capture the risk effects of these unavailabilities for applications such as an online facility configuration assessment.

Quantitative screening is primarily focused on a fire compartment level (i.e., Tasks 7A and 7B). Quantitative screening on a fire scenario level (i.e., Tasks 7C and 7D) is presented as optional tasks in this procedure. Quantitative screening does not imply that the logic models for the screened out compartments are removed from the fire QRVA model. The intent of the quantitative screening process is to limit the scope of detailed fire modeling and/or detailed circuit analysis by focusing on the significant fire compartments. All screened out compartments remain in the fire QRVA model, albeit at reduced levels of analysis detail.

The quantitative screening criteria were developed with the intent of ensuring that the cumulative risk contributions (i.e., LOFICF and AFRF) from the screened out fire compartments are small. Another goal of the quantitative screening criteria is to ensure that the cumulative incremental risk (i.e., ILOFICP and incremental acute fuel release probability [IAFRP]) from screened out compartments, when combined with equipment unavailability, is less than industry limits. For this reason, the procedure addresses quantitative risk screening criteria for LOFICF, AFRF, ILOFICP (optional), and IAFRP (optional). The criteria for ILOFICP and IAFRP are optional measures that can be applied by users who choose to integrate the fire QRVA model with risk-monitoring models. This approach is different from earlier fire compartment screening criteria, where the goal was to identify LOFICF risk vulnerabilities using a generic fixed compartment LOFICF screening criteria. This procedure addresses both single compartment risk screening criteria and cumulative compartment risk screening criteria; i.e., the sum of the risk contributions of all screened out compartments. The LOFICF/AFRF cumulative compartment risk criteria are based on limiting the cumulative risk of screened out compartments to less than 10 percent of the total internal events risk; i.e., from the internal events QRVA. The single compartment risk criteria (1.0E-07/year for LOFICF and 1.0E-08/year for AFRF) are set at values that are high enough to allow some screening, but sufficiently low that all risk-significant compartments should be retained and adequately analyzed in detail as part of the final quantification process. The single compartment risk criteria are adjusted downward, if necessary, to ensure that the cumulative compartment incremental risk criteria are met.

The ILOFICP/IAFRP cumulative compartment incremental risk criteria are based on limiting the cumulative incremental probability of screened out compartments to less



than 1.0E-06 for ILOFICP and to less than 1.0E-07 for IAFRP. The single compartment incremental risk criteria start with an initial criterion based on limiting the single compartment incremental probability to less than 1.0E-07 for ILOFICP and to less than 1.0E-08 for IAFRP. The single compartment risk criteria are adjusted downward, if necessary, to ensure that the cumulative compartment incremental risk criteria are met.

The quantitative screening criteria described in this procedure are intended to be minimum standards for focusing the detailed analyses on significant compartments while ensuring that the risk contribution of screened out compartments is minimal (thereby justifying their screening). While this quantitative screening procedure should be acceptable for most applications of the fire QRVA model, users of this procedure may decide to impose more restrictive criteria to support other unique applications, such as online risk monitoring. For example, the user may decide to bypass the ILOFICP/IAFRP screening process by reducing the LOFICP/AFRF screening process. However, the user should confirm that the LOFICP/AFRF screening criteria are sufficiently low to ensure that the cumulative incremental risk of screened out compartments is less than industry limits. The bases for the quantitative screening criteria are provided in Appendix D of NUREG/CR-6850.

This procedure assumes that the user is familiar with the QRVA methodology and software employed at the facility. The user should also be familiar with the procedures for quantifying the QRVA model.

Task 7A (Quantitative Screening I) uses input from Task 6, Fire Ignition Frequencies, Task 5, Fire-Induced Risk Model, and Task 12, Post-Fire HRA – the Screening Portion. Task 7B (Quantitative Screening II) uses input from Task 8, Scoping Fire Modeling including any effects to the inputs used in Task 7A. Optional Tasks 7C and 7D use input from Task 9, Detailed Circuit Failure Analysis, Task 10, Circuit Failure Mode Likelihood Analysis and Task 11, Detailed Fire Modeling, including any effects to the inputs used in prior screening steps.

The internal events QRVA model for the facility is needed to support this task. The user should also have access to the software tools needed to quantify the QRVA model.

No walkdown is needed to support this task.

Unscreened fire compartments from Task 7A are input to Task 8, Scoping Fire Modeling. Unscreened fire compartments from Task 7B are used in performing Task 11, Detailed Fire Modeling, and Task 12, Post-Fire HRA, the detailed analysis portion. Additionally, the insights from Task 7B, and in particular any limitations on the allowance of manual action credit within the analyses conducted in Task 9, are communicated to those analysts performing Task 9, Detailed Circuit Failure Analysis. Optional Tasks 7C and 7D are performed in parallel with detailed fire scenario analysis, and unscreened fire scenarios are input to Task 14, Fire Risk Quantification.

### **2.6.13.2 Scoping Fire Modeling**

Scoping fire modeling is the first task in the fire QRVA framework where fire modeling tools are used to identify ignition sources that may impact the fire risk of the facility.



Screening some of the ignition sources in the room, along with the application of severity factors to the unscreened ones, may reduce the compartment fire frequency previously calculated in Task 6.

This task has two main objectives:

- To screen out those fixed ignition sources that do not pose a threat to the targets within a specific fire compartment, and
- To assign severity factors to unscreened fixed ignition sources.

It must be noted that only those ignition sources should be considered in this task that were included in establishing the fire ignition frequency in Task 6. All other potential ignition sources that were screened out in Task 6 should neither be addressed in this task. With this task, the level of effort for detailed fire propagation analysis may be reduced. Furthermore, applying severity factors may reduce the compartment frequency calculated in Task 6, resulting in some compartments being screened before detail fire modeling studies are conducted.

This procedure contains instructions for identifying and screening fixed ignition sources. The procedure also provides some general notes on how to assign severity factor values for ignition sources included in the generic fire frequency model.

The procedure recommends two work forms: (1) the walkdown screening form, and (2) the zone of influence (ZOI) form. The walkdown screening form should be filled during the walkdown.

It compiles information about the ignition sources relative to nearby equipment. The ZOI form specifies a zone of influence for ignition sources in a specific compartment.

The focus of this task is twofold.

1. Refine the information about fixed ignition sources. The direct fire effects on fire QRVA components or circuits are not addressed. The basic assumption about loss of all fire QRVA components (including cables) present in the fire compartment is still maintained in this task. That is, no equipment in the fire QRVA component list is screened. Therefore, the location and specific characteristics of the cables carrying fire QRVA component-related circuits are not needed for performing this task.
2. Application of severity factors to each ignition source. After applying the severity factor, the compartment fire frequencies calculated in Task 6 are reevaluated.

This task is the first attempt at identifying fire scenarios in terms of ignition sources and propagation patterns. In the first quantitative screening task, the LOFICF for each compartment is calculated assuming that all the targets within the compartment would fail due to fire-generated conditions. In this task, the possibility of the fixed ignition sources causing the postulated damage is examined. Those that cannot cause target



damage are screened out from further analysis. For the purpose of this task, a target can be considered:

1. The closest equipment (including cabinets and cables trays) to the fixed ignition source if no specific knowledge about target location in the compartment is currently available; or
2. Known fire QRVA components (targets of interest to the analysis) in the compartment, if the specific target locations are known.

A set of conservative fire modeling calculations are performed for predicting fire conditions near a target in order to assess if target damage or ignition can occur. The analyst can then be confident that an ignition source can be screened out if no relevant targets receive thermal damage. Ignition sources that are part of the fire QRVA components cannot be screened. For the ignition sources that do not screen out, the severity level of the fire needed to cause damage is established and the corresponding severity factor is estimated. The severity factor is used to adjust the fire frequencies for a second round of quantitative screening. Technical details on the determination of severity factors are provided in Appendix E of NUREG/CR-6850.

In general terms, the direct impact of a fire on a target can be described with the following five mechanisms:

1. Engulfed in flames,
2. Within fire plume,
3. Within the ceiling jet,
4. Within the smoke layer, or
5. Within the flame irradiation zone.

Flame temperatures in typical enclosure fires are expected to be between 800°C and 1200°C. These temperatures are above piloted ignition temperatures for many combustibles, including cables. The time for ignition of solid combustibles in contact with flames will depend on its thermophysical properties and the heat flux generated at the flames. Any additional passive fire protection feature, such as barriers, shields, or retardant substances, can also affect the damage or ignition time.

A fire plume is a buoyant stream of hot gases rising above a localized area undergoing combustion into surrounding space of essentially uncontaminated air. Therefore, depending on the fire intensity and elevation of the equipment above it, targets located within this region are subjected to a distinct and relatively high level of thermal hazard.

The ceiling jet refers to the relatively rapid gas flows in a shallow layer beneath the ceiling surface that is driven by buoyancy of hot combustion products. Ceiling jets form when a fire plume impinges under a ceiling and hot gasses spread away. Temperatures in the ceiling jet are expected to be lower than in the fire plume. Still, as in the case of the plume, targets located within the ceiling jet are subjected to a distinct thermal hazard. Notice, however, that ceiling jet applications in facilities are limited due to the generally large number of cables, conduits, pipes, and structural members interfering with ceiling jet flows.



A smoke layer usually forms below the ceiling jet. Depending on the fire intensity, the smoke layer temperature may reach damage or ignition temperatures of many materials. The fire plume transports the heat and smoke generated in the combustion process into the smoke layer, which is affected by the air injected into or extracted from the compartment. The smoke layer temperature is usually lower than the ceiling jet temperature due to air entrainment.

Finally, diffusion flames usually irradiate heat to the surroundings. This irradiation is mainly emanated from the soot particles inside the flame. The intensity of this impinging heat flux decreases with distance. Therefore, there is a critical region near a flame where a target would be adversely affected by incident heat flux.

Table 2-15 recommends ZOIs and severity factors calculation methods for the ignition source bins in the frequency model. Note that the severity factor for all the frequency bins are not calculated based on fire modeling.

DRAFT







**Table 2-15. Zone of Influence and Severity Factor Recommendations (Continued)**

ID	Location	Ignition Source	Ignition Source Screening Approach	Recommended Method or Probability Distribution <sup>1</sup> for Calculating Severity Factor
15	Plant-Wide Components	Electrical cabinets	Calculate ZOI using Figure F-2	Electrical cabinets
16	Plant-Wide Components	High-energy arcing faults	Do not screen in Task 8	Assume 1.0
17	Plant-Wide Components	Hydrogen tanks	Do not screen in Task 8	Assume 1.0
18	Plant-Wide Components	Junction box	Calculate ZOI using Figure F-2	Electric motors
19	Plant-Wide Components	Miscellaneous hydrogen fires	Do not screen in Task 8	Assume 1.0
20	Plant-Wide Components	Off-gas/H <sub>2</sub> recombiner (BWR)	Do not screen in Task 8	Assume 1.0
21	Plant-Wide Components	Pumps	Do not screen in Task 8	Assume 1.0
22	Plant-Wide Components	RPS MG sets	Calculate ZOI using Figure F-2	Electric motors
23a	Plant-Wide Components	Transformers (oil filled)	Do not screen in Task 8	Assume 1.0
23b	Plant-Wide Components	Transformers (dry)	Calculate ZOI using Figure F-2	Electric motors
24	Plant-Wide Components	Transient fires caused by welding and cutting	Do not screen in Task 8	Assume 1.0
25	Plant-Wide Components	Transients	Do not screen in Task 8	Assume 1.0
26	Plant-Wide Components	Ventilation subsystems	Calculate ZOI using Figure F-2	Assume 1.0
27	Transformer Yard	Transformer - catastrophic	Do not screen in Task 8	Assume 1.0
28	Transformer Yard	Transformer - noncatastrophic	Do not screen in Task 8	Assume 1.0
29	Transformer Yard	Yard transformers (Others)	Do not screen in Task 8	Assume 1.0
30	Turbine Building	Boiler	Do not screen in Task 8	Assume 1.0

1. Appendix E provides technical details for calculating severity factors



**Table 2-15. Zone of Influence and Severity Factor Recommendations (Continued)**

<b>ID</b>	<b>Location</b>	<b>Ignition Source</b>	<b>Ignition Source Screening Approach</b>	<b>Recommended Method or Probability Distribution<sup>1</sup> for Calculating Severity Factor</b>
31	Turbine Building	Cable fires caused by welding and cutting	Do not screen in Task 8	Assume 1.0
32	Turbine Building	Main feedwater pumps	Do not screen in Task 8	Assume 1.0
33	Turbine Building	T/G excitor	Do not screen in task 8	Assume 1.0
34	Turbine Building	T/G hydrogen	Do not screen in Task 8	Assume 1.0
35	Turbine Building	T/G oil	Do not screen in Task 8	Assume 1.0
36	Turbine Building	Transient fires caused by welding and cutting	Do not screen in Task 8	Assume 1.0
37	Turbine Building	Transients	Do not screen in Task 8	Assume 1.0

1. Appendix E provides technical details for calculating severity factors.





The type of exposure will depend on the location of the target with respect to the fire. Clearly, during the course of a fire event, a target may be exposed to more than one of the conditions listed above. However, for the purpose of this task, a target is assumed to be subjected to only one type of exposure with constant flammability and thermophysical characteristics. The fire ZOI is defined using fire models to determine the regions where fire conditions will cause target damage. Technical details on the determination of the ZOI are provided in Appendix F of NUREG/CR-6850.

Note that transient combustibles are not screened in this task. This is because the characterization of transient fire sources; i.e., fire size, type, duration, and location, necessitate facility-specific considerations that demand level of effort beyond that anticipated for this task. Analysis of the impact of transient combustibles is discussed in Task 11, Detailed Fire Modeling, in order to avoid postulating them in rooms that may be screened in earlier tasks.

An important part of this task is a facility walkdown to ensure that the specific conditions of each fire compartment are obtained and included in the analysis. During the walkdown, the analysts may attempt to screen out some of the ignition sources based on clear indications that no targets could be damaged. If such qualitative screening is attempted, the analysts may need to adhere to the following:

- The fixed ignition source screening conducted in this task relies exclusively on thermal damage. Therefore, fixed ignition sources considered capable of high energy (explosive) events should not be screened in this task. Examples of such fixed ignition sources are:
  - High voltage transformers (480V or higher),
  - Switchgears (480V or higher) and diesel generator cabinets supplied with AC power by the running diesel generator (e.g., DG excitation cabinets, DG switchgear, and some DG control cabinets), and
  - Diesel generators.
- Because of their position on the electrical lineup, most motor control centers will have adequate breaker protection and may be screened out if they are not vented. However, analysts should consult facility drawings or knowledgeable facility personnel to ascertain whether exceptions exist.

The following is a list of assumptions used to develop the procedure for this task.

- Altered conditions of a fixed ignition source that may lead to a fire more severe than the most severe postulated fires are very unlikely to occur. The altered conditions of a fixed ignition source may be addressed as part of the transient combustible fire analysis.
- Equipment damage can only occur from exposure to fire generated temperatures exceeding a pre-defined threshold.



- No consideration is given to duration of exposure; i.e., a one-second fire exposure of 330°C (625°F) is as capable of damage as a 30-minute fire exposure of 330°C (625°F). As a screening task, this conservatism is acceptable. In detailed fire modeling, Task 11, the element of time should be included in the analysis, which generally includes a growing heat release rate profile and time to target heating.
- No credit is given to the possibility of suppressing a fire before damage. That is, the non-suppression probability is assumed to be 1.0.
- All targets are a part of the QRVA equipment, and loss of a target would always lead to an initiating event or cause a failure modeled for CLOFICP calculations, or both.

The list of unscreened fire compartments from previous screening tasks and the fire QRVA components from Task 2 are needed for this task.

The following documentation may support the walkdown recommended in this task:

- List of equipment in compartments,
- Equipment layout drawings, and
- Elevation drawings of rooms and equipment.

Information that an analyst can use to establish the characteristics of a credible fire associated with a specific ignition source is also needed in this task. The exact nature of the information will depend on the specific characteristics of the ignition source. The following is a sample of such information:

- Quantity of the oil maintained inside rotating machinery,
- Power and voltage of a motor,
- Power of electrical cabinets, and
- Quantity and nature of combustible and flammable materials maintained in an enclosure.

At least one walkdown is needed to support this task. The purpose of the walkdown is to identify fixed ignition sources in each compartment that may be screened. The analyst should visit facility compartments in order to:

- Review the location of ignition sources with respect to the targets,
- Ascertain that no potential target exists within ZOIs of the screened fixed ignition source(s), and
- Verify if proper assumptions were made in characterizing the compartment, the ignition source, and the target.



The output of this task can be summarized as follows:

- Revised compartment fire frequency after screened fixed ignition sources and application of severity factors. The revised compartment fire frequencies are used in future quantitative screening tasks.
- List of unscreened fixed ignition sources within each fire compartment and associated severity factors. This information is used in the detailed fire modeling (Task 11) for defining and quantifying fire scenarios.

### 2.6.13.3 Quantitative Screening Phase 2

In this task, the process described and applied in Section 2.6.13.1 is re-performed, based on the results of the scoping fire modeling.

### 2.6.13.4 Detailed Circuit Failure Analysis

Conducting a fire QRVA in accordance with this methodology necessitates an analysis of fire-induced circuit failures beyond that typically conducted during original fire QRVAs. The circuit analysis elements of the project are conducted in three distinct phases:

1. Fire QRVA cable selection (Task 3),
2. Detailed circuit failure analysis (Task 9), and
3. Circuit failure mode likelihood analysis (Task 10).

This chapter provides methods and instructions for conducting the second phase of circuit analysis—detailed circuit failure analysis (Task 9). The purpose of Task 9 is to conduct a more detailed analysis of circuit operation and functionality to determine equipment responses to specific cable failure modes. These relationships are then used to further refine the original cable selection by screening out cables that cannot prevent a component from completing its credited function. The output of this task supports the quantitative screening process under Task 7.

As discussed in Chapter 3 of NUREG/CR-6850, in most cases it is advantageous to perform some aspects of Task 9 along with the basic cable selection process of Chapter 3 of NUREG/CR-6850. Analysts are encouraged to screen out early in the cable selection/analysis process those cables that are readily identifiable as not posing a risk to the credited QRVA function. A full and complete detailed circuit failure analysis can be time consuming and resource intensive. Accordingly, this level of analysis should be reserved for cases in which the quantitative screening demonstrates a clear need and advantage to fully developing a circuit's failure modes and response to fire-induced cable failures. Ultimately, each facility will need to find the most efficient balance point with respect to how much detailed circuit analysis is conducted coincident with the cable section.

Chapter 9 of NUREG/CR-6850 provides methods and technical considerations for identifying the potential response of circuits and equipment to specific cable failure modes associated with fire-induced cable damage. The term “circuit” and “cable” are



often used interchangeably for fire-related circuit analyses. A circuit is comprised of electrical components, subcomponents, and cables/connection wire. Within the context of fire-induced equipment failures, it is understood that “circuit failure” or “circuit response” refers to the impact of “cable failure modes” that may affect the behavior of related components and subcomponents in a complete circuit. This task contains the following key elements:

- Determine the component response to postulated conductor/cable failure modes, and
- Screen out cables that do not impact the ability of a component to complete its credited function.

This task does not address implementation of facility-specific quality assurance and configuration control requirements that might apply to a fire QRVA. Nor is it intended that this procedure validate the accuracy of facility-specific data extracted from facility drawings, documents, or databases. Each facility should follow appropriate quality assurance, administrative, and configuration control procedures applicable to the work being conducted. The need to validate input source documents should be addressed as part of assembling the prerequisite information in Step 1.

The cable failure modes of particular interest here include shorts-to-ground and hot shorts. Open circuit failures<sup>###</sup>, as the initial cable failure mode, will typically not be considered in this procedure. However, an open circuit condition resulting from the predictable operation of a circuit protection device (e.g., circuit breaker and fuse) in response to fire-induced short circuits will be considered with regard to its impact on the operation of the component(s) affected by the cable under consideration.

An Equipment Failure Response Report<sup>####</sup> is a consolidated list of possible component responses resulting from fire damage to the cable. This aspect of the circuit analysis is fundamentally a deterministic study and does not include failure mode probabilities (the probabilistic analysis of circuit failure modes is covered in Chapter 10 of NUREG/CR-6850). However, the results of this task will serve as the basis for estimating the likelihood of specific equipment functional failures at a compartment or scenario level.

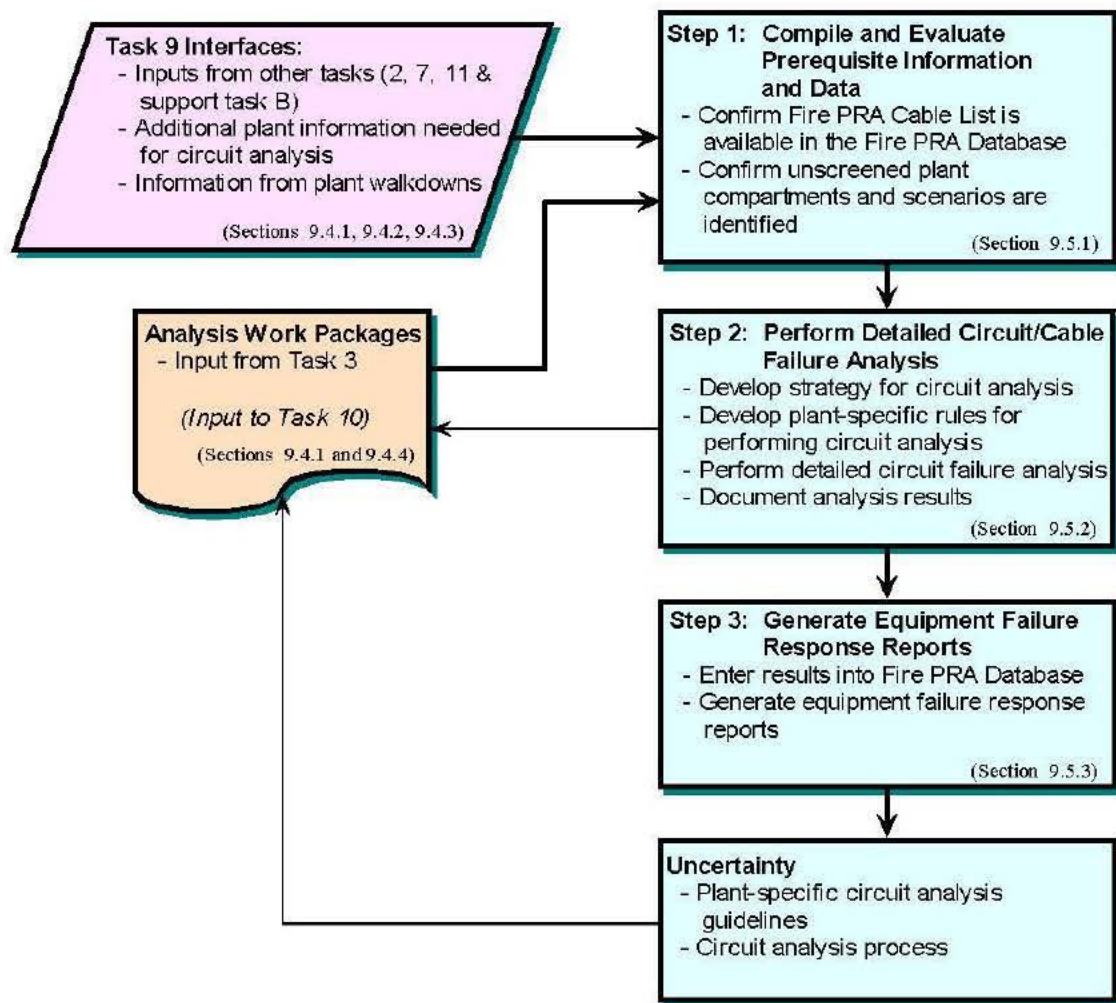
Development of the equipment failure response report involves three principal steps. Generic instructions for completing these steps are provided in this chapter. Figure 2-21 provides a summary of the task work flow. Before beginning this task, it is important to clearly define how various cable failure modes are handled.

---

<sup>###</sup> Within the context of this procedure, “open circuit failure” refers to the loss of continuity due to direct physical damage to the conductor; e.g., melted wire.

<sup>####</sup> The term “Equipment Failure Response Report” is used in the generic sense to depict a matrix-type listing of equipment failure modes correlated to the component’s circuit conductors/cables.





**Figure 2-21. Detailed Circuit Failure Analysis Work Flow**

The following assumptions form the basis for this task:

- An Appendix R analysis for the facility has been completed and documented, and is available for identifying equipment failure responses to specific cable failure modes. Additional effort will be necessary to address systems that are not part of the Appendix R analysis, and to address systems/trains for which the Appendix R analysis assumes failure without performing detailed circuit analysis.
- Component analysis packages have been assembled as part of the activities under Task 3, Fire QRVA Cable Selection, and are available for use in this task.
- Equipment is assumed to be in its normal expected position or condition at the onset of the fire. Where the status of a component is indeterminate or could change as a



result of expected facility conditions, the analysis assumes the worst-case initial conditions.

- Users of this procedure are knowledgeable and have experience with circuit design and analysis methods. Work under this procedure is assumed to be conducted by or supervised by personnel familiar with circuit failure analysis; i.e., Appendix R safe shutdown analysis or similar.

The detailed circuit failure analysis task needs, as a prerequisite, the fire QRVA equipment list from Task 2, Fire QRVA Equipment Selection. The fire QRVA equipment list is used to verify that all fire QRVA cables located in the unscreened compartment(s) or raceway(s) are analyzed. In addition, the fire QRVA equipment list provides the specific functional requirements for each component. Any discrepancies or inconsistencies should be discussed and resolved with the fire QRVA analysts as part of completing the detailed circuit failure analysis.

This detailed circuit failure analysis task needs, as a prerequisite, the list of fire QRVA cables from Task 3, Fire QRVA Cable Selection. The fire QRVA cable list is used to identify fire QRVA cables routed within unscreened facility locations. In addition, the analysis packages assembled for each component during Task 3 provide the baseline documentation needed to complete the detailed circuit analyses.

The fire QRVA database system (database structure and relationships) is a prerequisite for Task 9. The database system provides a structured framework for maintaining fire QRVA data. The database is populated with the data and information generated by previously completed tasks, and, in part, will be used to establish the fire QRVA equipment and cable locations. The data structure and functional relationships established within the database system are specifically designed to provide the necessary sort and query capability to identify fire compartment contents.

To maximize efficiency, an overall project objective is to minimize the number of components for which a detailed circuit failure analysis is conducted. Focusing the scope of the detailed circuit failure analyses is accomplished using the preliminary screening results from Task 7, Quantitative Screening.

An alternate way to identify the cables requiring detailed analysis is to provide a list of raceways affected by fire within a compartment. Such fire scenario-specific input would be generated from the output of Task 11, Detailed Fire Modeling.

Additional information required to support this task includes:

- Component Elementary Circuit Diagrams
- Component Cable Block Diagrams
- Component Wiring/Connection Diagrams
- Electrical Distribution System Single-Line Diagrams
- Instrument Loop Diagrams and Block Diagrams
- Cable Raceway Schedules and Routing Drawings



Facility walkdowns are not considered a fundamental part of this task. Rather, facility walkdowns should be considered on a case-by-case basis as a way of obtaining necessary information about cable and/or raceway locations.

The target equipment response reports are used principally as reference information for conducting additional quantitative screenings. Cables are screened based on their potential to impact the desired functionality of a component. Target equipment response reports also serve as input into the probabilistic circuit failure mode likelihood analysis (Task 10).

### **2.6.13.5 Circuit Failure Mode and Likelihood Analysis**

Conducting a fire QRVA in accordance with this methodology necessitates an analysis of fire-induced circuit failures beyond that typically conducted during original fire QRVAs. The circuit analysis elements of the project are conducted in three distinct phases:

1. Fire QRVA cable selection (Task 3),
2. Detailed circuit failure analysis (Task 9), and
3. Circuit failure mode likelihood analysis (Task 10).

This task provides methods and instructions for conducting the third phase of circuit analysis—circuit failure mode likelihood analysis for fire QRVA cables. Task 10 estimates the probability of hot short cable failure modes of interest, which in turn can be correlated to specific component failure modes. As discussed in Section 3.3.2 of Volume 1 of NUREG/CR-6850, the methods and techniques for deriving circuit failure mode probability estimates are based on limited data and experience. Consequently, this area of analysis is not yet a mature technology, and undoubtedly further advances and refinements will come with time. Nonetheless, the methods and techniques presented in this chapter represent the current state of knowledge and provide a reasonable approach for establishing first-order circuit failure mode probability estimates, albeit with relatively high uncertainty tolerances.

Chapter 10 of NUREG/CR-6850 provides methods and technical considerations for assigning probability estimates to specific cable failure modes associated with fire-induced cable damage.

This task does not address the implementation of facility-specific quality assurance or configuration control requirements that might apply to a fire QRVA. Nor is it intended to validate the accuracy of facility-specific data extracted from facility drawings, documents, or databases. Each facility should follow appropriate quality assurance, administrative, and configuration control procedures applicable to the work being conducted. The need to validate input source documents should be addressed as part of assembling the prerequisite information in Step 1.

Task 10 is intended to provide a probabilistic assessment of the likelihood that a cable will experience one or more specific failure modes; e.g., short-to-ground, intra-cable conductor-to-conductor short, inter-cable conductor-to-conductor short, etc. The results of this assessment are entered into the fire QRVA database, allowing generation of



equipment failure reports, including the estimated likelihood of the failure modes of concern.

Estimating the likelihood of occurrence of specific cable failure modes involves three principal steps. Generic instructions for completing these steps are shown in Figure 2-22. An important element of this task is obtaining the necessary cable and configuration data needed to establish correlations to conditions for which cable failure data is available.

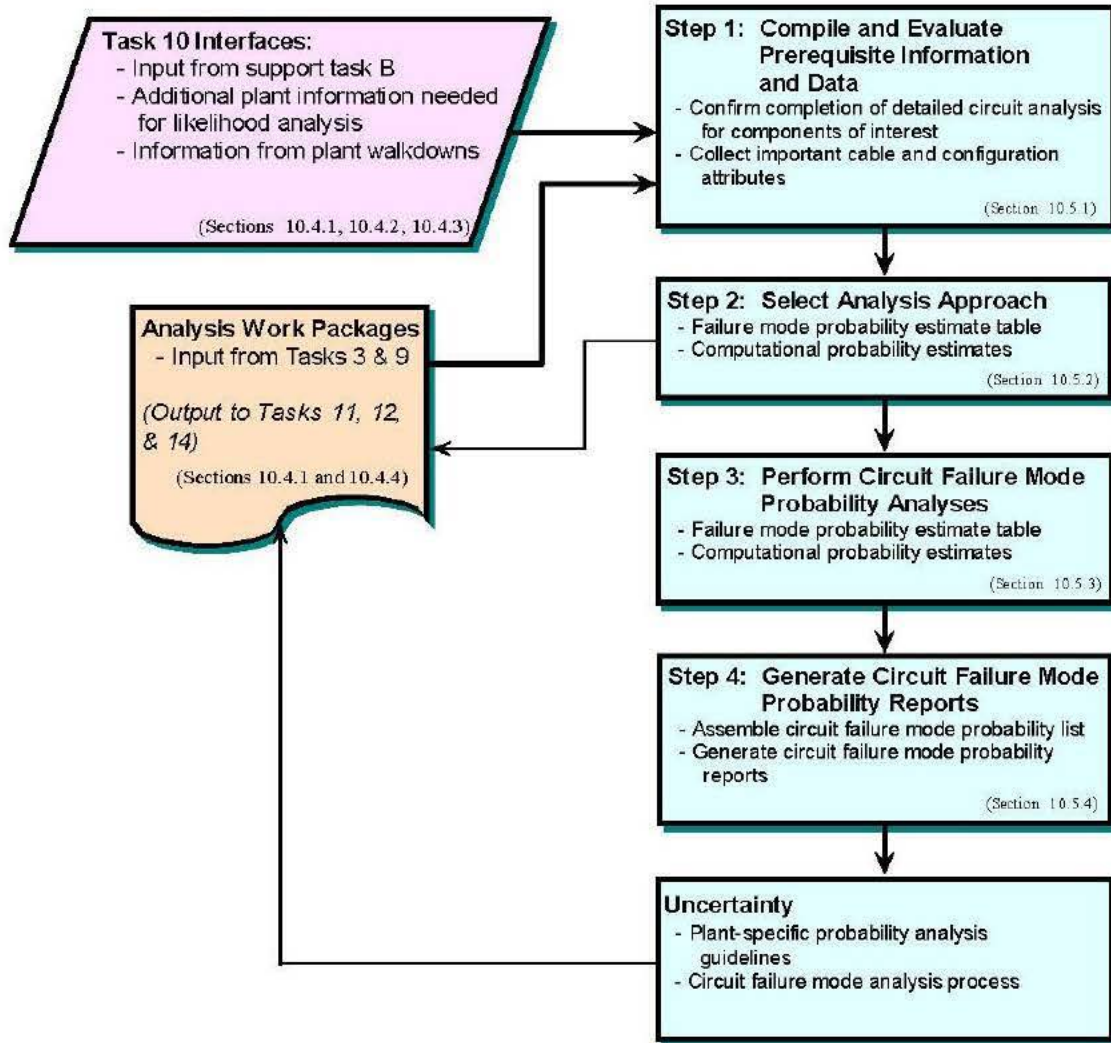


Figure 2-22. Circuit Failure Mode Likelihood Analysis Work Flow



The following assumptions form the basis for this task.

- Requisite cable and configuration attributes are available or can be determined as part of the analysis.
- The equipment is in its normal operating position or condition at the onset of the fire. Where the status of a component is indeterminate or could change as a result of expected facility conditions, the analyst should assume the worst-case initial conditions, consistent with the detailed circuit analysis conducted under Task 9.
- Users of this procedure are knowledgeable and have experience with circuit design and analysis methods and probability estimation techniques.
- The analysis methods presented here can be reasonably applied to multi-conductor cables that contain no more than 15 conductors. Multi-conductor cables with more than 15 conductors are considered to carry a substantially higher uncertainty.

This circuit failure mode likelihood analysis task needs, as a prerequisite, the list of fire QRVA cables from Task 3, Fire QRVA Cable Selection. The fire QRVA cable list is used as the basis for identifying important cable and configuration attributes (e.g., insulation material, raceway type, fire barrier wraps [if any], target and source conductors, etc.) of the cables of interest within the compartments under evaluation.

The fire QRVA database system (database structure and relationships) is a prerequisite for Task 10. The database system provides a structured framework for maintaining fire QRVA data. The database system is populated with the data and information generated by previously completed tasks, and, in part, will be used to establish the fire QRVA equipment and cable routing locations. The data structure and functional relationships established within the database system are specifically designed to provide the necessary sort and query capability to identify fire compartment contents.

The basis for identifying circuit failure modes requiring a probabilistic assessment stems from the detailed analysis of possible failures conducted under Task 9, Detailed Circuit Failure Analysis. This information is essential in establishing a starting point for the probabilistic analysis.

Specific scenarios that need circuit failure mode likelihood analysis to refine equipment failure mode probabilities are identified by Task 11, Detailed Fire Modeling and Task 14, Quantification of Fire Risk. In general, the number of circuits requiring a failure mode likelihood analysis should be small compared to the total circuit population in the study.

Additional information required to support this task includes:

- Component elementary circuit diagrams
- Component cable block diagrams
- Component wiring/connection diagrams
- Instrument loop diagrams and block diagrams



- Cable raceway schedules and routing drawings
- Cable and circuit attribute data:
  - Cable insulating material
  - Cable size and number of conductors
  - Number of normally energized conductors (source conductors) and number of conductors susceptible to failure modes of concern (target conductors)
  - Number of normally grounded conductors
  - Power source characteristics
- Configuration attributes:
  - Type of raceway (i.e., ladder tray or conduit)
  - Quantity and type of other cables contained in the raceway

Facility walkdowns are not considered a fundamental part of this task. Rather, facility walkdowns should be considered on a case-by-case basis as a way of obtaining/confirming necessary information about cables and/or raceway configurations.

The circuit failure mode probability estimates are used principally as reference information for supporting Task 14, Quantification of Fire Risk. The primary objective is to assign probability values for equipment failure modes of concern and then reevaluate CLOFICP and LOFICF for acceptability with respect to compartment and/or scenario screening requirements. Equipment will be screened based on the likelihood of a fire-induced circuit failure causing a component failure mode of concern. The circuit failure probability estimates also serve as inputs to the detailed fire scenario quantification process (Task 11). The results of this task might also be used in Task 12 (Post-fire HRA).

#### **2.6.13.6 Detailed Fire Scenario Modeling (including fire phenomenology)**

In the preceding tasks, the analyses were organized around compartments, assuming that a fire would have widespread impact within the compartment. In Task 11, for those compartments found to be potentially risk-significant (i.e., unscreened compartments), a detailed analysis approach is provided. As part of the detailed analysis, fire growth and propagation is modeled and possibility of fire suppression before damage to a specific target set is analyzed.

The detailed fire modeling process generally follows a common step structure, but the details of the analyses often vary depending on the specifics of the postulated fire scenario. This chapter provides separate procedures for three general categories of fire scenarios: fires affecting target sets located inside one compartment (discussed in Section 11.5.1 of NUREG/CR-6850); fires affecting the main control room (Section 11.5.2 of NUREG/CR-6850); and fires affecting target sets located in more than



one fire compartment (multi-compartment fire analysis; Section 11.5.3 of NUREG/CR-6850).

Task 11 provides final estimates for the frequency of occurrence of fire scenarios involving a specific fire ignition source failing a predefined target set before fire protection succeeds in protecting the target set. This result is combined in the final quantification steps that follow this task, with the CLOFICP/CAFRP given failure of the target set to estimate the LOFICF/AFRF contribution for each fire scenario. The CLOFICP/CAFRP may include modified human error probabilities based on fire scenario specifics.

Detailed fire modeling encompasses an analysis of the physical fire behavior (i.e., fire growth and propagation analysis), equipment damage, fire detection, and fire suppression. The fire scenarios to analyze as part of this detailed analysis task are divided into three categories:

- **General Single Compartment Fire Scenarios.** This general category covers fire scenarios damaging target sets located within the same compartment, exclusive of those scenarios within or impacting the MCR. In general, in this category, the fire ignition source is in the same compartment as the target set. The majority of fire scenarios analyzed generally falls into this category. The procedures applicable to the analysis of these fire scenarios are presented in Section 11.5.1 of NUREG/CR-6850.
- **MCR Fire Scenarios.** This general category covers all fires that occur within the MCR. This category also covers scenarios involving fires in compartments other than the MCR that may force MCR abandonment. The MCR analysis procedures are presented in Section 11.5.2 of NUREG/CR-6850.
- **Multi-Compartment Fire Scenarios.** This general category covers all fire scenarios where

It is postulated that a fire may spread from one compartment to another and damage target elements in multiple compartments. In this category of scenarios, damaging effects of a fire (e.g., heat) are assumed to spread beyond the compartment of fire origin. The multi-compartment fire analysis procedures are presented in Section 11.5.3 of NUREG/CR-6850.

A detailed fire modeling analysis is performed for each fire scenario in each unscreened fire compartment. For many compartments, it may be appropriate to develop several fire scenarios to appropriately represent the range of unscreened fire ignition sources (i.e., scenarios that would not screen out in Task 8) that might contribute to the fire risk. Detailed fire modeling may utilize a range of tools to assess fire growth and damage behavior, and the fire detection and suppression response, for specific fire scenarios.

The ultimate output of Task 11 is a set of fire scenarios, frequency of occurrence of those scenarios, and a list of target sets (in terms of fire QRVA components) associated with the scenarios. For scenarios involving the MCR, the possibility of forced abandonment is also noted. Note that a fire scenario represents a specific chain of



events starting with ignition of a fire ignition source, propagation of the fire effects to other items, and possibility of damaging a set of items identified as target set before successful fire suppression.

Task 11 encompasses the final stages of analysis of the physical fire behaviors associated with fire scenarios in unscreened compartments. A fire scenario in the fire QRVA context begins with initiation of a fire and ends with either safe containment of fuel or a loss of fuel inventory control event. Task 11 is concerned only with the analysis of the physical fire scenario; that is, those aspects of the analysis related to the fire ignition, fire growth, propagation, target set damage, and fire detection and suppression.

In the preceding tasks, the analysis is organized around compartments. The fire initiation frequency, CLOFICP/CAFRP given a fire, and all other parameters assumed that any fire in a compartment would damage all fire QRVA components related items in that compartment. In this task, the focus is shifted towards specific fire scenarios within the compartment, and the objective is to estimate their frequencies of occurrence. All fire scenario frequencies can, in general, be represented by the following:

$$\lambda_k = \lambda_{i,k} \cdot W_{g,k} \cdot SF_k \cdot P_{ns,k}$$

where

$\lambda_k$  = Frequency of Fire Scenario k.

$\lambda_{i,k}$  = Fire ignition frequency of the ignition source i associated with Fire Scenario k.

$W_{g,k}$  = Floor area ratio for transient Fire Scenario k. The floor area ratio is 1.0 for fixed ignition source fire scenarios.

$SF_k$  = Severity factor of Fire Scenario k

$P_{ns,k}$  = Non-suppression probability of Fire Scenario k.

These parameters are further defined in this task and the appendices addressing specific aspects of detailed fire modeling.

Prior tasks will likely have screened out many fire compartments as low risk contributors (i.e., in Tasks 4 and 7, Qualitative and Quantitative Screening respectively). Furthermore, a number of specific fire ignition sources in the unscreened compartments may be screened out as well (accomplished in Task 8, Scoping Fire Modeling). These screening steps will generally reduce the number of possible fire scenarios considered in this task.

In Task 11, the analyst identifies one or more fire scenarios for each unscreened fire ignition source located in the unscreened compartments. The overall analysis process



applied to each fire scenario is illustrated in Figure 2-23. A summary description of the steps defined in Figure 2-23 is provided below:

- Step 11.1: Characterize relevant features of the compartment:
  - Identify the fire compartment in which the fire scenario would be postulated (for multi-room scenarios, identify any adjacent compartments assumed to be involved in the fire scenario) and characterize compartment features relevant to fire propagation, target damage and operator actions. For multiple compartment fire scenarios, characterize the boundaries that separate all involved compartments.
  - Define general compartment characteristics of importance (e.g., size, construction, ventilation conditions, and adjacency features, if relevant).
  - Identify and characterize detection and suppression features and systems to be credited in the fire suppression scenario analysis.
- Step 11.2: Identify and characterize fire detection and suppression features of the compartment:
  - Identify fire detection and suppression features such as smoke and heat detectors, continuous fire watch, automatic and manual fixed suppression systems and fire brigade capabilities.
  - Characterize the operation the fire detection and suppression features in the compartment.
- Step 11.3: Identify and characterize fire ignition sources:
  - Identify and characterize fire ignition sources to be analyzed in terms of location within the compartment, type, size, initial intensity, growth behavior, severity/likelihood relationship, etc.
  - Estimate frequency of ignition for the ignition source.
- Step 11.4: Identify and characterize secondary combustibles:
  - Identify and characterize secondary combustibles. These are nearby fixed equipment such as cables that may be damaged by a fire in the selected ignition source. These combustibles will most likely be within the zone of influence of the ignition source.
- Step 11.5: identify and characterize target sets:
  - Identify the target set relevant to each fire ignition source considered in the fire growth and damage analysis. The locations of a target set in relation to the fire ignition source, target types, failure modes, failure criteria, and other relevant information are collected. If target sets will be treated progressively



(e.g., progressive failure of one tray after another in a stack of cable trays), identify such progressions and determine which target subsets will be treated as unique sub-scenarios.

- Identify secondary combustible fuel elements to be considered in the fire growth and damage analysis (locations relative to fire ignition source, material types, configuration, etc.).
- Step 11.6: Define fire scenarios:
  - Once the ignition source, secondary combustibles and targets have been identified and characterized, fire scenarios in the room can be defined. Fire scenarios should include transient and fixed ignition sources.
- Step 11.7: Conduct fire growth and spread analysis:
  - Select the appropriate fire modeling tool(s).
  - Analyze growth behavior of the initial fire source (if applicable).
  - Analyze fire spread (propagation) to secondary combustibles (as applicable).
  - Analyze growth of fire in secondary combustibles (as applicable).
  - Estimate the resulting adverse environmental conditions relevant to the assessment of target set damage; e.g., temperature, heat flux, smoke density.
  - Estimate time to target set damage (probability versus time).
- Step 11.8: Conduct fire detection and suppression analysis:
  - Assess fire detection timing (if applicable, detection triggers manual fire suppression response).
  - Assess timing, reliability, and effectiveness of fixed fire suppression systems (if applicable).
  - Assess manual fire brigade response (if applicable).
  - Estimate probability of fire suppression as a function of time.
  - Calculate conditional non-suppression probability for each ignition source/target set (or target subset) combination.



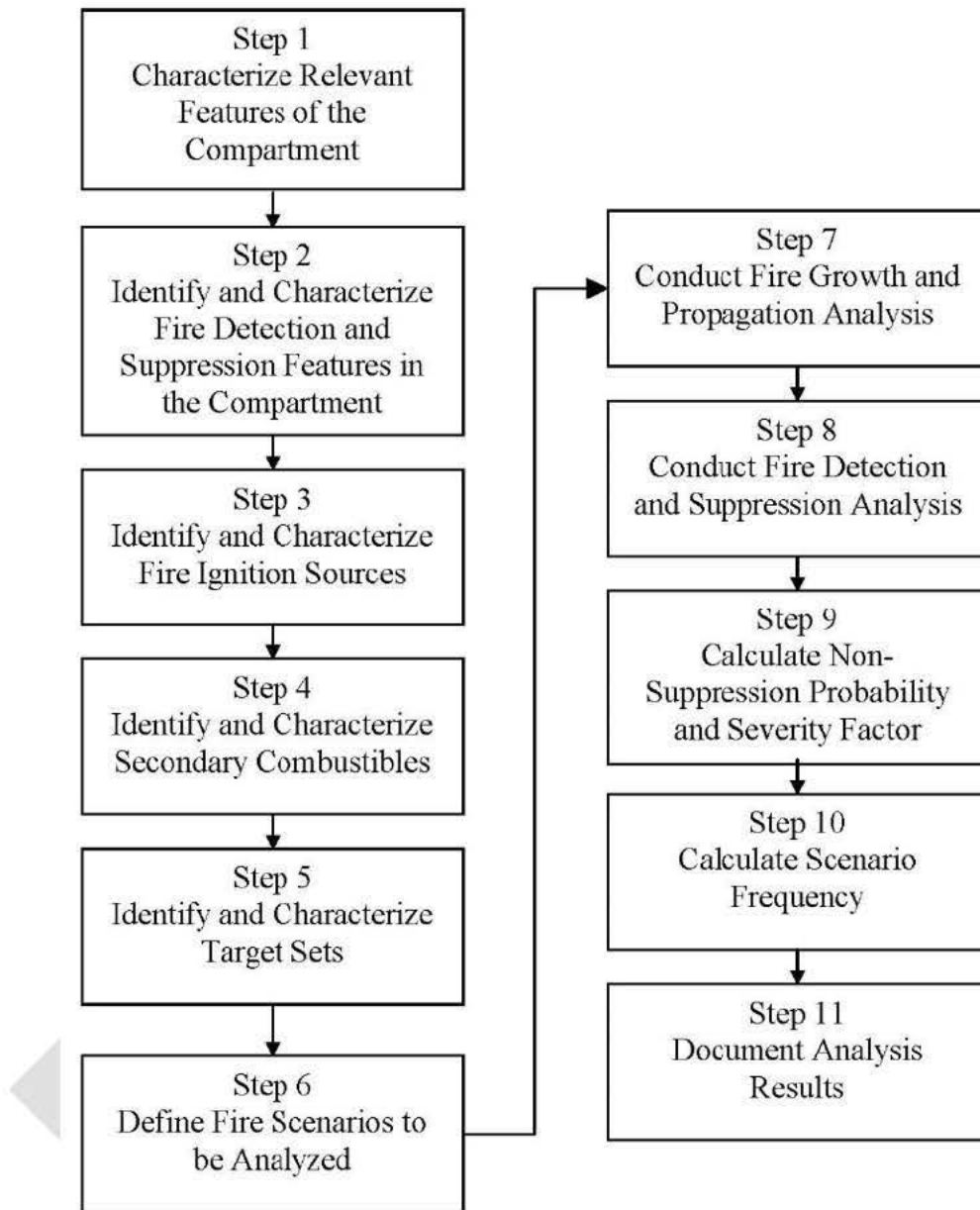
- Step 11.9: Calculate non-suppression probability and the severity factor:
  - Based on the results of fire growth and spread analysis, and stochastic distributions of various input parameters of the models, the conditional probability of the fire being of the postulated severity level is established.
  - Based on the operation of the detection and suppression fire protection systems in the room, and the calculated time(s) to target damage, non-suppression probability is calculated.
- Step 11.10: Calculate scenario frequency:
  - Using the fire ignition frequency, non-suppression probability, and severity factor of the scenario, the overall scenario occurrence frequency can be established. Additional factors (e.g., probability of control room abandonment) may need to be multiplied to obtain final scenario frequency.

- Step 11.11: Document the analysis results:

In conducting these steps, the analyst may select from a wide range of strategies to minimize the level of effort. Different strategies may be used for different fire scenarios or compartments. The following are a few examples:

- The worst possible fire severity may be assigned to an ignition source while using a severity factor equal to one. Based on this worst-case fire propagation, detection and suppression analysis is conducted and target damage is determined. This strategy may be useful if the CLOFICP associated with the target set is small.
- Detailed circuit analysis may be conducted before the severity factor and probability of non-suppression are estimated to verify that the postulated failure modes are possible. After target sets are identified, there could be an interaction between that step of this task and Tasks 9 and 10, where detailed circuit analysis is conducted. Under certain conditions or at certain segments of a circuit, some of the postulated failure modes may be impossible. With this strategy, the analyst can reduce the number of target set elements.
- Assuming worst-case circuit failure, the combination of severity factor and probability of non-suppression may be established first. This strategy may be used when the target set elements are far from the ignition source, which means that the severity factor and non-suppression probability may lead to a small fire scenario frequency.





**Figure 2-23. General Analysis Flow Chart for Task 11 – Detailed Fire Modeling**

Each fire scenario identified in this task begins with fire ignition involving an ignition source. All fire ignition sources that did not screen out in Task 8 should be addressed in this task. The intent is to capture all fire ignition sources with the potential to contribute to fire risk. This should include fire ignition sources involving both fixed and transient fuel packages. Note that the ignition source also establishes the scenario initiation frequency; i.e.,  $\lambda_{i,k}$ .



In some cases, it may be possible to simultaneously capture the contribution of a number of individual fire ignition sources through the analysis of a single fire scenario. This is possible if the fire conditions, including the relative proximity of other combustible fuels and the target set of interest, are essentially identical for all fire ignition sources in the set, and/or are conservatively bounded by the selected representative case.

As an example, consider a fire compartment where the QRVA target set of interest is made of cables routed in cable trays. Further assume that a bank (or row) of electrical panels runs directly below the raceways containing the target cables. In this case, it may not be necessary to model each individual electrical panel as a unique physical fire scenario. Rather, it may be possible to represent the entire row of panels with a single physical fire scenario involving one particular panel as the fire ignition source. It would be appropriate to consider whether or not the panels serve a similar purpose and contain roughly the same type of components. The relative proximity of the secondary fuels and target set cables to each of the panels should also be considered. Even if these factors vary somewhat across the length of the panel bank, it may still be possible to represent the panel bank using a single physical fire scenario whose assumed characteristics conservatively bound those of the individual panels in the set. This approach might also apply if the exact location of target cables in the compartment is unknown, and conservative assumptions regarding their location are made.

The objective of fire growth and spread analysis is to: (1) establish the possibility of the fire involving the ignition source adversely affecting the target set, and (2) estimate the target set damage time. Detailed fire modeling may consider the fire growth behavior within the initiating fire ignition source; that is, the development of fire within the initiating fuel package. The analysis also considers the potential for the spread of fire to other combustible materials and the subsequent fire behavior. As a result, the analyst should characterize both the initial fire source and those combustible materials to which the fire might spread. Note that in the fire modeling process, the intent is to capture the fire damage potential in the absence of fire suppression activities. Fire suppression likelihood is then captured as an explicit, but separate, step in the analysis process.

A wide range of tools is available for the analyst to conduct fire growth and spread analysis. A brief description of these tools is provided below, as in Section 11.5.1 of NUREG/CR-6850. The tools range from simple empirical equations to computerized, numerical, three-dimensional models. For each fire ignition source, or a collection of sources, a range of fire conditions may be postulated to reflect the uncertainty associated with fire growth and damage. In general, transient fuel fires and each unscreened fixed fire source present in the fire compartment should be considered. Note that, in the most general terms, because of the wide variability in the characteristics of ignition sources, a “typical fire cannot be easily defined”. Each fire has unique features and behaviors. Fire growth and spread are dependent on a range of scenario-specific features, and on random behaviors that occur during fire growth and spread. As a result, two fires involving the exact same fire ignition source may burn quite differently in the context of, for example, fire growth rate, peak fire intensity, and fire duration. The intent of the fire modeling process is to explicitly capture this behavioral uncertainty in the quantification process.



Care should also be exercised when extrapolating fire conditions from events in the fire event database directly to a specific fire scenario. For example, a fire occurring in one particular location in one particular facility might not represent a significant threat of fire spread or damage because of available separation and the lack of a potential fire spread path. However, that same fire occurring in a different location, or at a different facility, might be capable of spreading to other nearby combustibles and/or causing significant damage to facility components and cables. Furthermore, a fire event may not have led to substantial damage in a particular case because of prompt fire suppression intervention. That same fire, had it burned longer, might have caused substantial damage under the same facility conditions.

Characterizing the fire ignition source will appropriately capture the uncertainty in fire intensity. That is, the fire ignition source characterization will generally include a recognition and characterization of the fire severity-likelihood relationship.

Any given fire ignition source could lead to fires of varying intensity. The variability in fire intensity for a given source results from both epistemic and aleatory uncertainties. For example, fire intensity will be impacted by factors related to the conditions that led to initiation of the fire; e.g., overheating component versus catastrophic failure of the same component. The current state of knowledge regarding the influence of such factors is imperfect at best. Fires are somewhat chaotic in nature, and, therefore, will exhibit a seemingly random variability in development and intensity regardless of the knowledge state.

In the development of the nominal fire ignition frequency values (i.e., Task 6), some concepts of fire severity have already been incorporated. In particular, the process of quantifying the frequencies presented in Task 6 included screening of reported fire events that did not, and could not, lead to a self-sustained or potentially damaging fire (labeled as non-challenging fires in that task). Furthermore, in Task 8, fire ignition sources that cannot damage any items nearby or cannot spread beyond the ignition source (even given that a self-sustaining fire of conservative intensity is ignited) are screened out. Hence, the postulated fires in Task 11 are self-sustaining, and intervention will be necessary to prevent fire spread to secondary fuels and/or cause fire-induced damage to QRVA components and/or cables.

Application of severity factors has been a point of debate in past QRVA approaches. This is in part because fire severity-likelihood relationships are heavily influenced by expert judgment. Severity factor approaches introduce a number of potential pitfalls. In particular, extreme care is needed to ensure that dependencies between fire severity factors, fire ignition frequencies, assumed fire conditions, and fire detection/suppression analysis are appropriately captured. The recommended fire ignition source characterization approaches have been explicitly integrated with both the fire frequency and fire detection/suppression analysis tasks to ensure a consistent approach.

The fire modeling activities of this Task 11 will consider a range of fire conditions that might be experienced involving the fire sources. That is, the analysis approach is not based on the analysis of only the most likely fire conditions; rather, it provides explicit treatment of less likely, but potentially more challenging, fires.



Table 2-16 lists the recommended methods for calculating severity factors for the different ignition sources in the frequency model.

**Table 2-16. Recommended Severity Factors and Suppression Curves for Ignition Sources in the Frequency Model**

ID	Location	Ignition Source	HRR Probability Distribution for Calculation of Severity Factor	Suppression Curve
1	Battery Room	Batteries	Electric motors	Electrical
2	Containment (PWR)	Reactor coolant Pump	Pumps (Electrical)/Oil spills	Containment
3	Containment (PWR)	Transients and hotwork	Transients	Containment
4a	Control Room	Electrical cabinets	Applicable electrical cabinet	Control room
4b	Control Room	Main control board	See Appendix L	See Appendix L
5	Control/Auxiliary/Reactor Building	Cable fires caused by welding and cutting	See Appendix R of this report	Welding
6	Control/Auxiliary/Reactor Building	Transient fires caused by welding and cutting	Transients	Welding
7	Control/Auxiliary/Reactor Building	Transients	Transients	Transients
8	Diesel Generator Room	Diesel generators	Oil spills	Electrical/Oil
9	Plant-Wide Components	Air compressors	Electrical/Oil spills	Electrical/Oil
10	Plant-Wide Components	Battery chargers	Electrical cabinets	Electrical
11	Plant-Wide Components	Cable fires caused by welding and cutting	See Appendix R of this report	Welding
12	Plant-Wide Components	Cable run (Self-ignited cable fires)	See Appendix R of this report	Electrical

**Table 2-16. Recommended Severity Factors and Suppression Curves for Ignition Sources in the Frequency Model (Continued)**

<b>ID</b>	<b>Location</b>	<b>Ignition Source</b>	<b>HRR Probability Distribution for Calculation of Severity Factor</b>	<b>Suppression Curve</b>
13	Plant-Wide Components	Dryers	Transients	Transients
14	Plant-Wide Components	Electric motors	Electric motors	Electrical
15	Plant-Wide Components	Electrical cabinets	Electrical cabinets	Electrical
16	Plant-Wide Components	High energy arcing faults	See Appendix M of this report	See Appendix M
17	Plant-Wide Components	Hydrogen Tanks	See Appendix N	Flammable gas
18	Plant-Wide Components	Junction box	Electric motors	Electrical
19	Plant-Wide Components	Miscellaneous hydrogen fires	See Appendix N	Flammable gas
20	Plant-Wide Components	Off-gas/H <sub>2</sub> recombiner (BWR)	See Appendix N	Flammable gas
21	Plant-Wide Components	Pumps	Pump (Electrical)/Oil spills	Electrical/Oil
22	Plant-Wide Components	RPS MG sets	Electric motors	Electrical
23a	Plant-Wide Components	Transformers (Oil filled)	Oil spills	Oil
23b	Plant-Wide Components	Transformers (Dry)	Electric motors	Electrical
24	Plant-Wide Components	Transient fires caused by welding and cutting	Transients	Welding
25	Plant-Wide Components	Transients	Transients	Transients
26	Plant-Wide Components	Ventilation subsystems	Electric motors/Oil spills	Electrical/Oil/Transients
27	Transformer Yard	Transformer - catastrophic	See section 6.5.6	Outdoor transformers



**Table 2-16. Recommended Severity Factors and Suppression Curves for Ignition Sources in the Frequency Model (Continued)**

ID	Location	Ignition Source	HRR Probability Distribution for Calculation of Severity Factor	Suppression Curve
28	Transformer Yard	Transformer - noncatastrophic	See section 6.5.6	Outdoor transformers
29	Transformer Yard	Yard transformers (others)	See section 6.5.6	Outdoor transformers
30	Turbine Building	Boiler	Oil spills	Oil
31	Turbine Building	Cable fires caused by welding and cutting	See Appendix R of this report	Welding
32	Turbine Building	Main feedwater pumps	Pump (Electrical)/Oil spills	Electrical/Oil
33	Turbine Building	T/G excitor	See Appendix O	Turbine generator
34	Turbine Building	T/G hydrogen	See Appendix O	Turbine generator
35	Turbine Building	T/G oil	See Appendix O	Turbine generator
36	Turbine Building	Transient fires caused by welding and cutting	Transients	Welding
37	Turbine Building	Transients	Transients	Transients

The primary objective of detection and suppression analysis is to estimate the time to fire control. It is assumed that by achieving fire control, the processes that would lead to target set damage slow down significantly so that no further damage would be experienced. The detailed fire-modeling task includes explicit treatment of the detection and suppression process. All fires are eventually suppressed. However, in the fire QRVA context, the critical factor is the likelihood that the fire will be suppressed before damage to the fire QRVA target set occurs.

The detection and suppression analysis considers intervention by fixed fire protection systems and facility personnel, including the manual fire brigade or onsite fire department. Current modeling tools provide only a very limited capability for directly integrating fire detection and suppression. For example, some compartment fire models now allow for the simulation of a fire detector or a sprinkler head as a thermal target, and can, therefore, predict the approximate actuation time of such devices. Closed-form empirical correlations can also estimate detector or sprinkler response times. However, these capabilities address only a limited subset of the overall detection and suppression processes.

In general, the detection and suppression analysis is performed independently from the fire growth and damage modeling applications. However, the assumptions made in the development of fire scenarios can be relevant to the fire detection and suppression analysis. In particular, there are dependencies between screening of fire events in the fire frequency analysis, the fire severity-likelihood relationship, the fire ignition source

characteristics assumed in the fire modeling, and the detection-suppression analysis. These dependencies should be explicitly treated.

Appendix P of NUREG/CR-6850 describes detection and suppression analysis methodology. The analyst may choose a different approach, as long as it can properly model the likelihood of target set damage before successful suppression.

Results from the detection and suppression analysis are reflected in the probability of no suppression before target damage. Table 2-16 lists the manual suppression probability curves for the different ignition sources in the frequency model.

The following are key assumptions associated with the detailed fire-modeling task.

- The analysis is limited to considering a single fire occurring at any given time. The analysis does not consider the possibility of multiple, concurrent fires. Notice that a scenario involving fire propagation to adjacent compartments is still considered a “single fire”. The risk of such scenario is evaluated in the multi-compartment fire analysis.
- The analysis does not explicitly try to quantify the risk contribution of seismic-induced fires.
- Hence, the conditions that may be encountered during a post-earthquake fire are not considered in the discussions provided for fire modeling.
- If a fixed, water-based fire suppression system is available, actuation of that system is assumed to disrupt the process of fire growth and spread sufficient to achieve and maintain effective control of the fire so that additional damage to potential fire QRVA targets will not occur.
- If a fixed, gaseous fire suppression system is available, actuation of that system is assumed to disrupt the process of fire growth and spread sufficient to achieve effective control of the fire. However, the duration of control is assumed to be the time period over which it has been demonstrated, by test or analysis, that a sufficient suppressant concentration, per applicable standards, can be maintained. If the suppressant concentration cannot be maintained for the prescribed sufficient time period, it should be assumed that the fire would reflash. In such cases, either a second discharge of the fire suppression system (if available) or intervention by facility personnel would be necessary to regain effective control of the fire.
- Loss of fuel inventory control would occur if the control room operators are unable to use the main control board and no actions are taken from outside the control room.

Additional instructions on the definition and characterization of physical fire scenarios are provided in Appendices G, H, and L through T of NUREG/CR-6850, Volume 2.

The inputs to this task are a list of unscreened fire compartments (Task 7B, Quantitative Screening II) and fixed ignition sources in their respective locations generated in Task 8,



Scoping Fire Modeling. In addition, information on all fire QRVA components and cables that have been mapped into each unscreened fire compartment is used in this task. This information is derived during Tasks 2 through 4. This task will also draw on fire compartment characterization information documented in the fire QRVA information database from Task 4. This task is also supported by facility walkdowns, as discussed in Support Task A.

In addition, the analyst conducting this task may need to interact with the analysts conducting Task 7 to establish the CLOFICP/CAFRP associated with a specific target set and with the analysts for Tasks 10 and 11 for assessing the possibility of certain circuit failures.

The detailed fire modeling task utilizes information from a wide range of internal (i.e., facility) and external sources. Much of this information is summarized in Appendices G through T of NUREG/CR-6850. For example, the analyst may need raceway and equipment layout drawings, various operating procedures, fire protection system description and related procedures, HVAC system descriptions, etc. Focused walkdowns of the unscreened compartments are an important part of the information gathering process. Focused walkdowns allow information gathering on site-specific configuration, especially with respect to the physical proximity of fire ignition sources to other combustible materials and to fire QRVA components and cables. In addition to focused walkdowns and detailed document review, it may be necessary to obtain information about actual fire event experience and fire experiments from external sources.

This task, as it is noted in the preceding section, typically includes a focused walkdown of the facility. For the single compartment fire analysis, the unscreened compartments should be visited to gather information supporting the processes of selection and description of fire scenarios. The information needed for detailed fire modeling is best obtained through walkdowns of the compartments of interest.

For the MCR fire analysis, a walkdown would also be beneficial. Specifically, it is recommended for the analyst to inspect the backside of the control panels to gain an understanding of the wiring conditions, cable and wiring layout, separation barriers between panel sections, and overall density of the combustibles inside the panels.

The multi-compartment fire analysis includes a complete walkdown of all facility locations where fire QRVA related components and cables might be present. In that walkdown, the analyst should identify the communication paths between compartments, the condition of the doors, penetration seals, ventilation openings, and any other features that may aid the propagation of hot gases between compartments.

The walkdown process is discussed in Support Task A, Fire QRVA Walkdown Procedure.

The primary output of the detailed fire modeling task is a list of fire scenarios for each unscreened compartment; frequency of occurrence of each fire scenario; and a list of QRVA components and associated failure modes. These results are carried forward into

the final stages of quantitative screening (i.e., Tasks 13 and 15) and into the final risk quantification and uncertainty analysis task steps; i.e., Tasks 17 and 18.

In the course of conducting Task 11 steps, as shown in Figure 2-23, it may become necessary to interact with the detailed circuit analysis tasks (i.e., Tasks 9 and 10) and with the quantitative screening task; i.e., Task 7.

### **2.6.13.7 Final Fire Risk Quantification**

This section describes the procedure for performing fire risk quantification. This procedure provides the user a general method for quantifying the final fire QRVA model to generate the final fire risk results.

This procedure addresses the following major steps for each of the major fire risk quantification tasks:

- Step 1 – Quantify Final Fire LOFICF Model
- Step 2 – Quantify Final Fire AFRF Model
- Step 3 – Conduct Uncertainty Analysis

In this task, the final fire QRVA model is quantified to obtain the final fire risk results. The final LOFICF and AFRF models are quantified for each fire scenario.

Note that per Task 7, Quantitative Screening, it is expected that a number of fire compartments or fire scenarios will be screened out from the formal fire quantification results (i.e., not added into the calculated total facility fire-related LOFICF and AFRF). It is expected that as a minimum, total facility LOFICF and AFRF estimates will be provided by summing all the LOFICFs and AFRFs for the unscreened fire compartments/scenarios. The significant contributors to the facility LOFICF and AFRF should also be provided. In addition, it is also expected that the nature (e.g., type of sequences) of the screened out compartments/scenarios are at least identified and as a check of the cumulative screening criteria discussed in Task 7, it is recommended that the screened LOFICFs and AFRFs also be summed separately to provide a perspective on the total residual risk from the screened compartments/scenarios. It should be emphasized that these screened portions of the results represent various levels of analysis (for instance, some may only involve fire scoping modeling; others may involve both detailed fire modeling and some detailed circuit analysis, etc.). Thus any ranking of these screened scenarios is not particularly appropriate and these screened summations of LOFICF/AFRF are upper bounds of the residual risk and that in actuality, the residual risk is probably much less than these sums would indicate.

This task uses the facility response model (risk model) to quantify LOFICF and AFRF. The model is initially developed in Task 5 (Fire Induced Risk Model), and modified in the quantitative screening done in Task 7. This task also requires input from Task 10 (Circuit Failure Mode Likelihood Analysis), Task 11 (Detailed Fire Modeling), and Task 12 (Post-Fire Human Reliability Analysis).



The internal events QRVA model as modified for the fire QRVA of the NPP facility is needed to support this task. Additional information may be needed from the QRVA model as insights are gained from quantifying the fire risk model. The fire QRVA analysts should also have access to the software tools required to quantify the QRVA model. Access to the ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications (ASME RA-S-2002) (Reference 56), and particularly the accident sequence quantification and AFRF requirements in the standard, may be beneficial, as well.

No walkdown is required to support this task.

This task provides a general approach for quantifying the fire QRVA model and generates the final fire risk results. There are at least two different approaches for developing the internal events QRVA model (which also apply to the fire QRVA model). These two models, in the evolution of QRVA methodology development efforts have come to be known as the “Fault Tree Linking Approach” and “Event Trees with Boundaries Approach”. There is a number of different QRVA software products available in the market designed around these two approaches. The approach described in this procedure is based on standard state-of-the-art QRVA practices and is intended for any QRVA methodology or software product. This procedure allows the user to quantify LOFICF and AFRF or CLOFICP and CAFRP. The only difference is that the quantified values of the fire scenario frequencies are used for LOFICF and AFRF calculations, while the fire scenario frequencies are set to 1.0 or TRUE for CLOFICP and CAFRP calculations.

This procedure assumes that the fire QRVA analyst is familiar with the QRVA methodology and software employed at the facility. The analyst should also be familiar with the procedures for quantifying the QRVA model. The analyst should be familiar with the ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications (ASME RA-S-2002) (Reference 56) and should use the approach therein covering Sections 4.5.8 (for HLR-QU-A, B, C, D) and 4.5.9 (for HLR-LE-A, B, C, D, E, and F1) of NUREG/CR-6850 when quantifying the fire QRVA model following the steps below.

This is the final task of the fire QRVA quantification process. The output of this task is used in Task 16 (Fire QRVA Documentation). Note that Task 15 (Uncertainty Analysis) is addressed during preceding tasks and this task as well.

#### **2.6.14 Internal Fire Risk Uncertainty Analysis**

This procedure describes the approach for identifying and treating uncertainties throughout the fire QRVA process and identifying sensitivity analysis cases. It also prescribes a review for the identified uncertainties among the fire QRVA analysts to establish an integrated approach of addressing the effects of these uncertainties on the results of the analysis. At this time, the procedure provides a general approach to be followed and does not provide a comprehensive list of specific uncertainties to be addressed. As pilot fire QRVAs and other studies are completed, this procedure may be revised accordingly.

This procedure covers the identification and treatment of uncertainties throughout the fire QRVA. As such, it provides: (1) background on the subject of uncertainty found in Appendix U of NUREG/CR-6850, (2) classification of types of uncertainty, and (3) a general approach with regard to practical implementation of treating expected uncertainties in the fire QRVA, as described in Appendix V of NUREG/CR-6850.

Many of the inputs that make up LOFICF and AFRF estimates are uncertain; e.g., fire frequencies, extent of fire growth, equipment failure probabilities, operator action probabilities, etc. Since many of these inputs are commonly treated as the result of random processes in the QRVA, the loss of fuel inventory control events and acute fuel release events are modeled as possible results of a set of interacting random processes, specifically, those involving a fire that causes a facility transient, the response of mitigating systems to the transient including fire effects, and the associated actions of human operators. Hence, the occurrences of loss of fuel inventory control and acute fuel release events are also, therefore, treated as random events.

The various fire-induced accident sequences and their frequencies modeled in the fire QRVA characterize the aleatory uncertainties (see Appendix U of NUREG/CR-6850 for a discussion on this type of uncertainty) associated with the occurrence of a fire and possible facility and operator responses. Each input of the modeled accident sequences (i.e., initiating event frequency, equipment failure probabilities, and human error probabilities) also includes epistemic uncertainties (see Appendix U of NUREG/CR-6850) with regard to the frequencies and probabilities described by distributions. Sampling techniques (e.g., Monte Carlo, Latin hypercube) are typically used to propagate the epistemic uncertainties to generate a probability distribution for each accident sequence frequency, and from that, LOFICF and AFRF uncertainty distributions.

In light of this, it is important that users of the results of the fire QRVA understand the fundamental modeling assumptions underlying the analysis and the sources of uncertainty associated with the results. In particular, in the case of a QRVA, it is important to understand how the analysis deals with uncertainties that arise because of issues not explicitly modeled or imperfect knowledge concerning issues that are modeled. Some uncertainties may be specifically included in the quantification of the results as described above; others may only be qualitatively addressed or not addressed at all. This understanding of what uncertainties are addressed and how, will affect how a user perceives and uses the analysis results in subsequent decision-making activities.

It is important that the uncertainties with the most significant effect on the accuracy and precision of the results be identified and their effects summarized. This procedure serves three purposes toward this overall goal; it: (1) provides background on the subject of uncertainty useful for the fire QRVA analysts, (2) offers a general approach on the identification and treatment of uncertainties for each respective task area, and (3) provides helpful notes and practices for a team of analysts when performing an integrated review of the uncertainties and making final decisions as to the treatment of the uncertainties.



The reader is referred to Appendix U of NUREG/CR-6850 for the underlying principles and theory upon which the identification and treatment of uncertainties, as espoused in this procedure, are based.

The analysts for Tasks 1 through 13 are expected to follow the overall approach provided in this procedure to articulate and quantify, when necessary, the uncertainties in their numerical results. For each affected task, the following information will be needed for uncertainty analysis:

- Sources of uncertainties, and
- Proposed approach for addressing each of the identified uncertainties.

This information has been developed in writing this procedure and the results are provided in Appendix V of NUREG/CR-6850. It is expected that specific uncertainties worthy of uncertainty or sensitivity analyses will be identified during the performance of a facility-specific fire QRVA. To that extent, the issues addressed here should be modified to reflect the key uncertainties identified on a facility-specific basis.

This procedure provides an overall approach to all the other tasks on suggested ways to address the uncertainties associated with each task in the fire QRVA process. In addition to uncertainty analysis, the identification of possible sensitivity analysis cases is addressed in this procedure. Once the integrated uncertainty review is performed and specific strategies for uncertainty analysis are identified and implemented, the results of those analyses should be reflected in the documentation of the fire QRVA (Task 16), including the overall results and conclusions of the QRVA. Similarly, sensitivity analysis cases are proposed to be executed in Task 14.

As the fire QRVA process is carried out (as alluded to in Section 15.4.1 of NUREG/CR-6850), the level of analysis detail evolves and the results, including their significant drivers, will become clear. During this time, modifications of the uncertainties and their treatment may be appropriate. At whatever level of specificity, acknowledging the uncertainties and whether they are modeling or data uncertainties should be made part of the overall documentation of the fire QRVA. Therefore, this procedure may have to be revisited as fire QRVA task execution progresses, and as new information and results are collected or obtained. The intermediate task results may shed new light on the relative importance of various sources of uncertainty and sensitivity analyses.

### **2.6.15 Risk Results Presentation and Interpretation**

FQRVA risk results presentation and interpretation is conducted using the same approach as that outline in Sections 2.1 through 2.4.

### **2.6.16 QRVA Vulnerability Assessment**

FQRVA risk vulnerability assessment is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.1 Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences)**

FQRVA risk decomposition is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events**

FQRVA risk importance measure determination and evaluation is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.2.1 Fractional Importance**

FQRVA risk decomposition is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.2.2 Risk Achievement Worth -**

FQRVA risk importance measure determination and evaluation is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.2.3 Risk Reduction Worth**

FQRVA risk contribution sensitivity analysis is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.16.3 Risk Contribution Sensitivity Analysis**

FQRVA risk contribution sensitivity analysis is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.6.17 Vulnerability Assessment Results Presentation and Interpretation**

FQRVA risk vulnerability assessment results presentation and interpretation is conducted using the same approach as that outline in Sections 2.1 through 2.4.

**2.7 Seismic QRVA**

The key elements of a seismic QRVA (SQRVA) are:

- Seismic Hazard Analysis
- Seismic Fragility Evaluation
- Systems/Accident Sequence Analysis
- Risk Quantification



Figure 2-24 shows a simplified flow chart of the analysis tasks for a SQRVA. While useful as an overview, the flow chart does not indicate the degree of interrelationships among tasks, nor the necessary prerequisites to begin tasks.

In the following, we describe the procedures used and data available to perform each of these tasks in a seismic QRVA. We also describe the prerequisites for each task in terms of the outputs from earlier tasks.

DRAFT

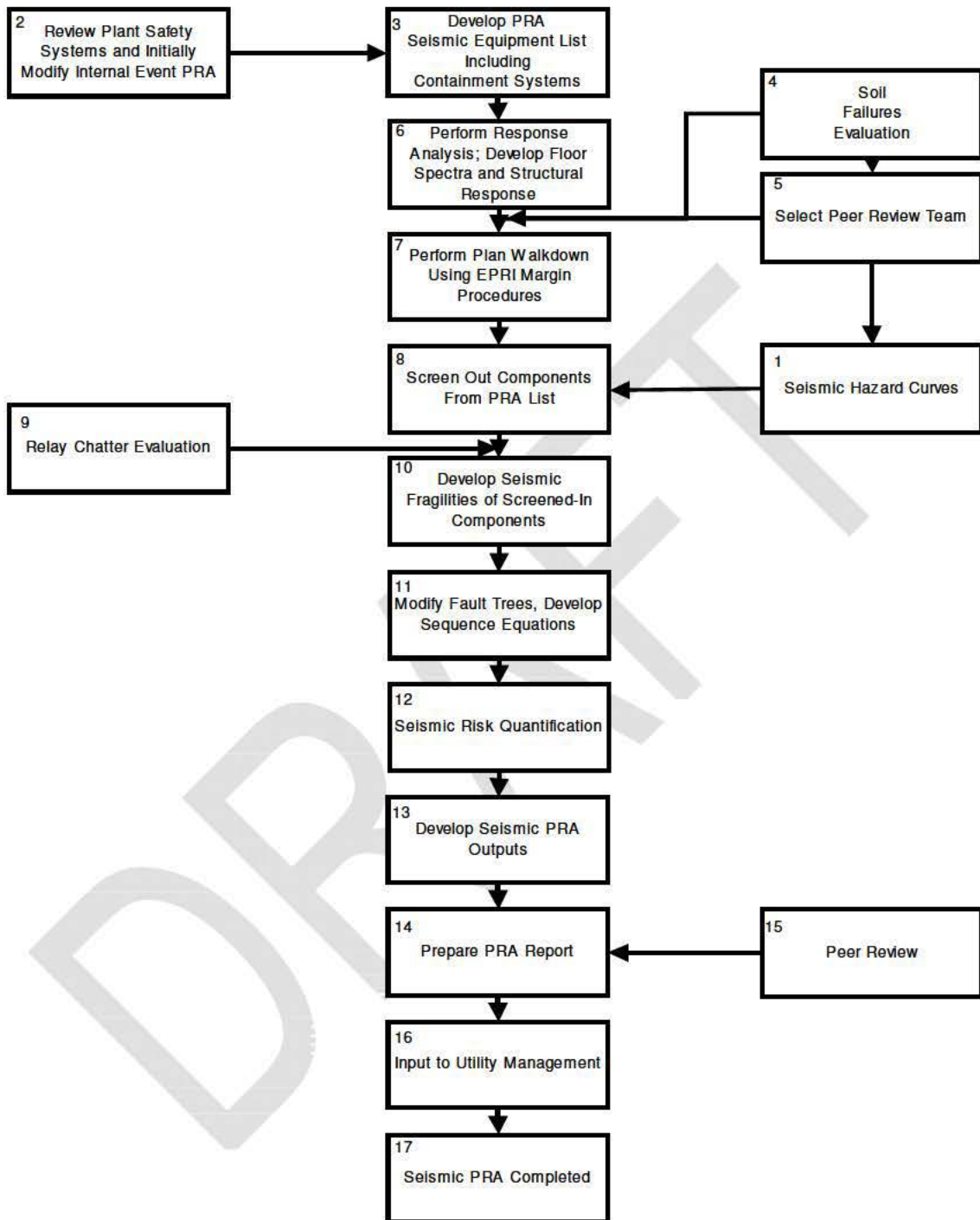


Figure 2-24. SQRVA Task Flowchart



### **2.7.1 Develop Facility-Specific Risk Hazard Curves**

The family of seismic hazard curves is developed for the site in terms of the selected ground motion parameter; e.g., peak ground acceleration. Along with the family of hazard curves for horizontal ground motion, there must be guidance on how the fragility analysts are to account for vertical ground motion. Also, the uniform hazard spectra to be used must be documented.

The hazard curves must extend to sufficiently low ground motion levels so that no damage is expected at still lower ground motions. They must also extend to sufficiently high ground motion levels so that the risks from still stronger earthquakes can be either neglected or conservatively mapped to AFRF. All historical records of ground motion must be compiled. All credible sources of earthquakes surrounding the site, including distant, infrequent potential sources of strong ground motion and close in more frequent, lower magnitude events must be included.

### **2.7.2 Review Facility Safety Systems and Perform Initial Modification to Facility Internal Events QRVA System Models**

The systems analyst will review the internal event QRVA facility safety systems from the viewpoint of seismic safety, identify any seismic-specific initiating events, and modify the event trees and fault trees accordingly. Some review of the internal event models is necessary to develop the initial QRVA seismic equipment list. This explains why this task appears before Task 3. To the extent that the internal QRVA trees may be modified for seismic initiating events before the unscreened list of components selected for fragility analysis is determined, this effort is included here. Normally this initial effort would include the identification of the seismic induced initiating events and the construction of the seismic sequence event tree. The remaining effort to develop the SQRVA event trees and fault trees is performed as part of Task 11.

### **2.7.3 Develop QRVA Seismic Equipment List**

Based on preliminary insights from the seismic hazard analysis (Task 1), the available QRVA model for internal events, and past SQRVAs of similar facilities, the systems analysts and fragility analysts develop a preliminary SEL. The list includes the equipment and systems required to provide protection for all seismically induced initiating events and the structures that house them. The list should include all components needed to mitigate seismic induced fires and floods and to prevent early containment failure in an earthquake. Equipment in non-safety systems are also placed on the list, if credit for these systems is to be included to achieve a safe shutdown. Components on a previously developed USI A-46 list or IPEEE Seismic Margin Assessment List, if available, should also be included.

Some equipment may be initially screened from the list if the conservative assumption is made that no credit will be taken for it performing its function. Equipment may also be removed from the list if a bounding analysis can demonstrate that the seismic LOFICF and AFRF are not sensitive to its seismic induced failure probability.

The initial list maybe augmented by the fragility analyst following the facility walkdown; e.g., to account for sources of fires, floods, and spatial interactions not already on the list.

#### **2.7.4 Conduct Facility Soil Failures Evaluation**

The potential for soil liquefaction, slope failures and damage to buried pipelines is assessed in this task. For most facilities, a review based on design and construction records is considered adequate to screen these types of failures out. A detailed analysis is needed only if soil failure is deemed significant. This task is usually carried out by specialist geotechnical engineers. To the extent that soil failures may impact facility structures housing QRVA components, this task should be performed early in the assessment. The structures and components of interest are provided by the output from Task 3.

#### **2.7.5 Perform Seismic Response Analysis (including developing floor spectra and structural response analyses)**

This task involves the derivation of the best estimate (or median-centered) seismic responses and their variability in the form of structural loads or floor response spectra. The loads and floor response spectra define the demand for which structures, systems and components are evaluated. These best estimate loads and floor response spectra and their variabilities are obtained through simulation probabilistic response analysis, by new deterministic analysis with estimated variability, or by scaling of the safe shutdown earthquake (SSE) responses and assigning variability. The ground response spectrum usually used as input for this analysis is the median spectral shape for a 10,000-year return period along with variability estimates. If available in time, results from the soil failures evaluation should also be considered.

#### **2.7.6 Perform Facility Walkdowns for Seismic QRVA**

The facility walkdown task of essential components is particularly emphasized in modern SQRVAs. The walkdown is conducted by a team of systems engineers and seismic fragility analysts. In order for the walkdown to be efficiently performed, review of the design basis, preparation of procedures, collection of design/qualification data, and technical orientation of the walkdown team is essential. It is also necessary that the floor spectra from Task 6 be available. All items on the initial QRVA components list must be physically examined for seismic vulnerabilities, if possible, and the location recorded. The emphasis is on compliance to screening caveats, anchorage and attachment of subassemblies and parts, and seismic spatial systems interactions, including the potential for seismic induced fires and floods. Items on the initial list may have to be subdivided or combined as appropriate for further assessment. Each component on the QRVA component list is to be assigned an initial screening value for its failure acceleration.

In addition to the list of structures and components, the systems analysts should also provide to the walkdown team a summary of the human actions following facility trip that are to be included in the SQRVA model and whose control stations are outside the



control room. The normal access paths for these actions should also be included. During the walkdown, the access paths are to be inspected to ensure that following an earthquake, the control stations can still be accessed.

### **2.7.7 Screen Components from Internal Events QRVA Equipment List**

Certain high capacity components may be screened out of the QRVA components list based on a review of seismic qualification criteria and qualification documents and the walkdown screening. The decision to screen components should be based on the seismic hazard curves and the associated unconditional failure rate of a component with a fragility corresponding to the screening acceleration, usually compared to the component high confidence in low probability of failure (HCLPF). The screening level must be chosen so that the contribution of screened components can be judged not significant to the final seismic LOFICF or AFRF. The screening HCLPF assigned to each QRVA component is done by seismic fragility analysts using earthquake experience and facility specific qualifications criteria. The contribution of screened components can be estimated by assuming a conservative representation of its mean fragility curve with the assigned HCLPF and convoluting this curve with the mean hazard curve to bound the frequency of seismic caused component failure.

### **2.7.8 Perform Relay Chatter Evaluation**

Relays whose chatter during an earthquake could result in adverse effects on facility safety must be identified and evaluated. The initial SEL is used as the basis for determining which relays to examine. The relays associated with components on the A-46 list may not be sufficiently complete. This evaluation may be done probabilistically or by deterministic methods. The identification of relays and the evaluations of the consequence of chatter on the electrical circuits are done by the systems analysts and electrical engineers. The seismic ruggedness of the relays, including the amplification of response through the cabinet into the relays, is evaluated by the seismic fragility analysts.

Often, rather than later, modeling the response of the systems to relay chatter, a deterministic screening is conducted to identify relays with high and low capacity and to determine if relay chatter is detrimental. Low ruggedness relays that can cause adverse effects are then usually replaced. Some relays with intermediate capacities may be modeled depending on their impact on the facility. Relay chatter that can lead to the spurious actuation of valves resulting in a bypass of fuel containment functions are of particular concern. The particular impacts on the facility of those relays that are to be modeled must be identified as part of this task. Since frequency screening is often a part of this evaluation, the results from the hazard curve analysis is also required for this task.

### **2.7.9 Develop Seismic Fragility Parameters for Screened-In Equipment**

This task is to estimate the conditional probabilities of structural or equipment failures for a given level of seismic ground motion for the screened-in components; i.e., from Task 8. Curves are developed using the fragility model whose parameters are the

median acceleration capacity ( $A_m$ ), and logarithmic standard deviations reflecting randomness in capacity ( $\beta_R$ ) and uncertainty in the median capacity; i.e.,  $\beta_U$ . In developing these curves, the focus is on the part of the curves between the HCLPF and the median capacity, since this region generally contributes most to seismic risk.

This task is performed by the seismic fragility analysts. The fragility analyst must also define the failure modes associated with the fragility curves and the location of the components. The fragility analyst must also specify any unique correlations between fragility curves so that the systems analyst can incorporate them into the seismic sequence models. Task 6 must be completed previously so that the floor response spectra are available.

### **2.7.10 Modify Internal Events QRVA Boolean Logic Models**

This task is to perform the remaining changes to the internal events accident sequence models to specialize them for seismic initiating events. This remaining effort is completed after the list of unscreened QRVA components, for which fragilities will be developed, is identified. It is important that the seismic sequence models reflect the actual failure mode assessed by the fragility analysts. To the extent that the failure modes are well known before completion of the fragility analysis, this effort can be started before the completion of Task 10. Those components that have been screened out, need not be included in the final seismic sequence models. Assumptions about how to include each seismic failure mode into the seismic sequence models should account for the dependencies between trains in multi-train systems, and for any other correlations identified by the fragility analysts. In addition to LOFICF, the seismic sequence model must be capable of computing AFRF. Therefore an effort is required as part of this task to adopt results from the Level 2 analysis performed for internal events so that it can be used for seismic events.

### **2.7.11 Seismic Events Human Reliability Analysis**

HFEs evaluated in the QRVA described in Sections 2.1 through 2.4 will need to be reviewed and reanalyzed to account for seismic event scenario impacts on HFE HEP PSFs. There may be cases where certain human actions credited in the other internal events QRVA may be determined to be infeasible due to structural failures and debris at the human action location. Additionally, some seismic event specific human actions may be identified associated with mitigating potential flood scenario impacts on the facility. SQRVA HRA applies the same general approach outlined for HRA in Sections 2.1 through 2.4; however, the PSFs for specific HFEs need to be re-evaluated for the seismic event scenarios. Additionally, new HFEs may be defined for seismic event scenarios to incorporate human actions to suppress or mitigate seismic event scenario impact and severity.

SQRVA scenario HFE HEP development is performed following the approach outlined in Sections 2.1 through 2.4, as supplemented by guidance in NUREG-1921 and EPRI 1025294.



### **2.7.12 Seismic Events Accident Sequence Analysis**

After the final adjustments have been made to the event trees and fault trees for the SQRVA, as outlined in Section 2.7.10, including the incorporation of the HRA outlined in Section 2.7.11, the seismic accident sequence analysis is performed following the same general approach as that outlined in Sections 2.1 through 2.4.

### **2.7.13 Seismic Events QRVA Data Analysis**

The data analyses for the SQRVA are conducted following the same general approach as has been outlined for the internal events QRVA in Sections 2.1 through 2.4. Input from the fragility analysis performed as described in Section 2.7.9 is applied to determine in which event sequences specific SSCs should be considered failed (a conditional failure probability of 1.00) for seismic event sequence quantification.

### **2.7.14 Seismic Events Risk Quantification**

This task involves assembling the results of the seismic hazard analysis, fragility analysis, and seismic sequence models, once completed, to estimate the LOFICF and FRF. Both point estimate results using only the mean hazard and fragility curves and the full uncertainty distributions are to be computed. The points estimate results may be used to identify the dominant seismic sequences and to perform uncertainty analysis involving just the frequency of these dominant sequences. The risk quantification must consider both seismic failures and non-seismic failures, and the applicable operator actions.

### **2.7.15 Seismic Events Risk Uncertainty Analysis**

SQRVA risk uncertainty analysis is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

### **2.7.16 Risk Results Presentation and Interpretation**

SQRVA risk results presentation and interpretation is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

### **2.7.17 QRVA Vulnerability Assessment**

SQRVA risk vulnerability assessment is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

#### **2.7.17.1 *Risk Decomposition (risk by initiating event category, specific initiating events, specific event sequences)***

SQRVA risk decomposition is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

### **2.7.17.2 Risk Importance Measure Determination and Evaluation for Event Tree Split Fractions and Fault Tree Basic Events**

SQRVA risk importance measure determination and evaluation is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

### **2.7.17.3 Risk Contribution Sensitivity Analysis**

SQRVA risk contribution sensitivity analysis is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

### **2.7.18 Vulnerability Assessment Results Presentation and Interpretation**

SQRVA vulnerability assessment results presentation and interpretation is conducted using the same approach as that outlined in Sections 2.1 through 2.4.

## **2.8 - External Flooding QRVA (including tsunami and heavy precipitation)**

External flooding QRVA is conducted using the same general approach as has been described herein for internal flooding (Section 2.5). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of external flooding scenarios on facility structural integrity and human action PSFs. Included in this analysis is the impact of potential tsunamis on the RHFSF. However, it is anticipated, at least preliminarily, that any tsunamis large enough to be expected to have any risk-significant impact on the RHFSF and associated LOFICF and AFRF will have direct impacts on loss of life and injury to the general public of Oahu far greater than any associated impacts from potential fuel release at the RHFSF.

## **2.9 - External Fire QRVA**

External fire QRVA is conducted using the same general approach as has been described herein for internal fires (Section 2.6). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of external fire scenarios on facility structural integrity and human action PSFs.

## **2.10 - Other External Events QRVA**

Analysis of other external events hazards should be included in a comprehensive facility QRVA.

### **2.10.1 High Winds and Storms (e.g., tornados, hurricanes, etc.)**

High winds and storms QRVA is conducted using the same general approach as has been described herein for internal events (Sections 2.1 through 2.4). The major differences are in the evaluation of initiating events, the determination of initiating event



frequencies, and the potential impact of high wind and storm scenarios on facility structural integrity and human action PSFs.

### **2.10.2 Landslides (including mudslides, sinkholes, etc.)**

Landslides QRVA is conducted using the same general approach as has been described herein for internal events (Sections 2.1 through 2.4). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of landslide, mudslide, and sinkhole scenarios on facility structural integrity and human action PSFs.

### **2.10.3 Proximity Transportation Accidents (e.g., aircraft crash, external hazardous material spill or release, etc.)**

Proximity transportation accident QRVA is conducted using the same general approach as has been described herein for internal events (Sections 2.1 through 2.4). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of proximity transportation accident scenarios on facility structural integrity and human action PSFs.

For some sources of acute release, such as aircraft or internal rail car impacts with tanks or piping, it is likely that tank and/or piping finite element analysis FEA will be required to support realistic predictions of fuel release from such event scenarios.

### **2.10.4 Extreme Weather (e.g., high temperature, etc.) -**

Extreme weather QRVA is conducted using the same general approach as has been described herein for internal events (Sections 2.1 through 2.4). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of extreme weather scenarios on human action PSFs.

### **2.10.5 Other Facility-Specific Hazards**

During the course of any thorough facility QRVA, facility-specific hazards other than those previously discussed herein are frequently identified that could be risk-significant. For example, the RHFSF has an internal rail system in its tunnels designed to support transport of heavy loads throughout the facility. Derailing of the system rail cars and/or associated heavy loads could result in impact events involving other critical facility SSCs (e.g., fuel piping). Consideration of such hazards should be included in any comprehensive facility QRVA. Other facility-specific hazards QRVA is conducted using the same general approach as has been described herein for internal events (Sections 2.1 through 2.4). The major differences are in the evaluation of initiating events, the determination of initiating event frequencies, and the potential impact of other facility-specific hazard scenarios on facility structural integrity and human action PSFs.

### **2.11 - Environmental Transport and Consequence Analysis for Levels 3+ QRVA (optional)**

In the Phase 2 QRVA project, there is no current plan to conduct Level 3+ analyses that will require associated environmental transport or consequence analysis within the AOC Section 8 activities. The current plan is to communicate Level 2 QRVA fuel release frequency and probability results information to the technical teams addressing AOC Sections 6 and 7 and to work with those teams to help them address, evaluate, and report potential impacts on the water table; e.g., specific impacts on the Red Hill Water Shaft.

### **2.12 - Risk Management Decision Support Metric Development and Analysis (optional)**

Facility QRVA results can be extended to develop risk-informed performance-based asset management utility functions and decision-support metrics. Such functions and metrics can provide valuable decision-making support for facility improvement options involving facility design changes and/or revisions to facility operations, maintenance, and/or testing procedures and policies. In the Phase 2 QRVA project, there are no current plans to develop such utility functions or metrics, or to apply such functions or metrics in facility alternatives analyses.



## **3. QRVA Proposed Work Breakdown Structure (WBS)**

---

A proposed preliminary work breakdown structure for Phase 2 of the project are presented in Table 3-1.

### **3.1 Proposed Project Phases**

It is recommended that the Phase 2 QRVA project be pursued in sub-phases.

#### **3.1.1 Level 1 QRVA for Internal Events**

It is recommended that the Level 1 QRVA for internal events excluding internal flooding and fire be performed in Sub-Phase 1.

#### **3.1.2 Level 2 QRVA for Internal Events**

It is recommended that the Level 2 QRVA for internal events excluding internal flooding and fire be performed in Sub-Phase 1.

#### **3.1.3 Level 2 QRVA for Flooding and Fire**

It is recommended that the Levels 1 and 2 QRVA for internal and external flooding and fire be performed in Sub-Phase 2.

#### **3.1.4 Level 2 QRVA for Seismic Events**

It is recommended that the Levels 1 and 2 QRVA for seismic events be performed in Sub-Phase 3.

#### **3.1.5 Level 2 QRVA for Other External Events**

It is recommended that the Levels 1 and 2 QRVA for other external events be performed in Sub-Phase 4.

### **3.2 Proposed Task WBS**

Table 3-1 presents a proposed WBS for the Phase 2 QRVA project.





**Table 3-1. Phase 2 Preliminary WBS (Continued).**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	1	17	All Sub-Phase 1	Not Applicable	QRVA Peer Review Finding and Observation Resolution Support
2	1	18	All Sub-Phase 1	Not Applicable	Project Management, Overview, and Quality Control
2	2	19	Internal Flood	Not Applicable	Events Scope Determination
2	2	20	Internal Flood	Not Applicable	Facility Partitioning
2	2	21	Internal Flood	Not Applicable	Flood Source Identification and Characterization
2	2	22	Internal Flood	Not Applicable	Flood-Induced Initiating Event Analysis
2	2	23	Internal Flood	Not Applicable	Scenario Development
2	2	24	Internal Flood	Not Applicable	Human Reliability Analysis
2	2	25	Internal Flood	Not Applicable	Accident Sequence Analysis
2	2	26	Internal Flood	Not Applicable	Data Analysis
2	2	27	Internal Flood	Not Applicable	Risk Quantification
2	2	28	Internal Flood	Not Applicable	Risk Uncertainty Analysis
2	2	29	Internal Flood	Not Applicable	Risk Results Presentation and Interpretation
2	2	30	Internal Flood	Not Applicable	Risk Vulnerability Assessment
2	2	31	Internal Flood	Not Applicable	QRVA Documentation
2	2	32	External Flood	Not Applicable	Events Scope Determination
2	2	33	External Flood	Not Applicable	Facility Partitioning
2	2	34	External Flood	Not Applicable	Flood Source Identification and Characterization





**Table 3-1. Phase 2 Preliminary WBS (Continued)**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	2	54	Internal Fire	Not Applicable	Quantitative Screening Phase 1
2	2	55	Internal Fire	Not Applicable	Scoping Fire Modeling
2	2	56	Internal Fire	Not Applicable	Quantitative Screening Phase 2
2	2	57	Internal Fire	Not Applicable	Detailed Circuit Failure Analysis
2	2	58	Internal Fire	Not Applicable	Circuit Failure Mode and Likelihood Analysis
2	2	59	Internal Fire	Not Applicable	Detailed Fire Modeling
2	2	60	Internal Fire	Not Applicable	Post-Fire HRA Detailed and Recovery Assessment
2	2	61	Internal Fire	Not Applicable	Seismic-Fire Interactions Assessment
2	2	62	Internal Fire	Not Applicable	Fire Risk Quantification
2	2	63	Internal Fire	Not Applicable	Uncertainty and Sensitivity Analyses
2	2	64	Internal Fire	Not Applicable	QRVA Documentation
2	2	65	External Fire	Not Applicable	Plant Walkdowns
2	2	66	External Fire	Not Applicable	QRVA Database Development
2	2	67	External Fire	Not Applicable	Plant Boundary and Partitioning Definition
2	2	68	External Fire	Not Applicable	QRVA Component Selection
2	2	69	External Fire	Not Applicable	QRVA Cable Selection
2	2	70	External Fire	Not Applicable	Qualitative Screening
2	2	71	External Fire	Not Applicable	Fire-Induced Risk Model Development
2	2	72	External Fire	Not Applicable	Fire Ignition Frequencies Development

**Table 3-1. Phase 2 Preliminary WBS (Continued)**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	2	73	External Fire	Not Applicable	Post-Fire HRA Screening Assessment
2	2	74	External Fire	Not Applicable	Quantitative Screening Phase 1
2	2	75	External Fire	Not Applicable	Scoping Fire Modeling
2	2	76	External Fire	Not Applicable	Quantitative Screening Phase 2
2	2	77	External Fire	Not Applicable	Detailed Circuit Failure Analysis
2	2	78	External Fire	Not Applicable	Circuit Failure Mode and Likelihood Analysis
2	2	79	External Fire	Not Applicable	Detailed Fire Modeling
2	2	80	External Fire	Not Applicable	Post-Fire HRA Detailed and Recovery Assessment
2	2	81	External Fire	Not Applicable	Seismic-Fire Interactions Assessment
2	2	82	External Fire	Not Applicable	Fire Risk Quantification
2	2	83	External Fire	Not Applicable	Uncertainty and Sensitivity Analyses
2	2	84	External Fire	Not Applicable	QRVA Documentation
2	2	85	All Sub-Phase 2	Not Applicable	QRVA Peer Review Support
2	2	86	All Sub-Phase 2	Not Applicable	QRVA Peer Review Finding and Observation Resolution Support
2	2	87	All Sub-Phase 2	Not Applicable	Project Management, Overview, and Quality Control
2	3	88	Seismic Events	Not Applicable	Develop Facility-Specific Risk Hazard Curves
2	3	89	Seismic Events	Not Applicable	Perform Initial Modification to Internal Events Systems Models
2	3	90	Seismic Events	Not Applicable	Develop Seismic Equipment List (SEL)



**Table 3-1. Phase 2 Preliminary WBS (Continued).**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	3	91	Seismic Events	Not Applicable	Conduct Soil Failures Evaluation
2	3	92	Seismic Events	Not Applicable	Perform Seismic Response Analysis
2	3	93	Seismic Events	Not Applicable	Perform Facility Walkdowns
2	3	94	Seismic Events	Not Applicable	Screen Components from SEL
2	3	95	Seismic Events	Not Applicable	Perform Relay Chatter Evaluation
2	3	96	Seismic Events	Not Applicable	Develop Seismic Fragility Parameters
2	3	97	Seismic Events	Not Applicable	Modify Internal Events QRVA Boolean Logic Models
2	3	98	Seismic Events	Not Applicable	Human Reliability Analysis
2	3	99	Seismic Events	Not Applicable	Accident Sequence Analysis
2	3	100	Seismic Events	Not Applicable	Data Analysis
2	3	101	Seismic Events	Not Applicable	Risk Quantification
2	3	102	Seismic Events	Not Applicable	Risk Uncertainty Analysis
2	3	103	Seismic Events	Not Applicable	Risk Results Presentation and Interpretation
2	3	104	Seismic Events	Not Applicable	Risk Vulnerability Assessment
2	3	105	Seismic Events	Not Applicable	QRVA Documentation
2	3	106	All Sub-Phase 3	Not Applicable	QRVA Peer Review Support
2	3	107	All Sub-Phase 3	Not Applicable	QRVA Peer Review Finding and Observation Resolution Support
2	3	108	All Sub-Phase 3	Not Applicable	Project Management, Overview, and Quality Control

**Table 3-1. Phase 2 Preliminary WBS (Continued)**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	4	109	Other External Events	High Winds and Storms	Initiating Events Analysis
2	4	110	Other External Events	High Winds and Storms	Event Sequence Analysis
2	4	111	Other External Events	High Winds and Storms	Systems Analysis
2	4	112	Other External Events	High Winds and Storms	Human Reliability Analysis
2	4	113	Other External Events	High Winds and Storms	Data Analysis
2	4	114	Other External Events	High Winds and Storms	Event Sequence Quantification
2	4	115	Other External Events	High Winds and Storms	Acute Release from Accident Sequences Analysis
2	4	116	Other External Events	High Winds and Storms	Risk Results Presentation and Interpretation
2	4	117	Other External Events	High Winds and Storms	Risk Vulnerability Assessment
2	4	118	Other External Events	High Winds and Storms	QRVA Documentation
2	4	119	Other External Events	Landslides	Initiating Events Analysis
2	4	120	Other External Events	Landslides	Event Sequence Analysis
2	4	121	Other External Events	Landslides	Systems Analysis
2	4	122	Other External Events	Landslides	Human Reliability Analysis
2	4	123	Other External Events	Landslides	Data Analysis
2	4	124	Other External Events	Landslides	Event Sequence Quantification
2	4	125	Other External Events	Landslides	Acute Release from Accident Sequences Analysis
2	4	126	Other External Events	Landslides	Risk Results Presentation and Interpretation
2	4	127	Other External Events	Landslides	Risk Vulnerability Assessment



**Table 3-1. Phase 2 Preliminary WBS (Continued).**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	4	128	Other External Events	Landslides	QRVA Documentation
2	4	129	Other External Events	Proximity Transportation Accidents	Initiating Events Analysis
2	4	130	Other External Events	Proximity Transportation Accidents	Event Sequence Analysis
2	4	131	Other External Events	Proximity Transportation Accidents	Systems Analysis
2	4	132	Other External Events	Proximity Transportation Accidents	Human Reliability Analysis
2	4	133	Other External Events	Proximity Transportation Accidents	Data Analysis
2	4	134	Other External Events	Proximity Transportation Accidents	Event Sequence Quantification
2	4	135	Other External Events	Proximity Transportation Accidents	Acute Release from Accident Sequences Analysis
2	4	136	Other External Events	Proximity Transportation Accidents	Risk Results Presentation and Interpretation
2	4	137	Other External Events	Proximity Transportation Accidents	Risk Vulnerability Assessment
2	4	138	Other External Events	Proximity Transportation Accidents	QRVA Documentation
2	4	139	Other External Events	Extreme Weather	Initiating Events Analysis

**Table 3-1. Phase 2 Preliminary WBS (Continued)**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	4	140	Other External Events	Extreme Weather	Event Sequence Analysis
2	4	141	Other External Events	Extreme Weather	Systems Analysis
2	4	142	Other External Events	Extreme Weather	Human Reliability Analysis
2	4	143	Other External Events	Extreme Weather	Data Analysis
2	4	144	Other External Events	Extreme Weather	Event Sequence Quantification
2	4	145	Other External Events	Extreme Weather	Acute Release from Accident Sequences Analysis
2	4	146	Other External Events	Extreme Weather	Risk Results Presentation and Interpretation
2	4	147	Other External Events	Extreme Weather	Risk Vulnerability Assessment
2	4	148	Other External Events	Extreme Weather	QRVA Documentation
2	4	149	Other External Events	Other Facility-Specific Hazards	Initiating Events Analysis
2	4	150	Other External Events	Other Facility-Specific Hazards	Event Sequence Analysis
2	4	151	Other External Events	Other Facility-Specific Hazards	Systems Analysis
2	4	152	Other External Events	Other Facility-Specific Hazards	Human Reliability Analysis
2	4	153	Other External Events	Other Facility-Specific Hazards	Data Analysis
2	4	154	Other External Events	Other Facility-Specific Hazards	Event Sequence Quantification



**Table 3-1. Phase 2 Preliminary WBS (Continued).**

Project Phase Number	Project Sub-Phase Number	Project Task Number	QRVA Hazard Category	QRVA Hazard Sub-Category	Task Title
2	4	155	Other External Events	Other Facility-Specific Hazards	Acute Release from Accident Sequences Analysis
2	4	156	Other External Events	Other Facility-Specific Hazards	Risk Results Presentation and Interpretation
2	4	157	Other External Events	Other Facility-Specific Hazards	Risk Vulnerability Assessment
2	4	158	Other External Events	Other Facility-Specific Hazards	QRVA Documentation
2	4	159	All	Not Applicable	Total Aggregate Risk Consolidation
2	4	160	All	Not Applicable	Risk Results Presentation and Interpretation
2	4	161	All	Not Applicable	Risk Vulnerability Assessment
2	4	162	All	Not Applicable	QRVA Documentation
2	4	163	All Sub-Phase 4	Not Applicable	QRVA Peer Review Support
2	4	164	All Sub-Phase 4	Not Applicable	QRVA Peer Review Finding and Observation Resolution Support
2	4	165	All Sub-Phase 4	Not Applicable	Project Management, Overview, and Quality Control

## **4. QRVA Project Management Considerations -**

---

Considerations and recommendations for project management in Phase 2 are presented in this section. For Phase 2, it is recommended that a project manager (PM) be assigned as the single point of contact for all project activities. Included in this function activity will be development of the project plan, project task plans, and milestone scheduling.

The project plan will identify the overall Phase 2 project scope, project quality requirements, roles and responsibilities, internal/external project interfaces, design input requirements, interfacing RHFSF procedures, project deliverables, performance measures for the project, requirements for project review(s), project software and associated software requirements, project schedule, and any associated project instructions and training requirements.

It is recommended that the draft project plan be reviewed during the Phase 2 project kickoff meeting. Also, during the project kickoff meeting, the PM will coordinate personnel mobilization for the project. As part of the project schedule and activities, the PM will schedule and coordinate all interim and final reviews for project deliverables, to include review comment resolution and incorporation. The PM will coordinate status reports, project conference calls, and project status meetings.

The project plan will define the quality assurance requirements for this project. Project work results will be documented in a format that facilitates effective and efficient review by an independent reviewer. The scope and content of the quality assurance will be sufficient to satisfy Capability Category II requirements of the PRA Standard.

### **Bases and Assumptions (applicable to all sub-tasks of project management)**

- The project plan and individual task plans will be submitted to NAVFAC for review and approval.
- One cycle of review and comment incorporation is assumed for all project deliverables.

### **Recommended Deliverables of Project Management**

- Project Plan
- Project Schedule
- Task Plans, as Applicable
- Kickoff Meeting and Project Status Meeting Support



- Monthly Status Reports
- Weekly E-Mail Reports and Project Leadership Conference Calls, or More Frequently as Necessary, with a Status and Action Item Tracking Report

These deliverables include a project work breakdown structure, as discussed in Section 3 of this work plan, and a project schedule. The WBS will be defined in the project plan, and is anticipated to closely follow the tasks as described in Sections 2 and 3 of this work plan. The task structure will be sufficiently detailed to establish accurate project cost plans and schedule. The QRVA work breakdown structure will incorporate all Navy, contractor, subcontractor, and other applicable organization tasks.

The Phase 2 project manager will develop and maintain a project schedule. The project schedule will be based on the WBS, incorporating all Navy, contractors, subcontractors, and other organizations. The project schedule will be sufficiently detailed to demonstrate project critical path and evaluate changes to critical path in the event of schedule advances or delays.

It is recommended that project administration and controls be established prior to or during the Phase 2 project kickoff meeting as part of the project ground rules. These will support delivery of high quality products on time and within budget. In addition to the project management approach discussed above, additional features of the project plan approach are discussed in the remainder of this section.

The scope and schedule for this project are sufficient to warrant a project controls officer. The project controls officer is a senior manager who can monitor progress and provide senior mentoring advice such that project delays are minimized. The project controls officer will provide input to the weekly status meetings. Additionally, it is recommended that a senior oversight director be assigned for the project. The senior oversight director will review project management and project controls activities throughout the project to ensure compliance with the project work plan and to ensure that high-quality deliverables are being prepared and issued as part of this project.

## **5. QRVA Quality Assurance Considerations**

---

This section describes the recommended quality assurance and quality controls practices to be applied to the QRVA Phase 2 project.

### **5.1 ISO 9001 Quality Assurance**

Work on this project is recommended to be conducted following the standard ISO 9001 Quality Management System. Experience has shown that this approach provides sufficient quality controls and assurance of product quality for high-quality analyses and evaluations, while also providing a significant basis for cost savings.

The Phase 2 QRVA project should commit to operate consistent with applicable environmental legislation and regulations and to provide services consistent with international standards developed to avoid, reduce, or control pollution to the environment.

The Phase 2 QRVA project should monitor performance as an ongoing activity, to strive for continual improvement, and to provide a framework for establishing and reviewing quality and environmental objectives and targets.

### **5.2 ASME/American Nuclear Society (ANS) Standard RA-S-2008 - (with current addenda) Capability Categories**

It is recommended that the Phase 2 QRVA project be designed to achieve and clearly document compliance with Capability Category II high level and supporting level requirements stipulated in ASME/ANS Standard RA-S-2008 with updated addenda through RA-Sb-2013.



## **6. QRVA Software Considerations**

---

A number of commercial and government software packages exist, which are designed to support QRVA of complex facilities. Examples of these software packages are, as follows:

- RISKMAN
- CAFTA
- WinNUPRA
- Risk Spectrum
- SAPHIRE
- BlockSim
- ExtendSim
- Maros
- Miriam
- Optimise
- RAMCAP
- @Risk

As it supports comprehensive full-scope application of event tree analysis, fault tree analysis, initiating events analysis, data analysis (including Bayesian updating), uncertainty propagation, and risk decomposition capabilities, it is recommended that the RISKMAN software package be considered as a primary selection choice for risk assessment software application on this project.

Also, there are existing software packages designed to support specific areas of QRVA technical tasks. For example, the EPRI HRA Calculator software is a convenient tool frequently applied to HRA for QRVA.

## **7. References**

---

1. United States Navy Contract N62742-14-D-1884, Task Order 0028, 10 March 2016.
2. 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>).
3. 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.
4. OREDA 2015 Handbook, Offshore and Onshore Reliability Database, 2015.
5. NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, 2007.
6. Fault Tree Handbook, NUREG-0492, 1981.
7. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, MIL-STD-1629A, 1980.
8. Swain, A. D., and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, 1983.
9. An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, 1992, EPRI-TR-100259.
10. Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Revision 1, May 2000, U.S. Nuclear Regulatory Commission, NUREG-1624.
11. Systematic Human Action Reliability Procedure, 1984, EPRI NP-3583.
12. SHARP1 – A Revised Systematic Human Action Reliability Procedure, 1990, EPRI NP-7183-SL.
13. Swain, A. D., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, 1987.
14. Kaplan, S., "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems (preprint), 1981.
15. Chhikara, R. S., and J. L. Folks, "The Inverse Gaussian Distribution as a Lifetime Model," Technometrics, Vol. 19, pp. 461–468, 1977.



16. Hahn, G. J., and S. S. Shapiro, Statistical Models in Engineering, John Wiley & Sons, Inc., New York, Chapter B, 1967.
17. 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.
18. Barlow, R. E., and F. Proschan, Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York, 1975.
19. Lapedes, 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.
20. 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.
21. 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.
22. Green, A. E., and A. J. Bourne, Reliability Technology, Wiley-Interscience, New York, 1972.
23. Hald, A., Statistical Theory with Engineering Applications, John Wiley & Sons, Inc., New York, 1952.
24. 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.
25. Parry, T. W., and P. W. Winter, "Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis," Nuclear Safety, Vol. 22, pp. 28–42, 1981.
26. Bayes, T., "Essay Toward Solving a Problem in the Doctrine of Chances" (reprinted), Biometrika, Vol. 45, pp. 293–315, 1958.
27. 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.
28. Martz, H. F., and R. Waller, Bayesian Reliability Analysis, John Wiley & Sons, New York, 1982.
29. Jeffreys, H., Theory of Probability, 3<sup>rd</sup> ed., Clarendon Press, Oxford, England, 1961.
30. 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.

31. Smith, A. M., and I. A. Watson, "Common Cause Failures – A Dilemma in Perspective," Reliability Engineering, Vol. 1, pp. 127–142, 1980.
32. 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.
33. 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.
34. 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.
35. Parry, G. W., "Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty," 1984 Annual Meeting of the Society for Risk Analysis.
36. 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.
37. 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.
38. Mosleh, A., "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data," Nuclear Engineering and Design, August 1985.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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, 1978.



44. Worrell, R. B., and O. W. Stack, "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, Calif., pp. 363–366, 1981.
45. 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.
46. 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.
47. Putney, B. F., WAMCOM, Common Cause Methodologies Using Large Fault Trees, NP-1851, Electric Power Research Institute, Palo Alto, California, 1981.
48. Fussell, J. B., "How to Hand Calculate System Reliability Characteristics," IEEE Transactions of Reliability, Vol. R-24, No. 3, 1975.
49. Birnbaum, Z. W., "On the Importance of Different Components in a Multi-System in Multivariate Analysis," Academic Press, New York, 1969.
50. Lambert, H. E., and F. M. Gilman, "The Importance Computer Code," ERDA Report UCRL-79269, Lawrence Livermore National Laboratory, Livermore, California, 1977.
51. 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.
52. Lambert, H. E., "Fault Trees for Decision-Making in Systems Analysis," Ph.D. thesis, UCRL-51829, Lawrence Livermore National Laboratory, Livermore, California, 1975.
53. Apostolakis, G. E., and S. Kaplan, "Pitfalls in Risk Calculations," Reliability Engineering, Vol. 2, pp. 135–145, 1981.
54. 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, pp. 77–100 (1975).
55. Alan D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, February 1987.
56. Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, American Society of Mechanical Engineers, April 5, 2002, and Addenda ASME RA-Sa-2003, December 5, 2003.

- 
57. Kaplan, "On a 'Two-Stage' Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems, Volume PAS-102, 1983, pp. 195–202.
  58. Fire PRA Implementation Guide, EPRI, TR-105928, 1995.
  59. Fire Event Database and Generic Ignition Frequency Model for U.S. Nuclear Power Plants, EPRI, TR-1003111, 2001.
  60. An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide 1.174, Revision 1, November 2002.

DRAFT



## **Appendix A. RHFSF QRVA Initial Information Item Request**

---

The following information items were requested from and discussed with the Navy during Phase 1 of this project:

1. RHFSF general site and facility layout and arrangement drawings.
2. A comprehensive set of RHFSF P&IDs 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 ASME code information for tanks.
7. Structure and component seismic design criteria.
8. RHFSF 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., 2011 to present) of facility operation.
11. A list of all historical incidents involving hydrocarbon or other fuel or material release from facility tanks and systems, 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.
12. Loss of fuel inventory incident reports.

**DRAFT, PREDECISIONAL FOR DISCUSSION PURPOSES ONLY,  
DO NOT CITE OR QUOTE**

*Appendix A. RHFSF QRVA Initial Information Item Request*

---

13. The full text of any previous facility risk and vulnerability assessments and other risk assessment reports performed for the RHFSF, along with all associated appendices, models, and databases.
14. Other documentation deemed pertinent to RHFSF QRVA, as determined by NAVFAC and Navy Fuel Department staff.

DRAFT



## **Appendix B. RHFSF QRVA – Requested Navy Support Interfaces and Activities**

---

It is recommended that the Phase 2 project manager conduct a bi-weekly project status conference call where progress, status, open issues, schedule, and cost performance will be discussed. The Phase 2 project manager will provide a project status summary and action item tracking report one day in advance of each weekly status meeting. Successful implementation of Phase 2 will require close communication with and some support from Navy organizations and offices. Specifically, it is recommended that close lines of communication be established among the following:

- Phase 2 QRVA Project Director (assumed to be a member of the NAVFAC, Pacific staff)
- Phase 2 QRVA Project Manager (Phase 2 QRVA Consulting Firm; e.g., ABS Consulting Senior Consultant Mr. James K. Liming)
- Navy Red Hill Regional Program Director, Code N4
- Naval Supply Systems Command Fleet Logistics Center, Joint Base Pearl Harbor Hickam Fuel Department Head, Code 700, or Operations designee
- Others, as Directed by NAVFAC, Pacific

These lines of communication will be critical to the effective and efficient implementation of Phase 2 QRVA activities, particularly those activities associated with information collection and familiarization and with RHFSF walkdowns. As there will likely be several detailed RHFSF walkdowns required to complete all portions of the QRVA, it will be critical to coordinate with the Fuel Department (Code 700) to arrange for escorts in the facility.

## **Appendix C. Bibliography**

---

A list of useful QRVA information sources that were not called out as specific references in the body of this work plan is presented in the following bibliography:

1. PSA Procedures Guide, NUREG/CR-2815, 1985.
2. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150, 1990.
3. Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-S-2008 with update addenda through RA-Sb-2013, 2013.
4. Fire PRA Methodology for Nuclear Power Facilities: Detailed Methodology, Final Report, (NUREG/CR-6850, EPRI 1011989), 2005, with Supplements and Errata, 2010.
5. Seismic Evaluation Guidance, Screening, Prioritization and Implementation Details (SPID) for the Resolution of Fukushima Near-Term Task Force Recommendation 2.1: Seismic, EPRI 1025287, 2013.
6. Seismic Probabilistic Risk Assessment Implementation Guide, EPRI 1002989, 2003.
7. Uncertainty Analysis: "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making," NUREG-1855, Revision 1, 2013.
8. McCormick, N. J., "Reliability and Risk Analysis," Academic Press, New York, NY, 1981 (ISBN 0-12-482360-2).
9. Henley, E. J., and H. Kumamoto, "Reliability Engineering and Risk Assessment," Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.
10. Lloyd, David K., and Myron Lipow, "Reliability: Management, Methods, and Mathematics," Second Edition, ASQC, Milwaukee, WI, 1984.
11. Kumamoto, H., and E. J. Henley, "Probabilistic Risk Assessment and Management for Engineers and Scientists," Second Edition, IEEE Press, Piscataway, NJ, 1996.
12. Modarres, Mohammad, Mark Kaminskiy, and Vasilii Krivtsov, "Reliability Engineering and Risk Analysis," Marcel Dekker, Inc., New York, NY, 1999.
13. Garrick, B. John, et al., "Quantifying and Controlling Catastrophic Risks," Elsevier, London, United Kingdom, 2008.
14. Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition, American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), October 1999.



15. Layer of Protection Analysis, Simplified Process Risk Assessment, American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), 2001.
16. Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), Wiley, 2015.
17. API RP 580, Risk-Based Inspection, American Petroleum Institute, 2016.
18. API RP 581, Risk-Based Inspection Technology, American Petroleum Institute, 2008.
19. Nuclear Power Experience, S. M. Stoller Corporation, updated monthly.
20. 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.

DRAFT

## Appendix D. Glossary

This glossary is an adaptation of information found in NUREG-2122.

### D.1. Terms and Definitions

Table D-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 D-1. Terms and Definitions**

Term and Definition	Discussion
<b>Accident Consequence</b>	
The health effects or the economic costs resulting from a facility accident. <i>(see Health Effects, Accident Consequence Analysis)</i>	In a Level 3 QRVA, the consequences can be measured by health effects and economic costs resulting from a nuclear accident. 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 nuclear 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) radiation doses 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).
<b>Accident Consequence Analysis</b>	
The calculation of the extent of health effects or the economic costs resulting from a facility accident. <i>(see Accident Consequence)</i>	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 nuclear 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?
<b>Accident Event Sequence</b>	
<i>(see Accident Sequence)</i>	The term accident event sequence has the same meaning as accident sequence and is defined under "Accident Sequence."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Accident Mitigation</b>	
<p>Actions taken to reduce the severity of an accident. (<i>see Accident Prevention, Emergency Preparedness, Emergency Response</i>)</p>	<p>In a QRVA, accident mitigation typically refers to actions taken to reduce the severity of an accident once core damage has started, as opposed to actions to prevent a core damage event from occurring. Successful accident mitigation implies that a core damage event occurred, but its consequences were minimized.</p> <p>Some strategies used for accident mitigation include preventing fission product releases by maintaining barrier integrity, or reducing fission product releases by filtration.</p> <p>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.</p>
<b>Accident Mitigation</b>	
<p>Actions taken to reduce the severity of an accident. (<i>see Accident Prevention, Emergency Preparedness, Emergency Response</i>)</p>	<p>In a QRVA, accident mitigation typically refers to actions taken to reduce the severity of an accident once core damage has started, as opposed to actions to prevent a core damage event from occurring. Successful accident mitigation implies that a core damage event occurred, but its consequences were minimized.</p> <p>Some strategies used for accident mitigation include preventing fission product releases by maintaining barrier integrity, or reducing fission product releases by filtration.</p> <p>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.</p>
<b>Accident Precursor, Precursor Event</b>	
<p>A change in facility status that could lead to core damage accidents.</p>	<p>A QRVA is used to evaluate an event to determine if it will be considered an accident precursor. A 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 damage to the reactor fuel." 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."</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Accident Prevention</b>	
<p>Actions taken to reduce the likelihood of an accident. <i>(see Accident Mitigation )</i></p>	<p>In a QRVA, accident prevention typically refers to actions taken to prevent a core damage event from occurring, as opposed to reducing the severity once core damage has started. Successful accident prevention implies that a core damage event does not occur.</p> <p>Some strategies used for accident prevention include: physical protection, maintaining facility stable operation, reactor protective systems, and maintaining barrier integrity.</p>
<b>Accident Progression Event Tree</b>	
<p>A logic diagram that begins with the onset of core damage and identifies the potential responses of the containment and associated equipment, as well as operator actions, to the severe accident loads. <i>(see Bridge Tree, Containment Event Tree, Event Tree)</i></p>	<p>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.</p>
<b>Accident Scenario</b>	
<p><i>(see Accident Sequence)</i></p>	<p>The term accident scenario has the same meaning as accident sequence and is defined under "Accident Sequence."</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Accident Sequence Analysis, Event Sequence Analysis</b>	
The process used to determine the series of events that can lead to undesired consequences. (see Accident Sequence)	<p>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., core damage 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.</p> <p>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 core damage, and the terminology “event” does not necessarily reflect a negative outcome such as core damage.</p> <p>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 core damage or large early release.”</p>
<b>Accident Sequence Class, Accident Sequence Group, Accident Sequence Type, Event Sequence Class, Event Sequence Group, Event Sequence Type</b>	
A grouping of accident sequences with similar characteristics or end states. (see Accident Sequence)	<p>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 (e.g., loss-of-coolant accidents, loss of offsite power (LOOP), and loss of heat removal or similar safety function responses. The purpose for combining like sequences is generally done to understand the type of sequences contributing to the risk.</p> <p>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.</p>
<b>Accident Sequence Frequency</b>	
(see Frequency)	Accident sequence frequency is a type of frequency used in QRVA and is defined in the discussion under “Frequency.”
<b>Accident Sequence Group</b>	
(see Accident Sequence Class)	The term accident sequence group has the same meaning as accident sequence class and is defined under “Accident Sequence Class.”
<b>Accident Sequence Type</b>	

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<i>(see Accident Sequence Class)</i>	The term accident sequence type has the same meaning as accident sequence class and is defined under "Accident Sequence Class."
<b>Accident Sequence, Accident Event Sequence, Accident Scenario, Event Sequence, Event Scenario, Event Tree Sequence</b>	
A series of events that can lead to undesired consequences. <i>(see Accident Sequence Analysis, Severe Accident, End State, Event Tree)</i>	<p>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 core damage. If the end state involves extensive core damage and radioactive material release into the reactor vessel and 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.</p> <p>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.</p> <p>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., core damage or large early release)."</p> <p>The following figure is an example of an accident sequence:</p> <div style="text-align: center;"> </div>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Active Component</b>	
A component whose operation or function depends on an external source of power (e.g., air, electrical, hydraulic). <i>(see Passive Component)</i>	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)."  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.  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.  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.
<b>Acute Exposure</b>	
<i>(see Exposure)</i>	The term acute exposure is a type of exposure and is defined in the discussion under "Exposure."
<b>Acute Fuel Release</b>	
<i>(see Radioactive Material Release)</i>	The term acute fuel release is a type of radioactive material release and is defined in the discussion under "Radioactive Material Release."
<b>Acute Fuel Release Frequency</b>	
<i>(see Frequency)</i>	The term acute fuel release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency."
<b>Acute Fuel Release Frequency Analysis</b>	
<i>(see Radioactive Material Release Frequency Analysis)</i>	The term acute fuel release frequency analysis is a type of radioactive material release frequency analysis and is defined under "Radioactive Material Release Frequency Analysis."
<b>Acute Health Effects</b>	
<i>(see Health Effects)</i>	The term acute health effect refers to a type of health effect and is defined in the discussion under "Health Effects."

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Aging</b>	
General process in which characteristics of a structure or component gradually change (e.g., degrade) with time or use. (see <i>Bathtub Curve</i> )	<p>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.</p> <p>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.</p> <p>The definition provided is based on the definition in the IAEA Safety Glossary.</p>
<b>Air Submersion</b>	
(see <i>Cloudshine</i> )	Air submersion has the same meaning as cloudshine and is defined under "Cloudshine."
<b>Aleatory Uncertainty</b>	
(see <i>Uncertainty</i> )	The term aleatory uncertainty is a specific type of uncertainty and is defined under the term "Uncertainty."
<b>As-Built As-Operated (As-Designed)</b>	
The accurate and current design and operation of the facility. (see <i>QRVA Configuration Control, Living QRVA, Facility Configuration Control</i> )	<p>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 or combined operating license stage, in which the facility is not yet built or operated.</p> <p>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.</p> <p>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."</p>
<b>As-Designed</b>	
(see <i>As-Built As-Operated</i> )	The term as-designed is defined in the discussion of the term "As-Built As-Operated."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Assumption (Key)</b>	
<p>A decision or judgment that is made in the development of a model or analysis. <i>(see Model Uncertainty)</i></p>	<p>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.</p> <p>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 LOFICF or AFRF, event importance measures). Key sources of model uncertainty are identified in the context of an application.</p> <p>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 (IPE), individual plant examinations for external events (IPEEE), and probabilistic risk assessments (PRA), assumptions are those parts of the mathematical models that the analyst expects will hold true for the range of solutions used for making decisions.”</p>
<b>Atmospheric Transport and Diffusion</b>	
<p>The movement and variation in concentration of a radioactive plume after release to the environment. <i>(see Atmospheric Transport and Diffusion Analysis, Level 1, 2, 3 QRVA)</i></p>	<p>In a QRVA, assumptions about atmospheric transport and diffusion of the radioactive plume are used in the calculation of the health effects or economic consequences of a severe accident. A Level 3 QRVA takes the result of a Level 2 QRVA (frequencies, amounts, timing durations, and energies of radioactivity releases) and produces offsite consequences (health effects, economic consequences) as output.</p> <p>To calculate the offsite consequences, the movement and concentration of the radioactive plume under various weather conditions (e.g., high winds, rain) has to be determined. The plume characteristics can then be combined with the population information to calculate the health effects. The plume characteristics also can be used to determine land contamination and economic consequences of a severe accident.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Atmospheric Transport and Diffusion Analysis</b>	
An analysis to determine the movement and concentration of a radioactive plume. (see <i>Atmospheric Transport and Diffusion</i> )	In a Level 3 QRVA, atmospheric transport and diffusion (ATD) models are used in the consequence calculations. ATD models range from simple straight-line, steady-state Gaussian dispersion models, which 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 and atmospheric stability. Probabilistic consequence modeling codes typically include sampling of meteorological data from a site-specific annual database of hourly weather data to determine appropriately weighted scenarios of plume transport under different weather conditions to provide probabilistic results.



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<p><b>At-Power</b></p> <p>The state of operation in which the reactor is critical and producing power from a range of states between full and low power. (see <i>Full Power, Low Power/Shutdown, Facility Operational State</i>)</p>	<p>A QRVA models the different facility operating states (FOS), generally defined as at-power, low-power, and shutdown. These FOSs are distinguished in the QRVA model because the facility responses (e.g., accident sequences) are different.</p> <p>At-power facility status includes all power levels above low-power. In this instance, the reactor is producing a significant amount of power from fission in the core fuel, above and beyond the decay heat levels. The safety systems are on automatic actuation and not blocked or defeated (as they might be in low-power and shutdown states). The support systems are aligned in their normal configuration (e.g., electric power is being drawn from the grid). These are all important initial conditions for QRVA modeling.</p> <p>The borderline between at-power and low-power and shutdown depends on facility evolution (the changes in configuration used to bring the facility down from full power or up from low-power and shutdown) and is typically on the order of 15%–25% of full power.</p> <p>Historically, the term “full power” was used for all power levels between low-power and 100% power. This has been modified such that at-power now refers to intermediate power levels ranging from low-power and up to and including 100% power, while “full power” is reserved for just 100% reactor power. The figure below is a pictorial representation of the different facility operating states.</p> <div style="text-align: center;"> </div> <p>Note: The overlap shows that QRVAs have used different denominations for at-power and low-power.</p> <p>The ASME/ANS PRA Standard defines at-power as “those plant operating states characterized by the reactor being critical and producing power, with automatic actuation of critical safety systems not blocked and with essential support systems aligned in their normal power operation configuration.”</p>

**Table D-1. Terms and Definitions (Continued) -**

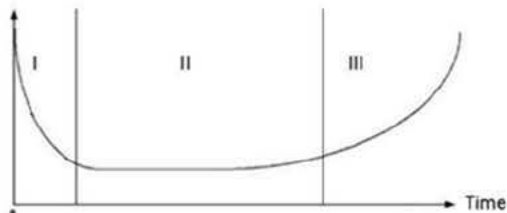
Term and Definition	Discussion
<b>Availability (Unavailability)</b>	
The probability that a system, structure, or component of interest is functional at a given point in time. (see <i>Reliability</i> )	<p>In a QRVA, unavailability is one of the attributes of a system, structure, or component that may affect the facility's response to an initiating event.</p> <p>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."</p> <p>The definition provided is based on the definition in NFPA-805.</p>
<b>Base QRVA, Baseline QRVA</b>	
(see <i>QRVA</i> )	The terms base QRVA and baseline QRVA represent a specific type of QRVA and are defined under "QRVA."



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Basic Event</b>	
<p>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. <i>(see Component, Fault Tree)</i></p>	<p>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.</p> <p>The term basic event can have other (more specific) definitions, as stated below:</p> <ul style="list-style-type: none"> <li>• “An event in a fault tree model that requires no further development, because the appropriate limit of resolution has been reached.” (NUREG-0492).</li> <li>• 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).</li> </ul> <p>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.</p> <p>The following figure is an example of a basic event:</p> <div style="text-align: center;"> <pre> graph TD     Root[Pump Systems failed] --- S1[Pump System I failed]     Root --- S2[Pump System II failed]     Root --- S3[Transfer to AC Power Failed FT]     S1 --- P1[Pump A failed]     S1 --- P2[Pump B failed]     S1 --- P3[Pump C failed]     S2 --- P4[Pump D failed]     S2 --- P5[Pump E failed]     P1 --- A((A))     P2 --- B((B))     P3 --- C((C))     P4 --- D((D))     P5 --- E((E))     A --- BE[These are basic events in the fault tree.]     B --- BE     C --- BE     D --- BE     E --- BE                     </pre> </div>
<b>Basic Event Failure Probability</b>	
<p><i>(see Probability)</i></p>	<p>The term basic event failure probability is a specific type of failure probability and is defined under “Probability.”</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Bathtub Curve</b>	
<p>Graphical representation of failure rate time dependency in the life of a typical component. (see <i>Aging</i>)</p>	<p>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:</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Region II – The failure rate becomes stable and remains constant in the middle of the component's life.</li> <li>• Region III – The failure rate increases toward the end of the component's life.</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Bayesian Analysis, Bayesian Estimation, Bayesian Statistics</b>	
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 <i>Frequentist, Bayesian Update</i> )	<p>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.</p> <p>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.”</p> <p>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.</p> <p>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.</p> <p>The terms Bayesian analysis, Bayesian estimation, and Bayesian statistics are used interchangeably.</p>
<b>Bayesian Estimation</b>	
(see <i>Bayesian Analysis</i> )	The term Bayesian estimation has the same meaning as Bayesian analysis and is defined the same as the term “Bayesian Analysis.”
<b>Bayesian Statistics</b>	
(see <i>Bayesian Analysis</i> )	The term Bayesian statistics has the same meaning as Bayesian analysis and is defined the same as the term “Bayesian Analysis.”

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Bayesian Update</b>	
<p>Modification of a probability (frequency) of an event by incorporating additional observations of event occurrence. <i>(see Bayesian Analysis)</i></p>	<p>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.</p> <p>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.</p> <p>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.</p>
<b>Best Estimate</b>	
<p>Approximation of a quantity based on the best available information. <i>(see Mean, Point Estimate)</i></p>	<p>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.</p> <p>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.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Beyond-Design-Basis Accident</b>	
<p>A postulated accident that is more severe than those accidents used to establish the design of a nuclear facility. <i>(see Design-Basis Accident, Severe Accident)</i></p>	<p>In a QRVA, beyond-design-basis accidents (BDBA) are a major focus of the analysis. For example, QRVAs for currently operating light-water reactors (LWR) have focused almost exclusively on BDBAs. Recent QRVAs for proposed high-temperature graphite reactors have included design-basis accidents and anticipated occurrences in the analysis.</p> <p>A nuclear facility must be designed and built to withstand a design-basis accident (DBA) without threatening public health and safety. However, the nuclear facility is not necessarily designed to withstand BDBAs. Therefore, an important role of QRVA is to determine how a nuclear 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 core damage. Those BDBAs that do result in significant core damage are termed severe accidents. All severe accidents are by definition BDBAs since their challenges exceed the design envelope of the facility.</p> <p>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 nuclear 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.”</p>
<b>Beyond-Design-Basis Event</b>	
<p>An event more severe than the events for which the facility was designed to withstand and specified in the safety analysis. <i>(see Design-Basis Event, Severe Accident)</i></p>	<p>In a QRVA, beyond-design-basis events (BDBE) represent conditions beyond the facility design envelope and, therefore, exceed the already considered anticipated transients (e.g., tripping of turbine generator), anticipated operational occurrences (AOO), DBAs, and design-basis natural phenomena.</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Bin, Binning</b>	
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 (e.g., failure of a main steam isolation valve and failure of a feedwater pump are generally grouped (or binned) into a loss of feedwater initiator group).  Bin is the actual group and binning is the process.
<b>Birnbaum Importance</b>	
<i>(see Importance Measure)</i>	The term Birnbaum importance is one type of importance measure and is defined under "Importance Measure."
<b>Bounding Analysis</b>	
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. <i>(see Conservative Analysis)</i>	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.  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.  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.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Bridge Event Tree</b>	
<i>(see Bridge Tree)</i>	The term bridge event tree has the same meaning as bridge tree and is defined under "Bridge Tree."



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Bridge Tree, Bridge Event Tree</b>	
<p>An event tree used to transfer information from one analysis stage to another in a manner that ensures the critical information is preserved. (see <i>Containment Event Tree, Event Tree, Accident Progression Event Tree</i>)</p>	<p>In a QRVA, the most common use of bridge trees is in linking the core damage 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 core damage, but that can influence further accident progression. The terms bridge tree and bridge event tree are similar in meaning and often correctly used interchangeably.</p> <p>The figure below is an example of a bridge tree:</p> <div style="text-align: center;"> <pre> graph LR     CDAS[Level-1 Core Damage Accident Sequences (CDAS)] --&gt; BET[Bridge Event Tree (containment systems)]     BET --&gt; PDS[Plant Damage State]     PDS --&gt; L2[Level-2 Containment Event Tree]     L2 --&gt; ST[Source Terms]     CDAS_Cutsets[CDAS cutsets binned by reactor core coolant and containment status] --&gt; PDS             </pre> </div>
<b>Capability Categories</b>	
<p>Categories used to indicate different levels of detail, facility specificity, and realism in defining technical requirements for an acceptable QRVA.</p>	<p>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.</p> <p>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.</p> <p>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.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Chemical Element Group</b>	
A group of radioactive materials with similar physical and chemical properties used to simplify the estimate for offsite health effects. <i>(see Source Term)</i>	In a QRVA, the source term used to characterize the radioactive material release is based on the defined chemical element groups. During a core damage accident, the number of different radioactive materials released from the fuel, reactor vessel, and containment to the environment can be quite large. The number of radioactive materials considered can be reduced to a manageable size by grouping those with similar physical and chemical properties. For example, in NUREG-1150 the 60 radionuclides considered in the consequence calculation were not dealt with individually in the source term calculation. Since some different elements behave similarly enough both chemically and physically that they can be considered together, the 60 isotopes were placed in nine radionuclide groups. These nine groups were treated individually in the source term analysis.
<b>Chronic Exposure</b>	
<i>(see Exposure)</i>	The term chronic exposure is a type of exposure and is defined in the discussion under "Exposure."
<b>Cloudshine</b>	
Direct external exposure from radioactive material in the atmosphere. <i>(see Exposure Pathways, Water Immersion, Groundshine, Inhalation, Ingestion, Skin Deposition)</i>	In a Level 3 QRVA, cloudshine, also referred to as air immersion, is one of the assumed pathways by which an individual can receive doses in the consequence calculation. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.
<b>Cohort</b>	
A group of individuals that is defined by some statistical or demographic factor. <i>(see Emergency Response)</i>	In the emergency response modeling of a Level 3 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).
<b>Collective Dose</b>	
<i>(see Dose)</i>	The collective dose is a summation of dose that is defined under "Dose."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Committed Dose Equivalent</b>	
<i>(see Dose Equivalent)</i>	The committed dose equivalent is one measure of dose that can be used to calculate the effect of radiation received by an individual and is defined under "Dose Equivalent."
<b>Committed Effective Dose Equivalent</b>	
<i>(see Dose Equivalent)</i>	The committed effective dose equivalent is one measure of dose that can be used to calculate the effect of radiation received by an individual and is defined under "Dose Equivalent."
<b>Common Cause Component Group</b>	
Similar components that are modeled as a group because they are subject to failure by a common cause. (see Common-Cause Failure)	<p>In a QRVA, one failure mechanism of a component may be from a common cause that also fails other components.</p> <p>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.</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion																																
<b>Common Cause Failure</b>																																	
<p>A failure of two or more structures, systems, or components as a result of a single shared cause. (see <i>Common-Mode Failure, Failure Mode</i>)</p>	<p>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.</p> <p>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.</p> <p>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 (FTS) and fails to run (FTR).</p> <table border="1" style="margin: 10px auto; border-collapse: collapse; text-align: center;"> <thead> <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> </thead> <tbody> <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> </tbody> </table> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>	Failure Cause	Failure Mode		Basic Event	Comments	CCF Types	EDG A	EDG B	Plugged radiator	FTS	FTR	CCF-DG-AB-FTS/R-1	Same cause results in a different failure mode of each DG	CCF without CMF	Failed load sequencer	FTR	FRT	CCF-DG-AB-FTR	Same cause results in the same failure mode of both EDGs	CCF with CMF	Bad fuel oil	FTS	FTS	CCF-DG-AB-FTS	Same cause results in the same failure mode of both EDGs	CCF with CMF	Faulty Bearings	FTS	FTR	CCF-DG-AB-FTS-R2	Same cause results in a different failure mode of each DG	CCF without CMF
Failure Cause	Failure Mode		Basic Event	Comments				CCF Types																									
	EDG A	EDG B																															
Plugged radiator	FTS	FTR	CCF-DG-AB-FTS/R-1	Same cause results in a different failure mode of each DG	CCF without CMF																												
Failed load sequencer	FTR	FRT	CCF-DG-AB-FTR	Same cause results in the same failure mode of both EDGs	CCF with CMF																												
Bad fuel oil	FTS	FTS	CCF-DG-AB-FTS	Same cause results in the same failure mode of both EDGs	CCF with CMF																												
Faulty Bearings	FTS	FTR	CCF-DG-AB-FTS-R2	Same cause results in a different failure mode of each DG	CCF without CMF																												



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Common-Mode Failure</b>	
<p>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 <i>Common-Cause Failure, Failure Mode</i>)</p>	<p>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.</p> <p>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.</p> <p>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."</p> <p>The definition provided was based on the definition in the IAEA Safety Glossary.</p>
<b>Complementary Cumulative Distribution Function</b>	
<p>(see <i>Cumulative Distribution Function</i>)</p>	<p>The term complementary cumulative distribution function is a type of cumulative distribution function and is defined under "Cumulative Distribution Function."</p>
<b>Completeness Uncertainty</b>	
<p>(see <i>Uncertainty</i>)</p>	<p>The term completeness uncertainty is related to epistemic uncertainty and defined under "Uncertainty."</p>
<b>Component</b>	
<p>A part of a system in a facility. (see <i>Basic Event</i>)</p>	<p>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."</p> <p>Basic events are associated with individual components, such that different basic events will be associated with different failure modes of a particular component.</p>
<b>Conditional Acute Fuel Release Probability</b>	
<p>(see <i>Conditional Probability</i>)</p>	<p>The term conditional acute fuel release probability is a type of conditional probability and is defined under "Conditional Probability."</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Conditional Containment Failure Probability</b>	
<i>(see Conditional Probability)</i>	The term conditional containment failure probability is a type of conditional probability and is defined under “Conditional Probability.”
<b>Conditional Core Damage Probability</b>	
<i>(see Conditional Probability)</i>	The term conditional core damage probability is a type of conditional probability and is defined under “conditional probability.”
<b>Conditional Probability (Containment Failure, Core Damage, Acute Fuel Release)</b>	
Probability of occurrence of an event, given that a prior event has occurred. <i>(see Probability)</i>	<p>In a QRVA, a conditional probability can be calculated for containment failure, core damage, and acute fuel release given the knowledge of a variety of prior events have occurred. Examples include:</p> <ul style="list-style-type: none"> <li>• Conditional containment failure probability can be calculated given that a particular accident type (large loss-of-coolant accident, transient) has occurred.</li> <li>• Conditional core damage probability can be calculated given an initiating event (a facility upset causing a demand for shutdown) has occurred, or given that a certain facility system has been taken out of service.</li> <li>• Conditional acute fuel release probability can be calculated given that a core damage event has occurred, or given that a bypass sequence has occurred.</li> </ul> <p>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.</p>



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Confidence Interval</b>	
<p>A range of values that has a specified likelihood of including the true value of a random variable. (see <i>Uncertainty Interval</i>)</p>	<p>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 <math>p</math> is defined such that the probability that the true value of a random variable contained within that interval <math>p</math> 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.</p> <div style="text-align: center;"> </div>
<b>Configuration Risk Profile</b>	
<p>(see <i>QRVA Configuration Control</i>)</p>	<p>The configuration risk profile is related to configuration control and is defined under “QRVA Configuration Control.”</p>
<b>Consequence</b>	
<p>(see <i>Accident Consequence</i>)</p>	<p>In the context of a QRVA, the term consequence has the same meaning as accident consequence, which is defined under “Accident Consequence.”</p>
<b>Consequence Analysis</b>	
<p>(see <i>Accident Consequence Analysis</i>)</p>	<p>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.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Consequential Steam Generator Tube Rupture, Induced Steam Generator Tube Rupture</b>	
<p>A break or breach in a steam generator tube caused by the consequences of an accident. (see <i>Steam Generator Tube Rupture, Containment Bypass</i>)</p>	<p>In a QRVA for a pressurized-water reactor, steam generator tube ruptures (SGTR) are modeled either as an initiating event or a subsequent failure as part of an accident sequence. If the SGTR occurs randomly while the facility is operating, it is an initiating event modeled in the QRVA. However, if the SGTR occurs because of excessive conditions produced as a result of the accident, it is considered to be a consequential or induced SGTR and is modeled in the QRVA as an event in an accident sequence. These excessive conditions generally involve high pressures or high temperatures that could rupture a steam generator tube. For example, this might occur if the steam generator were to boil dry (steam generator dryout).</p> <p>Accidents involving SGTRs are modeled in QRVAs because it allows reactor coolant to flow from the reactor vessel to the secondary side of the steam generator. As such, an SGTR can become a significant contributor to risk because it can serve as a possible mechanism for radioactive material transport to the environment. There is the potential that if a tube bursts while a facility is operating, radioactivity from the primary coolant system could escape directly to the atmosphere through the safety valves on the secondary side. This scenario is referred to as containment bypass.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Conservative Analysis (Demonstrably)</b>	
<p>An analysis that uses assumptions such that the assessed outcome is meant to be less favorable than the expected outcome. <i>(see Bounding Analysis)</i></p>	<p>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 licensee’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.</p> <p>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.</p> <p>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.</p> <p>The terms conservative and demonstrably conservative are used interchangeably.</p> <p>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.”</p>
<b>Containment Building</b>	
<p><i>(see Containment)</i></p>	<p>The term containment building has the same meaning as containment and is defined under “Containment.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Containment Bypass</b>	
A flow path that allows the unintended release of radioactive material directly to the environment, bypassing the containment. (see Containment Failure, Containment Isolation Failure, Interfacing Systems Loss-of-Coolant Accident)	<p>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 radioactive material. Therefore, a containment bypass can lead to a significant release of fission products in the event of a core damage accident. A containment bypass can result from the failure of various containment components so that a direct path to the environment is opened. For example, a containment bypass can result from an interfacing-system loss-of-coolant accident (i.e., an accident in which a high-pressure system containing fission products leaks into a lower- pressure system, part of which is outside of containment). For example, a steam generator tube rupture in a core damage accident provides a pathway for the fission products in the high-pressure primary system to enter the low-pressure side of the steam generator, which has relief valves outside of containment.</p> <p>Containment bypass is distinct from containment isolation failure in which the containment is not acceptably leak-tight.</p> <p>The definition provided is based on the definition found in the ASME/ANS PRA Standard.</p>
<b>Containment Capacity</b>	
The ability of the containment to withstand the challenges that result from accidents. (see Containment, Containment Capacity Analysis, Containment Pressure Boundary)	<p>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-core damage. As such, the containment performance in response to severe accident conditions can be assessed.</p> <p>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.</p>
<b>Containment Capacity Analysis</b>	
A calculation that estimates the ability of the containment to withstand the challenges that result from accidents. (see Containment Capacity)	<p>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.</p>



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Containment Event Tree</b>	
<p>A logic diagram that graphically represents the status of the containment and containment equipment when subjected to severe accident loads. (see <i>Accident Progression Event Tree, Event Tree</i>)</p>	<p>In a QRVA, a CET begins with the onset of core damage 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).</p> <p>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.</p> <p>The end states of both the CET and the APET are: no containment failure, various containment failure modes, or containment bypass.</p> <p>The figure below represents a containment event tree with the following acronyms: Core Damage (CD), Reactor Coolant System depressurization (RCS Depress), Vessel Breach (VB), Steam Generator Tube Rupture (SGTR).</p>
<b>Containment Failure Mode</b>	
<p>The various ways in which the ability of the containment to prevent radioactive material release is compromised. (see <i>Containment Failure, Containment Bypass, Containment Isolation Failure</i>)</p>	<p>In a QRVA, the modes of containment failure define the manner in which containment integrity is lost (i.e., the way a radioactive material 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 such as interfacing-systems loss-of-coolant accidents.</p> <p>The definition provided is based on the definition in the ASME/ANS PRA Standard.</p>
<b>Containment Failure Probability</b>	
<p>(see <i>Probability</i>)</p>	<p>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."</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Containment Failure (Early, Late)</b>	
Loss of integrity of the containment from a core damage accident that is expected to result in an unacceptable release of radioactive materials. (see <i>Containment, Containment Bypass,</i>	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 can be potentially high. For specific containments there can be selected severe accident scenarios in which the containment fails before fission 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 radioactive material release.  Containment failure is often categorized as early or late. Early containment failure occurs in a timeframe before the surrounding population within 1 mile of the site boundary can be evacuated. Late containment failure occurs in a timeframe that allows the surrounding population from 1 to 10 miles to be evacuated.
Containment Pressure Boundary)	Containment bypass failures (e.g., interfacing-system loss-of-coolant accidents) occur in the early timeframe but usually are categorized separately from early structural failures of the containment.  The definition is derived from the ASME/ANS PRA Standard.
<b>Containment Integrity</b>	
The ability of the containment to function as a barrier to prevent release of radioactive materials as a result of an accident. (see <i>Containment Failure Mode</i> )	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 reactor 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, melt-through, and bypass.



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Containment Isolation Failure</b>	
<p>A failure in the piping, valves, or actuators that isolate the containment. <i>(see Containment Bypass, Containment Failure Mode)</i></p>	<p>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 fission products that may result from postulated accidents. In a containment isolation failure, fission products can pass to the environment through the containment because the containment is not properly isolated (i.e., not acceptably leak-tight).</p> <p>In some severe accident scenarios, an accident management strategy, referred to as containment venting, may be used. Containment venting involves a deliberate breach of containment isolation by the facility operators who open a controlled, filtered or unfiltered, pathway from the containment to the environment to prevent an uncontrolled overpressure failure of the containment.</p> <p>The containment isolation system consists of the piping, valves, and actuators that are designed so that fluid lines penetrating the containment boundary are isolated in the event of an accident.</p>
<b>Containment Pressure Boundary</b>	
<p>Those parts of the reactor containment that sustain loading and provide a pressure boundary in the performance of the containment function. <i>(see Containment)</i></p>	<p>In a Level 2 QRVA, the evaluation of containment integrity is an evaluation of the structures, systems, and components of the reactor containment pressure boundary that perform the containment function (i.e., that form the containment system). As stated in NUREG-0800, the reactor containment system design must include the functional capability of enclosing the reactor system and of providing a final barrier (boundary) against the release of radioactive fission products in case of postulated accidents.</p> <p>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.</p> <p>The definition provided is derived from Chapter 6 of NUREG-0800.</p>
<b>Containment Structure</b>	
<p><i>(see Containment)</i></p>	<p>The term containment structure has the same meaning as containment and is defined under "Containment."</p>

**Table D-1. Terms and Definitions (Continued) -**

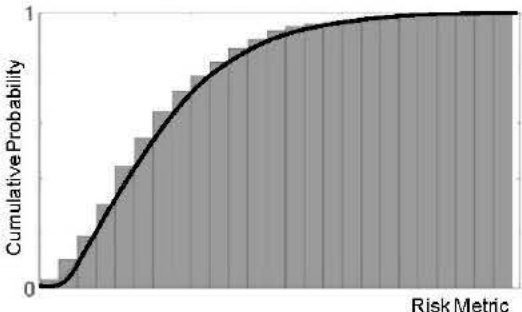
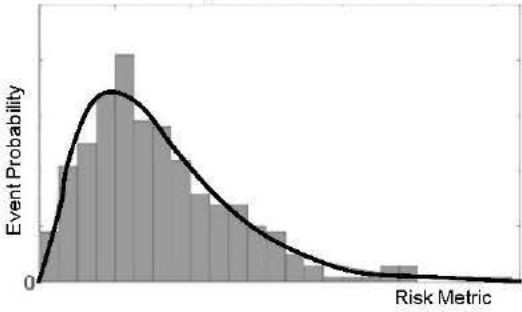
Term and Definition	Discussion
<b>Containment, Containment Building, Containment Structure</b>	
<p>A physical structure surrounding a reactor that is designed to prevent or control the release of radioactive material. (see <i>Containment Capacity, Containment Failure, Containment Failure Mode, Containment Integrity, Containment Pressure Boundary</i>)</p>	<p>In a Level 2 QRVA, the ability of the containment (containment building or containment structure) to contain fission products that have escaped from the reactor is analyzed to estimate the limits of the containment's capacity.</p> <p>A containment, containment building, or containment structure, in its most common usage, is a steel or reinforced concrete structure enclosing a nuclear reactor designed to contain the escape of radiation to the environment. The containment is the final barrier to radioactive material release.</p> <p>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 core melt accidents) that are significantly higher than those of DBAs.</p> <p>The NRC Website Glossary defines the term containment building as an "air-tight building, which houses a nuclear reactor and its pressurizer, reactor coolant pumps, steam generator, and other equipment or piping that might otherwise release fission products to the atmosphere in the event of an accident. Such buildings usually are made of steel-reinforced concrete."</p> <p>The NRC Website Glossary also defines the term containment structure as "a gas-tight shell or other enclosure around a nuclear reactor to confine fission products that otherwise might be released to the atmosphere in the event of an accident. Such enclosures are usually dome-shaped and made of steel-reinforced concrete."</p>



**Table D-1. Terms and Definitions (Continued)**

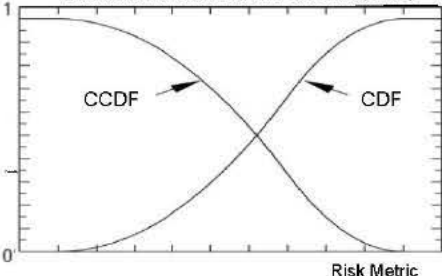
Term and Definition	Discussion
<b>Core Damage</b>	
<p>Sufficient damage that could lead to a release of radioactive material from the core that could affect public health. <i>(see Core Melt, Loss of Fuel Inventory Control Frequency, Core Damage Probability)</i></p>	<p>In a QRVA, the potential for core damage is evaluated in the Level 1 part of the analysis. Specifically, a Level 1 QRVA calculates the LOFICF given the design and operation of the facility. In this context, core damage in a Level 1 QRVA is actually the onset of core damage; that is, being the onset of sufficient damage to the core that (1) if not immediately arrested could potentially result in a release of radioactive material from the core, and (2) if released from the vessel and containment, could result in offsite public health effects.</p> <p>In deterministic analyses, quantitative criteria often are used to define the onset of core damage (e.g. a peak clad temperature of 2,200 degrees Fahrenheit).</p> <p>The ASME/ANS PRA Standard defines core damage as “uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, if released, to result in offsite public health effects.”</p> <p>The terms core damage and core melt are sometimes incorrectly used as synonyms.</p> <p>However, core melt occurs after the onset of core damage. Core damage does not necessarily indicate that the reactor fuel has melted, only that radioactive material could be released from the core into the reactor vessel. An illustration differentiating the concepts of core damage, core melt, and their timing is provided below.</p> <div style="text-align: center;"> </div>
<b>Core Damage Probability</b>	
<p><i>(see Probability)</i></p>	<p>The term core damage probability is a type of probability used in QRVA and is defined under “Probability.”</p>
<b>Cumulative Distribution Function (Complementary)</b>	
<p>A function that provides the probability that a parameter is less than or equal to a given value. <i>(see</i></p>	<p>In a QRVA, the cumulative distribution function is often used to present the results of the analysis.</p> <p>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</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<i>Probability Distribution)</i>	<p>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.</p> <div style="text-align: center;"> <p>Cumulative Distribution Function</p>  <p>Probability Distribution Function</p>  </div> <p>The cumulative distribution function may be used to calculate the quantiles or the probability of not exceeding the mean of a risk metric. 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. NUREG/CR-6823 defines cumulative distribution function as one that “gives the probability that the random variable does not exceed a given value.”</p> <p>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.</p>



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
	<p style="text-align: center;">Complementary Cumulative Distribution Function (CCDF) Vs. Cumulative Distribution Function (CDF)</p>  <p>Some examples of using the complementary cumulative distribution function are calculating the probability of exceeding a certain release fraction of radioactive material in core melt 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.</p> <p>The definition provided was based on the definition in NUREG/CR-6823.</p>
<b>Cumulative Dose</b>	
<i>(see Dose)</i>	The cumulative dose is a total dose that is defined under "Dose."
<b>Cut set (Minimal Cut set)</b>	
A combination of failures that result in a particular outcome. <i>(see Truncation Limit)</i>	<p>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 core damage or containment failure. 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 core damage or containment failure.</p> <p>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. 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 core damage or containment failure)." 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."</p> <p>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."</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion																											
	<p>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:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p style="text-align: center;">Cutset Example for Pump Systems:</p> <p style="text-align: center;">Possible Cutsets:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">A'D</td> <td style="width: 33%;">A'C'D'E</td> <td style="width: 33%;">C'E</td> </tr> <tr> <td>A'E</td> <td>A'B'D'E</td> <td>C'D'E</td> </tr> <tr> <td>A'B'D</td> <td>B'D</td> <td rowspan="10" style="font-size: 3em; vertical-align: middle;">}</td> </tr> <tr> <td>A'B'E</td> <td>B'E</td> </tr> <tr> <td>A'C'D</td> <td>B'C'D</td> </tr> <tr> <td>A'C'E</td> <td>B'C'E</td> </tr> <tr> <td>A'B'C'D</td> <td>B'D'E</td> </tr> <tr> <td>A'B'C'E</td> <td>B'C'D'E</td> </tr> <tr> <td>A'B'C'D'E</td> <td>C'D</td> </tr> </table> <p style="text-align: center;">Minimal Cutsets:</p> <table style="width: 100%; border: none;"> <tr> <td>A'D</td> </tr> <tr> <td>A'E</td> </tr> <tr> <td>B'D</td> </tr> <tr> <td>B'E</td> </tr> <tr> <td>C'D</td> </tr> <tr> <td>C'E</td> </tr> </table>	A'D	A'C'D'E	C'E	A'E	A'B'D'E	C'D'E	A'B'D	B'D	}	A'B'E	B'E	A'C'D	B'C'D	A'C'E	B'C'E	A'B'C'D	B'D'E	A'B'C'E	B'C'D'E	A'B'C'D'E	C'D	A'D	A'E	B'D	B'E	C'D	C'E
A'D	A'C'D'E	C'E																										
A'E	A'B'D'E	C'D'E																										
A'B'D	B'D	}																										
A'B'E	B'E																											
A'C'D	B'C'D																											
A'C'E	B'C'E																											
A'B'C'D	B'D'E																											
A'B'C'E	B'C'D'E																											
A'B'C'D'E	C'D																											
A'D																												
A'E																												
B'D																												
B'E																												
C'D																												
C'E																												
<b>Deep Dose Equivalent</b>																												
<i>(see Dose Equivalent)</i>	The deep dose equivalent is one measure of dose that can be used to calculate the effect of radiation received by an individual and is defined under “Dose Equivalent.”																											
<b>Defense-in-Depth</b>																												
Formal definition requires Commission approval. <i>(see</i>	In a QRVA, defense-in-depth is not an explicitly modeled element. Rather, the results of the QRVA provide insights into defense-in-depth. Over time, various definitions have been used for defense-in-depth, including:																											



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<p><i>Safety Margin, Uncertainty, Rationalist, Structuralist)</i></p>	<ul style="list-style-type: none"> <li>• three barriers to contain radioactive material: fuel cladding, primary system boundary, and the containment</li> <li>• the use of successive measures to prevent an accident or to mitigate the consequences of an accident</li> <li>• the use of redundancy and diversity</li> <li>• implementation of the single failure criterion</li> </ul> <p>Regardless of its definition, defense-in-depth is an integral part of the NRC's safety philosophy. The NRC Website Glossary defines defense-in-depth as: "An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."</p> <p>The NRC Commission has referred to defense-in-depth as a concept that:</p> <p style="padding-left: 40px;">Has always been and will continue to be a fundamental tenet of regulatory practice in the nuclear field, particularly regarding nuclear facilities. Risk insights can make the elements of defense-in-depth clearer by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense. Decisions on the adequacy of, or the necessity for, elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.</p> <p>The Commission further states:</p> <p style="padding-left: 40px;">Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.</p>
<b>Demonstrably Conservative Analysis</b>	
<p><i>(see Conservative Analysis)</i></p>	<p>A demonstrably conservative analysis has the same meaning as a conservative analysis and is defined under "Conservative Analysis."</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Dependency</b>	
<p>Reliance of a function, system, component, or human action on another part of the system or another human action to accomplish its function.</p>	<p>Dependency is significant to the fidelity of a QRVA model to capture the interrelationship between the modeled systems and human actions.</p> <p>As an example of systems dependency, many core cooling systems depend on electric power or cooling water systems. Also, operator actions closely spaced in time may have dependency in that a failure to perform a certain action may negatively affect successful performance of a subsequent action.</p> <p>Dependency has also been defined as:</p> <ul style="list-style-type: none"> <li>• “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.”</li> <li>• “Requirement external to a SSC, and upon which the SSC’s function depends.”</li> </ul>
<b>Design-Basis Accident</b>	
<p>A postulated accident that a nuclear 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)</p>	<p>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 core damage occurred; however, the term “beyond-design-basis accident” merely indicates that the accident exceeded the design limits of the facility.</p> <p>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 reactor coolant up to and including the double-ended rupture of the largest pipe containing reactor coolant.</p> <p>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 (e.g., tripping of turbine generator), external events, and natural phenomena.</p> <p>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.”</p> <p>The definition provided was based on the definition in the NRC Website Glossary.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Design-Basis Event</b>	
<p>Any of the events specified in the facility's safety analysis that are used to establish acceptable performance for safety-related functions. (see <i>Design-Basis Accident, Severe Accident</i>)</p>	<p>In a QRVA, the outcome of concern is whether or not a particular accident leads to core damage. Therefore, BDBA that exceed the design envelope and lead to core damage are typically modeled. In this instance, these BDBAs that lead to core damage 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 (e.g., tripping of turbine generator), AOO, DBAs, external events, and natural phenomena.</p> <p>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 nuclear plant unit," (e.g., example loss of all offsite power).</p> <p>DBAs are a subset of DBEs, as noted above. An example of a DBA is a major rupture of a pipe containing reactor coolant up to and including the double-ended rupture of the largest pipe containing reactor coolant. The definition provided was based on the definition in NUREG-1560.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Deterministic (Analysis, Approach, Regulation)</b>	
A characteristic of decision-making in which results from engineering analyses, not involving probabilistic considerations, are used to support a decision. (see <i>Risk-Informed, Probabilistic</i> )	<p>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 core damage are based on deterministic analyses. Another example of a deterministic analysis would be the calculation of peak cladding temperatures after emergency core cooling system actuation in a loss-of-coolant accident, or the timing of vessel breach in a core melt accident.</p> <p>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.</p> <p>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. As applied in nuclear technology, it generally deals with evaluating the safety of a nuclear power plant in terms of the consequences of a predetermined bounding subset of accident sequences.” 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.</p>
<b>Deterministic Analysis</b>	
(see <i>Deterministic</i> )	The term deterministic analysis is defined under “Deterministic.”
<b>Deterministic Approach</b>	
(see <i>Deterministic</i> )	The term deterministic approach is defined under “Deterministic.”
<b>Deterministic Regulation</b>	
(see <i>Deterministic</i> )	The term deterministic regulation is defined under “Deterministic.”
<b>Direct Containment Heating</b>	
(see <i>High-Pressure Melt Ejection</i> )	The term direct containment heating is a mechanism for challenging containment integrity and is defined under “High-Pressure Melt Ejection.”



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Dose</b>	
<p>A measure of the amount of radiation absorbed by a person. (<i>see Dose Equivalent</i>)</p>	<p>In a Level 3 QRVA, dose is calculated to assess offsite health effects. The NRC Website Glossary defines dose as “a general term, which may be used to refer to the amount of energy absorbed by an object or person per unit mass. Known as the ‘absorbed dose,’ this reflects the amount of energy that ionizing radiation sources deposit in materials through which they pass, and is measured in units of radiation-absorbed dose (rad). The related international system unit is the gray (Gy), where 1 Gy is equivalent to 100 rad. By contrast, the biological dose or dose equivalent, given in rems or sieverts (Sv), is a measure of the biological damage to living tissue as a result of radiation exposure.”</p> <p>The collective dose (i.e., total dose obtained by summing over individual exposures of the affected population) is also used as a risk measure in value-impact analyses carried out in conjunction with QRVAs. NUREG-0713, Vol. 28, states that the concept of collective dose is used by the NRC to denote the summation of the total effective dose equivalent received by all monitored workers at a nuclear facility, usually over the course of a year, and is reported in units of person-rem per year.</p> <p>The cumulative dose is the total dose that an individual receives as a result of repeated exposures to ionizing radiation to the same portion of the body, or to the whole body, over time. Cumulative dose usually is used for measuring occupational exposures of workers in the nuclear industry.</p> <p>When defining dose and the way it is used in QRVAs to estimate health effects the following considerations are relevant:</p> <p style="padding-left: 40px;">Under ‘radiation dose’ two concepts commonly used are: deterministic or non-stochastic dose and stochastic dose. The former implies that a health effect will occur within a short period following exposure with near certainty; the latter that a health effect may occur at some later time with some probability. In a QRVA, the former is used with a threshold (depending on organ) to estimate early health effects. The latter is used, usually with a linear no-threshold model, to estimate latent cancers.</p>
<b>Dose Coefficient</b>	
<p>Dose coefficients relate the dose to organs and tissues of the body from concentrations of radionuclides. (<i>see Dose, Dose Conversion Factor</i>)</p>	<p>In a Level 3 QRVA, dose coefficients are incorporated into the consequence model. Dose coefficients relate the dose to organs and tissues of the body from concentrations of radionuclides. Dose coefficients for external exposure relate the organ and tissue doses to the concentrations of radionuclides in environmental media. Since the radiation arises outside the body, this is referred to as external exposure, while dose coefficients for internal exposure relate the organ and tissue doses to the intake of radionuclides by inhalation or ingestion, where the radiation is emitted inside the body.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Dose Conversion Factor</b>	
A factor used to determine the biological effect of different types of radiation on an individual's organs. <i>(see Dose)</i>	In a Level 3 QRVA, dose conversion factors are incorporated into the consequence model and used to calculate the effect of radiation received by an individual on different organs.  As discussed in WASH-1400, dose conversion factors for the incorporation of radioactive material in the body give the dose received by individual organs over a time interval per curie intake by inhalation or ingestion. For external exposure, the dose conversion factors give the dose received by each organ per curie of radioactive material in a cubic meter of air or per curie of radioactive material deposited uniformly on a square meter of horizontal surface. The calculation of these dose conversion factors requires elaborate computer models with appropriate physiological parameters for a human body. These calculations need only be performed once for each type of radioactive material, organ, exposure mode, and time interval. From these calculations, a table can be prepared for use in the consequence model.



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Dose Equivalent</b>	
<p>A measure of the biological damage to living tissue as a result of radiation exposure. (see <i>Dose</i>)</p>	<p>In a Level 3 QRVA, a measure of biological damage because of radiation exposure is needed to estimate health effects. The dose equivalent is calculated as the product of absorbed dose in tissue multiplied by a quality factor and then sometimes multiplied by other necessary modifying factors at the location of interest. The dose equivalent is expressed numerically in units of rems or sieverts.</p> <p>The NRC Website Glossary states that as defined in Title 10 of the <i>Code of Federal Regulations</i> (10 CFR) 20.1003, "Definitions", the committed dose equivalent (CDE) is the dose to some specific organ or tissue of reference that will be received from an intake of radioactive material by an individual during the 50-year period following the intake. In the event that an individual inhales or ingests radioactive material, the individual will continue to receive a dose from this event for the rest of his or her life.</p> <p>The NRC Website Glossary also states that as defined in 10 CFR 20.1003, the committed effective dose equivalent (CEDE) is the sum of the products of the committed dose equivalents for each of the body organs or tissues that are irradiated, multiplied by the weighting factors applicable to each of those organs or tissues. The CEDE reflects the fact that different organs in the body are affected differently by radiation.</p> <p>The total effective dose equivalent (TEDE) is the sum of the external and the internal doses to an individual exposed to radiation. In a QRVA, the total effective dose equivalent is needed to calculate offsite health effects. According to the NRC Website Glossary, the TEDE is the sum of the deep-dose equivalent (for external exposures) and the CEDE (for internal exposures). The deep-dose equivalent is the external whole-body exposure dose equivalent at a tissue depth of 1 cm. Whole body exposure includes at least the external exposure, head, trunk, arms above the elbow, or legs above the knee. Where a radioisotope is uniformly distributed throughout the body tissues, rather than being concentrated in certain parts, the irradiation can be considered as whole-body exposure.</p>
<b>Dose Rate</b>	
<p>The amount of absorbed dose delivered per unit time. (see <i>Dose, Exposure, Exposure Time</i>)</p>	<p>In a Level 3 QRVA a dose rate is needed to calculate the health effects. The units in which the dose rate is expressed are usually rems or sieverts per hour. Dose rate is the same as exposure rate. A QRVA considers two types of exposures: acute and chronic. An acute exposure involves a large exposure received over a short period of time; i.e., a high exposure rate. Chronic exposures involve exposure at a low rate received over a long period of time, such as during a lifetime.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Dose Response Model</b>	
A model that reflects the relationship between low doses of ionizing radiation and the potential for cancer. (see <i>Dose, Linear No-Threshold Model</i> )	In a Level 3 QRVA, a dose response model is used to calculate frequency of latent cancers in the affected population, based on the dose received from the postulated accidents.  There is some debate about the appropriate dose-response relationship for cancer risk following exposure to ionizing radiation. For example, in most QRVAs, a linear relationship is assumed in which the cancer risk increases in direct proportion to the dose and there is no lower dose limit below which there is no risk. Others believe there is a nonlinear relationship, in which cancer risk increases in a more complex manner relative to dose.
<b>Dosimetry</b>	
The measurement and calculation of the absorbed dose in matter and tissue resulting from the exposure to ionizing radiation. (see <i>Dose</i> )	In a Level 3 QRVA, dose is calculated to estimate health effects on the population affected by a severe accident. Dosimetry is the process of determining dose from exposure to radiation.  To determine the dose received by exposed individuals, dosimetry attempts to estimate the dose received directly or indirectly via the various dose pathways, including cloudshine, water immersion, groundshine, skin deposition, inhalation, and ingestion.
<b>Dynamic QRVA</b>	
A QRVA that accounts for time-dependent effects by integrating them directly into the computer model. (see <i>QRVA, Living QRVA</i> )	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.  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.  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 represents the as-built as-operated facility.
<b>Early Containment Failure</b>	
(see <i>Containment Failure</i> )	The term early containment failure is discussed under the discussion for the term "Containment Failure."
<b>Early Fatality</b>	



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<i>(see Fatality)</i>	The term early fatality is discussed under the discussion for the term "Fatality."
<b>Early Fatality Risk</b>	
<i>(see Fatality)</i>	The term early fatality risk is a type of risk-involved fatality caused by exposure to radioactive materials and is defined under "Fatality."
<b>Economic Factors</b>	
The considerations taken into account when assessing costs related to a release of radioactive material to the environment. <i>(see Economic Impact)</i>	<p>The Level 3 portion of a QRVA assesses the injuries and economic losses that might result if radioactivity 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.</p> <p>An illustrative list of required cost inputs from NUREG/CR-2300 includes:</p> <ul style="list-style-type: none"> <li>• evacuation cost per person</li> <li>• value of residential, business, and public areas per person</li> <li>• relocation cost per person</li> <li>• decontamination cost per acre for farm areas</li> <li>• decontamination cost per person for residential, business, and public areas</li> <li>• compensation rate per year for residential, business, and public areas (i.e., fraction of value)</li> <li>• average value of farmland per acre for state, county, or smaller areas</li> <li>• average annual value of farm sales per acre for state, county, or smaller areas</li> <li>• miscellaneous information, such as seeding and harvesting month, fraction of land devoted to farming, and fraction of farm sales due to dairy production.</li> </ul>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Economic Impact</b>	
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. <i>(see Economic Factors)</i>	In a Level 3 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 QRVA.  The economic model in a Level 3 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 radiation protection measures. Other direct costs may include costs of treatment of individuals exposed to radiation. Some models may include indirect economic impacts (e.g., litigation costs, government spending for disaster relief, regional economic activity impacts).
<b>Economic Impact Risk</b>	
<i>(see Economic Impact)</i>	The economic impact risk is the risk resulting from the economic impact of the accident and is defined in the discussion under "Economic Impact."
<b>Emergency Preparedness</b>	
The actions put into place to prepare personnel to rapidly identify, evaluate, and react to emergencies. <i>(see Emergency Response, Accident Mitigation)</i>	In a Level 3 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 radiological emergency.  The definition provided is based on the definition in the NRC Website Glossary.



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Emergency Response</b>	
The actions initiated by the facility to mitigate the consequences of an accident that could potentially result in radioactive material release. (see <i>Emergency Preparedness, Accident Mitigation, Cohort</i> )	<p>In a Level 3 QRVA, the emergency response is taken into account when calculating the consequences of the postulated accidents.</p> <p>The emergency response encompasses the actions used to mitigate the consequences of an emergency, such as a severe nuclear accident, 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).</p> <p>The definition provided is based on the definition in the IAEA Safety Glossary.</p>
<b>End State</b>	
A set of conditions selected to characterize the facility states at the end of a chain of events. (see <i>Accident Sequence</i> )	<p>In most QRVAs, end states associated with Level 1 accident sequences typically include: success states (i.e., those states with negligible impact), and core damage or facility damage states. End states associated with Level 2 sequences usually are containment failure modes or release categories.</p> <p>The following figure illustrates different end states of an event tree:</p> <div style="text-align: center;"> <pre> graph LR     IE[Initiating Event: Jump from airplane] --&gt; MC[Main Chute]     IE --&gt; RC[Reserve Chute]     MC -- "System succeeds" --&gt; ES1[Main chute works, float to ground]     MC -- "System fails" --&gt; RC     RC -- "System succeeds" --&gt; ES2[Reserve chute works, float to ground]     RC -- "System fails" --&gt; ES3[Both chutes fail, jumper casualty]     </pre> </div> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Environmental Qualification</b>	

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
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, radiation levels, 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 reactors 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.  The definition provided was based on the definition in the NRC Website Glossary.
<b>Epistemic Uncertainty</b>	
<i>(see Uncertainty)</i>	Epistemic uncertainty is a type of uncertainty and is defined under "Uncertainty."
<b>Error Factor (Human)</b>	
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.  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.  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 <sup>th</sup> percentile divided by the median (i.e., the 50 <sup>th</sup> percentile).
<b>Event Scenario</b>	
<i>(see Accident Sequence)</i>	The term event scenario has the same meaning as accident sequence and is defined under "Accident Sequence."
<b>Event Sequence</b>	
<i>(see Accident Sequence)</i>	The term event sequence has the same meaning as accident sequence and is defined under "Accident Sequence."
<b>Event Sequence Analysis</b>	
<i>(see Accident Sequence Analysis)</i>	The term event sequence analysis is another way of describing an accident sequence and is defined under "Accident Sequence Analysis."



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Event Sequence Class</b>	
<i>(see Accident Sequence Class)</i>	The term event sequence class has the same meaning as accident sequence class and is defined under "Accident Sequence Class."
<b>Event Sequence Diagram</b>	
<p>A flowchart that represents various accident scenarios that can occur as a result of a facility upset condition. <i>(see Event Tree, Top Event)</i></p>	<p>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.</p> <p>The following figure illustrates a simple ESD. The oval to the left corresponds to top events in the "jump from airplane" event tree.</p> <pre> graph TD     A([Initiating Event— Jump from Airplane]) --&gt; B[Evaluate the Status of Both Chutes (Main and Reserve)]     B -- Yes --&gt; C{Main Chute Works?}     C -- Yes --&gt; D([Float to Ground])     C -- No --&gt; E{Reserve Chute Works?}     E -- Yes --&gt; F([Float to Ground])     E -- No --&gt; G([Jumper Casualty])     </pre>
<b>Event Sequence Group</b>	
<i>(see Accident Sequence Class)</i>	The term event sequence group has the same meaning as accident sequence group and is defined under "Accident Sequence Class."
<b>Event Sequence Type</b>	
<i>(see Accident Sequence Class)</i>	The term event sequence type has the same meaning as accident sequence type and is defined under "Accident Sequence Class."

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<p><b>Event Tree</b></p> <p>A logic diagram that graphically represents the various scenarios that can occur as a result of an upset condition. (see <i>Accident Sequence, Containment Event Tree, Top Event, Accident Progression Event Tree, Bridge Tree</i>)</p>	<p>In a QRVA, event trees are used in various parts of the analysis:</p> <ul style="list-style-type: none"> <li>• Level 1 event trees provide the facility response logic from the initiating event to the successful prevention of core damage or core damage end states.</li> <li>• 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 core damage occurs.</li> <li>• 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.</li> </ul> <p>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. An example of a simple event tree is shown below:</p> <div style="text-align: center;"> </div> <p>An event tree has also been defined as:</p> <ul style="list-style-type: none"> <li>• “A logic diagram that begins with an initiating event or condition and progresses through a series of branches that represent expected</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
	<p>system or operator performance that either succeeds or fails. The progression arrives at either a successful or failed end state.”</p> <ul style="list-style-type: none"> <li>• “An event tree graphically represents the various accident scenarios that can occur as a result of an initiating event (i.e., a challenge to plant operation). Toward that end, an event tree starts with an initiating event and develops scenarios, or sequences, based on whether a plant 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 reactor core damage.”</li> </ul>
<b>Event Tree Sequence</b>	
<i>(see Accident Sequence)</i>	The term event tree sequence is a specific description of an accident sequence and is defined under “Accident Sequence.”
<b>Event Tree Top Event</b>	
<i>(see Top Event)</i>	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.”
<b>Exclusion Area Boundary</b>	
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.	<p>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.</p> <p>The exclusion area and its boundary are important for reactor siting considerations as a location where acceptable dose limits following a release must be met. For example, Title 10 of the CFR 100.11, “Determination of Exclusion Area, Low Population Zone, and Population Center Distance”, states that the applicant (of a siting permit) should determine the following: an exclusion area of such size that an individual located at any point on its boundary for 2 hours immediately following onset of the postulated fission product release would not receive a total radiation dose to the whole body in excess of 25 rem or a total radiation dose in excess of 300 rem to the thyroid from iodine exposure.</p> <p>The definition provided is based on the definition in the NRC Website Glossary.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Expert Elicitation</b>	
<p>A formal, structured, and documented process in which judgments from expert(s) are obtained. <i>(see Expert Judgment)</i></p>	<p>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.</p> <p>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."</p> <p>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.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Expert Judgment</b>	
<p>Information (or opinion) provided by one or more technical experts that is based on their experience and knowledge. <i>(see Expert Elicitation)</i></p>	<p>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.</p> <p>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.</p> <p>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."</p> <p>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."</p>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Exposure</b>	
The state of being subjected to ionizing radiation. (see <i>Exposure Time, Cloudshine, Groundshine, Inhalation, Ingestion, Skin Deposition, Health Effects</i> )	In a Level 3 QRVA, the offsite health effects resulting from exposure to ionizing radiation is considered. As stated in the NRC Website Glossary, exposure occurs through absorption of ionizing radiation because of an external source or an internal exposure caused by inhalation or ingestion of a radioisotope. 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.
<b>Exposure Pathways</b>	
The various means by which exposure to radiation occurs and dose to recipients is delivered. (See <i>Exposure, Exposure Time, Cloudshine, Water Immersion, Groundshine, Inhalation, Ingestion, Skin Deposition, Health Effects</i> )	In a Level 3 QRVA, exposure pathways to an individual are assumed for the consequence calculations. Cloudshine, sometimes referred to as air submersion, is the pathway by which external dose is given to an individual exposed to contaminated air; water immersion is a pathway by which external dose is given to an individual immersed in contaminated water (e.g., by bathing or swimming); inhalation is the pathway by which internal dose is given by breathing in contaminated air (resuspension inhalation is the pathway by which internal dose is given to an individual from breathing resuspended material previously deposited on the ground); ingestion is the pathway by which internal dose is given from consuming contaminated food or water; groundshine is the pathway by which external dose is given to an individual standing on contaminated ground; and skin deposition is exposure resulting from radioactive material deposited directly onto the surface of the body.
<b>Exposure Rate</b>	
(see <i>Dose Rate</i> )	The exposure has the same meaning as dose rate and is defined under "Dose Rate".
<b>Exposure Time</b>	
Duration of radiation exposure used to estimate the dose received by an individual. (see <i>Health Effects, Exposure</i> )	In a Level 3 QRVA, the exposure time is needed to calculate the dose and subsequent health consequences to affected individuals.  The QRVA considers two types of exposures: acute and chronic. An acute exposure involves a large exposure received over a short period of time. Chronic exposures involve exposure received over a long period of time, such as during a lifetime.

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>External Event</b>	
<p>The term external event is no longer used and has been replaced by the term external hazard. (see Hazard)</p>	<p>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.</p> <p>The no-longer-used term, external event, is defined in the ASME/ANS PRA Standard as “an event originating outside a nuclear power plant that directly or indirectly causes an initiating event and may cause safety system failures or operator errors that may lead to core damage or acute fuel release. Events such as earthquakes, tornadoes, and floods from sources outside the plant and fires from sources inside or outside the plant are considered external events. By historical convention, loss of offsite power not caused by another external event is considered to be an internal event.”</p> <p>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.</p> <p>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.</p>
<b>External Flood</b>	
<p>A flood initiated outside the facility boundary that can affect the operability of the facility. (see Hazard, External Flood Analysis, Internal Flood)</p>	<p>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.</p> <p>The definition provided was based on the definition in NUREG-1742.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>External Flood Analysis</b>	
A process used to assess potential risk from external floods. <i>(see Hazard Analysis, External Flood)</i>	In a QRVA, an external flood analysis quantifies the risk contribution (e.g., LOFICF and large release frequency) 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.
<b>External Flood Fragility Analysis</b>	
<i>(see Fragility Analysis)</i>	The term external flood fragility analysis is a type of fragility analysis and is included in the discussion to the term "Fragility Analysis."
<b>External Flood Hazard Analysis</b>	
<i>(see Hazard Analysis)</i>	The term external flood hazard analysis is a specific type of hazard analysis and is defined under "Hazard Analysis."
<b>External Flood Facility Response Analysis/Model</b>	
<i>(see Facility Response Analysis/Model)</i>	The term external flood facility response analysis is a type of facility response analysis and is included under "Facility Response Analysis/Model."
<b>External Hazard</b>	
<i>(see Hazard)</i>	The term external hazard is related to the term hazard and is defined under "Hazard."
<b>External Hazard Analysis</b>	
<i>(see Hazard Analysis)</i>	The term external hazard analysis is a type of hazard analysis and is defined under "Hazard Analysis."
<b>Failure Mechanism</b>	
The fault associated with a component that causes it to malfunction. <i>(see Failure Mode)</i>	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.  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."  While failure mechanism is a cause of failure, failure mode is the functional manifestation of failure (e.g., failure to start, failure to run).

**Table D-1. Terms and Definitions (Continued) -**

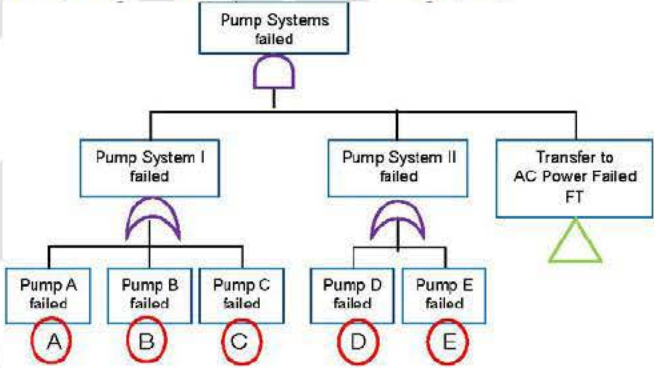
Term and Definition	Discussion
<b>Failure Mode</b>	
<p>The manner in which a component fails to perform its function. (see <i>Failure Mechanism, Failure Modes and Effects Analysis</i>)</p>	<p>In a QRVA, the failure modes of a component are represented as basic events, and while it is a visible manifestation 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.</p> <p>In a fire QRVA, spurious (unintended) operation is also defined as a failure mode.</p> <p>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).”</p> <p>A failure modes and effects analysis can be used to identify component failure modes and evaluate their effects on other components, subsystems, and systems.</p>
<b>Failure Modes and Effects Analysis</b>	
<p>A process for identifying failure modes of specific components and evaluating their effects on other components, subsystems, and systems. (see <i>Failure Mode</i>)</p>	<p>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).</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Failure Probability</b>	
<p>(see <i>Probability</i>)</p>	<p>The term failure probability is a specific type of probability and is defined under “Probability.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Fatality (Early, Latent, Prompt, Latent Cancer)</b>	
Death occurring as a result of exposure to radioactive material. <i>(see Exposure, Quantitative Health Objectives)</i>	<p>In a Level 3 QRVA, one of the objectives is to calculate the dose received by the population surrounding the facility as a result of a potential release of radioactive material. Depending on the amount of dose 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 QRVA.</p> <p>Early fatalities, synonymous with prompt fatalities, are defined as deaths from the acute effects of radiation that may occur within a few months of the exposure. Latent cancer fatalities are defined as deaths from cancer caused by chronic effects of radiation exposure; latent cancer fatalities may occur years after the exposure.</p> <p>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., groundshine, cloudshine, and skin deposition), as well as long-term pathways (e.g., resuspension inhalation and ingestion).</p>
<b>Fatality Risk (Early, Latent, Prompt)</b>	
<i>(see Fatality)</i>	The fatality risk (early or prompt fatality risk, latent fatality risk) is the risk involving fatalities caused by exposure to radioactive materials and is defined in the discussion under "Fatality."

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Fault Tree</b>	
<p>A deductive logic diagram that graphically represents the various failures that can lead to a predefined undesired event. (see <i>Top Event, Event Tree</i>)</p>	<p>In a QRVA, fault trees are used to depict the various pathways that lead to a system failure.</p> <p>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.</p> <p>A fault tree also has been defined as:</p> <ul style="list-style-type: none"> <li>• “A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events.”</li> <li>• “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.”</li> </ul> <p>The following is an example of a fault tree diagram:</p> 
<b>Fault Tree Top Event</b>	
<p>(see <i>Top Event</i>)</p>	<p>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.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Feed and Bleed, Bleed and Feed</b>	
<p>A method of core cooling in a pressurized-water reactor by providing cooling water to the reactor while removing heated coolant through open reactor vessel relief valves.</p>	<p>In a QRVA, feed and bleed is often included as a core heat removal option for pressurized-water reactors when secondary cooling (e.g., auxiliary feedwater) is unavailable. To remove the core (i.e., decay) heat from the reactor vessel, water from a storage tank or recirculated from the containment sump is injected into the reactor vessel through safety or nonsafety grade pumping systems (feed), and the pressurizer power-operated relief valves (PORV) or safety valves are opened to discharge the heated coolant from the reactor vessel (bleed).</p> <p>The terms feed and bleed and bleed and feed are similar in meaning and often used interchangeably. However, in certain instances, these terms may be used to distinguish the manner in which this decay heat removal option is accomplished. In some facilities, the injection pumps may be capable of injecting coolant at full reactor coolant system pressure while discharging reactor coolant through the safety valves. In this design, the injection of water (feed) can occur before opening the safety valves (bleed), such that this decay heat option may be referred to as feed and bleed. In other facilities, the injection pumps are not capable of injecting coolant at full system pressure, but instead must rely upon operator actions to open one or more PORVs in a timely matter. In this situation, the reactor vessel pressure is first reduced by the release of coolant (bleed), with subsequent injection of coolant from the injection pumps (feed). This decay heat option may be referred to as bleed and feed.</p>
<b>Fire QRVA Facility Response Model (Analysis)</b>	
<p><i>(see Facility Response Analysis)</i></p>	<p>The term fire QRVA facility response analysis is a type of facility response analysis and is defined under “Facility Response Analysis/Model.”</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Fragility</b>	
The likelihood that a component, system, or structure will cease to function given the occurrence of a hazard event of a certain intensity. (see <i>Fragility Analysis, High Confidence of Low Probability of Failure, Fragility Curve</i> )	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.  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.  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.”
<b>Fragility Analysis (External Flood, High Winds, Other External Hazards, Seismic)</b>	
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 <i>Fragility, Fragility Curve</i> )	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.
<b>Fragility Curve</b>	
A graph that plots the likelihood that a structure, system or component will fail versus the increasing intensity of a hazard event. (see <i>Fragility, Fragility Analysis</i> )	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.
<b>Frequency (Accident Sequence, Core Damage, Initiating Event, Acute Fuel Release, Large Release, Radioactive Material Release)</b>	
The expected number of occurrences of an	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 core damage accident sequences; the latter frequencies are summed to



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<p>event or accident condition expressed per unit of time. (<i>see Probability</i>)</p>	<p>provide an overall LOFICF. For a Level 2 QRVA, frequencies are calculated for the facility damage states and for the release of radioactive material (e.g., AFRF, large release frequency, and the overall radioactive material release frequency). For a Level 3 QRVA, frequencies are calculated for accident consequences (i.e.; early and latent fatalities) and, sometimes, economic consequences.</p> <p>Frequency is normally expressed in events per facility (or reactor) operating year or events per facility (or reactor) calendar year.</p> <p>The subset terms of frequency can be defined as follows:</p> <ul style="list-style-type: none"> <li>• <b>Accident Sequence Frequency:</b> 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 core damage. (<i>see Accident Sequence</i>)</li> <li>• <b>Loss of Fuel Inventory Control Frequency:</b> The sum of the accident sequence frequencies of those accident sequences whose end state is core damage.</li> <li>• <b>Initiating Event Frequency:</b> The frequency of an event originating from an internal or external hazard that both challenges normal facility operation and requires successful mitigation.</li> <li>• <b>Acute Fuel Release Frequency:</b> The frequency of a rapid, unmitigated release of airborne fission products 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.</li> <li>• <b>Large Release Frequency:</b> The Commission has not approved a formal definition of a large release or a large release frequency. One informal definition for large release frequency is the frequency of an unmitigated release of airborne fission products from the containment to the environment that is of sufficient magnitude to cause severe health effects, regardless of its timing. The history of the use of the term “Large Release Frequency” is provided in SECY-13-0029. (<i>see Large Release</i>)</li> <li>• <b>Radioactive Material Release Frequency:</b> The frequency of the release of radioactive material from the containment to the environment. This may refer to the total frequency of all releases regardless of size or timing. The radioactive material release frequency may also be subdivided depending on the size and timing of the release. AFRF and large release frequency are defined above. A small early 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</li> </ul>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
	<p>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. <i>(see Radioactive Material Release)</i></p> <p>In some instances, the terms frequency and probability are used interchangeably, but incorrectly. Unlike frequency, probability represents a unitless quantity.</p>
<b>Frequentist Analysis, Frequentist Estimation, Frequentist Statistics</b>	
<p>A type of data analysis that relies solely on actual occurrences of the event under consideration. <i>(see Bayesian Analysis)</i></p>	<p>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.</p> <p>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.</p> <p>In risk analysis, both frequentist and Bayesian analysis may be used, depending on whether occurrence data is sufficiently abundant.</p> <p>The terms frequentist analysis, frequentist estimation, and frequentist statistics are used interchangeably.</p>
<b>Frequentist Estimation</b>	
<i>(see Frequentist Analysis)</i>	The term frequentist estimation has the same meaning as frequentist analysis and is defined the same as the term "Frequentist Analysis."
<b>Frequentist Statistics</b>	
<i>(see Frequentist Analysis)</i>	The term frequentist statistics has the same meaning as frequentist analysis and is defined the same as the term "Frequentist Analysis."
<b>Frontline System</b>	
<p>A system used to directly provide a safety function. <i>(see Support System)</i></p>	<p>In a QRVA, frontline systems are modeled to help represent the ways in which a facility can prevent core damage 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 (e.g., core or containment cooling, coolant makeup, reactivity control, or reactor vessel pressure control) modeled in the PRA."</p> <p>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.</p>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Full Power</b>	
The state of operation in which the reactor is critical and producing 100-percent power. <i>(see At-Power, Low Power and Shutdown)</i>	A QRVA models the different FOS of the facility. Operation at full power is one FOS, while several FOSs are needed to characterize the facility during the various stages of low-power and shutdown. These FOSs are distinguished in the QRVA model because the facility response (e.g., accident sequences) differs during different FOSs.  Historically, the term full power was used to denote any power level between low power and 100-percent power. This definition has been recently modified so that full power currently refers just to 100-percent power of the reactor core, while at-power covers the range of powers from low power up to and including 100-percent power.
<b>Full-Scope QRVA</b>	
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. <i>(see QRVA, Risk Metric)</i>	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 (core damage), Level 2 (radioactive material release) and Level 3 (consequences) QRVA that addresses both internal and external hazards at all power modes (at-power, low-power, and shutdown). These power modes commonly are referred to as FOS.  A full-scope site QRVA may also consider risks from the spent fuel pool and any other fuel storage facility on site. Offsite risk metrics in the Level 3 portion may include both health effects and economic considerations brought about by the release of radioactive material.
<b>Fussell-Vesely Importance</b>	
<i>(see Importance Measure)</i>	The term Fussell-Vesely importance is one type of importance measure and is defined under "Importance Measure."
<b>General Transient</b>	
<i>(see Transient)</i>	The term general transient has the same meaning as transient and is defined under "Transient."
<b>Groundshine</b>	
Exposure from radioactive material deposited on the ground. <i>(see Exposure Pathways, Cloudshine, Water Immersion, Inhalation, Ingestion, Skin Deposition)</i>	In a Level 3 QRVA, for the consequence calculation groundshine is one of the assumed pathways by which an individual can receive doses. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Hazard (Type (Internal, External), Group, Event)</b>	
<p>Anything that has the potential to cause an undesired event or condition that leads to equipment damage. <i>(see Hazard Analysis, Initiating Event)</i></p>	<p>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 core damage or radioactive material release.</p> <p>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.”</p> <p>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 trip and possibly other damage when the facility is at-power or result in the loss of a key safety function during non-power operations. 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:</p> <ul style="list-style-type: none"> <li>• Earthquakes are a hazard;</li> <li>• 0.1g, 0.3g, 0.5g earthquakes and their associated spectral shapes and time histories may be defined as hazard events;</li> <li>• A manual facility trip is typically the initiating event for the 0.1g earthquake, and a loss of offsite power is typically assumed as the initiating event for the 0.3g and 0.5g earthquakes.</li> </ul> <p>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 plant. External hazards include events such as flooding and fires external to the plant, tornadoes, earthquakes, and aircraft crashes.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Hazard Analysis (External, External Flood, High Wind, (Probabilistic) Seismic, Other Hazards)</b>	
<p>A process used to assess potential facility challenges, including natural phenomena, and to assess their likelihood, typically as a function of severity.</p>	<p>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 hazard analysis are used as input to the QRVA, which subsequently examines the hazards with respect to risk.</p> <p>Listed below are specific types of hazard analyses:</p> <ul style="list-style-type: none"> <li>• <u>External hazard analysis</u>: 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).</li> <li>• <u>External flood hazard analysis</u>: The objective is to evaluate the frequency of occurrence of different external flood severities.</li> <li>• <u>High wind hazard analysis</u>: The objective is to evaluate the frequency of occurrence of different intensities of high winds.</li> <li>• <u>(Probabilistic) seismic hazard analysis</u>: 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.</li> <li>• <u>Other hazards analysis</u>: Evaluates the frequency of occurrence of different intensities of other internal or external hazards (e.g., external fires).</li> </ul> <p>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.”</p> <p>An example of a hazard curve is shown below.</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
	<p>Typical Seismic Hazard Curves for a Nuclear Power Plant Site</p>
<b>Hazard Event</b>	
<i>(see Hazard)</i>	The term hazard event is related to the term hazard and is defined under "Hazard."
<b>Hazard Group</b>	
<i>(see Hazard)</i>	The term hazard group is related to the term hazard and is defined under "Hazard."
<b>Hazard Type</b>	
<i>(see Hazard)</i>	The term hazard type is related to the term hazard and is defined under "Hazard."
<b>Health Effects</b>	
The effects of radioactive material on the health and safety of exposed individuals. <i>(see Quantitative Health Objectives, Accident Consequence, Exposure Time, Land Contamination)</i>	<p>In a Level 3 QRVA, the health effects represent the main component of the calculated risk. Health effects from radioactive material (i.e., ionizing radiation) usually are distinguished as acute or latent.</p> <p>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 radiation doses. Acute fatalities and injuries are expected to occur within 1 year of an accident or sooner.</p> <p>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.</p> <p>Public health effects refer to illnesses or fatalities to the population beyond the site boundary resulting from the release of radiation.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>High Confidence of Low Probability of Failure</b>	
<p>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 <i>Seismic Margin, Fragility</i>)</p>	<p>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.</p> <p>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 core damage. It is used extensively in a seismic margin analysis.</p> <p>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.”</p>
<b>High-Level Requirements</b>	
<p>The minimum requirements for a technically acceptable baseline QRVA, independent of application. (see <i>Supporting Requirements</i>)</p>	<p>For a base QRVA, NRC RG 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.</p> <p>RG 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.”</p> <p>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.”</p> <p>The definition provided was based on the definition in the introduction section of ASME/ANS PRA Standard.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>High-Pressure Melt Ejection</b>	
A phenomenon in which molten core material penetrates the reactor vessel and is forcibly ejected under high pressure. (see <i>Core Melt</i> )	In a QRVA, high-pressure melt ejection (HPME) is a phenomenon that could lead to containment failure and release of radioactive material to the environment before evacuation of the surrounding population.  If the core melts and penetrates the reactor pressure vessel while the reactor coolant system is at high pressure (>400 psi), the core debris would be ejected into the reactor cavity. This phenomenon is called HPME.  A phenomenon often associated with HPME is direct containment heating (DCH). DCH can occur in the following manner: As the core debris is being ejected from the reactor vessel (depending on the configuration of the reactor cavity), it is possible that it will be transported into the containment atmosphere and directly heat the atmosphere. This heating can substantially increase the pressures in containment. It is also possible that combustible gases in the containment atmosphere could ignite and burn as a result of the transported core debris, adding to the containment heating and therefore the pressure in containment.
<b>High-Wind Fragility Analysis</b>	
(see <i>Fragility Analysis</i> )	High-wind fragility analysis is a type of fragility analysis and is included in the discussion under "Fragility Analysis."
<b>High-Wind Hazard Analysis</b>	
(see <i>Hazard Analysis</i> )	The term high-wind hazard analysis is a specific type of hazard analysis and is defined under "Hazard Analysis."
<b>High-Wind Facility Response Analysis/Model</b>	
(see <i>Facility Response Analysis/Model</i> )	The high-wind facility response analysis is a type of facility response analysis and is included in the discussion under "Facility Response Analysis/Model."
<b>High Winds</b>	
Winds of a certain size that could potentially damage or affect the operability of a facility. (see <i>Hazard</i> )	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.



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Human Action (Operator Action)</b>	
<p>An action performed by facility personnel. (see <i>Human Failure Event, Human Reliability Analysis</i>)</p>	<p>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.</p> <p>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 licensed individual in the control room.</p> <p>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.</p>
<b>Human Error (Operator Error)</b>	
<p>Any human action, including inaction, which exceeds some limit of acceptability, excluding malevolent behavior. (see <i>Human Failure Event, Human Reliability Analysis</i>)</p>	<p>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.</p> <p>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 licensed individual (i.e., operator) in the control room.</p> <p>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.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Human Error Event</b>	
<p>(see <i>Human Failure Event</i>)</p>	<p>A human error event is a type of human error modeled in a QRVA and is defined under “Human Failure Event.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Human Error Factor</b>	
<i>(see Error Factor)</i>	A human error factor is a specific type of error factor applicable to human reliability analysis and is defined under “Error Factor.”
<b>Human Error Probability</b>	
<i>(see Probability)</i>	A human error probability is a specific type of probability applicable to human reliability analysis and is defined under “Probability.”
<b>Human Failure Event, Human Error Event</b>	
A basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action. <i>(see Human Action, Human Error)</i>	<p>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.</p> <p>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.</p> <p>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.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Human Reliability Analysis</b>	
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. <i>(see Human Action, Human Error)</i>	<p>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.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Importance Measure (Risk Reduction Worth, Risk Achievement Worth, Fussell-Vesely, Birnbaum Importance, Uncertainty Importance)</b>	
<p>A metric that provides either the absolute or relative contribution of a component, system, structure, or human action to the defined risk.</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Risk Reduction Worth:</b> 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.”</li> <li>• <b>Risk Achievement Worth:</b> 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.”</li> <li>• <b>Fussell-Vesely:</b> 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.</li> <li>• <b>Birnbaum Importance (Bi):</b> 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.</li> <li>• <b>Uncertainty Importance:</b> 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.</li> </ul>
<b>Important to Safety</b>	

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<i>(see Safety Significant)</i>	The term important to safety has a safety connotation and is defined under "Safety Significant."
<b>Incremental Conditional Probability (Core Damage, Acute Fuel Release)</b>	
A measure of the impact of a temporary facility modification on the probability of an undesired end state. <i>(see Conditional Probability, Instantaneous Conditional Probability).</i>	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 core damage when compared to the baseline core damage probability. Because the probability of core damage depends on the temporary modification or change at the facility, it is therefore a conditional probability.  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.
<b>Ingestion</b>	
Exposure from intake of food and water contaminated with radioactive material. <i>(see Exposure Pathways, Exposure, Exposure Time, Cloudshine, Water Immersion, Groundshine, Inhalation, Skin Deposition, Health Effects)</i>	In a Level 3 QRVA, for the consequence calculation ingestion is one of the assumed pathways by which an individual can receive doses. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Inhalation</b>	
Exposure from breathing radioactive material. ( <i>see Exposure Pathways, Cloudshine, Water Immersion, Groundshine, Ingestion, Skin Deposition</i> )	In a Level 3 QRVA, for the consequence calculation inhalation is one of the assumed pathways by which an individual can receive doses. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Initiating Event, Initiator</b>	
<p>An event that perturbs the steady-state operation of the facility and could lead to an undesired facility condition.</p>	<p>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 core damage.</p> <p>Initiating events can arise from the following:</p> <ul style="list-style-type: none"> <li>• Internal Hazards, which include: <ul style="list-style-type: none"> <li>- Internal event (<i>see Internal Event</i>)</li> <li>- Floods (<i>see Internal Flood</i>)</li> <li>- Fires (<i>see Appendix A for fire terms</i>)</li> </ul> </li> <li>• External Hazards, which include: <ul style="list-style-type: none"> <li>- Floods (<i>see External Flood</i>)</li> <li>- High winds (<i>see High Winds</i>)</li> <li>- Seismic events (<i>see Hazard Analysis</i>)</li> <li>- Other external hazards</li> </ul> </li> </ul> <p>These hazards result in different types of initiating events. Examples of initiating events are transients (<i>see Transient</i>) and loss-of-coolant accidents (<i>see Loss-of-Coolant Accident</i>).</p> <p>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 (e.g., loss of a feedwater pump resulting in a transient).</p> <p>The ASME/ANS PRA Standard defines an initiating event as “an event either internal or external to that which perturbs the steady state operation of the plant by challenging plant control and safety systems whose failure could potentially lead to core damage or release of airborne fission products. These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds).”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Initiating Event Analysis</b>	
<p>The process used to identify events that perturb the steady-state operation of the facility and could lead to an undesired facility condition. <i>(see Initiating Event, Master Logic Diagram)</i></p>	<p>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 core damage 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.</p> <p>NRC Regulatory Guide 1.200 states that initiating event analysis “identifies and characterizes the events that both challenge normal plant operation during power or shutdown conditions and require successful mitigation by plant equipment and personnel to prevent core damage from occurring. Events that have occurred at the plant and those that have a reasonable probability of occurring are identified and characterized. An understanding of the nature of the events is performed such that a grouping of the events, with the groups defined by similarity of system and plant responses (based on the success criteria), may be performed to manage the large number of potential events that can challenge the plant.”</p>
<b>Initiating Event Frequency</b>	
<i>(see Frequency)</i>	The term initiating event frequency is a type of frequency that is defined under “Frequency.”
<b>Initiator</b>	
<i>(see Initiating Event)</i>	The term initiator is similar in meaning to initiating event and is defined under “Initiating Event.”

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Instantaneous Conditional Probability (Core Damage, Acute Fuel Release)</b>	
Event probability at the specific time the facility is analyzed, given that a prior event has occurred. (see Conditional Probability, Incremental Conditional Probability)	<p>Using a QRVA, instantaneous conditional probability can be calculated for core damage 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, core damage or acute fuel release is “conditional” on the probability of a prior event occurring.</p> <p>The following are other definitions that could describe instantaneous conditional probability:</p> <ul style="list-style-type: none"> <li>• The probability that an undesired facility end state is reached given an initiating event and the actual (instantaneous) facility configuration.</li> <li>• The average probability that an undesired facility end state is reached, weighted over all credible initiating events, for the actual (instantaneous) facility configuration.</li> </ul> <p>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.</p>
<b>Interfacing-Systems Loss-of-Coolant Accident</b>	
A loss-of-coolant accident characterized by high-pressure reactor coolant being released into a low-pressure system. (see <i>Loss-of-Coolant Accident</i> )	<p>In a QRVA, accidents involving an interfacing-systems loss-of-coolant accident (ISLOCA) are modeled because they represent a loss of isolation between an ancillary system and the reactor coolant system, which contains radioactive material. This type of accident is important in the QRVA because it may lead to radioactive material bypassing containment and loss of reactor coolant inventory.</p> <p>The ASME/ANS PRA Standard defines ISLOCA as “a loss of coolant accident (LOCA) when a breach occurs in a system that interfaces with the reactor coolant system, where isolation between the breached system and the reactor coolant system fails. An ISLOCA is usually characterized by the over-pressurization of a low-pressure system when subjected to reactor coolant system pressure and can result in containment bypass.”</p> <p>ISLOCAs of most concern are those accidents during which the break flow is discharged outside the reactor containment building. The two main reasons for this concern are:</p> <p>(1) potential high offsite radiological consequences caused by radioactive material bypassing the containment and (2) potential loss of long-term core cooling resulting from loss of reactor coolant system inventory that would otherwise be available for recirculation from the containment sumps.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Internal Event</b>	
<p>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. <i>(see Hazard)</i></p>	<p>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. An example of an internal event modeled in a QRVA would be the random structural failure of a reactor coolant system pipe resulting in a LOCA initiating event. Until the 2009 ASME/ANS PRA Standard revision, this term did not have a consistent definition. In some cases, a fire or flood or both occurring within the facility were considered an internal event. The ASME/ANS PRA Standard has been revised and internal flood and internal fire are not considered internal events.</p> <p>The ASME/ANS PRA Standard defines an internal event as “an event resulting from or involving random mechanical, electrical, structural, or human failures from causes originating within a nuclear power plant that directly or indirectly causes an initiating event and may cause safety system failures or operator errors that may lead to core damage or acute fuel release. By historical convention, loss of offsite power is considered to be an internal event, and internal fire is considered to be an external event, except when the loss is caused by an external hazard that is treated separately (e.g., seismic-induced loss of offsite power). Internal floods sometimes have been included with internal events and sometimes considered as external events. For this standard, internal floods are considered to be internal hazards separate from internal events.”</p>
<b>Internal Fire</b>	
<p>A fire initiated within the facility that can affect the operability of the facility. <i>(see Hazard and Appendix A)</i></p>	<p>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.</p>
<b>Internal Flood, Internal Flooding Event</b>	
<p>A flood initiated within the facility that can affect the operability of the facility. <i>(see Hazard, External Flood)</i></p>	<p>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.</p> <p>The term internal flooding event represents the occurrence of an internal flood.</p>
<b>Internal Flooding Event</b>	
<p><i>(see Internal Flood)</i></p>	<p>The term internal flooding event is the occurrence of an internal flood and is defined under “Internal Flood.”</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Internal Hazard</b>	
<i>(see Hazard)</i>	The term internal hazard is a specific type of hazard and is defined under "Hazard."
<b>Key Assumption</b>	
<i>(see Assumption)</i>	The term key assumption is a specific type of assumption and is defined under "Assumption."
<b>Key Model Uncertainty</b>	
<i>(see Uncertainty)</i>	The term key model uncertainty is a type of uncertainty and is defined under "Uncertainty."
<b>Key Source of Model Uncertainty</b>	
<i>(see Uncertainty)</i>	The term key source of model uncertainty is defined under "Uncertainty."
<b>Key Source of Uncertainty</b>	
<i>(see Uncertainty)</i>	The term key source of uncertainty is defined under "Uncertainty."
<b>Land Contamination</b>	
Contamination of land outside of the facility site boundary with radioactive material released in an accident. <i>(see Health Effects)</i>	In a Level 3 QRVA, land contamination often is evaluated along with health effects. Land contamination refers to the radioactive material deposited on the ground by gravitational settling or the impact during plume passage. Land contamination depends on the characteristics of the radioactivity release and how the land surrounding the facility is used. Land contamination risk involves the frequency and amount of land contamination and its associated cost.
<b>Land Contamination Risk</b>	
<i>(see Land Contamination)</i>	Land contamination risk is sometimes calculated in a Level 3 QRVA and is defined in the discussion under "Land Contamination."
<b>Large Late Release</b>	
<i>(see Radioactive Material Release)</i>	The term large late release is a type of radioactive material release and is defined in the discussion under "Radioactive Material Release."
<b>Large Late Release Frequency</b>	
<i>(see Frequency)</i>	The term large late release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency."
<b>Large Late Release Frequency Analysis</b>	
<i>(see Radioactive Material Release Frequency Analysis)</i>	The term large late release frequency analysis is a type of radioactive material release frequency analysis and is defined under "Radioactive Material Release Frequency Analysis."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Large Release</b>	
Formal definition requires Commission approval. ( <i>see Radioactive Material Release</i> )	<p>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.</p> <p>In the past, the NRC staff has considered several alternate definitions of a large release. These include:</p> <ul style="list-style-type: none"> <li>• A release that would result in one or more early fatalities;</li> <li>• A release that has the potential to result in one early offsite fatality within 1 mile of the facility boundary;</li> <li>• A definition of a large release source term in the traditional form of a fractional release of the core inventory of various radionuclide groups to the environment, the timing of the release, etc.</li> <li>• Any release from an event that involves severe core damage, primary system pressure boundary failure, and early containment failure.</li> </ul> <p>The Commission has not approved a formal definition for the term large release.</p>
<b>Large Release Frequency</b>	
( <i>see Frequency</i> )	The term large release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency."
<b>Late Containment Failure</b>	
( <i>see Containment Failure</i> )	The term late containment failure is a type of containment failure and is defined under "Containment Failure."
<b>Latent Cancer Fatality</b>	
( <i>see Fatality</i> )	The term latent cancer fatality is a type of fatality caused by exposure to radioactive materials and is defined under "Fatality."
<b>Latent Fatality</b>	
( <i>see Fatality</i> )	The term latent fatality is a type of fatality caused by exposure to radioactive materials and is defined under "Fatality."
<b>Latent Fatality Risk</b>	

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<i>(see Fatality)</i>	The term latent fatality risk is a type of risk-involved fatality caused by exposure to radioactive materials and is defined under “Fatality.”
<b>Latent Health Effects</b>	
<i>(see Health Effects)</i>	The term latent health effect refers to a type of health effect and is defined in the discussion under “Health Effects.”
<b>Level 1, 2, 3 QRVA</b>	
A characterization of the scope of a QRVA in terms of increasing specification of consequences. <i>(see QRVA)</i>	<p>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 radioactivity releases as the risk measure, and Level 3 refers to offsite consequences as the risk measure.</p> <p>A Level 2 QRVA takes the results of the Level 1 QRVA (accident sequences resulting in core damage) as input and produces frequencies of radioactivity releases as output. A Level 3 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 QRVA includes both the Level 1 and Level 2 analyses. The figure below illustrates the different QRVA “Levels” and what each calculates.</p> <div style="text-align: center;"> <pre> graph LR     L1[Level 1] --&gt; L2[Level 2]     L2 --&gt; L3[Level 3]     style L1 fill:#add8e6,stroke:#000,stroke-width:1px     style L2 fill:#f08080,stroke:#000,stroke-width:1px     style L3 fill:#90ee90,stroke:#000,stroke-width:1px             </pre> <p>← Level 1 → Level 2 → Level 3 →</p> <p>Computation of core damage frequency    Computation of radioactive material release frequency    Analysis of early and latent fatality</p> </div>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Level of Detail</b>	
<p>The degree of resolution or specificity in the analyses performed in the QRVA. (see <i>Model, Capability Categories</i>)</p>	<p>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).</p> <p>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.</p> <p>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.</p>
<b>Licensing Basis</b>	
<p>The collection of documents or technical criteria that provides the basis upon which the NRC issues a license to construct or operate a facility.</p>	<p>A QRVA is part of the licensing basis for facilities licensed under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." A QRVA also is used to support changes to the licensing basis carried out using regulatory guidance documents such as Regulatory Guide 1.174, RG 1.175, or RG 1.177.</p> <p>The NRC Website Glossary defines licensing basis as "the collection of documents or technical criteria that provides the basis upon which the NRC issues a license to construct or operate a nuclear facility; to conduct operations involving the emission of radiation; or to receive, possess, use, transfer, or dispose of source material, byproduct material, or special nuclear material."</p> <p>10 CFR Part 54 defines current licensing basis (CLB) as "the set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect." The CLB includes NRC regulations, orders, license conditions, exemptions, technical specifications, final safety analysis reports, and licensee commitments to NRC bulletins, generic letters, enforcement actions, and licensee event reports.</p> <p>The definition provided was based on the definition in the NRC Website Glossary.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Licensing-Basis Event</b>	
A postulated accident that a nuclear facility must be designed and built to withstand.	<p>The term licensing-basis event (LBE) is not used in current QRVAs or the current facility regulatory licensing structure. It is a term being used for a potentially new regulatory process. Further information on this regulatory framework can be found in NUREG-1860.</p> <p>This potential future licensing structure is a process that uses both deterministic and probabilistic criteria for selecting the postulated accidents, called LBEs, which a nuclear facility must demonstrate it can withstand (i.e., the facility design and operation must be able to withstand the impact of LBEs without loss to the SSCs needed to ensure public health and safety).</p>
<b>Linear No-Threshold Model</b>	
A dose response model that assumes cancer risk is proportional to the dose received no matter how small the dose. ( <i>see Dose, Dose Response Model</i> )	<p>In a Level 3 QRVA, a dose response model is used to calculate the cancer risk for given levels of a dose to individuals after a severe accident.</p> <p>There is some debate on the appropriate dose response relationship for cancer risk following exposure to ionizing radiation. A linear relationship in which the cancer risk increases in direct proportion to the dose is one view. Another view advocates a nonlinear relationship, in which cancer risk increases in a more complex manner relative to dose. There is also a question about whether a minimum dose exists, below which no increased risk of cancer is found (threshold model), or whether any dose, no matter how small, increases cancer risk (no-threshold model).</p>
<b>Living QRVA</b>	
A QRVA that is maintained so that it reflects the current facility design and operational features. ( <i>see Dynamic QRVA, QRVA Configuration Control, As-Built As-Operated</i> )	<p>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, such as facility-specific changes to the licensing basis discussed in NRC Regulatory Guide 1.174. QRVA configuration control is part of the process used to support a living QRVA.</p> <p>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.</p>
<b>Loss-of-Coolant Accident (Small, Medium, Large)</b>	
An accident that results in a loss of coolant from the reactor. ( <i>see Interfacing-Systems</i> )	<p>In a QRVA, two major categories of initiating events are evaluated; namely, transients and LOCAs). LOCAs represent a particularly challenging accident because reactor coolant, usually water, cannot be replaced at a sufficient rate to prevent uncovering the reactor core leading to core damage and potential fueling melting. Once considered to be the most severe design-basis accident, QRVAs have</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<i>Loss-of-Coolant Accident)</i>	<p>revealed that other accident initiators, such as long-term station blackout, are far more frequent and can lead to equally undesired consequences.</p> <p>LOCA initiating event frequencies used in the QRVA are dependent on the size of LOCA. These sizes are typically referred to as small, medium, or large LOCAs. The break sizes which define small, medium, and large LOCAs are also dependent on the type of reactor, either pressurized water reactor (PWR) or BWR, and whether the lost coolant is liquid or steam. NUREG/CR-6928 provides the following description for BWRs:</p> <ul style="list-style-type: none"> <li>• <u>Small LOCA (SLOCA)</u>: A break size less than 0.004 square feet (1-inch inside diameter pipe equivalent) for liquid and less than 0.05 square feet (approximately 4-inch inside diameter pipe equivalent) for steam in a primary system pipe with leakage rate greater than 100 gallons per minute.</li> <li>• <u>Medium LOCA (MLOCA)</u>: A break size between 0.004 to 0.1 square feet (approximately 1- to 5-inch inside diameter pipe equivalent) for liquid and between 0.05 to 0.1 square feet (approximately 4- to 5-inch inside diameter pipe equivalent) for steam in a primary system pipe.</li> <li>• <u>Large LOCA (LLOCA)</u>: A break size greater than 0.1 square feet (approximately 5- inch inside diameter pipe equivalent) for liquid or steam in a primary system pipe.</li> </ul> <p>NUREG/CR-6928 also provides the following description for PWRs:</p> <ul style="list-style-type: none"> <li>• <u>Small LOCA</u>: A pipe break in the primary system boundary with an inside diameter between 0.5- and 2-inches.</li> <li>• <u>Medium LOCA</u>: A pipe break in the primary system boundary with an inside diameter between 2- and 6-inches.</li> <li>• <u>Large LOCA</u>: A pipe break in the primary system boundary with an equivalent inside diameter greater than 6-inches.</li> </ul> <p>Historically, NUREG-1150 defines SLOCA as &lt; 1 inch, MLOCA as 1 to 5 inches, and LLOCA as &gt; 5 inches for BWRs and SLOCA as 0.5 to 2 inches, MLOCA as 2 to 6 inches, and LLOCA as &gt; 6 inches for PWRs. Appendix A to 10 CFR Part 50 and the NRC Website Glossary define the term LOCAs as “those postulated accidents that result in a loss of reactor coolant at a rate in excess of the capability of the reactor makeup system from breaks in the reactor coolant pressure boundary, up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system.”</p>
<b>Loss of Fuel Inventory Control Frequency</b>	
<i>(see Frequency)</i>	The term loss of fuel inventory control frequency is a type of frequency used in QRVA and is defined under “Frequency.”

**Table D-1. Terms and Definitions (Continued) -**

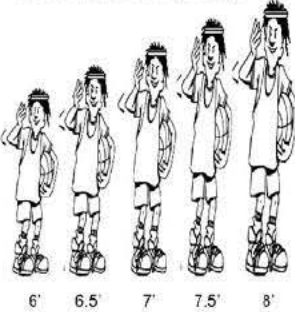
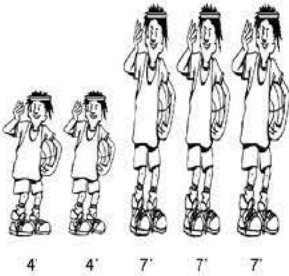
Term and Definition	Discussion
<b>Loss of Offsite Power</b>	
<p>The loss of all AC power from the electrical grid to the facility. (see <i>Transient</i>)</p>	<p>In a QRVA, LOOP is referred to as both an initiating event and an accident sequence class. As an initiating event, LOOP to the facility can 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.</p> <p>NUREG/CR-6890 defines a LOOP as “the simultaneous loss of electrical power to all plant safety buses, requiring all emergency power generators to start and supply power to the safety buses.”</p>
<b>Low-Power and Shutdown</b>	
<p>The states of facility operation when the reactor is producing power in a range below a specified level or is shutdown. (see <i>Full Power, At-Power</i>)</p>	<p>A QRVA models the different facility operating states of the facility. Operation at-power is one FOS, while several FOSs are needed to characterize the facility during the various stages of low-power and shutdown. These FOSs are distinguished in the QRVA model because the facility response (e.g., accident sequences) differs during different FOSs.</p> <p>Low power and shutdown is the term applicable for other than at-power conditions (i.e., the reactor is typically producing less than 15–25% of its rated power). Low-power and shutdown analysis is further separated into consideration of low power and shutdown states.</p> <p>In a low-power initial condition, the core is producing power from fissioning of fuel, over and above the decay heat levels, although at lower amounts than at-power. Most safety systems are on automatic actuation but some may be disabled or blocked (e.g., main feedwater trip in boiling-water reactors). The support systems are aligned in their normal configuration (e.g., electrical power is being drawn from the grid). In these FOSs, the power level may be changing as the reactor is shutting down or starting up, or the power level may be constant at a reduced level. The power level that distinguishes nominal full power from low power is the power level below which major facility evolutions are required to reduce or increase power that significantly increase the likelihood of a facility trip (e.g., taking manual control of feedwater level).</p> <p>In shutdown conditions, the core is not producing power (i.e., the reactor is subcritical). The reactor temperature and pressure are lower than at-power, coolant inventory may be lower or higher, the reactor may be relying on alternate cooling systems, some safety systems may be defeated, or containment may be open.</p> <p>A representation of the different facility operating states (i.e., low power and shutdown) is shown under the discussion for the term At-Power.</p>



**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Master Logic Diagram</b>	
<p>A graphical model that can be constructed to guide the selection of initiating events. (see <i>Fault Tree</i>)</p>	<p>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.</p> <p>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. An example of an MLD is provided below.</p> <div style="text-align: center;"> <pre> graph TD     IE[Initiating Event] --&gt; T[Transients]     IE --&gt; LOC[LOCAs]     T --&gt; IRC[Insufficient Reactivity Control]     T --&gt; ICHE[Insufficient Core Heat Removal]     LOC --&gt; PR[Pipe Rupture]     LOC --&gt; SRO[Safety/Relief Valve Opens]     IRC --- D1{ }     ICHE --- D2{ }     PR --- D3{ }     SRO --- D4{ }                     </pre> </div> <p>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.”</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Mean</b>	
<p>The expected value of a random variable. (see <i>Median, Best Estimate, Point Estimate, Probability Distribution</i>)</p>	<p>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.</p> <p>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.</p> <p>The mean and median provide different information and cannot be used interchangeably. An illustration of the difference between mean and median is shown below.</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p><u>Team A</u> The mean height and the median height of this team are both 7' (213cm).</p>  <p>6'   6.5'   7'   7.5'   8'</p> </div> <div style="text-align: center;"> <p><u>Team B</u> The median height of this team is 7', but the mean height of this team is only 5'8" (173cm).</p>  <p>4'   4'   7'   7'   7'</p> </div> </div>
<b>Mechanistic Source Term</b>	
<p>A source term that is calculated considering the characteristics of specific accidents. (see <i>Source Term</i>)</p>	<p>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 radioactive material inventories and the time-dependent radioactive material transport mechanisms necessary and sufficient to predict the source term.</p> <p>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 licensing purposes.</p>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Median</b>	
That value of a random variable for which the occurrence of larger values is just as likely as occurrence of smaller values. <i>(see Mean, Probability Distribution)</i>	<p>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.</p> <p>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 <math>2 \times 10^{-4}/\text{hr}</math> then half of all electric motors of that type would have failure rates below <math>2 \times 10^{-4}/\text{hr}</math> and half would have failure rates above <math>2 \times 10^{-4}/\text{hr}</math>.</p> <p>An illustration of the difference between mean and median is under the discussion of the term "Mean."</p>
<b>Minimal Cut set</b>	
<i>(see Cut set)</i>	The term minimal cut set is a type of cut set used in QRVA and is defined under "Cut set."
<b>Mission Time</b>	
The time period that a system or component is required to operate to successfully perform its function.	<p>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.</p> <p>The definition provided is based on the definition in the ASME/ANS PRA Standard.</p>
<b>Mitigating System</b>	
A facility system designed to minimize the effects of initiating events. <i>(see Initiating Event, Frontline System, Support System)</i>	<p>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 (e.g., core or containment cooling, coolant makeup, reactivity control, or reactor vessel pressure control).</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Model (QRVA)</b>	
A representation of a physical process or system that allows one to predict the system's behavior. <i>(see Uncertainty)</i>	<p>The term "model" is used in a variety of ways in a QRVA:</p> <ul style="list-style-type: none"> <li>• The entire QRVA is sometimes referred to as a QRVA model or risk model.</li> <li>• Different submodels are used inside the QRVA in the performance of the various technical elements (system model, human reliability analysis model).</li> <li>• Other submodels may be phenomenological models (e.g., direct containment heating or core-concrete interaction).</li> </ul> <p>All of these types of models may be sources of model uncertainty in the QRVA.</p>
<b>Model Uncertainty</b>	
<i>(see Uncertainty)</i>	The term model uncertainty is related to epistemic uncertainty and is defined under "Uncertainty."
<b>Nonsafety Related</b>	
<i>(see Safety Significant)</i>	The term nonsafety related indicates the safety category of a structure, system, or component and is defined under "Safety Significant."
<b>Operating-Basis Earthquake</b>	
An earthquake that could be expected to affect the site of a nuclear reactor, but for which the facility's power production equipment is designed to remain functional without undue risk to public health and safety. <i>(see Safe-Shutdown Earthquake)</i>	<p>In a seismic QRVA, the operating-basis earthquake (OBE) is sometimes used in the initiating event selection process to develop a hierarchy to ensure that every earthquake greater than a certain defined size produces a facility shutdown within the systems model. As noted in the ASME/ANS PRA Standard, it is generally a requirement at all facilities that any earthquake larger than a certain size—usually defined as the OBE—will require the facility to shut down to reduce energies that may cause loss-of-coolant accidents and to enable inspection for possible earthquake-caused damage.</p> <p>The ASME/ANS PRA Standard defines an OBE as "that earthquake for which those features of the nuclear power plant necessary for continued operation without undue risk to health and safety are designed to remain functional. In the past, the OBE was commonly chosen to be one-half of the safe shutdown earthquake (SSE)."</p> <p>The definition provided is based on the definition in the NRC Website Glossary.</p>
<b>Operator Action</b>	
<i>(see Human Action)</i>	The term operator action is a specific type of human action that is defined under the term "Human Action."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Operator Error</b>	
<i>(see Human Error)</i>	The term operator error is a specific type of human error that is defined under the term “Human Error.”
<b>Other External Hazard Fragility Evaluation/ Analysis</b>	
<i>(see Fragility Analysis)</i>	The term other external hazard fragility analysis is a type of fragility analysis and is included in the discussion under “Fragility Analysis.”
<b>Other External Hazard Facility Response Analysis/Model</b>	
<i>(see Facility Response Analysis)</i>	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.”
<b>Other Hazards Analysis</b>	
<i>(see Hazard Analysis)</i>	The term other hazards analysis is a specific type of hazard analysis and is defined under the term “Hazard Analysis.”
<b>Parameter</b>	
The variables used to calculate and describe frequencies and probabilities. <i>(see Uncertainty, Point Estimate)</i>	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.  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.
<b>Parameter Uncertainty</b>	
<i>(see Uncertainty)</i>	The term parameter uncertainty is related to epistemic uncertainty and is defined under “Uncertainty.”

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Passive Component</b>	
A component whose operation or function does not depend on an external source of motive power. (see <i>Active Component</i> )	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.  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.”
<b>Performance-Based (Approach, Regulation, Regulatory Action)</b>	
Focusing on measurable outcomes, rather than prescriptive processes, techniques, or procedures. (see <i>Risk-Based</i> )	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 measurable outcomes are used to show compliance with regulation.  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) Licensees 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.”  The terms performance-based regulation and performance-based regulatory action are defined below based on the NRC Website Glossary: <ul style="list-style-type: none"> <li>• <u>Performance-Based Regulation</u>: “A regulatory approach that focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based regulation leads to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives for licensees to improve safety without formal regulatory intervention by the agency.”</li> <li>• <u>Performance-Based Regulatory Action</u>: “Licensee attainment of defined objectives and results without detailed direction from the NRC on how these results are to be obtained.”</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Performance-Based Approach</b>	
<i>(see Performance-Based)</i>	The term performance-based approach indicates an evaluation that is based on measureable outcomes and is defined under "Performance-Based."
<b>Facility Configuration Control</b>	
The process of maintaining consistency between the physical condition of a facility and its associated design and engineering records.	<p>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.</p> <p>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.</p>
<b>Facility Damage State</b>	
A group of accident sequence end states that share similar characteristics with accident progression, and containment or engineered safety feature operability. <i>(see Bin)</i>	<p>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.</p> <p>The definition provided is based on the definition in the ASME/ANS PRA Standard.</p>
<b>Facility Hazard</b>	
<i>(see Hazard)</i>	The term facility hazard has the same meaning as hazard and is defined under "Hazard."
<b>Facility Operational Mode</b>	
<i>(see Facility Operational State)</i>	The term facility operational mode has the same meaning as facility operational state and is defined with "Facility Operational State."

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Facility Operational State, Facility Operational Mode</b>	
<p>A particular facility configuration with specified operational characteristics.</p>	<p>The scope of the QRVA determines the various individual FOS that the QRVA model must include for the risk estimation results (i.e., if a QRVA is being conducted for at-power operations, the facility configuration in that state or mode will be considered to obtain the risk results). The term facility operational state has the same meaning as facility operational mode.</p> <p>The facility conditions that define a FOS usually include core decay heat level, primary water level, primary temperature, primary vent status, containment status, and decay heat removal mechanisms. A FOS can be a steady state or represent a transition between steady-state FOSs. For example, full power and cold shutdown while on residual heat removal cooling may be two steady-state FOSs. To transition from full power to cold shutdown, there may be one or more transition FOSs to cover the range of temperatures and pressures the facility goes through in shutting down to cold shutdown.</p> <p>Note that the impacts of unavailability of individual systems or components because of test or maintenance typically are not included as part of the definition of a FOS. The complete set of FOSs for a specific outage type shows a discrete representation of the outage from a risk perspective.</p>
<b>Facility Partitioning</b>	
<p>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.</p>	<p>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 core damage.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Facility Response Analysis, Facility Response Model (External Floods, Internal Fire, High Winds, Other External Hazard, Seismic)</b>	
The logic framework for identification and analysis of accident scenarios resulting from the effects of a hazard on the facility.	<p>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.</p> <p>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.</p> <p>A simplified facility response model also can be constructed “from scratch” (ad hoc model), without starting with the internal events model. 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.</p>
<b>Facility Response Model</b>	
<i>(see Facility Response Analysis)</i>	The term facility response model has the same meaning as facility response analysis and is defined under “Facility Response Analysis.”
<b>Facility Risk Profile</b>	
<i>(see Risk Profile)</i>	The term facility risk profile has the same meaning as risk profile and is defined under “Risk Profile.”

**Table D-1. Terms and Definitions (Continued) -**

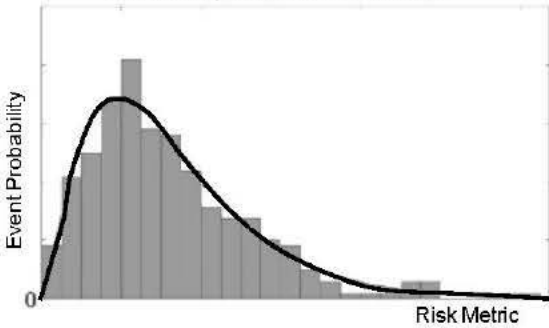
Term and Definition	Discussion
<b>Point Estimate</b>	
An estimate of a parameter in the form of a single value. <i>(see Mean)</i>	<p>In a QRVA, the preferred parameter point estimate is the mean of the value obtained from a probability distribution for the parameter.</p> <p>NUREG-1855 states, “a point 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.”</p> <p>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.</p> <p>The definition provided was based on the definition in NUREG/CR-6823.</p>
<b>Precursor Event</b>	
<i>(see Accident Precursor)</i>	The term precursor event is the same as accident precursor and is defined under “Accident Precursor.”
<b>Probabilistic (Analysis, Approach)</b>	
A characteristic of an evaluation that includes consideration of events with regard to their likelihood. <i>(see Deterministic, QRVA, Risk-Based, Risk-Informed)</i>	<p>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 core damage are based on deterministic analyses.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Probabilistic Analysis</b>	
<i>(see Probabilistic)</i>	The term probabilistic analysis is defined under “Probabilistic.”



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Probabilistic Approach</b>	
<i>(see Probabilistic)</i>	The term probabilistic approach is defined under “Probabilistic.”
<b>Probabilistic Safety Assessment</b>	
<i>(see QRVA)</i>	The term probabilistic safety assessment is another term for QRVA and is defined under “QRVA.”
<b>Probabilistic Seismic Hazard Analysis</b>	
<i>(see Hazard Analysis)</i>	The term probabilistic seismic hazard analysis is a specific type of hazard analysis and is defined under “Hazard Analysis.”
<b>Probability (Basic Event Failure, Containment Failure, Core Damage, Failure, Human Error)</b>	
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. <i>(see Frequency)</i>	<p>In a QRVA, probability is calculated for various types of QRVA input and output parameters (e.g., failures of equipment associated with basic events, core damage, and containment failure).</p> <p>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 fission products.</p> <p>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.”</p> <p>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.</p> <p>Some QRVA studies also calculate the probability of core damage, also referred to as core damage probability, given a particular initiating event or set of initiating events.</p> <p>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.</p> <p>The definition provided was based on the definition in NUREG/CR-6823.</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Probability Density Function</b>	
<i>(see Probability Distribution)</i>	The term probability density function is an equivalent term for probability distribution and is defined under "Probability Distribution."
<b>Probability Distribution (Probability Density Function)</b>	
A curve that shows all the values that a random variable can take and the likelihood that each will occur. <i>(see Cumulative Distribution Function, Mean, Median, Uncertainty Interval)</i>	<p>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.</p> <p>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."</p>
<p>Probability Distribution Function</p> 	
<b>Prompt Fatality</b>	
<i>(see Fatality)</i>	The term prompt fatality is a type of fatality caused by exposure to radioactive materials and is defined under "Fatality."
<b>Prompt Fatality Risk</b>	
<i>(see Fatality)</i>	The term prompt fatality risk is a type of fatality caused by exposure to radioactive materials and is defined under "Fatality."
<b>Public Health Effects</b>	
<i>(see Health Effects)</i>	The term public health effect refers to a type of health effect and is defined in the discussion under "Health Effects."
<b>Qualitative Risk Assessment</b>	



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<i>(see Risk)</i>	A qualitative risk assessment is one type of risk assessment and is defined under "Risk."
<b>Qualitative Risk and Vulnerability Assessment, Probabilistic Safety Assessment (Base, Baseline)</b>	
A systematic method for assessing the likelihood of accidents and their potential consequences. <i>(see Probability, Dynamic QRVA, Full-Scope QRVA, Level 1, 2, 3 QRVA)</i>	<p>The term quantitative risk and vulnerability assessment has numerous, similar definitions. Some of the formal definitions used are presented below:</p> <ul style="list-style-type: none"> <li>• "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 core damage or a radioactive material release and its effects on the health of the public (also referred to as a probabilistic safety assessment (PSA))."</li> <li>• "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., core damage or large early release) and their frequencies, and (2) is comprised of specific technical elements in performing the quantification."</li> <li>• "A systematic method for assessing three questions used to define "risk." These questions consider (1) what can go wrong, (2) how likely it is, and (3) what its consequences might be. 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."</li> </ul> <p>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 certification or combined operating license 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 (core damage), Level 2 (radioactive material release), and Level 3 (consequences).</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>QRVA Configuration Control (Maintenance, Upgrade)</b>	
<p>A process that maintains and updates the quantitative risk and vulnerability assessment so that it reflects the as-built as-operated facility. <i>(see Living QRVA, Risk Management)</i></p>	<p>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.”</p> <p>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).”</p> <p>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.”</p> <p>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).</p> <p>Listed below are definitions of related terms:</p> <ul style="list-style-type: none"> <li>• <u>Configuration risk management</u>: The term configuration risk management is the same as risk management and is defined under “Risk Management.”</li> <li>• <u>Configuration risk profile</u>: 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). The configuration risk profile can depend on the facility operational status. For example, during certain shutdown operations when the containment function is not maintained, the risk metric represented by acute fuel release fraction is not applicable; therefore, licensees may use more stringent baseline LOFICF guidelines to maintain an equivalent risk profile.</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>QRVA Maintenance</b>	
<i>(see QRVA Configuration Control)</i>	The term QRVA maintenance is part of QRVA configuration control and is defined under "QRVA Configuration Control."
<b>QRVA Model</b>	
<i>(see Model)</i>	The term QRVA model is a specific type of model and is defined under the term "Model."
<b>QRVA Technical Acceptability</b>	
<i>(see Technical Acceptability)</i>	The term QRVA technical acceptability is discussed in the discussion for the term "Technical Acceptability."
<b>QRVA Technical Adequacy</b>	
<i>(see Technical Adequacy)</i>	The term QRVA technical adequacy is discussed in the discussion for the term "Technical Adequacy."
<b>QRVA Technical Elements</b>	
The basic pieces (or analyses) required to produce the QRVA model. <i>(see Appendix B)</i>	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.
<b>QRVA Upgrade</b>	
<i>(see QRVA Configuration Control)</i>	The term QRVA upgrade is part of QRVA configuration control and is defined under "QRVA Configuration Control."
<b>Qualitative Screening</b>	
<i>(see Screening)</i>	A qualitative screening is one type of screening performed and is defined under "Screening."

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Quantitative Health Objectives</b>	
Numerical criteria for the acceptable levels of risk to public health and safety in the population surrounding a facility that satisfy the NRC's reactor safety goals. <i>(see Fatality, Risk to Average individual)</i>	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 the NRC's reactor safety goals.  The NRC safety goals are 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 (non-nuclear) 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 (non-nuclear) causes.
<b>Quantitative Screening</b>	
<i>(see Screening)</i>	A quantitative screening is one type of screening and is defined under "Screening."
<b>Radioactive Material</b>	
A substance that emits ionizing radiation. <i>(see Radionuclide, Fission Product)</i>	In a QRVA, the terms radionuclide, radioactive material, and fission product are used interchangeably. These terms are meant to refer to the substance that is the source of the risk being evaluated. However, a release of this substance (i.e., radioactive material) from the reactor and from the containment, or from another source such as the spent fuel pool, could have an adverse impact on public health and safety is generally not referred to as radioactive material release. Generally, either radionuclide release or fission product release, or just 'release' is used.



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Radioactive Material Release (Large Early, Small Early, Large Late, Small Late)</b>	
<p>The release of radioactive material to the environment. <i>(see Radioactive Material, Radioactive Material Release Frequency Analysis, Health Effects)</i></p>	<p>In a Level 2 QRVA, the release of radioactive material from the reactor core to the environment is calculated. Usually this is referred to as the 'release,' 'radionuclide release,' or 'fission product release.' This release may occur early or late and may be large or small.</p> <p>In the ASME/ANS PRA Standard, an acute fuel release is defined as a rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of offsite emergency response and protective actions so there is a potential for early health effects.</p> <p>A small early release is of low enough magnitude to have minimal potential for early health effects.</p> <p>A large late release can be defined as a release of airborne fission products from the containment to the environment of sufficient magnitude to cause severe health effects. However, the release occurs in a timeframe that allows the effective implementation of offsite emergency response and protective actions such that the offsite health effects can be significantly reduced compared to those of an acute fuel release.</p> <p>A small late release is of low enough magnitude and is delayed long enough to have minimal potential for health effects.</p> <p>For both early and late large releases, significant land contamination and property damage is to be expected. The term large release is discussed as its own entry in this glossary. The Commission has not approved a formal definition for the term large release.</p>
<b>Radioactive Material Release Frequency (Large Early, Small Early, Large Late, Small Late)</b>	
<p><i>(see Frequency)</i></p>	<p>The term radioactive material release frequency (large early, small early, large late, small late) is a type of frequency used in QRVA and is defined in the discussion under "Frequency."</p>
<b>Radioactive Material Release Frequency Analysis (Large Early, Small Early, Large Late, Small Late)</b>	
<p>An estimation of the frequency of radioactive material releases by evaluating the core and containment behavior under severe accident conditions. <i>(see Radioactive Material Release, Health Effects)</i></p>	<p>In a Level 2 QRVA, the frequency of release of radioactive material from the reactor core to the environment is calculated. This release may occur early or late and may be large or small. For operating reactors, an AFRF is one of the risk metrics used for risk-informed decisions. For new reactors, a large release frequency is one of the risk metrics used for risk-informed decisions.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Radiological Source Term</b>	
<i>(see Source Term)</i>	The term radiological source term has the same meaning as source term and is defined under "Source Term."
<b>Radiological Source Term Analysis</b>	
<i>(see Source Term Analysis)</i>	The term radiological source term analysis has the same meaning as source term analysis and is defined under "Source Term Analysis."
<b>Radionuclide</b>	
An atom with an unstable nucleus that emits radiation <i>(see Radioactive Material, Fission Product)</i>	In a QRVA, the terms radionuclide, radioactive material, and fission product are used interchangeably. These terms are meant to refer to the substance that is the source of the risk being evaluated. A radionuclide release, therefore, refers to the release of the substance (i.e., radionuclides) from the reactor and from the containment that could have an adverse impact on public health and safety.  The NRC Website Glossary defines radionuclide as "an unstable isotope of an element that decays or disintegrates spontaneously, thereby emitting radiation. Approximately 5,000 natural and artificial radioisotopes have been identified."
<b>Random Failure</b>	
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.
<b>Random Uncertainty</b>	
<i>(see Uncertainty)</i>	The term random uncertainty is related to aleatory uncertainty and defined under "Uncertainty."
<b>Rare Initiator</b>	
An initiating event that is extremely unlikely and not expected to occur in facilities. <i>(see Initiating Event)</i>	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.  The ASME/ANS PRA Standard defines the term rare event as "one that might be expected to occur only a few times throughout the world nuclear industry over many years (e.g., <math>1E-4/r\text{-yr}</math>)." However, the ASME/ANS PRA Standard only allows screening of initiating events if the frequency is much lower than $1E-4/yr$ (e.g., if the frequency $<1E-7/yr$ and the event does not involve either an ISLOCA, containment bypass, or reactor, or reactor pressure vessel rupture).



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Rationalist</b>	
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. ( <i>see Structuralist, Defense-in-Depth</i> )	<p>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.</p> <p>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.</p> <p>The Advisory Committee on Reactor Safeguards describes that the rationalist will “(1) establish quantitative acceptance criteria, such as the quantitative health objectives, core damage 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.”</p>
<b>Reactor Core</b>	
The location within a nuclear reactor where the fission process occurs.	<p>In a QRVA, the source of risk generally evaluated is the reactor core with an understanding that the actual risk is from the fuel. The reactor core includes the fuel assemblies, moderator, neutron poisons, control rods, and support structures. The other sources of risk at the facility site (e.g., spent fuel) generally are not included in the reactor core QRVA; however, there are several QRVA's, separate from the reactor core QRVA's, which evaluate the risk of the spent fuel.</p> <p>The NRC Website Glossary defines reactor core as “the central portion of a nuclear reactor, which contains the fuel assemblies, moderator, neutron poisons, control rods, and support structures. The reactor core is where fission takes place.”</p>
<b>Reactor-Operating-State-Year</b>	
( <i>see Reactor-Year</i> )	The term reactor-operating-state-year is related to the term reactor-year and is defined under “Reactor-Year.”

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Reactor-Year (Reactor-Operating-State-Year)</b>	
A unit of time by which risk parameters are measured in a QRVA. ( <i>see Facility Operational State</i> )	In a QRVA, the terms reactor-year and reactor-operating-state-year refer to units of time by which risk parameters (e.g., LOFICF, AFRF) are measured. The ASME/ANS PRA Standard defines the term reactor-year as “a calendar year in the operating life of one reactor, regardless of power level.” The term reactor-year assumes that more than one reactor can operate during a year (e.g., a calendar year during which five reactors operated would be the experience equivalent of 5 reactor-years).  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. For at-power operation, this basis is sometimes referred to as per reactor critical year (i.e., assuming that the reactor operated continuously for a year). On a more general basis, it could be considered to be per reactor-operating-state-year. The ASME/ANS PRA Standard defines the term reactor-operating state-year as “an equivalent calendar year of operation in a particular facility operating state.”
<b>Realistic Analysis</b>	
( <i>see Conservative Analysis</i> )	The term realistic analysis is discussed in the discussion for “Conservative Analysis” and is defined there.
<b>Recovery</b>	
Restoration of a failed function. ( <i>see Repair</i> )	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.  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.”
<b>Release</b>	
( <i>see Radioactive Material Release</i> )	For purposes of a Level 2 and Level 3 QRVA, the term release is used interchangeably with “Radioactive Material Release.”



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Release Category</b>	
A group of radioactive material releases expected to result in similar consequences. (see <i>Source Term</i> )	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 radioactive material.  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 radioactive material species released from the facility as a result of an accident.
<b>Release Fraction</b>	
The amount of radioactive material released from the reactor core expressed as a fraction of the original inventory of the radioactive material. (see <i>Source Term</i> )	In a Level 2 QRVA, the release fraction specifies the amount of radioactive materials released to the environment and provides the basis for the subsequent dose calculations to the affected population.  NUREG-1489 states that the release fraction is expressed as the amount of radioactive material released from the containment as a function of time given as a fraction of the fission product inventory in the core at the time of the start of the accident.
<b>Release Timing and Duration</b>	
The time of release and the timeframe over which the radioactive materials are released to the environment during an accident. (see <i>Source Term</i> )	In a Level 3 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.

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Reliability (Unreliability)</b>	
<p>The likelihood that a system, structure, or component performs its required function(s) for a specified period of time. (see <i>Availability</i>)</p>	<p>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.</p> <p>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. 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.”</p>
<b>Repair</b>	
<p>The restoration of a failed function by correcting the cause of failure. (see <i>Recovery</i>)</p>	<p>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).</p> <p>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.</p> <p>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.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Response Time</b>	
The period of time something takes to react to a given input.	<p>In a QRVA, the term response time has different connotations, depending on the situation. Some of these connotations are as follows:</p> <ul style="list-style-type: none"> <li>• 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.”</li> <li>• 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.”</li> <li>• When referring to a Level 3 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).</li> </ul>
<b>Risk (Assessment, Analysis)</b>	
The combined answer to three questions that consider (1) what can go wrong, (2) how likely it is, and (3) what its consequences might be. (see QRVA, Level 1, 2, 3 QRVA, Risk Metric)	<p>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.</p> <p>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 core damage and each level of the QRVA uses different risk metrics, which can be found in the discussion of Level 1, 2, 3 QRVA.</p> <p>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?”</p> <p>The definition provided was based on the definition in the NRC Website Glossary.</p>
<b>Risk Achievement Worth</b>	
(see Importance Measure)	The term risk achievement worth is one type of importance measure and is defined under “Importance Measure.”

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Risk Characterization</b>	
<i>(see Risk Metric)</i>	The term risk characterization is a process that uses risk metrics to determine risk and is defined under “Risk Metric.”
<b>Risk Insights</b>	
The understanding about a facility’s response to postulated accidents. <i>(see Risk, Risk-Based, Risk-Informed)</i>	<p>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.</p> <p>Risk insights can be obtained via both quantitative and qualitative investigations. As noted in RG 1.174, 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.</p> <p>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.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Risk Management</b>	
<p>A process used at a facility to keep the risk at acceptable levels.</p>	<p>A QRVA is a tool used to evaluate a nuclear 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. Examples of risk management activities that are supported by QRVA are listed below:</p> <ul style="list-style-type: none"> <li>• A QRVA represents an important risk management tool that, as stated in Regulatory Guide 1.177, “ensures that other potentially lower probability, but nonetheless risk-significant, configurations resulting from plant maintenance and other operational activities are identified and compensated for.”</li> <li>• Regarding the use of QRVA findings and risk insights to support licensee requests for changes to a facility’s licensing basis, RG 1.174 states the following: “All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk and not just to eliminate requirements the licensee sees as undesirable. For those cases in which risk increases are proposed, the benefits should be described and should be commensurate with the proposed risk increases. The approach used to identify changes in requirements should be used to identify areas in which requirements should be increased as well as those in which they can be reduced.”</li> <li>• In reference to the Maintenance Rule, 10 CFR 50.65 states, “the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.”</li> </ul> <p>Risk Management is used in a broader context in NUREG-2150, “A Proposed Risk Management Regulatory Framework,” to refer to an approach for achieving a more comprehensive, holistic, risk-informed, performance-based regulation for reactors, materials, waste, fuel cycle, and transportation that would continue to ensure the safe and secure use of nuclear material. The objective of such an approach is described NUREG-2150 as managing the risks from the use of byproduct, source and special nuclear materials through appropriate performance based regulatory controls and oversight.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Risk Metric</b>	
A measure that is used to express the risk quantity of interest. ( <i>see Risk, Level 1, 2, 3 QRVA, Risk Profile, Full-Scope QRVA</i> )	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 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 radiation syndrome 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 core damage) 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.
<b>Risk Monitor</b>	
A facility-specific analysis tool used to determine the risk in real-time based on the current facility configuration. ( <i>see Living QRVA</i> )	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.
<b>Risk Profile (Facility)</b>	
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: <ul style="list-style-type: none"> <li>• LOFICF and AFRF for internally and externally initiated events during various modes of operation.</li> <li>• Percentage contributions to LOFICF and AFRF by initiating event and accident sequence type.</li> <li>• Ranking of the contribution of individual basic events and cut sets to LOFICF and AFRF, based on various importance measures.</li> <li>• Comparison of QRVA results to QRVAs for other facilities.</li> <li>• Qualitative risk insights on facility design features.</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Risk Reduction Worth</b>	
<i>(see Importance Measure)</i>	The term risk reduction worth is one type of importance measure and is defined under “Importance Measure.”
<b>Risk Significant</b>	
A level of risk associated with a facility’s system, structure, component, human action or modeled accident sequence that exceeds a predetermined level. <i>(see Safety Significant, Significant)</i>	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 nuclear facility can be calculated in terms of LOFICF (Level 1 QRVA), or releases (Level 2 QRVA), or health effects (Level 3 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.  The term also describes a level of risk exceeding a predetermined ‘significance’ level.
<b>Risk Significant Equipment</b>	
<i>(see Significant)</i>	The term risk significant equipment is related to the term significant and is defined under “Significant.”
<b>Risk to Average Individual</b>	
A measure of the risk to an individual that represents an average over the parameters characterizing the population at risk <i>(see Fatality, Quantitative Health Objectives)</i>	In a Level 3 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.
<b>Risk-Based Approach</b>	
<i>(see Risk-Based)</i>	The term risk-based approach is related to the term risk-based and is defined under “Risk-Based.”

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Risk-Based (Approach, Decision-Making, Regulation)</b>	
<p>A characteristic of decision-making in which a decision is solely based on the results of a risk assessment. (see <i>Risk-Informed</i>)</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Risk-Based Approach:</b> A philosophy on decision-making “in which a safety decision is solely based on the numerical results of a risk assessment.”</li> <li>• <b>Risk-Based Decision-Making:</b> “An approach to regulatory decision-making that considers only the results of a probabilistic risk assessment.”</li> <li>• <b>Risk-Based Regulation:</b> An approach to regulation that uses the results of a risk assessment to develop applicable regulations.</li> </ul> <p>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.</p> <p>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.</p>
<b>Risk-Based Decision-Making</b>	
<p>(see <i>Risk-Based</i>)</p>	<p>The term risk-based decision-making is related to the term risk-based and is defined under “Risk-Based.”</p>
<b>Risk-Based Regulation</b>	
<p>(see <i>Risk-Based</i>)</p>	<p>The term risk-based regulation is related to the term risk-based and is defined under “Risk-Based.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Risk-Informed (Approach, Decision-making, Regulation)</b>	
<p>A characteristic of decision-making in which risk results or insights are used together with other factors to support a decision. (see <i>Risk-Based, Deterministic, Probabilistic</i>)</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• <u>Risk-Informed Approach</u>: “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 licensee 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.”</li> <li>• <u>Risk-Informed Decision-Making</u>: “An approach to regulatory decision making, in which insights from probabilistic risk assessment are considered with other engineering insights.”</li> <li>• <u>Risk-Informed Regulation</u>: “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.”</li> </ul> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Risk-Informed Approach</b>	
<i>(see Risk- Informed)</i>	The term risk-informed approach is related to the term risk-informed and is defined under “Risk- Informed.”
<b>Risk-Informed Decision-Making</b>	
<i>(see Risk- Informed)</i>	The term risk-informed decision-making is related to the term risk-informed and is defined under “Risk-Informed.”
<b>Risk-Informed Regulation</b>	
<i>(see Risk- Informed)</i>	The term risk-informed regulation is related to the term risk-informed and is defined under “Risk-Informed.”
<b>Safe-Shutdown Earthquake</b>	
<p>The maximum earthquake for which certain structures, systems, and components are designed to remain functional to shut down the reactor. <i>(see Seismic Margin Analysis)</i></p>	<p>In a seismic QRVA, the facility’s response to earthquakes of all magnitudes appropriate for the site are evaluated. In a seismic margin analysis, the capability of the facility to withstand an earthquake larger than the SSE is often assessed. The ASME/ANS PRA Standard defines the SSE as “that earthquake for which certain structures, systems and components (SSC) are designed to remain functional. In the past, the SSE has been commonly characterized by a standardized spectral shape anchored to a peak ground acceleration value.”</p> <p>Appendix S to 10 CFR 50 states that the “safe-shutdown earthquake ground motion (SSE) is the vibratory ground motion for which certain structures, systems, and components must be designed to remain functional.” The SSCs required to withstand the effects of the safe-shutdown earthquake ground motion are those necessary to ensure:</p> <ol style="list-style-type: none"> <li>1. The integrity of the reactor coolant pressure boundary;</li> <li>2. The capability to shut down the reactor and maintain it in a safe-shutdown condition;</li> </ol> <p>or</p> <ol style="list-style-type: none"> <li>3. The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 CFR 50.34(a)(1).</li> </ol> <p>The definition provided is based on the definition in the NRC Website Glossary.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Safe Stable State</b>	
Condition of the reactor in which the necessary safety functions are achieved.	<p>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.</p> <p>The ASME/ANS PRA Standard defines the term safe stable state as “a facility condition, following an initiating event, in which reactor coolant system conditions are controllable at or near desired values.”</p>
<b>Safety Function</b>	
Those functions needed to shut down the reactor, remove the residual heat, and contain any radioactive material release.	<p>A QRVA involves the analysis of the performance of the facility safety functions in response to accidents. The common general safety functions for a facility as stated in the IAEA Safety Glossary are:</p> <ul style="list-style-type: none"> <li>• The capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions.</li> <li>• The capability to remove residual heat from the reactor core after shutdown, and during and after appropriate operational states and accident conditions.</li> <li>• The capability to reduce the potential for the release of radioactive material and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design-basis accidents.</li> </ul> <p>The ASME/ANS PRA Standard defines safety function as “function that must be performed to control the sources of energy in the plant and radiation hazards.”</p>

**Table D-1. Terms and Definitions (Continued)**

Term and Definition	Discussion
<b>Safety Margin</b>	
<p>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. <i>(see Defense-in-Depth, Uncertainty)</i></p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <div style="text-align: center;"> </div>
<b>Safety-Related</b>	
<p><i>(see Safety Significant)</i></p>	<p>The term safety-related indicates the safety significance of a structure, system, or component and is defined under “Safety Significant.”</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Safety Significant (Important to Safety, Safety-Related, Nonsafety-Related)</b>	
<p>A qualifying term that indicates if something does not meet some predetermined criterion, it has the potential to affect safety.</p>	<p>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 full-power 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.</p> <p>The term important to safety refers to both safety related and non-safety related SSCs that have been deemed important. In Regulatory Guide 1.201, the NRC has stated that it does not endorse the Nuclear Energy Institute usage of important to safety as having the same connotation as safety significant.</p> <p>Another term, safety related, has a specific meaning in the regulatory arena. Part 50 of the Code of Federal Regulations, as well as the NRC Website Glossary state that the term “safety-related applies to systems, structures, components, procedures, and controls (of a facility or process) that are relied upon to remain functional during and following design basis events. Their functionality ensures that key regulatory criteria, such as levels of radioactivity released, are met. Examples of safety related functions include shutting down the nuclear reactor and maintaining it in a safe-shutdown condition.” Conversely, nonsafety-related indicates that the SSCs, procedures, and controls are <i>not</i> relied upon to remain functional during a design-basis event.</p> <p>The NRC Website Glossary makes the following statement about the term safety significant: “When used to qualify an object, such as a system, structure, component, or accident sequence, this term identifies that object as having an impact on safety, whether determined through risk analysis or other means, which exceeds a predetermined significance criterion.” Safety significance is not evaluated in a QRVA.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Screening (Analysis, Criteria, Qualitative, Quantitative)</b>	
A process that distinguishes items that should be included or excluded from an analysis based on defined criteria.	<p>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.</p> <p>The definitions of the grouped terms are presented below as they apply to screening:</p> <ul style="list-style-type: none"> <li>• <u>Screening criteria</u>: “The values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences.”</li> <li>• <u>Qualitative screening</u>: The objective is to identify portions of the analysis whose potential risk contribution can be judged negligible without quantitative analysis.</li> <li>• <u>Quantitative screening</u>: 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.</li> </ul> <p>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.”</p>
<b>Screening Analysis</b>	
<i>(see Screening)</i>	The term screening analysis is similar in meaning to screening and is discussed under “Screening.”
<b>Screening Criteria</b>	
<i>(see Screening)</i>	The term screening criteria is defined under “Screening.”
<b>Seismic Fragility Analysis</b>	
<i>(see Fragility Analysis)</i>	Seismic fragility analysis is a type of fragility analysis and is included in the discussion under “Fragility Analysis.”
<b>Seismic Hazard Analysis</b>	
<i>(see Hazard Analysis)</i>	The term seismic hazard analysis is a type of hazard analysis and is defined under “Hazard Analysis.”



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Seismic Margin</b>	
A measure of the capacity of the facility to withstand an earthquake more severe than the design-basis earthquake. (see <i>High Confidence of Low Probability of Failure, Safe Shutdown Earthquake, Seismic Margin Analysis</i> )	<p>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 core damage. 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 core damage either independently or in combination with other failures.”</p> <p>NUREG-1742 defines seismic margin as “the ability of a plant, system, component or structure to safely withstand seismic demands or input ground-motion levels beyond those imposed by the design basis earthquake.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Seismic Margin Analysis</b>	
<p>The process to estimate the seismic margin of the facility and to identify any seismic vulnerabilities in the facility. <i>(see High Confidence of Low Probability of Failure, Seismic Margin, Safe-Shutdown Earthquake)</i></p>	<p>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. IPEEE facilities were assessed against a review-level earthquake whose intensity was higher than the design-basis earthquake and varied according to the facility location.</p> <p>Seismic margin analysis is performed to show HCLPF at a certain earthquake level (peak ground acceleration) above the design-basis (safe-shutdown) earthquake.</p> <p>A number of methods can be used to calculate seismic margin:</p> <ul style="list-style-type: none"> <li>• In the IPEEEs, most licensees that carried out a seismic margin analysis used a method developed by the EPRI. In the EPRI method, two success paths, addressing transients, are developed based on a group of safety functions capable of bringing the facility to a safe-shutdown condition after an earthquake. Each success path has to rely on different equipment and each path assumes a loss of offsite power. One path also has to be capable of mitigating a small LOCA. HCLPFs are developed for the two success paths.</li> </ul> <p>The NRC also developed a seismic margin method for the IPEEEs, used by a few licensees. In the NRC IPEEE method, accident sequence models are developed for transients and small LOCAs and HCLPF values are evaluated for the accident sequences developed from these two initiators. Neither the EPRI nor the NRC method requires fragility curves to be developed and allow HCLPFs to be based on the conservative deterministic failure margin method.</p> <ul style="list-style-type: none"> <li>• More recently, the NRC has endorsed a seismic margin method in which fragility curves are developed. In this QRVA-based method, accident sequence models are developed for all the initiators and HCLPF values are evaluated for the accident sequences developed from all the initiators.</li> </ul> <p>The definition provided is based on the definition in the ASME/ANS PRA Standard.</p>
<b>Seismic Facility Response Analysis/Model</b>	
<p><i>(see Facility Response Analysis/Model)</i></p>	<p>The term seismic facility response analysis is a type of facility response analysis and is included in the discussion under "Facility Response Analysis/Model."</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Sensitivity Analysis</b>	
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).  The definition provided was based on the definition in NUREG-1560.
<b>Severe Accident (Sequence, Progression Sequence)</b>	
A type of accident that involves core damage. (see <i>Accident Sequence, Beyond-Design-Basis Accident, Design-Basis Accident</i> )	In a QRVA, BDBAs are analyzed to determine which ones could lead to core damage. The BDBAs that have an end state resulting in core damage are termed severe accidents. All severe accidents are by definition beyond-design-basis accidents since their challenges exceed the design envelope of the facility. However, not all beyond-design-basis accidents are severe accidents, since the design envelope can be exceeded without core damage occurring.  The ASME/ANS PRA Standard defines a severe accident as “an accident that involves extensive core damage and fission product release into the reactor vessel and containment, with potential release to the environment.”  In a Level 1 QRVA, severe accident sequences are a subset of the accident sequences (i.e., many of the accident sequences in a Level 1 QRVA do not result in core damage). In a Level 2 QRVA, severe accident sequences are the only sequences considered because they involve core damage. The term severe accident progression sequence usually is used correctly as a synonym for the term severe accident sequence.
<b>Severe Accident Progression Sequence</b>	
(see <i>Severe Accident</i> )	Severe accident progression sequence has the same meaning as severe accident sequence and is defined under “Severe Accident.”
<b>Severe Accident Sequence</b>	
(see <i>Severe Accident</i> )	A severe accident sequence is an accident sequence that results in a severe accident and is defined under “Severe Accident.”
<b>Shutdown</b>	
(see <i>Low-Power and Shutdown</i> )	The term shutdown is part of low power and shutdown operation and is defined under “Low- Power and Shutdown.”
<b>Significant (Accident Sequence, Accident Progression Sequence, Basic Event, Containment Challenge, Contributor, Cut set, Equipment)</b>	
A factor that can have a major or notable influence on	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

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<p>the results of a risk analysis.</p>	<p>have the same meaning in a QRVA context and are often used interchangeably, which is correct and appropriate in this context.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• <b>Significant Accident Sequence:</b> “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 core damage frequency for that hazard group, or that individually contribute more than a specified percentage of core damage 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.”</li> <li>• <b>Significant Accident Progression Sequence:</b> “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.”</li> <li>• <b>Significant Basic Event:</b> “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.”</li> <li>• <b>Significant Containment Challenge:</b> “A containment challenge that results in a containment failure mode that is represented in a significant accident progression sequence.”</li> <li>• <b>Significant Cut set:</b> “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 core damage frequency (or large early release frequency) for that hazard group, or that individually contribute more than a specified percentage of core damage frequency (or large early release</li> </ul>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
	<p>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.”</p> <ul style="list-style-type: none"> <li>• <b>Risk Significant Equipment:</b> “Equipment associated with a significant basic event.”</li> </ul> <p>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 (e.g., containment failure mode, physical phenomena) of a significant accident progression sequence, and if not modeled would lead to the omission of the sequence.”</p>
<b>Significant Accident Progression Sequence</b>	
<i>(see Significant)</i>	The term significant accident progression sequence is related to the term significant and is defined under “Significant.”
<b>Significant Accident Sequence</b>	
<i>(see Significant)</i>	The term significant accident sequence is related to the term significant and is defined under “Significant.”
<b>Significant Basic Event</b>	
<i>(see Significant)</i>	The term significant basic event is related to the term significant and is defined under “Significant.”
<b>Significant Containment Challenge</b>	
<i>(see Significant)</i>	The term significant containment challenge is related to the term significant and is defined under “Significant.”
<b>Significant Contributor</b>	
<i>(see Significant)</i>	The term significant contributor is related to the term significant and is defined under “Significant.”
<b>Significant Cut set</b>	
<i>(see Significant)</i>	The term significant cut set is related to the term significant and is defined under “Significant.”

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Skin Deposition</b>	
Exposure resulting from radioactive material deposited directly onto the surface of the body. (see <i>Exposure Pathways, Exposure, Exposure Time, Cloudshine, Water Immersion, Groundshine, Inhalation, Ingestion, Health Effects</i> )	In a Level 3 QRVA, for the consequence calculation skin deposition is one of the assumed pathways by which an individual can receive doses. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.
<b>Small Early Release</b>	
(see <i>Radioactive Material Release</i> )	The term small early release is a type of radioactive material release and is defined in the discussion under "Radioactive Material Release."
<b>Small Early Release Frequency</b>	
(see <i>Frequency</i> )	The term small early release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency."
<b>Small Early Release Frequency Analysis</b>	
(see <i>Radioactive Material Release Frequency Analysis</i> )	The term small early release frequency analysis is a type of radioactive material release frequency analysis and is defined under "Radioactive Material Release Frequency Analysis."
<b>Small Late Release</b>	
(see <i>Radioactive Material Release</i> )	The term small late release is a type of radioactive material release and is defined in the discussion under "Radioactive Material Release."
<b>Small Late Release Frequency</b>	
(see <i>Frequency</i> )	The term small late release frequency is a type of frequency used in QRVA calculation and is defined in the discussion under "Frequency."
<b>Small Late Release Frequency Analysis</b>	
(see <i>Radioactive Material Release Frequency Analysis</i> )	The term large late release frequency analysis is a type of radioactive material release frequency analysis and is defined under "Radioactive Material Release Frequency Analysis."



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Source of Risk</b>	
<p>A substance that can pose danger or threat to public health. (<i>see Hazard, Initiating Event</i>)</p>	<p>In a QRVA, sources of risk at facilities include, for example, the nuclear fuel contained within the reactor core and the spent fuel pool. 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 core damage or radioactive material release. For instance, in a non-nuclear application, a leak in a pool may not cause a negative consequence other than having an empty pool. However, because the pool at a facility contains nuclear fuel, there could be a negative consequence if that pool drained and radioactive material (the source of risk) was released.</p> <p>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 core damage. For example, an earthquake (hazard) with particular frequency could cause a loss-of-coolant accident (initiating event) which may result in core damage of the nuclear fuel (source of risk).</p>
<b>Source Term</b>	
<p>Types and amounts of radioactive or hazardous material released to the environment following an accident. (<i>see Release Category, Mechanistic Source Term, Chemical Element Group, Release Fraction, Release Timing and Duration, Source Term Analysis</i>)</p>	<p>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.</p> <p>This characterization involves a description of the radionuclide 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.</p> <p>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 consequence assessment, it may be necessary to provide more detailed source term information than if no Level 3 assessment will be performed. For a Level 3 assessment, the source term information needs to be sufficient to estimate offsite radiation doses and, in some cases, other radiological consequences such as land contamination.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Source Term Analysis</b>	
An analysis to determine the characteristics of the radioactive material released to the environment following an accident. (see <i>Source Term</i> )	In a Level 2 QRVA, the source term analysis determines the release of radioactive material from the fuel or core debris and the transport of this material through the primary system and containment to the environment. (The scope of the QRVA source term analysis usually does not include releases from the spent fuel pool.)  NUREG-1489 states that there are three parts to a source term analysis: (1) the estimation of the release of radioactive material from the fuel and core debris, (2) the transport of this material through the primary system and the containment, and (3) the characterization of the release from containment to the environment.
<b>Split Fraction</b>	
The likelihood that one specific outcome from a set of possible outcomes will be observed. (see <i>Event Tree, Probability</i> )	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.  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.”
<b>State-of-Knowledge Correlation</b>	
A type of dependency that arises when the same data is used to quantify the individual probabilities of two or more basic events. (see <i>Uncertainty</i> )	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.  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.  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.”



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>State-of-Knowledge Uncertainty</b>	
<i>(see Uncertainty)</i>	The term state-of-knowledge uncertainty is related to epistemic uncertainty and defined under “Uncertainty.”
<b>Station Blackout</b>	
The complete loss of alternating current electric power in a nuclear facility. <i>(see Transient)</i>	<p>In a QRVA, station blackout (SBO) accidents are analyzed because AC power is an important support system for numerous facility systems and components. A facility subjected to an SBO condition must achieve safe-shutdown by relying on mitigating systems and components that do not require AC power; e.g., steam-driven pumps and battery-powered valves and instrumentation. However, for operating facilities, core cooling may not be indefinitely maintained without AC power. Important factors that influence the risk associated with SBO include the potential for recovery of AC power, battery depletion times, and the reliability of the mitigating systems and components that do not require AC power.</p> <p>10 CFR 50.2 defines the term station blackout as “the complete loss of AC electric power to the essential and nonessential switchgear buses in a facility (i.e., loss of offsite electric power system concurrent with turbine trip and unavailability of the onsite emergency ac power system). SBO does not include the loss of available AC power to buses fed by station batteries through inverters or by alternate AC sources, nor does it assume a concurrent single failure or design basis accident.”</p> <p>The ASME/ANS PRA Standard defines the term SBO as “complete loss of AC electric power to the essential and nonessential switchgear buses in a nuclear power plant.”</p>
<b>Steam Generator Tube Rupture</b>	
A break or breach of a steam generator tube. <i>(see Consequential (Induced) Steam Generator Tube Rupture)</i>	<p>In a QRVA for a pressurized-water reactor, SGTRs are modeled either as an initiating event or a subsequent failure as part of an accident sequence. If the SGTR occurs randomly while the facility is operating, it is an initiating event modeled in the QRVA. However, if the SGTR occurs because of excessive conditions produced as a result of an accident, it is considered to be a consequential or induced SGTR.</p> <p>An SGTR allows reactor coolant to flow from the reactor vessel to the secondary side of the steam generator. As such, it can become a significant contributor to risk because an SGTR can serve as a possible mechanism for radioactive material transport to the environment because it can be a containment bypass mechanism. There is the potential that if a tube bursts or leaks while a facility is operating, radioactivity from the primary coolant system could escape directly to the atmosphere through the safety valves on the secondary side.</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Stochastic Uncertainty</b>	
<i>(see Uncertainty)</i>	The term stochastic uncertainty is related to aleatory uncertainty and defined under “Uncertainty.”
<b>Structuralist</b>	
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. <i>(see Rationalist, Deterministic, Defense-in-Depth)</i>	<p>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.</p> <p>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.</p>
<b>Success Criteria</b>	
The minimum combination of systems and components needed to carry out the safety functions given an initiating event.	<p>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.</p> <p>Success criteria may be defined in a number of ways, including the following:</p> <ul style="list-style-type: none"> <li>• In terms of the equipment required (e.g., one out of two service water pumps).</li> <li>• In terms of equipment performance (e.g., at least 50 percent of the maximum system flow rate).</li> <li>• In terms of the timing (e.g., system must be initiated within 30 minutes and operate for 24 hours).</li> </ul> <p>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.”</p>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Success Path</b>	
<p>A sequence of events (responding to an upset condition) that result in a successful state of a system, the reactor, or the containment. (see <i>Event Tree, Safe Stable State</i>)</p>	<p>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 reactor. 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.</p> <p>A successful state of a system occurs when the system is able to perform its intended function (e.g., provide injection water at a sufficient flow rate and pressure). A successful state of a reactor is achieved if adequate core cooling is maintained throughout the sequence of events following an upset condition. For the containment, a successful state is achieved if the containment pressure boundary remains intact throughout the sequence of events following an upset condition.</p> <p>The ASME/ANS PRA Standard defines a success path as “a set of systems and associated components that can be used to bring the plant to a stable hot or cold condition and maintain this condition for at least 72 hrs.”</p>
<b>Supplementary Analysis</b>	
<p>Any evaluation that is performed to support another study or evaluation.</p>	<p>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.</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Support System</b>	
<p>A system that enables the operation of one or more systems. (<i>see Frontline System, Support System Initiating Event</i>)</p>	<p>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 component cooling water, 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.</p> <p>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 core damage from occurring. In this situation, the support system failure would be characterized as a support system initiating event.</p> <p>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.”</p>
<b>Support System Initiating Event</b>	
<p>A support system failure that perturbs the steady-state operation of the facility and could lead to an undesired facility condition. (<i>see Initiating Event, Support System</i>)</p>	<p>In a QRVA, the failures of support systems are evaluated to determine if they could potentially cause an undesired facility condition; i.e., a manual trip or a reactor shutdown. 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.</p> <p>An example of a support system initiating event would be the loss of the component cooling water (CCW) system at a pressurized-water reactor. The failure of this system would, in turn, lead to the consequential failure of a number of other important systems that depend on CCW, which might include the reactor coolant pumps (RCP) and emergency core cooling system (ECCS) equipment. Loss of the RCPs would result in a facility trip, and loss of ECCS functionality would reduce the number of facility mitigating systems that could be used to maintain core cooling following the facility trip.</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Supporting Requirements</b>	
<p>Requirements that support the high-level requirements in defining the minimum needed for a technically acceptable baseline QRVA. (see <i>High-Level Requirements, Capability Categories</i>)</p>	<p>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.</p> <p>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."</p> <p>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.</p>
<b>Systems Analysis</b>	
<p>The evaluation of the reliability and availability of a system. (see <i>Availability, Reliability</i>)</p>	<p>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).</p>

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Technical Acceptability, Technical Quality (QRVA)</b>	
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. <i>(see Technical Adequacy)</i>	For a QRVA to be technically acceptable, it must satisfy a set of technical characteristics and associated attributes. Regulatory Guide 1.200 defines such a set of characteristics and accompanying attributes that need to be addressed in a technically acceptable base QRVA (i.e., independent of the application for which the QRVA is used). RG 1.200 guidance is for operating reactors and contains cautions for new advanced light-water reactors.  Technical acceptability and technical quality mean the same thing and are used interchangeably.
<b>Technical Adequacy (QRVA)</b>	
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. <i>(see Technical Acceptability)</i>	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 (e.g., extension of diesel generator allowed outage time) 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.
<b>Technical Elements</b>	
<i>(see QRVA Technical Elements)</i>	The term technical elements has the same meaning as QRVA technical elements in the context of QRVA and is defined under “QRVA Technical Elements.”
<b>Technical Quality</b>	
<i>(see Technical Acceptability)</i>	The term technical quality has the same meaning as technical acceptability and is defined the same as the term “Technical Acceptability.”



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Top Event (Event Tree Top Event)</b>	
The events across the top of an event tree needed to mitigate an accident. <i>(see Event Tree, Fault Tree)</i>	<p>The NRC Website Glossary defines top events as “the events across the top of the event tree, which graphically represent the systems needed to keep the plant in a safe state following an initiating event (i.e., a challenge to plant 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.</p> <p>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.”</p> <p>An illustration of a top event is shown under the discussion for the term “Event Tree.”</p>
<b>Total Effective Dose Equivalent</b>	
<i>(see Dose Equivalent)</i>	The total effective dose equivalent is one measure of dose that can be used to calculate the effect of radiation received by an individual and is defined under “Dose Equivalent.”
<b>Transient, General Transient</b>	
An event that could require a facility trip that might challenge safety systems but does not lead to a loss of significant quantities of reactor coolant. <i>(see Initiating Event, Station Blackout)</i>	<p>In a QRVA, two major categories of initiating events are evaluated; namely, transients and loss-of-coolant accidents. Transients can represent a variety of initiating events; e.g., manual reactor trip, loss of main feedwater, turbine trip, loss of offsite power, and loss of primary flow.</p> <p>Each of these initiating events subsequently leads to changes in reactor temperature or pressure that could demand functioning of safety systems. Transients are modeled in the QRVA if they lead to a facility trip, thus challenging safety systems leading to positive or negative outcomes. The terms transient and general transient often are used interchangeably, which is appropriate and correct in a QRVA context.</p> <p>NUREG/CR-6572 defines the term general transient as “events in which high pressure can be maintained in the primary system, active core cooling is required, and high pressure makeup may be needed.”</p> <p>The NRC Website Glossary defines the term transient as “a change in the reactor coolant system temperature, pressure, or both, attributed to a change in the reactor’s power output. Transients can be caused by (1) adding or removing neutron poisons, (2) increasing or decreasing electrical load on the turbine generator, or (3) accident conditions.”</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
<b>Truncation Limit</b>	
The minimum value of contributors retained in the QRVA quantification process. (see <i>Accident Sequence, Cut set</i> )	<p>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.</p> <p>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.</p> <p>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).”</p>
<b>Unavailability</b>	
(see <i>Availability</i> )	The term unavailability is the opposite of availability and is defined under “availability.”
<b>Uncertainty (Aleatory, Random, Stochastic, Epistemic, State-of-Knowledge, Model, Source of Model, Key Source of Model, Parameter, Completeness)</b>	
Variability in an estimate because of the randomness of the data or the lack of knowledge.	<p>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.</p> <p>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.</p> <p>The QRVA model itself reflects aleatory uncertainty. The QRVA model contains epistemic uncertainty that includes model uncertainty, parameter uncertainty, or completeness uncertainty.</p> <p>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.”</p> <p>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</p>



**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
	<p>additional information. (Aleatory uncertainty is sometimes called 'randomness.')</p> <p>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.')</p> <p>Model uncertainty is discussed in NUREG-1855 as follows:</p> <p>"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:</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• The nature of the failure modes is not completely understood or is unknown (e.g., digital instrumentation and controls)."</li> </ul> <p>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."</p> <p>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.</p>

**Table D-1. Terms and Definitions (Continued) -**

Term and Definition	Discussion
	<p>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.</p> <p>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.</p> <p>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.</p>
<b>Uncertainty Analysis</b>	
<p>A process for determining the level of imprecision in the results of the QRVA and its parameters.</p>	<p>In a QRVA, the ways in which the uncertainty in the results is presented includes the following:</p> <ul style="list-style-type: none"> <li>• A continuous probability distribution on numerical results.</li> <li>• A discrete probability distribution representing the impact of different models or assumptions.</li> <li>• 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.</li> <li>• Bounds or ranges of results that represent the results of the extreme assumptions.</li> <li>• An identification of limitations in the scope of the model (e.g., incompleteness) and how they might influence the applicability of the QRVA.</li> </ul> <p>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.”</p>
<b>Uncertainty Distribution</b>	
<p><i>(see Probability Distribution)</i></p>	<p>The term uncertainty distribution is related to the term probability distribution and is defined under “Probability Distribution.”</p>



**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Uncertainty Interval, Uncertainty Range</b>	
A range that bounds the uncertainty value(s) of a parameter or analysis result by establishing upper and lower limits. <i>(see Confidence Interval, Probability Distribution)</i>	<p>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.</p> <p>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 core damage frequency.”</p> <p>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.”</p> <p>The definition provided was based on definitions in the NRC Website Glossary and in NUREG-1855.</p>
<b>Uncertainty Range</b>	
<i>(see Uncertainty Interval)</i>	The term uncertainty range has the same meaning as uncertainty interval and is defined under “Uncertainty Interval.”
<b>Unreliability</b>	
<i>(see Reliability)</i>	The term unreliability is the opposite of reliability and is defined under “Reliability.”
<b>Up-to-Date</b>	
<i>(see QRVA Configuration Control, As-Built As-Operated)</i>	The term up-to-date is related to QRVA configuration control and is defined under “QRVA Configuration Control” or “As-Built As-Operated.”

**Table D-1. Terms and Definitions (Continued) -**

<b>Term and Definition</b>	<b>Discussion</b>
<b>Vulnerability</b>	
Weakness in the design or operation of a system, component, or structure that could disable its function.	<p>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 was used in Generic Letter (GL) 88-20, "Individual Facility Examination For Severe Accident Vulnerabilities". As part of GL 88-20, each licensee was asked to perform a systematic examination of its facility to identify any facility-specific vulnerabilities to severe accidents. The NRC, however, did not define vulnerability; it was the licensee's responsibility to define vulnerability. The method all licensees used to identify vulnerabilities was a QRVA.</p> <p>For some licensees, vulnerabilities were 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).</p>
<b>Water Immersion</b>	
Direct exposure from radioactive material in contaminated water given to an individual immersed in the water. ( <i>see Exposure Pathways, Cloudshine, Groundshine, Inhalation, Ingestion, Skin Deposition</i> )	In a Level 3 QRVA, for the consequence calculation, water immersion, is one of the assumed pathways by which an individual can receive doses. The pathways of exposure include: (1) direct external exposure from radioactive material in a plume, principally due to gamma radiation (air immersion or cloudshine), (2) direct exposure from radioactive material in contaminated water given to an individual immersed in the water, (3) exposure from inhalation of radioactive materials in the cloud and resuspended material deposited on the ground, (4) exposure to radioactive material deposited on the ground (groundshine), (5) radioactive material deposited onto the body surfaces (skin deposition), and (6) ingestion from deposited radioactive materials that make their way into the food and water pathway.



## D.2. Internal Fire Glossary

Table D-2 provides internal fire terms and their definitions with the associated discussion. The terms are listed alphabetically.

**Table D-2. Internal Fire Terms and Definitions**

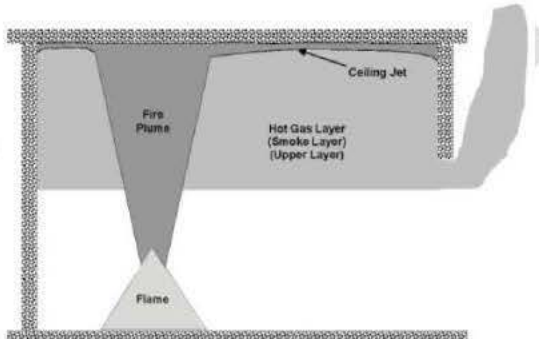
Term and Definition(s)	Discussion
<b>Active Fire Barriers</b>	
A fire barrier that must be physically repositioned from its normal configuration to an alternate configuration in order to provide its protective function.	In a fire QRVA, fire barriers impede the spread of fires and limit potential damage to safety equipment, thus reducing probabilities of fire spread to additional components and the probability of accident sequences. Ventilation system fire dampers, normally open fire doors, and water curtains are examples of passive fire barriers. The definition provided was based on the definition in NUREG-1805.
<b>Algebraic Fire Models</b>	
A type of fire model that provides a method for calculating simple fire phenomena based on a closed-form algebraic formulation.	In a fire QRVA, fire models predict fire damage of components, and thus contribute to the failure of those components, given failure of suppression. Algebraic models may be standalone equations found in the literature or may be contained within spreadsheets, such as the NRC's fire dynamics tools (FDTs). These equations are typically closed-form algebraic expressions, many of which were developed as correlations from empirical data. In some cases, they may take the form of a first-order ordinary differential equation and can provide an estimate of fire variables, such as hot gas layer (HGL) temperature, heat flux from flames or the HGL, smoke production rate, depth of the hot gas layer, and the actuation time for detectors. Algebraic models are helpful because they require minimal computational time and a limited number of input variables. Other than for very simple situations, algebraic models are useful primarily as screening tools. The definition provided was based on the definition in NUREG-1934.
<b>Authority Having Jurisdiction</b>	
The organization, office, or individual responsible for approving equipment, materials, an installation, or a procedure.	The NRC is the authority having jurisdiction for NFPA 805 as it is applied under 10 CFR 50.48. The definition provided was based on the definition in the NFPA 805 Standard.

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Cable and Raceway (Database) System</b>	
Cross-reference of power, control, or instrument cables associated with certain components or systems and their location throughout the facility, as it relates to specific cable raceways, tracks, or conduits where they may be situated.	<p>The Cable and Raceway System generally correlates cables to raceways, raceways to locations within the facility, and tracks basic cable and raceway attributes. Newer CRSs typically contain sophisticated database sort and query features.</p> <p>The information in the CRS may be used to determine how a fire in a certain location may affect the cables nearby and thus determine which components and systems may be affected. The location of cables is then used for the development of fire scenarios that are quantified in the fire QRVA. This is then used in a QRVA as input in constructing and calculating accident sequences.</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Cable Failure Mode</b>	
The behavior of an electrical cable upon fire-induced failure. ( <i>see Intercable Shorting, Intracable Shorting</i> )	In a fire QRVA, component failure modes can be attributed to cable failure modes resulting from fire. The ASME/ANS PRA Standard indicates that "failure modes for electrical cables include intractable shorting, intercable shorting, open circuit (loss of conductor continuity), and/or shorts between a conductor and an external ground."



**Table D-2. Internal Fire Terms and Definitions (Continued)**

Term and Definition(s)	Discussion
<b>Ceiling Jet</b>	
<p>The relatively rapid gas flow in a shallow layer beneath the ceiling surface that is driven by the buoyancy of hot combustion products.</p>	<p>Typically, a fire plume will form above a burning object. The fire plume will rise until obstructed by a horizontal surface, such as a ceiling. Upon hitting the ceiling, the hot gases in the fire plume will turn and flow along the ceiling in the form of a ceiling jet. When the ceiling jet gases are blocked by vertical surfaces, such as walls, they will accumulate into a hot gas layer or smoke layer. As more hot gas accumulates in the layer, the interface between the hot gas layer and cooler layer below will continue to drop toward the floor of the enclosure. As stated in NUREG/CR-6850, "ceiling jets form when a fire plume impinges under a ceiling and hot gases spread away."</p> <div style="text-align: center;">  <p>The diagram illustrates a fire plume rising from a flame on the floor of an enclosure. The plume hits the ceiling, creating a ceiling jet that flows along the top surface. Above the ceiling jet, a hot gas layer (smoke layer) or upper layer has formed. Labels include 'Flame', 'Fire Plume', 'Ceiling Jet', and 'Hot Gas Layer (Smoke Layer) (Upper Layer)'.</p> </div> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Circuit Failure Analysis</b>	
<p>The evaluation of electrical circuits to determine both the potential failure modes and their impact on the systems and equipment supported by the circuit.</p>	<p>Circuit failure analysis can include the assignment of probabilities to the likelihood of the cable failure modes of concern. Circuit failure analysis would include consideration of the impact of cable failures on circuit function. The equipment failures associated with those circuit failure modes would be input to the QRVA and contribute to accident sequence quantification.</p>
<b>Circuit Failure Mode</b>	
<p>The manner in which conductor failures from an electrical cable are manifested in the circuit. (see <i>Cable Failure Mode</i>)</p>	<p>In a fire QRVA, equipment failures associated with circuit failure modes are analyzed and contribute to accident sequence quantification. Examples of circuit failure modes include loss of motive power, loss of control, loss of or false indication, open circuit conditions, and spurious operation.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Code of Record</b>	
The edition of the code or standard in effect at the time the fire protection systems or feature was designed or specifically committed to the authority having jurisdiction. (see <i>Authority Having Jurisdiction</i> )	If the 1996 edition of NFPA 13 was in effect at the time a sprinkler system was designed, the code of record would be NFPA 13, <i>Standard for the Installation of Sprinkler Systems – 1996 edition</i> .  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Compensatory Actions</b>	
Actions taken to counteract or reduce an impairment to a required fire protection system, feature, or component.	In the NFPA 805 Standard, compensatory actions are described as “actions taken if an impairment to a required system, feature, or component prevents that system, feature, or component from performing its intended function. These actions are a temporary alternative means of providing reasonable assurance that the necessary function will be compensated for during the impairment, or an act to mitigate the consequence of a fire. Compensatory measures include, but are not limited to, actions such as fire watches, administrative controls, temporary systems, and features of components.”  The term compensatory measures may be used in place of compensatory actions (e.g., fire watch compensatory actions may improve detection in the affected vicinity).  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Concurrent Hot Shorts</b>	
The occurrence of two or more hot shorts such that the shorts overlap in time. (see <i>Conductor-to-Conductor Short</i> )	In a fire QRVA, concurrent hot shorts are important because they can cause multiple equipment failures, complicate operator response, and increase human error probabilities in a fire QRVA. These challenges may be more difficult to overcome than would be the case given only a single spurious operation at a time.  The definition provided was based on the definition in the ASME/ANS PRA Standard.



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Conductor-to-Conductor Short</b>	
An abnormal connection (including an arc) of relatively low impedance between two conductors.	<p>In a fire QRVA, conductor-to-conductor shorts may be caused by fire and in turn may cause failure of equipment, thus contributing to accident sequences.</p> <p>As described in NUREG/CR-6850, a conductor-to-conductor short can occur in the following manner: “a conductor-to-conductor short between an energized conductor of a grounded circuit and a grounded conductor results in a ground fault. A conductor-to-conductor short between an energized conductor and a non-grounded conductor results in a hot short. A conductor-to-conductor short between an energized conductor of an ungrounded circuit and a neutral conductor has the same functional impact as a ground fault.”</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Damage Criteria</b>	
Those characteristics of the fire-induced environment that are specified as indicating failure of a damage target or set of damage targets. (see <i>Damage Target, Damage Threshold</i> )	<p>In a fire QRVA, cables and their associated components are failed in the QRVA model upon damage. Damage criteria commonly refer to certain temperatures or heat fluxes at target locations that when exceeded indicate failure of the targets. The damage target may be a cable, set of cables, or a component in a location near the fire. The damage criteria also may be based on any other environmental effect of the fire; e.g., smoke density.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Damage Target</b>	
Any cable, equipment, or structural element in the fire QRVA whose function can be adversely affected by the modeled fire.	<p>In a fire QRVA, cables and their associated components are failed in the QRVA model upon damage.</p> <p>The ASME/ANS PRA Standard defines the term damage target as “a cable or equipment item that belongs to the Fire QRVA cable or equipment list and that is included in event trees and fault trees for fire risk estimation. Damage targets also may include structural elements (e.g., structural steel) in the case of certain high-hazard fire sources, such as very large oil spills.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Damage Threshold</b>	
The values corresponding to the damage criteria that will be taken as indicative of the onset of fire-induced failure of a damage target or set of damage targets. <i>(see Damage Criteria)</i>	An example of a damage threshold would be the temperature at a cable location that when exceeded would indicate failure of the cable.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Electrical Cable</b>	
A construct consisting of one or more insulated conductors designed to carry signals or power between points in a circuit.	In a fire QRVA, fire damage to a cable may result in disablement or spurious operation of safety-related equipment (affecting probability of failure of safety systems) and/or generation of an initiating event. Cables are used to connect points in a common electrical circuit and may be used to transmit power, control signals, indications, or instrument signals. Cables are important to risk because they connect equipment necessary for safe operation of the facility to sources of power and control over relatively long distances in the facility. This increases the possibility that an undesired event (e.g., a fire) at an intervening location will affect the cable and disrupt the continued operation of equipment.
<b>Electrical Raceway Fire Barrier System</b>	
Non-load-bearing partition type envelope system installed around electrical components and cabling that are rated by test laboratories in hours of fire resistance and used to maintain safe-shutdown functions free of fire damage. <i>(see Wrap)</i>	In a fire QRVA, electrical raceway fire barrier systems (ERFBSs) are modeled because they provide protection for electrical cables and delay or prevent damage from fires. A fire rated ERFBS provides additional time before damage for those protected cables in a fire QRVA.  The definition provided was based on the definition in Regulatory Guide 1.189.
<b>External Hot Short</b>	
A hot short in which the source conductor and target conductor are from separate cables. <i>(see Hot Short, Intercable Short Circuit)</i>	The term external hot short can be used interchangeably and correctly with intercable short circuit, which is also referred to as intercable conductor-to-conductor short circuit.  The definition provided was based on the definition in NUREG/CR-6850.



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Field Models</b>	
<p>A type of fire model that provides a method for calculating fluid flow through a volume using numerical solutions of the governing equations for conservation of total mass, chemical species, momentum, and energy.</p>	<p>In a fire QRVA, the results from a field model can be used as input in determining the probability of damage from a particular fire to targets nearby and to associated safety-related equipment.</p> <p>Field models are computational fluid dynamics models that can be used to predict fire-induced environmental conditions (e.g., temperature at different times). The equations used in field models are approximated using finite differences over discrete control volumes, and the solution is obtained using the discretized equations. The calculations are performed over a period of time to obtain a transient (time-dependent) solution, or iterated over many times to provide a steady-state (time-independent) solution. The model typically is comprised of a large number of control volumes from thousands to millions.</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Fire Analysis Tool</b>	
<p>A method used to estimate or calculate one or more physical fire effects. (<i>see Field Model, Zone Model, Algebraic Fire Model</i>)</p>	<p>Fire analysis tools include, but are not limited to, computerized compartment fire models, such as zone or field models, closed-form algebraic fire models, and empirical correlations such as those provided in a handbook, and lookup tables that relate input parameters to a predicted output. The fire analysis tool used is based on the objectives of the specific analysis and a predefined set of input parameter values as defined by the fire scenario being analyzed.</p> <p>Examples of calculated physical fire effects are temperature, heat flux, time to failure of a damage target, rate of flame spread over a fuel package, heat release rate for a burning material, and smoke density.</p> <p>The ASME/ANS PRA Standard defines the term fire analysis tool as “any method used to estimate or calculate one or more physical fire effects (e.g., temperature, heat flux, time to failure of a damage target, rate of flame spread over a fuel package, heat release rate for a burning material, smoke density, etc.) based on a predefined set of input parameter values as defined by the fire scenario being analyzed. Fire analysis tools include, but are not limited to, computerized compartment fire models, closed-form analytical formulations, empirical correlations such as those provided in a handbook, and lookup tables that relate input parameters to a predicted output.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Fire Area</b>	
<p>An area enclosed by rated fire barriers capable of preventing or inhibiting spread of fires to and from the outside. (see <i>Fire Barrier</i>)</p>	<p>In a fire QRVA, the spread of fire and fire effects is limited (reduced probability of propagation) across fire areas. A multi-compartment fire analysis is done across fire areas to evaluate the risk significance of these fire scenarios.</p> <p>A fire area must be made up of rated fire barriers with openings in the barriers provided with fire doors, fire dampers, and fire penetration seal assemblies with a fire resistance rating at least equivalent to the barrier in which it exists (e.g., this term is defined in the analysis in Appendix R to 10 CFR Part 50). Fire areas tend to confine most fires within the area. In a QRVA, the fire area concept may simplify analysis, as each fire area generally may be treated independently from others. Fires may spread from one area to the next should a portion of the barrier be defeated (e.g., fire door left open).</p> <p>Regulatory Guide 1.189 defines the term fire area as “the portion of a building or facility that is separated from other areas by rated fire barriers adequate for the fire hazard.”</p>
<b>Fire Barrier</b>	
<p>A component intended to impede spreading of a fire and its effects. (see <i>Passive Fire Barrier, Active Fire Barrier</i>)</p>	<p>In a fire QRVA, fire barriers are modeled to prevent or reduce the spread of fires between fire areas. Therefore, fire barriers reduce the probability of damage to safety-related equipment in adjacent areas, and thus reduce the frequency of undesired end states. Fire barriers can be active, indicating the barrier requires some physical repositioning to function, or passive, indicating the barrier provides protection in its normal orientation.</p> <p>Certification of a fire barrier’s fire resistance endurance rating typically is based on standardized tests, such as the American Society of Testing and Materials (ASTM) Standard E-119. Examples of solid construction made of fire-resistant material could be a wall or door.</p> <p>NUREG/CR-6850 defines the term fire barrier as “components of construction (walls, floors, and their supports), including beams, joists, columns, penetration seals or closures, fire doors, and fire dampers that are rated by approving laboratories in hours of resistance to fire, that are used to prevent the spread of fire and restrict spread of heat and smoke.”</p>



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Compartment</b>	
A subdivision of a building or facility that is a well-defined enclosed room, not necessarily bounded by rated fire barriers, which essentially confines the fire.	<p>In a fire QRVA, fire compartments are modeled because they reduce the probability of fire spread across boundaries. Boundaries of a fire compartment may have open equipment hatches, stairways, doorways, or unsealed penetrations.</p> <p>As discussed in the ASME/ANS PRA Standard, “a fire compartment generally falls within a fire area and is bounded by noncombustible barriers where heat and products of combustion from a fire within the enclosure will be substantially confined.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Fire Control</b>	
The stage of firefighting in which a fire incident is controlled and not allowed to escalate in magnitude.	<p>In current fire QRVA practice, the concept of fire control generally is not used because there is large uncertainty associated with declaring when a fire has been brought under control as opposed to having been fully extinguished. Also, fire control is not modeled in fire models. Fire control can be achieved by water-based fixed systems or through the application of other fire suppression means (e.g., hose streams, portable extinguishers). Furthermore, gaseous fixed systems can prevent fire damage from extending beyond the locations damaged when the system is actuated. The concept of fire control may also include managed fire burnout whereby a fire is allowed to continue burning until the fuel source is exhausted (e.g., in the case of a leak of flammable compressed gases such as hydrogen).</p> <p>The definition provided was based on the definition in NUREG-1805.</p>
<b>Fire Event</b>	
A particular case where a fire has occurred in a facility.	Fire events are characterized in the fire events database. A fire event is described by its initiation, the progression of the fire, detection and suppression, and the impact on facility systems.
<b>Fire Events Database</b>	
A collection of fire events that indicates characteristics of the fire and response by fire protection systems and facility personnel as well as the impact of the fire on facility equipment and operations.	In a fire QRVA, the fire events database is used to provide raw data to calculate fire ignition frequencies and manual suppression reliability for different types of fires.

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Extinguishment</b>	
The stage of a fire when combustible materials are no longer burning.	In a fire QRVA, fire extinguishment concludes the duration of a fire and implies that all burning materials have been fully suppressed. Fire damage generally is modeled in fire QRVA until fire extinguishment.
<b>Fire Hazard Analysis</b>	
An analysis to evaluate potential fire sources and combustibles, and appropriate fire protection systems, and features used to mitigate the effects.	Fire hazards analyses are generally of a qualitative or semi-quantitative nature as compared to a QRVA. Regulatory Guide 1.189 defines fire hazard analysis as “an analysis used to evaluate the capability of a facility to perform safe-shutdown functions and minimize radioactive releases to the environment in the event of a fire. The analysis includes the following features: identification of fixed and transient fire hazards; identification and evaluation of fire prevention and protection measures relative to the identified hazards; evaluation of the impact of fire in any facility area on the ability to safely shut down the reactor and maintain shutdown conditions, as well as to minimize and control the release of radioactive material.” The definition provided was based on the definition in the NFPA 805 Standard.
<b>Fire Human Reliability Analysis</b>	
A structured approach used to identify potential human error events that may occur in a sequence of events following a fire and to systematically estimate the probability of those errors using data, models, or expert judgment as applied to a fire.	Fire human reliability analysis is used to quantify the potential impact of fire-generated environmental effects and stressors on human performance and the likelihood that errors might occur during execution of fire response procedures for specific areas of the facility, including control room evacuation. The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Fire Ignition Frequency</b>	
Frequency of fire occurrence generally expressed as fire ignitions per reactor-year.	In a fire QRVA, fire ignition frequency is normally calculated based on fires events that have the potential to cause damage to targets outside the ignition source. Fire ignition frequency is the factor that, in quantification, introduces the frequency element into the fire-induced loss of fuel inventory control frequency. The definition provided was based on the definition in the ASME/ANS PRA Standard.



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Fire-Induced Initiating Event</b>	
<p>The initiating event assigned to occur in the fire QRVA facility response model for a given fire scenario. <i>(see Fire Facility Response Model)</i></p>	<p>The term initiating event is defined in the exact same context as is used in internal events QRVA. That is, the initiating event is not the fire, it is induced by the fire. For example, a fire affects a pilot operated relief valve control cable, causing spurious operation of a PORV, and thus an initiating event.</p> <p>Fire-induced initiating events trigger sequences of events that challenge facility control and safety systems whose failure potentially could lead to loss of fuel inventory control or acute fuel release.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Fire Model</b>	
<p>A mathematical prediction of fire growth, environmental conditions, and potential effects on structures, systems, or components based on the conservation equations or empirical data.</p>	<p>The ASTM Standard E176-10a, "Standard Terminology of Fire Standards", defines fire model as "a physical representation or set of mathematical equations that approximately simulate the dynamics of burning and associated processes."</p> <p>The definition provided was based on the definition in the NFPA 805 Standard.</p>
<b>Fire Facility Response Model</b>	
<p>A representation of a combination of equipment, cable, circuit, and system function, and operator failures or successes, of an accident that when combined with a fire-induced initiating event can lead to undesired consequences, with a specified end state (e.g., loss of fuel inventory control or acute fuel release).</p>	<p>In a fire QRVA, the fire facility response model contains the event trees and fault trees that will be used to analyze fire-induced initiating events. Given a fire scenario leading to fire-induced failure of a fire damage target set, a facility damage state (fire-induced damage to facility systems and components including equipment failure modes) is defined and incorporated into the fire facility response model. The event tree/fault tree models are then manipulated to depict the logical relationships among equipment failures (both random and fire-induced) and human failure events. As in internal events, the fire facility response model estimates the conditional loss of fuel inventory control probability given loss of a fire damage target set.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued)**

Term and Definition(s)	Discussion
<b>Fire Plume</b>	
<p>Buoyant stream of hot gases rising above a localized area undergoing combustion into surrounding space of essentially uncontaminated air.</p>	<p>Typically, a fire plume will form above a burning object. The fire plume will rise until obstructed by a horizontal surface, such as a ceiling. Upon hitting the ceiling, the hot gases in the fire plume will turn and flow along the ceiling in the form of a ceiling jet. When the ceiling jet gases are blocked by vertical surfaces, such as walls, they will accumulate into a hot gas layer or smoke layer. As more hot gas accumulates in the layer, the interface between the hot gas layer and cooler layer below will continue to drop toward the floor of the enclosure.</p> <div style="text-align: center;"> <p>The diagram shows a cross-section of a room with a fire source at the bottom center. A flame rises from the source, forming a fire plume that expands as it goes up. It hits the ceiling, where it spreads horizontally as a ceiling jet. This jet then accumulates at the top of the room, forming a hot gas layer (smoke layer) that is thicker at the top and tapers towards the walls. Labels include 'Flame', 'Fire Plume', 'Ceiling Jet', and 'Hot Gas Layer (Smoke Layer) (Upper Layer)'.</p> </div> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Fire QRVA, Fire QVRA</b>	
<p>An approach to quantitatively evaluate the risk from hazards associated with a fire. <i>(see Main Glossary: QRVA)</i></p>	<p>This quantitative approach consists of fire ignition frequencies, the associated initiating event produced by the ignition, the probability of fire damage from those ignition sources, and the resulting impact on the facility.</p> <p>The term QVRA is another term that can be used interchangeably and correctly with QRVA. Typically, the term QVRA is used internationally.</p>
<b>Fire Prevention</b>	
<p>Measures directed toward reducing the likelihood of fire.</p>	<p>Fire prevention is not generally modeled in fire QRVA, although it is reflected in fire ignition frequency. Lower fire frequencies could be due, at least in part, to an effective fire prevention program.</p> <p>The definition provided was based on the definition in the NFPA 805 Standard.</p>
<b>Fire QVRA</b>	
<p><i>(see Fire QRVA)</i></p>	<p>The term fire QVRA has the same meaning as fire QRVA and is defined under "Fire QRVA."</p>



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Protection Defense-In-Depth</b>	
The principle of providing multiple and diverse fire protection systems and features.	<p>Fire protection defense-in-depth is modeled explicitly in fire QRVA. In particular, fire QRVA will credit defense-in-depth fire protection measures and will predict the likelihood that those measures fail to prevent fire-induced damage to facility equipment and cables.</p> <p>The fire protection defense-in-depth objectives, as indicated in Appendix R to 10 CFR Part 50, are “(1) to prevent fires from starting; (2) to detect rapidly, control, and extinguish promptly those fires that do occur; and (3) to provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.” Multiple and diverse fire protection systems and features attain these objectives.</p>
<b>Fire Protection Design Elements</b>	
Any aspect of the fire protection program supported by specific design requirements and/or analyses.	<p>Fire protection design elements can include active fire protection systems such as sprinkler or smoke detector systems, passive systems such as electrical raceway fire barriers, and programmatic elements.</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Fire Protection Feature</b>	
Administrative controls, emergency lighting, fire barriers, fire detection and suppression systems, fire brigade personnel, and other features provided for fire protection purposes.	<p>In a fire QRVA, fire protection features would be credited in accident sequences in which a fire endangers stable operation of the facility. Fire protection features are important to risk because they reduce damage due to fire and thus the frequency of accidents with undesired consequences because of fires.</p> <p>The definition provided was based on the definition in Regulatory Guide 1.189.</p>
<b>Fire Protection Program</b>	
The integrated effort involving equipment, procedures, and personnel used in carrying out all activities of fire protection.	<p>The ASME/ANS PRA Standard states that the fire protection program includes “system and facility design, fire prevention, fire detection, annunciation, confinement, suppression, administrative controls, fire brigade organization, inspection and maintenance, training, quality assurance, and testing.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Protection Program Element</b>	
Any specific aspect or provision included as a part of the fire protection program.	As described in the ASME/ANS PRA Standard, fire protection program elements include “system and facility design, fire prevention, fire detection, annunciation, confinement, suppression, administrative controls, fire brigade organization, inspection and maintenance, training, quality assurance, and testing.”  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Fire Protection System</b>	
Fire detection, notification, and fire suppression systems designed, installed, and maintained in accordance with the applicable National Fire Protection Association codes and standards.	Fire protection systems are systems installed to provide detection, warning, or suppression of fires.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Fire Response Procedure</b>	
A procedure established for operators to respond to a fire.	An example of a fire response procedure is to evacuate the control room when certain environmental conditions are reached due to a control room fire.  Specific facilities may have alternate names for the fire response procedures such as fire emergency procedures, pre-fire plans, or emergency response procedures. The fire response procedures also may be embedded within a more general set of emergency operating procedures designed to deal with a range of potential off-normal facility operating states, including fires.
<b>Fire Risk Analysis</b>	
(see Fire QRVA)	The term fire risk analysis has the same meaning as fire QRVA and is defined under “Fire QRVA.”



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Safe-Shutdown Analysis</b>	
The deterministic process or method conducted to identify and evaluate the capability of structures, systems, and components necessary to accomplish and maintain safe shutdown conditions in the event of a fire.	<p>Fire safe shutdown analysis is conducted based on a fire scenario in fire QRVA and affects the facility response mode.</p> <p>For fire events, safe shutdown are those facility conditions specified in the facility technical specifications as hot standby, hot shutdown, or cold shutdown.</p> <p>The definition provided was based on the definition in Regulatory Guide 1.189.</p>
<b>Fire Scenario</b>	
A set of elements that describe a fire event.	<p>A fire scenario includes a description of the fire and any factors affecting it from ignition to suppression. As a result, the fire scenario describes the progression of the fire from ignition to damage in the fire QRVA.</p> <p>The ASME/ANS PRA Standard states that the elements of a fire scenario include “a physical analysis unit, a source fire location and characteristics, detection and suppression features to be considered, damage targets, and intervening combustibles.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Fire Suppression</b>	
The process of controlling and ultimately extinguishing fires.	<p>In fire QRVA, fire suppression is a process, but successful completion of that process implies fire extinguishment, which represents the termination of the fire itself. An accident sequence caused by the fire may continue beyond extinguishment of the fire. Traditional fire protection definitions refer to fire suppression as controlling and extinguishing fires, which is consistent with the term as applied in fire QRVA.</p> <p>Fire suppression can be either manual or automatic. Manual fire suppression is the use of hoses, portable extinguishers, or manually actuated fixed suppression systems by facility personnel. Automatic fire suppression is the use of automatic fixed systems, such as sprinkler, Halon, and CO<sub>2</sub> systems.</p> <p>Manual fire suppression is modeled as a time-dependent activity in fire QRVA, occurring at potentially different times in the scenario, in which automatic fixed suppression is modeled as occurring early in the scenario and often can be treated as time-independent.</p>

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire Suppression System</b>	
Typically, permanently installed fire protection systems provided for the express purpose of suppressing fires.	In a fire QRVA, the effectiveness of the fire suppression system is an important consideration, in addition to the system availability and reliability. The ASME/ANS PRA Standard states that a fire suppression system “may be either automatically or manually actuated. However, once activated, the system should perform its design function with little or no manual intervention.”  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Fire Wrap</b>	
A localized protective covering designed to protect cables, cable raceways, or other equipment from fire-induced damage.	Fire wrap, used to protect against thermal damage, is the common term usually used to denote a type of electronic raceway fire barrier system.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Fire Zone</b>	
<ol style="list-style-type: none"> <li>1. Subdivisions of a fire area not necessarily bounded by fire rated assemblies.</li> <li>2. Subdivisions of a fire detection or suppression systems, which provide alarm indications at the central alarm panel.</li> </ol>	The term fire zone is not widely used in current fire QRVA practice but, when used, can have different meanings. A fire zone may be a loosely defined spatial area such as a partially enclosed space within a larger fire compartment or fire area (per definition (1)). The term also may be used in the more traditional context of a zone of coverage for fixed fire protection features such as fire detection and fire suppression (per definition (2)). The term fire zone may also be encountered in older fire QRVAs in which terminology was as yet unsettled. That is, some older fire QRVAs may use the term fire zone in the same context that the ASME/ANS Standard uses the term physical analysis unit.  The definition provided was based on the definition in the NFPA 805 Standard.



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Fire-Resistance Rating</b>	
The time that materials or assemblies have withstood a fire exposure as established in accordance with an approved test procedure appropriate for the structure, building material, or component under consideration.	In a fire QRVA, the greater the fire-resistance rating, the longer time to damage is modeled. ASTM Standard E-119 is the test standard for determining fire resistance. The fire-resistance rating is provided in units of minutes or hours.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Flame Spread Rating</b>	
A relative measurement of the surface burning characteristics of building materials.	The flame spread rating is tested in accordance with NFPA 255, "Standard Method of Test Surface Burning Characteristics of Building Materials".  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Free of Fire Damage</b>	
The structure, system, or component under consideration remains capable of performing its intended function during and after the postulated fire.	A component free of fire damage in the fire QRVA model is given full credit to performing its function.  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Ground Fault</b>	
A type of short circuit involving an abnormal connection between a conductor and a grounded conducting medium.	NUREG/CR-6850 describes a ground fault as being characterized by "an abnormal current surge (fault current) attributable to the lack of any significant circuit burden (i.e., load). A ground fault should trigger over-current protective action for a properly designed circuit."  As used in the definition, the grounded conducting medium refers to any conduction path associated with the reference ground of the circuit. This might include structural elements (e.g., tray, conduit, enclosures, metal beams) or intentionally grounded conductors of the circuit (neutral conductor).  The term ground fault is used interchangeably and correctly with the term short-to-ground. The definition provided was based on the definition in NUREG/CR-6850.

**Table D-2. Internal Fire Terms and Definitions (Continued)**

Term and Definition(s)	Discussion																
<b>Heat Release Rate</b>																	
<p>The amount of heat generated by a burning object per unit time.</p>	<p>The heat release rate (HRR) is the key driver in determining the extent of damage in a fire scenario and is usually expressed in units of kW. An example of an HRR can be found in an HRR profile. An HRR profile refers to the behavior of the HRR as a function of time (an HRR versus time plot). For example, a fire with a constant HRR has an intensity that does not change.</p> <p>The ASTM Standard E176-10a, "Standard Terminology of Fire Standards", defines heat release rate as "the thermal energy released per unit time by an item during combustion under specified conditions." The following figure represents an HRR curve.</p> <div style="text-align: center;"> <table border="1" style="margin: 10px auto;"> <caption>Approximate HRR Curve Data</caption> <thead> <tr> <th>Time (s)</th> <th>Heat Release Rate (kW)</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td></tr> <tr><td>600</td><td>700</td></tr> <tr><td>1200</td><td>800</td></tr> <tr><td>1800</td><td>900</td></tr> <tr><td>2400</td><td>950</td></tr> <tr><td>3000</td><td>200</td></tr> <tr><td>3600</td><td>100</td></tr> </tbody> </table> </div> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>	Time (s)	Heat Release Rate (kW)	0	0	600	700	1200	800	1800	900	2400	950	3000	200	3600	100
Time (s)	Heat Release Rate (kW)																
0	0																
600	700																
1200	800																
1800	900																
2400	950																
3000	200																
3600	100																
<b>High-Energy Arcing Fault</b>																	
<p>A high-current, electrical fault that produces an energetic discharge of electrical and thermal energy and may be followed by a fire.</p>	<p>High-energy arcing faults are unique in fire QRVA since damage is assumed to occur instantaneously to targets, regardless of the potential presence of a fixed suppression system.</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>																



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>High-Hazard Fire Source</b>	
A fire source that can lead to fires of a particularly severe and challenging nature.	In a fire QRVA, high-hazard fire sources may cause extensive damage, potentially including the failure of structural elements such as steel, which is mapped into failures of equipment.  Examples of high-hazard fire sources include catastrophic failure of an oil-filled transformer, an unconfined release of flammable or combustible liquid, leaks from a pressurized system containing flammable or combustible liquids, and significant releases or leakage of hydrogen or other flammable gases (ASME/ANS PRA Standard).  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>High-Low Pressure Interface</b>	
Interface between the reactor coolant system and lower-pressure systems.	In a fire QRVA, regulations stipulate that at least one isolation valve at the interface of high- and low-pressure systems must remain closed despite any damage that may be caused by fire.
<b>Hot Gas Layer</b>	
The volume under the ceiling of a fire enclosure where smoke accumulates and high gas temperatures are observed.	Typically, a fire plume will form above a burning object. The fire plume will rise until obstructed by a horizontal surface, such as a ceiling. Upon hitting the ceiling, the hot gases in the fire plume will turn and flow along the ceiling in the form of a ceiling jet. When the ceiling jet gases are blocked by vertical surfaces, such as walls, they will accumulate into a hot gas layer or smoke layer. As more hot gas accumulates in the layer, the interface between the hot gas layer and cooler layer below will continue to drop toward the floor of the enclosure. Hot gas layer is the upper zone in a two-zone fire model formulation.  The definition provided was based on the definition in NUREG/CR-6850.
<b>Hot Short</b>	

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
The condition in which individual conductors of the same or different cables come in contact with each other. At least one of the conductors involved in the shorting is energized, resulting in an impressed voltage or current on the circuit being analyzed.	In a fire QRVA, a hot short can cause a spurious operation, which is one possible failure mode considered in the accident sequence model. Hot shorts also can cause misleading instrumentation and indication signals.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Ignition Source</b>	
A piece of equipment or activity that causes a fire.	Ignition source is the first link to an accident sequence caused by fire. A fire started by an ignition source may damage equipment, causing an initiating event, and possibly damaging safety systems required for response.  Fixed ignition sources are permanently installed, and transient ignition sources are temporarily located. Examples of transient ignition sources are a welder or grinder being used for hot work. Examples of fixed ignition sources are switchgear cabinets, transformers, pumps, and cables.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Intercable Short Circuit</b>	
Electrical contact between individual conductors in two or more separate cables due to damaged insulation and cable wrapping. (see <i>Intracable Short Circuit</i> )	As analyzed in a QRVA, an intercable short circuit may lead to any one of several possible conductor fault modes including hot shorts and ground faults. Such faults may disable safety-related systems, cause the spurious operation of facility components, and may lead to or contribute to an accident sequence. An intercable short circuit may be caused by fire- induced damage to grouped electrical cables.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Internal Fire</b>	



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
A hazard group in which a fire occurs from within the facility that is evaluated in fire QRVA.	For fire QRVA, the phrase within the facility as used in this definition is any location that lies within the global analysis boundary as defined by the facility partitioning technical element under Part 4 of the ASME/ANS PRA Standard. Examples of internal fires are fires that occur in the confines of the facility, including any buildings associated with facility operations, the switchyard, transformer yard, and service water supply. Forest fires are classified as external fires.
<b>Internal Hot Short</b>	
A hot short in which both the source conductor and target conductor are in the same multi-conductor cable. <i>(see Hot Short, Intracable Short Circuit)</i>	Internal hot shorts have greater probabilities of occurrence than external hot shorts. The term internal hot short can be used interchangeably and correctly with intracable short circuit, which is also referred to as intracable conductor-to-conductor short circuit.  The definition provided was based on the definition in NUREG/CR-6850.
<b>Intervening Combustibles</b>	
Materials that may burn but are not ignition sources.	The fire scenario becomes more extensive in the presence of intervening combustibles. This is because intervening combustibles, located between the ignition source and target, contribute to fire propagation along this path.  The definition provided was based on the definition in NUREG/CR-6850.
<b>Intracable Short Circuit</b>	
Electrical contact between individual conductors in a cable due to damaged insulation between the conductors. <i>(see Intercable Short Circuit)</i>	As analyzed in a QRVA, intractable short circuits may lead to any of the defined cable and circuit failure modes, including hot shorts and ground faults. Such faults may cause the spurious operation of facility components, disable safety-related systems, and lead to or contribute to an accident sequence. Intracable short circuits may occur because of a fire damaging insulation between the conductors of any multi-conductor cable, or they may occur because of insulation faults.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Limiting Fire Scenario</b>	

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
Fire scenario(s) in which one or more of the inputs to the fire modeling calculation are varied to the point that particular equipment is failed.	The intent of the limiting fire scenario is to determine that there is a reasonable margin between the expected fire scenario conditions and the point of this failure. Examples of fire modeling inputs that could be varied include heat, release rate, initiation location, or ventilation rate.  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Maximum Expected Fire Scenario</b>	
Scenarios that represent the most challenging fire that could be reasonably anticipated for the occupancy type and conditions in the space.	Maximum expected fire scenario is a term for an analysis in the fire modeling track of NFPA 805 and is not specifically related to fire QRVA. Maximum expected fire scenarios can be based on industry experience using facility-specific conditions and fire experience (NFPA 805).  The definition provided was based on the definition in the NFPA 805 Standard.
<b>Multiple Spurious Operations</b>	
Concurrent spurious operations of two or more equipment items. <i>(see Concurrent Hot Shorts)</i>	Multiple spurious operations may cause multiple equipment failures and complicate operator actions in a fire accident sequence in comparison to single spurious operations.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Natural Ventilation</b>	
The condition in which gas flows into or out of the room because of density differences between the fluids.	Ventilation (supplying fresh air) may cause the fire to burn more intensely, while at the same time potentially removing part of the hot gas layer. Therefore, ventilation may affect the probability of damage to equipment, given a fire in a certain location.  The definition provided was based on the definition in NUREG/CR-6850.
<b>Open Circuit</b>	
A loss of electrical continuity in an electrical circuit, either intentional or unintentional.	In a fire QRVA, open circuits will cause the associated electrical equipment to be inoperable. This may increase the probability of system failures and probabilities of relevant accident sequences. Open circuits could result from a loss of conductor continuity or from the triggering of circuit protection devices such as a blown fuse or open circuit breaker, or because of a loss of physical continuity in one or more cable conductors (NUREG/CR-6850).  The definition provided was based on the definition in NUREG/CR-6850.
<b>Passive Fire Barriers</b>	



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
A fire barrier that provides its protective function while in its normal orientation, without any need to be repositioned.	In a fire QRVA, fire barriers impede the spread of fires and limit potential damage to safety equipment, thereby reducing probabilities of fire spread to additional components and the probability of accident sequences. Walls and normally closed fire doors are examples of passive fire barriers.  The definition provided was based on the definition in NUREG-1805.
<b>Physical Analysis Unit</b>	
A spatial subdivision of the facility on which the fire QRVA is based.	In a fire QRVA, the physical analysis units are the fundamental spatial element considered as being affected by fires. While the fire QRVA will include consideration of fires affecting more than one physical analysis unit at a time (the multi-compartment analysis), most fire scenarios are assumed to remain confined to one physical analysis unit. Physical analysis units usually are based on fire areas or fire compartments, but they also may be based on factors such as spatial separation (as opposed to physical barriers), nonrated partitioning elements, and active fire barrier systems; e.g., a water curtain. Since a physical analysis unit substantially contains the effects of a fire, it generally reduces the probability of additional component damage.  This term was coined in relation to the fire portion of the ASME/ANS PRA Standard to refer generally to fire compartments, fire zones, and fire areas.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Probability of Nonsuppression</b>	
Probability of failing to suppress a fire before target damage occurs.	In a fire QRVA, probability of nonsuppression is used to calculate the probability of target damage (and, consequently, probability of component or system failure), given a fire of a certain intensity in a certain location. Probability of nonsuppression depends on the characteristics of the fire, fire suppression method, and the time available until target damage.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Qualified Cable</b>	
A cable that has been tested and certified as meeting all aspects of IEEE-383 standard including both the equipment qualification and flame spread elements.	The IEEE-383 standard primarily deals with the equipment qualification issues of cable aging and severe accident environmental exposures. The standard also includes a vertical flame spread test. In practice, cables that have been only tested against the flame spread portion of the standard, but have not been subjected to the equipment qualification elements, may be referred to as low flame spread cables, but they would not be considered fully qualified. A cable that does not meet this criterion is referred to as unqualified or nonqualified.

**Table D-2. Internal Fire Terms and Definitions (Continued) -**

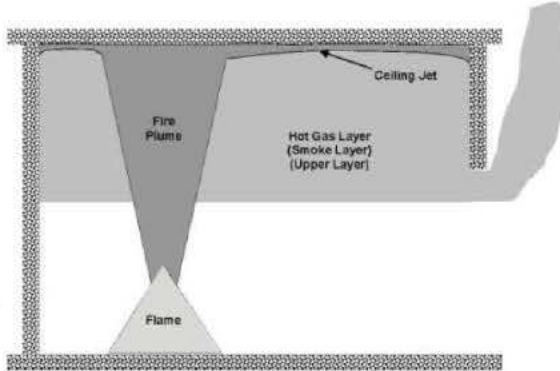
<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Raceway</b>	
An enclosed channel of metallic or nonmetallic materials designed expressly for holding wires, cables, or bus bars, with additional functions as permitted by code.	<p>In a fire QRVA, generally all cables in a raceway are affected equally by the modeled fire. Open cable trays (e.g., ladder style trays) also are referred to as raceways.</p> <p>The ASME/ANS PRA Standard states that raceways include, but are not limited to, “rigid metal conduit, rigid nonmetallic conduit, intermediate metal conduit, liquid-tight flexible conduit, flexible metallic tubing, flexible metal conduit, electrical nonmetallic tubing, electrical metallic tubing, underfloor raceways, cellular concrete floor raceways, cellular metal floor raceways, surface raceways, wireways, and busways.”</p> <p>The definition provided was based on the definition in the ASME/ANS PRA Standard.</p>
<b>Short Circuit</b>	
An abnormal connection (including an arc) of relatively low impedance between two conductors or points of different potential.	<p>With regard to control circuit failures, short circuits could involve a ground fault or hot short. Either may cause disablement or undesired operation of safety-related equipment and contribute to initiation or propagation of an accident sequence. Short circuits also can cause the failure or maloperation of the indication elements of a control circuit, instrument circuits, and power circuits.</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Short-to-Ground</b>	
A type of short circuit involving an abnormal connection between a conductor and a grounded conducting medium.	<p>NUREG/CR-6850 describes a ground fault as being characterized by “an abnormal current surge (fault current) attributable to the lack of any significant circuit burden; i.e., load. A ground fault should trigger over-current protective action for a properly designed circuit.”</p> <p>As used in the definition, the grounded conducting medium refers to any conduction path associated with the reference ground of the circuit. This might include structural elements (e.g., tray, conduit, enclosures, metal beams) or intentionally grounded conductors of the circuit (neutral conductor). The term short-to-ground is used interchangeably and correctly with the term ground fault.</p> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

Term and Definition(s)	Discussion
<b>Smoke Layer</b>	
The volume under the ceiling of a fire enclosure where smoke accumulates and high gas temperatures are observed. <i>(see Upper Layer, Hot Gas Layer)</i>	Typically, a fire plume will form above a burning object. The fire plume will rise until obstructed by a horizontal surface, such as a ceiling. Upon hitting the ceiling, the hot gases in the fire plume will turn and flow along the ceiling in the form of a ceiling jet. When the ceiling jet gases are blocked by vertical surfaces, such as walls, they will accumulate into a hot gas layer or smoke layer. As more hot gas accumulates in the layer, the interface between the hot gas layer and cooler layer below will continue to drop toward the floor of the enclosure. The smoke layer is the upper zone in a two-zone model formulation.  The definition provided was based on the definition in NUREG/CR-6850.
<b>Spurious Operation</b>	
The undesired operation of equipment resulting from a fire that could affect the capability to achieve and maintain safe shutdown.	Spurious operation results from a hot short and may result in undesired change of state or disablement of safety-related equipment, thereby resulting in initiation of an accident sequence or damage to a component within the accident sequence. In some cases, ground faults or open circuits also may cause spurious operation, depending on the specific circuit design.  The definition provided was based on the definition in the ASME/ANS PRA Standard.
<b>Transient Combustible</b>	
Combustible materials placed in a temporary location.	In a fire QRVA, a transient combustible is one of many potential ignition sources. As discussed in NUREG/CR-6850, transient combustibles “are usually associated with (but not limited to) maintenance or modifications involving combustible and flammable liquids, wood and plastic products, waste, scrap, rags, or other combustibles resulting from the work activity.”  The definition provided was based on the definition in NUREG/CR-6850.

**Table D-2. Internal Fire Terms and Definitions (Continued)**

Term and Definition(s)	Discussion
<b>Upper Layer</b>	
<p>The volume under the ceiling of a fire enclosure where smoke accumulates and high gas temperatures are observed. (see <i>Smoke Layer, Hot Gas Layer</i>)</p>	<p>Typically, a fire plume will form above a burning object. The fire plume will rise until obstructed by a horizontal surface, such as a ceiling. Upon hitting the ceiling, the hot gases in the fire plume will turn and flow along the ceiling in the form of a ceiling jet. When the ceiling jet gases are blocked by vertical surfaces, such as walls, they will accumulate into a hot gas layer or smoke layer. As more hot gas accumulates in the layer, the interface between the hot gas layer and cooler layer below will continue to drop toward the floor of the enclosure. The smoke layer is the upper zone in a two-zone model formulation.</p> <div style="text-align: center;">  <p>The diagram illustrates a cross-section of a fire enclosure. At the bottom center, a 'Flame' is shown. Above it, a 'Fire Plume' rises and spreads across the ceiling. An arrow points to the 'Ceiling Jet' where the plume meets the ceiling. The upper portion of the room is labeled as the 'Hot Gas Layer (Smoke Layer) (Upper Layer)'. The lower portion is the cooler layer.</p> </div> <p>The definition provided was based on the definition in NUREG/CR-6850.</p>
<b>Ventilation Rate</b>	
<p>Amount of air injected or extracted by a mechanical ventilation system into or from a location, respectively.</p>	<p>The ventilation rate is usually measured in cubic meters per second (m<sup>3</sup>/sec).</p>



**Table D-2. Internal Fire Terms and Definitions (Continued) -**

<b>Term and Definition(s)</b>	<b>Discussion</b>
<b>Zone Model</b>	
A type of fire model that provides a method for calculating fire environment conditions in control volumes, or zones, within a space by applying conservation equations and the ideal gas law.	<p>The fundamental idea behind a zone model is that each zone is well-mixed and that all fire environment variables (e.g., temperature, smoke concentration), therefore, are uniform throughout the zone. The variables in each zone change as a function of time and rely on the initial conditions that the user specifies. It is assumed that there is a well-defined boundary separating the two zones, though this boundary may move up or down throughout the simulation.</p> <p>Zone models can easily analyze conditions resulting from fires involving single compartments or compartments with adjacent spaces, and they are often used to compute the hot gas layer temperature, hot gas layer composition, and target heat fluxes. Zone models also are capable of modeling some effects of natural and mechanical ventilation in both horizontal and vertical directions. Smoke production, fire plume dynamics, ceiling jet characteristics, heat transfer, and ventilation flows are all algebraic models embedded within zone models.</p> <p>The definition provided was based on the definition in NUREG-1934.</p>
<b>Zone of Influence</b>	
That vicinity of the fire in which fire damage or fire spread to secondary combustibles is possible.	<p>Fire damage or spread may require some time to occur. The zone of influence is associated with the potential for fire damage or fire spread, regardless of the time available. Zone of influence generally does not encompass hot gas layer effects; instead, it focuses on direct radiant heating, plume, and ceiling jet effects.</p> <p>Typically a component is not damaged initially in the fire scenario if it is outside the zone of influence for an ignition source.</p>

### D.3. QRVA Technical Elements

Table D-3 provides the technical elements as defined in the ASME PRA Standard for Level 1, Level 2 and Level 3 QRVA with the associated discussion. The technical elements are listed alphabetically by level of the QRVA and hazard groups.

**Table D-3. QRVA Technical Elements**

Technical Element	Discussion
<b>Level 1 Internal Events</b>	
<b>Accident Sequence Analysis</b>	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.
<b>Data Analysis</b>	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.
<b>Human Reliability Analysis</b>	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.
<b>Initiating Event Analysis</b>	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.
<b>AFRF Analysis</b>	The term acute fuel release frequency (AFRF) analysis is a technical element of Part 2 of the ASME/ANS "Combined Standard: Requirements for Internal Events At-Power PRA." 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.
<b>Quantification</b>	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.
<b>Success Criteria</b>	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.
<b>Systems Analysis</b>	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 D-3. QRVA Technical Elements (Continued) -**

Technical Element	Discussion
<b>Level 1 Internal Flood At-Power</b>	
<b>Internal Flood Accident Sequences and Quantification</b>	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.
<b>Internal Flood Facility Partitioning</b>	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.
<b>Internal Flood Scenarios</b>	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.
<b>Internal Flood Source Identification and Characterization</b>	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.
<b>Internal Flood-Induced Initiating Events</b>	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 at power QRVA that is reasonably representative of this response is selected for each scenario.
<b>Internal Fire At-Power</b>	
<b>Circuit Failure Analysis</b>	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.
<b>Fire Ignition Frequency</b>	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).
<b>Fire QRVA Cable Selection</b>	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.
<b>Fire QRVA Equipment Selection</b>	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 D-3. QRVA Technical Elements (Continued) -**

<b>Technical Element</b>	<b>Discussion</b>
<b>Fire QRVA Facility Response Model</b>	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.
<b>Fire Risk Quantification</b>	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.
<b>Fire Scenario Selection and Analysis</b>	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.
<b>Facility Boundary Definition and Partitioning</b>	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.
<b>Post-Fire Human Reliability Analysis</b>	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 safe shutdown, including those called out in the relevant facility fire response procedures.
<b>Qualitative Screening</b>	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
<b>Quantitative Screening</b>	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.
<b>Seismic/Fire Interactions</b>	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.
<b>Uncertainty and Sensitivity Analyses</b>	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 D-3. QRVA Technical Elements (Continued) -**

Technical Element	Discussion
<b>Seismic Events</b>	
<b>Probabilistic Seismic Hazard Analysis</b>	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.
<b>Seismic Fragility Analysis</b>	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.
<b>Seismic Facility Response Analysis</b>	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, at-power QRVA model to incorporate those aspects that are different, because of the seismic hazard's effects, from the corresponding aspects of the at-power, internal events model.
<b>High Winds</b>	
<b>High Wind Fragility Analysis</b>	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.
<b>High Wind Facility Response Analysis</b>	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 at-power 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.
<b>High Winds Hazard Analysis</b>	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.
<b>External Floods</b>	
<b>External Flood Fragility Analysis</b>	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 D-3. QRVA Technical Elements (Continued) -**

<b>Technical Element</b>	<b>Discussion</b>
<b>External Flood Hazard Analysis</b>	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.
<b>External Flood Facility Response Model and Quantification</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• develop an external flood facility response model by modifying the internal events at-power QRVA model to include the effects of the external flood in terms of initiating events and failures caused;</li> <li>• quantify this model to provide the CLOFICP and conditional acute fuel release probability (CAFRP) for each defined external flood facility damage state;</li> <li>• 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.</li> </ul>
<b>Other External Hazards</b>	
<b>External Hazard Analysis</b>	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.
<b>External Hazard Fragility Evaluation/Analysis</b>	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.
<b>External Hazard Facility Response Model/Analysis</b>	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, at-power QRVA model to incorporate those aspects that are different, because of the external hazard's effects, from the corresponding aspects of the at-power, internal events model.
<b>Level 2</b>	
<b>Containment Capacity Analysis</b>	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 containment to withstand challenges.



**Table D-3. QRVA Technical Elements (Continued) -**

<b>Technical Element</b>	<b>Discussion</b>
<b>Interface between a Level 2 and Level 3 QRVA</b>	The term interface between Level 2 and Level 3 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 analysis is communicated, and to assure that all information required for the Level 3 analysis is provided in suitable form.
<b>Level 1–2 Interface</b>	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).
<b>Probabilistic Treatment of Event Progression and Source Terms</b>	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.
<b>Radiological Source Term Analysis</b>	The term radiological 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 radiological 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.
<b>Severe Accident Progression Analysis</b>	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 fission product release to the environment, and generating quantitative estimates of radioactive material release to the environment for accident sequences identified as contributors to the frequency of release.

**Table D-3. QRVA Technical Elements (Continued) -**

Technical Element	Discussion
<b>Level 3 QRVA</b>	
<b>Atmospheric Transport and Diffusion</b>	<p>The term atmospheric transport and diffusion is a technical element of a Level 3 QRVA that refers to the process by which material that has been released from containment, moves through and spreads upon release to the atmosphere. The objective of ATD is to model the transport of radioactive material as it travels for many hours in the atmosphere under the meteorological conditions prevailing at and beyond the site that can change in both space and time. ATD 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 and atmospheric stability.</p> <p>Probabilistic consequence modeling codes typically include sampling of meteorological data from a site-specific annual data base of hourly weather data to determine appropriately weighted scenarios of plume transport under different weather conditions to provide probabilistic results, model ATD for accident- and site-specific input parameters, accommodate temporal and spatial changes in meteorological conditions, calculate wet and dry deposition of particulate and halogen radionuclides, and document algorithms, assumptions, limitations, and uncertainties.</p>
<b>Dosimetry</b>	<p>The term dosimetry is a technical element in a Level 3 QRVA whose objectives are to determine dose by including all applicable dose pathways such as cloudshine, groundshine, skin deposition, inhalation and ingestion; apply the effect of mitigation actions such as shielding; apply recognized dose conversion factors; and document assumptions, limitation and uncertainties associated with dosimetry.</p>
<b>Economic Factors</b>	<p>The term economic factor is a technical element in a Level 3 QRVA whose objective is to determine the economic impacts of the release on the surrounding land and the population.</p>
<b>Meteorological Data</b>	<p>The term meteorological data is a technical element of a Level 3 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.</p>
<b>Protective Action Parameters and Other Site Data</b>	<p>The term protective action parameters and other site data is a technical element in a Level 3 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.</p>
<b>Quantification and Reporting</b>	<p>The term quantification and reporting is a technical element of a Level 3 QRVA whose objectives are to ensure that the Level 3 model executes properly, proves appropriate results, and is documented in a manner that facilitates risk assessments, QRVA applications, upgrades and peer reviews.</p>



**Table D-3. QRVA Technical Elements (Continued) -**

<b>Technical Element</b>	<b>Discussion</b>
<b>Risk Integration</b>	The term risk integration is a technical element of a Level 3 QRVA whose objective is to combine the Level 3 analyses with the results from the Level 1–2 analyses to obtain a characterization of the overall risk, including uncertainty.
<b>Transition from the Radionuclide (Radioactive Material) Release to Level 3</b>	The term transition from radioactive material release to Level 3 is a technical element of a Level 3 QRVA whose objectives are to provide clear traceability of the release category quantification back to the radioactive material release analysis, to ensure that initiating event information that could affect the Level 3 analysis is communicated, and to ensure that all information required for the Level 3 analysis is provided in suitable form.

DRAFT

## E. List of Acronyms

---

Table E-1 presents the acronyms used in this document.

**Table E-1. List of Acronyms**

<b>Acronym</b>	<b>Term</b>
AFRF	acute fuel release frequency
AFW	auxiliary feedwater
ANS	American Nuclear Society
AOC	administrative order on consent
AOO	anticipated operational occurrences
APET	accident progression event tree
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
ASTM	American Society of Testing and Materials
ATD	atmospheric transport and diffusion
BAPT	best available practicable technology
BDBA	beyond-design-basis accidents
BDBE	beyond-design-basis events
BFR	binomial failure rate
BWR	boiling water reactor
CAFRP	conditional acute fuel release probability
CCF	common cause failure
CCW	component cooling water
CD	complete dependence
CEDE	committed effective dose equivalent
CET	containment event tree
CLB	current licensing basis
CLOFICP	conditional loss of fuel inventory control probability
CMF	common-mode failure
CRS	cable and raceway database system



**Table E-1. List of Acronyms (Continued) -**

<b>Acronym</b>	<b>Term</b>
DBA	design-basis accident
DBD	design basis documentation
DBE	design-basis event
DCH	direct containment heating
DI	dependence importance
DLA	defense logistics agency
ECCS	emergency core cooling system
EDG	emergency diesel generator
EOP	emergency operating procedure
EP	emergency preparedness
EPRI	Electric Power Research Institute
ESD	event sequence diagrams
F-76	marine diesel
FEDB	Fire Events Database
FEP	fire emergency procedure
FMEA	failure modes and effects analysis
FOS	facility operating states
FQRVA	fire QRVA
FTR	fails to run
FTS	fails to start
GL	generic letter
HADA	human action dependency analysis
HD	high dependence
HCLPF	high confidence in low probability of failure
HEP	human error probability
HFE	human failure event
HPME	high-pressure melt ejection
HRA	human reliability analysis

**Table E-1. List of Acronyms (Continued) -**

<b>Acronym</b>	<b>Term</b>
HRR	heat release rate
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
IAFRP	incremental acute fuel release probability
IPEEE	individual plant examinations for external events
ISLOCA	Interfacing systems loss of coolant accident
JP-5	jet propulsion fuel no. 5
JP-8	jet propulsion fuel no.8
LBE	licensing-basis event
LD	low dependence
LLOCA	large LOCA
LOCA	Loss of coolant accidents
LOFICF	loss of fuel inventory control frequency
LOFICP	incremental loss of fuel inventory control probability
LOIA	loss of inventory accidents
LOOP	loss of offsite power
LWR	light-water reactors
MCR	main control room
MD	medium dependence
MFF	master frequency file
MGL	multiple Greek letter
MLD	master logic diagram
MLE	maximum-likelihood estimate
MLOCA	medium LOCA
NAVFAC	naval facilities engineering command
ND	navy distillate
NRC	U.S. Nuclear Regulatory Commission
NTP	notification to proceed



**Table E-1. List of Acronyms (Continued) -**

<b>Acronym</b>	<b>Term</b>
OBE	operating-basis earthquake
P&ID	pipng and instrument diagrams
PDB	plant damage bin
PM	project manager
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSD	partial system description
PSF	performance shaping factor
PWR	pressurized water reactor
QHO	quantitative health objectives
QRVA	quantitative risk and vulnerability assessment
RA	risk achievement
RCS	reactor coolant system
RCP	reactor coolant pumps
RHFSF	Red Hill Bulk Fuel Storage Facility
RG	Regulatory Guide
SBO	station blackout
SDM	system dependency matrix
s.e.	standard errors
SGTR	steam generator tube ruptures
SLOCA	small LOCA
SOKC	state-of-knowledge correlation
SQRVA	seismic QRVA
SSC	structure, system, or component
SSE	safe-shutdown earthquake
TEDE	total effective dose equivalent
THERP	Technique for Human Error Rate Prediction
UFM	unplanned fuel movement

**Table E-1. List of Acronyms (Continued) -**

<b>Acronym</b>	<b>Term</b>
UST	underground storage tanks
WBS	work breakdown structure
ZD	zero dependence
ZOI	zone of influence

**DRAFT**



Table E-2 presents additional useful QRVA abbreviations and acronyms.

**Table E-2. Additional Useful Abbreviations and Acronyms**

Acronym	Term
ACRS	Advisory Committee on Reactor Safeguards
ANS	American Nuclear Society
APET	accident progression event tree
ASME	(formerly) American Society of Mechanical Engineers
ATWS	anticipated transient without scram
BE	basic event
CCDF	complementary cumulative distribution function
CD	core damage
CM	core melt
CMF	common-mode failure core-melt frequency
CRM	configuration risk management
CY	calendar year
DCF	dose conversion factor
EAB	exclusion area boundary
ET	event tree
F&B	feed and bleed (bleed and feed)
FM	failure mode
FT	fault tree
HLR	high-level requirement
IM	importance measure
LOOP	loss of offsite power
NEI	Nuclear Energy Institute
OG	owners group
QA	quality assurance
QRA	quantitative risk assessment
QRVA	quantitative risk and vulnerability assessment
RAW	risk achievement worth

**Table E-2. Additional Useful Abbreviations and Acronyms (Continued) -**

<b>Acronym</b>	<b>Term</b>
RIDM	risk-informed decision making
RY	reactor-year
SA	systems analysis
SB, SBO	station blackout
SM	seismic margin
SOKC	state-of-knowledge correlation
SR	supporting requirement
ST	source term
VA	vulnerability assessment

**DRAFT**