

QA: NA

TDR-MGR-RL-000002 REV 00

February 2002

Preclosure Safety Analysis Guide



Prepared for:
U.S. Department of Energy
Yucca Mountain Site Characterization Office
P.O. Box 30307
North Las Vegas, Nevada 89036-0307

Prepared by:
Bechtel SAIC Company, LLC
1180 Town Center Drive
Las Vegas, Nevada 89144

Under Contract Number
DE-AC08-01NV12101

**PRELIMINARY DRAFT
INFORMATION ONLY**

L/m-70

DRAFT DISCLAIMER

This contractor document was prepared for the U.S. Department of Energy (DOE), but has not undergone programmatic, policy, or publication review, and is provided for information only. The document provides preliminary information that may change based on new information or analysis, and is not intended for publication or wide distribution; it is a lower level contractor document that may or may not directly contribute to a published DOE report. Although this document has undergone technical reviews at the contractor organization, it has not undergone a DOE policy review. Therefore, the views and opinions of authors expressed do not necessarily state or reflect those of the DOE. However, in the interest of the rapid transfer of information, we are providing this document for your information, per your request.

QA: NA

TDR-MGR-RL-000002 REV 00

February 2002

Preclosure Safety Analysis Guide

Prepared for:
U.S. Department of Energy
Yucca Mountain Site Characterization Office
P.O. Box 30307
North Las Vegas, Nevada 89036-0307

Prepared by:
Bechtel SAIC Company, LLC
1180 Town Center Drive
Las Vegas, Nevada 89144

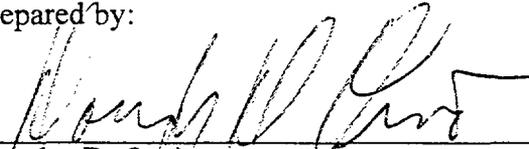
Under Contract Number
DE-AC08-01NV12101

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Preclosure Safety Analysis Guide

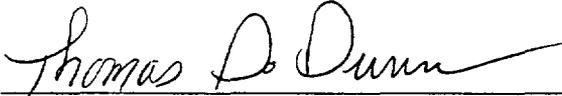
Prepared by:



Douglas D. Orvis
Preclosure Safety Analysis

2/27/2002
Date

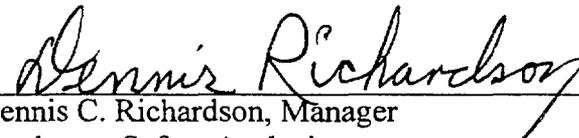
Reviewed by



Thomas D. Dunn
Preclosure Safety Analysis

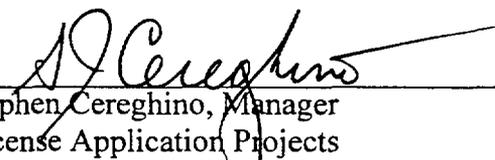
2/27/2002
Date

Approved by:



Dennis C. Richardson, Manager
Preclosure Safety Analysis

2/27/2002
Date



Stephen Cereghino, Manager
License Application Projects

2/27/2002
Date

ACKNOWLEDGEMENTS

The contributions of the following team members is hereby acknowledged:

Douglas A. Bownson, Robert J. Garrett, Dealis W. Gwyn, Richard P. Morissette,
Daniel A. Thomas, Sen-Sung Tsai, and Jo A. Ziegler

CONTENTS

	Page
1. INTRODUCTION AND OVERVIEW	1-1
1.1 PURPOSE	1-1
1.2 SCOPE.....	1-2
1.3 REFERENCES.....	1-3
1.3.1 Documents Cited	1-3
1.3.2 Codes, Standards, Regulations, and Procedures.....	1-3
2. REGULATORY REQUIREMENTS.....	2-1
3. PRECLOSURE SAFETY STRATEGY	3-1
3.1 INTRODUCTION.....	3-1
3.2 GENERAL PRINCIPLES.....	3-1
3.3 PRECLOSURE SAFETY CASE	3-1
3.3.1 Preclosure Safety Analysis.....	3-2
3.3.2 Margin and Defense-in-Depth.....	3-2
3.3.3 Consequence Analysis of Very Low Probability Events and Event Sequences	3-3
3.3.4 Nuclear Industry Precedent and Experience.....	3-4
3.3.5 Evaluation Approach.....	3-5
3.3.6 Conservative or Bounding Approaches.....	3-5
3.3.7 Preferred Approach	3-5
3.3.8 Retrievability	3-6
3.3.9 License Specifications and Surveillances.....	3-6
3.3.10 Preclosure Testing	3-7
3.4 STRATEGY FOR PREVENTING OR MITIGATING PRECLOSURE OFFSITE RADIATION EXPOSURE	3-7
3.4.1 Identification of Important-to-Safety Features and Controls	3-7
3.4.2 Design Bases for Facilities and Limits on Operations	3-8
3.4.3 Safety Strategy for Repository Preclosure Operational Functions.....	3-8
3.5 REFERENCES.....	3-9
3.5.1 Documents Cited	3-9
3.5.2 Codes, Standards, Regulations, and Procedures.....	3-9
4. OVERVIEW OF PRECLOSURE SAFETY ANALYSIS ELEMENTS AND APPROACHES	4-1
4.1 INTRODUCTION.....	4-1
4.2 BACKGROUND.....	4-1
4.3 OVERVIEW OF PROCESS FOR PERFORMING A PRECLOSURE SAFETY ANALYSIS	4-2
4.3.1 Flow Diagram of Preclosure Safety Analysis Process	4-3
4.4 DEVELOPING AND DOCUMENTING THE PRECLOSURE SAFETY ANALYSIS IN THE LICENSE APPLICATION.....	4-9

CONTENTS (Continued)

	Page
4.4.1 Level of Design Detail in the License Application for Construction Authorization.....	4-9
4.4.2 Information Base for Preclosure Safety Analysis in Support of License Application for Construction Authorization.....	4-9
4.4.3 Preclosure Safety Analysis Based on Level of Design Detail Available at Time of License Application.....	4-11
4.5 ENSURING PERFORMANCE OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY.....	4-12
4.6 REFERENCES.....	4-15
4.6.1 Documents Cited.....	4-15
4.6.2 Codes, Standards, Regulations, and Procedures.....	4-15
5. DESCRIPTION OF SITE, FACILITIES, AND OPERATIONS.....	5-1
5.1 INTRODUCTION.....	5-1
5.2 OVERVIEW OF APPROACH.....	5-1
5.3 REFERENCES.....	5-2
5.3.1 Documents Cited.....	5-2
5.3.2 Codes, Standards, Regulations, and Procedures.....	5-2
6. HAZARDS ANALYSIS.....	6-1
6.1 EXTERNAL EVENTS HAZARDS ANALYSIS.....	6-1
6.1.1 Introduction.....	6-1
6.1.2 Overview of Approach.....	6-1
6.1.3 Details of Basic Approach to Screening with Examples.....	6-3
6.2 INTERNAL EVENTS HAZARDS ANALYSIS.....	6-20
6.2.1 Introduction.....	6-20
6.2.2 Overview of Basic Approach.....	6-21
6.2.3 Approach for Evaluating Applicability of Generic Internal Events to Repository Functional Areas.....	6-22
6.2.4 Examples of Evaluating the Applicability of Generic Events to Repository Function Areas.....	6-27
6.2.5 Internal Events Hazards List.....	6-36
6.3 REFERENCES.....	6-37
6.3.1 Documents Cited.....	6-37
6.3.2 Codes, Standards, Regulations, and Procedures.....	6-38
APPENDIX 6A BIBLIOGRAPHY FOR DOCUMENTS POTENTIALLY RELEVANT TO EXTERNAL EVENTS HAZARDS ANALYSIS.....	6A-1

CONTENTS (Continued)

	Page
7. EVENT SEQUENCE (DESIGN BASIS EVENT) FREQUENCY ANALYSIS	7-1
7.1 EVENT TREE ANALYSIS	7-1
7.1.1 Purpose	7-1
7.1.2 Scope	7-1
7.1.3 Overview of Approach	7-1
7.1.4 Details of Approach	7-8
7.1.5 Examples of Applications of Event Tree Analysis	7-16
7.2 FAULT TREE ANALYSIS	7-28
7.2.1 Introduction	7-28
7.2.2 Overview of Approach	7-28
7.2.3 Details of Approach	7-31
7.2.4 Examples of Application	7-45
7.3 HUMAN RELIABILITY ANALYSIS	7-52
7.3.1 Purpose	7-52
7.3.2 Scope	7-52
7.3.3 Overview of Approach	7-52
7.3.4 Details of Approach	7-53
7.3.5 Examples	7-74
7.4 COMMON-CAUSE AND DEPENDENT FAILURES ANALYSIS	7-75
7.4.1 Purpose	7-75
7.4.2 Scope	7-75
7.4.3 Overview of Approach	7-75
7.4.4 Details of Approach	7-81
7.4.5 Steps in Performing Dependent Failure Analysis for a Repository	7-92
7.4.6 Examples of Application	7-95
7.5 TECHNICAL INFORMATION	7-99
7.5.1 Introduction	7-99
7.5.2 Overview of Approach	7-99
7.5.3 Details of Approach	7-101
7.6 EVENT SEQUENCE FREQUENCY BINNING	7-135
7.6.1 Purpose	7-135
7.6.2 Scope	7-135
7.6.3 Overview of Approach	7-135
7.6.4 Details of Approach	7-136
7.6.5 Examples of Application	7-138
7.7 REFERENCES	7-139
7.7.1 Documents Cited	7-139
7.7.2 Codes, Standards, Regulations, and Procedures	7-141
APPENDIX 7A - BIBLIOGRAPHY OF INFORMATION SOURCES	7A-1

CONTENTS (Continued)

	Page
8. CONSEQUENCE ANALYSIS	8-1
8.1 INTRODUCTION.....	8-1
8.2 EXAMPLES OF SOURCE TERMS.....	8-2
8.2.1 Source Terms for Commercial Spent Nuclear Fuel and Crud.....	8-2
8.2.2 Source Terms for U.S. Department of Energy Spent Nuclear Fuel	8-6
8.2.3 Source Terms for Vitrified High-Level Radioactive Waste.....	8-7
8.2.4 Source Terms for Plutonium Disposition Waste Form	8-7
8.3 CATEGORY 1 OFFSITE DOSES.....	8-7
8.3.1 GENII-S Dose Calculation Methodology	8-7
8.3.2 Dose Conversion Factors.....	8-9
8.3.3 Atmospheric Dispersion Factors	8-10
8.3.4 Breathing Rate.....	8-10
8.3.5 Category 1 Event Sequences	8-11
8.3.6 Uncertainty in Consequence Analysis.....	8-11
8.3.7 Category 1 Dose Calculation Examples.....	8-11
8.4 CATEGORY 2 OFFSITE DOSES.....	8-16
8.4.1 Category 2 Event Dose Calculation Methodology.....	8-17
8.4.2 Dose Conversion Factors.....	8-19
8.4.3 Atmospheric Dispersion Factors	8-19
8.4.4 Breathing Rate.....	8-20
8.4.5 Category 2 Event Sequences	8-20
8.4.6 Uncertainty in Consequence Analysis.....	8-20
8.4.7 Category 2 Dose Calculation Example	8-21
8.5 CATEGORY 1 WORKER DOSES AND EXPOSURES.....	8-24
8.6 RELEASE FRACTIONS	8-25
8.6.1 Commercial Spent Nuclear Fuel Release Fractions	8-25
8.6.2 U.S. Department of Energy Spent Nuclear Fuel Release Fractions	8-26
8.7 MITIGATION FACTOR	8-26
8.8 REFERENCES.....	8-27
8.8.1 Documents Cited	8-27
8.8.2 Codes, Standards, Regulations, and Procedures.....	8-29
8.8.3 Source Data	8-29
9. UNCERTAINTY AND SENSITIVITY ANALYSIS, GENERAL CONCEPTS, AND METHODS	9-1
9.1 INTRODUCTION.....	9-1
9.2 OVERVIEW OF APPROACH.....	9-1
9.3 DETAILS OF APPROACH.....	9-2
9.3.1 Background	9-2
9.3.2 Identifying Sources of Uncertainty in Models and Input Information.....	9-4
9.3.3 Representing Uncertainties in Input and Output Variables.....	9-6
9.3.4 Propagating Uncertainties in Frequency and Consequence Analyses.....	9-10

CONTENTS (Continued)

	Page	
9.3.5	Uncertainty Analysis versus Sensitivity Analysis.....	9-12
9.3.6	Importance Measures Analysis	9-13
9.3.7	Examples of Uncertainty Analyses	9-14
9.4	REFERENCES	9-14
9.4.1	Documents Cited	9-14
9.4.2	Codes, Standards, Regulations, and Procedures.....	9-15
10.	EXTERNAL EVENTS	10-1
10.1	SEISMIC ANALYSIS	10-1
10.1.1	Introduction	10-1
10.1.2	Overview of Approach	10-1
10.1.3	Details of Approach.....	10-4
10.1.4	Examples of Application of Seismic Analyses	10-6
10.1.5	Development and Application of Seismic Event Trees.....	10-8
10.1.6	Frequency Quantification of Seismic Sequences Using Deterministic, Step-Function Fragility Functions or Seismic Margins Analysis	10-19
10.1.7	Frequency Quantification of Seismic Sequences Using Fragility Functions or Seismic Margins Analysis.....	10-20
10.2	FLOODING.....	10-28
10.2.1	Purpose	10-28
10.2.2	Scope	10-28
10.2.3	Overview of Approach	10-28
10.2.4	Details of Approach.....	10-28
10.2.5	Flooding Protection Requirements.....	10-31
10.2.6	Consequence Analysis.....	10-31
10.3	WINDS and TORNADOS	10-32
10.3.1	Purpose	10-32
10.3.2	Scope	10-32
10.3.3	Overview of Approach	10-32
10.3.4	Details of Approach.....	10-32
10.3.5	Wind and Tornado Protection Requirements	10-36
10.3.6	Consequence Analysis.....	10-36
10.4	LIGHTNING AND EXTREME WEATHER.....	10-37
10.5	WILDLAND FIRES.....	10-37
10.6	OTHER EXTERNAL EVENTS	10-38
10.6.1	Loss-of-Offsite Power	10-38
10.6.2	Aircraft	10-38
10.6.3	Military and Industrial Hazards.....	10-43
10.7	REFERENCES	10-49
10.7.1	Documents Cited	10-49
10.7.2	Codes, Standards, Regulations, and Procedures.....	10-51
10.7.3	Source Data	10-52

CONTENTS (Continued)

	Page
11. CRITICALITY	11-1
11.1 INTRODUCTION.....	11-1
11.2 REGULATORY REQUIREMENTS	11-1
11.3 REPOSITORY PRECLOSURE CRITICALITY SAFETY STRATEGY	11-1
11.4 CRITICALITY RISK ANALYSIS PROCESS.....	11-1
11.4.1 Identify the Systems, Structures, Components and Processes Associated with Criticality Hazards.....	11-6
11.4.2 Identify Those Waste Forms That Have the Potential to Achieve Criticality.....	11-6
11.4.3 Develop Criticality Event Trees.....	11-7
11.4.4 Quantify the Criticality Event Trees.....	11-9
11.4.5 Perform Criticality Analysis to Determine k_{eff}	11-9
11.4.6 Perform Criticality Consequence Analyses.....	11-9
11.4.7 Document the Results.....	11-10
11.5 REFERENCES.....	11-10
11.5.1 Documents Cited	11-10
11.5.2 Codes, Standards, Regulations, and Procedures.....	11-10
12. QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY.....	12-1
12.1 INTRODUCTION.....	12-1
12.2 SUMMARY OF THE PRECLOSURE SAFETY ANALYSIS PROCESS.....	12-2
12.3 DEVELOPMENT OF A RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION PROCESS	12-5
12.4 QUALITY ASSURANCE CLASSIFICATION PROCESS.....	12-12
12.5 FUNCTIONAL FAILURE ANALYSIS IN RISK INFORMED QUALITY ASSURANCE CLASSIFICATION.....	12-12
12.6 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 1 EVENT SEQUENCES	12-13
12.7 COMPLIANCE DEMONSTRATION FOR NORMAL OPERATION RELEASES AND CATEGORY 1 EVENT SEQUENCES.....	12-14
12.8 PROCESS FOR RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IN CATEGORY 1 EVENT SEQUENCES.....	12-15
12.9 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 2 EVENT SEQUENCES	12-16
12.10 REFERENCES.....	12-19
12.10.1 Documents Cited	12-19
12.10.2 Codes, Standards, Regulations, and Procedures.....	12-19

CONTENTS (Continued)

	Page
13. SELECTION OF 10 CFR 63.2 DESIGN BASES FOR STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY	13-1
13.1 INTRODUCTION.....	13-1
13.2 BACKGROUND INFORMATION.....	13-1
13.3 METHOD FOR DEVELOPING 10 CFR 63.2 DESIGN BASES	13-3
13.4 EXAMPLES.....	13-5
13.5 REFERENCES.....	13-6
13.5.1 Documents Cited	13-6
13.5.2 Codes, Standards, Regulations, and Procedures.....	13-6
14. DOCUMENTATION AND PREPARATION OF LICENSE APPLICATION	14-1
14.1 PRECLOSURE SAFETY ANALYSIS DOCUMENTATION.....	14-1
14.1.1 Internal and External Hazards Analyses.....	14-1
14.1.2 Categorization of Event Frequencies.....	14-1
14.1.3 Consequence Analysis.....	14-2
14.1.4 Preclosure Safety Analysis.....	14-2
14.1.5 Identify Structures, Systems, and Components to Prevent or Mitigate Event.....	14-3
14.2 PRECLOSURE SAFETY ANALYSIS AND LICENSE APPLICATION SUBMITTAL	14-4
14.3 REFERENCES.....	14-4
14.3.1 Documents Cited	14-4
14.3.2 Codes, Standards, Regulations, and Procedures.....	14-4
GLOSSARY	Glossary-1

FIGURES

	Page
3-1	Margin For Dose Compliance..... 3-3
4-1	Preclosure Safety Analysis 4-4
4-2	Process for Preclosure Safety Analysis Using Available Level of Design Detail 4-14
7-1	Example of a Fork Style Event Tree for a Hypothetical Waste Handling System 7-3
7-2	Example of a Stair-Step Style Event Tree for a Hypothetical Waste Handling System..... 7-5
7-3	Step in Event Tree Construction 7-10
7-4	Event Tree for Hypothetical Uncontrolled Descent Due to Random-Failure Initiator..... 7-17
7-5	Simplified Event Tree for Hypothetical Uncontrolled Descent (First Example) 7-24
7-6	Simplified Event Tree for Hypothetical Uncontrolled Descent (Second Example) 7-25
7-7	Event Tree for Hypothetical Fire Initiated Uncontrolled Descent..... 7-26
7-8	Event Tree for Hypothetical Human Error Initiated Uncontrolled Descent 7-29
7-9	Standard Fault-Tree Symbols 7-33
7-10	Illustration of Fault Tree Development..... 7-40
7-11	Pressure Tank System 7-46
7-12	Fault Tree Example for Pressure Tank Rupture 7-49
7-13	Simplified Fault Tree for Pressure Tank Example 7-51
7-14	Example of Fault Tree Containing Type A Human Actions 7-57
7-15	Example of Fault Tree Containing Type B Human Actions..... 7-58
7-16	Example of Event Tree with Type C Human Action in Event Headings 7-59
7-17	Operator Action Tree: A Generalized Representation of Type C HAs 7-70
7-18	Example of Human Reliability Analysis Tree..... 7-73
7-19	Physical Elements of Dependent Events..... 7-81
7-20A	Baseline Event Tree Without CCFs..... 7-85
7-20B	Event Tree with Fire-Initiated Common-Cause Failure of a Heating, Ventilation, and Air-Conditioning, and High-Efficiency Particulate Air Filter System. 7-85
7-21	Illustration of Logic Models for Independent Failures 7-90
7-22	Illustration of Logic Models for Common Cause Failures 7-91
7-23	Exponential Probability of Failure..... 7-104
7-24	Unavailability with Inspection and Test 7-105
7-25	Probability of Restoration – Exponential Repair Model..... 7-106
10-1	Event Sequence Diagram for Internal Initiated Drop Event..... 10-12
10-2	Event Sequence Diagram for Seismic Initiated Drop Event..... 10-13
10-3	Event Sequence Diagram for Fire Initiated Drop Event..... 10-14
10-4	Event Sequence Diagram for Seismic & Fire Initiated Drop Event 10-14
10-5	Baseline Seismic Event Tree for Load Drop 10-15
10-6	Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake..... 10-21

FIGURES (Continued)

	Page
10-7 Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake, but Earthquake greater than Frequency Category 1	10-22
10-8 Example Fragility Curves	10-24
11-1 Criticality Risk Analysis Flow Chart	11-3
12-1 Preclosure Safety Analysis	12-3
12-2 Compliance or Acceptable Risk Region Based on 10 CFR Part 63	12-8
12-3 Example Quality Assurance Classification Risk Regions Developed from 10 CFR Part 63 Performance Objectives	12-10
12-4 Risk Informed Quality Assurance Classification Process	12-13
12-5 Example of the Quality Assurance Classification Process for a Category 2 Event Sequence	12-19
13-1 Relationship of Repository Design Bases to 10 CFR 63.2 Design Bases and the Safety Analysis Report (SAR)	13-2
13-2 Basic Steps in Developing 10 CFR 63.2 Design Bases	13-5

TABLES

	Page
3-1 Preclosure Safety Strategy	3-8
4-1 Sample Approach for Demonstrating Compliance with 10 CFR 63.112(e).....	4-13
6-1 Generic External Events	6-4
6-2 Example Summary of External Events Hazards Analysis Screening	6-11
6-3 Example External Events Hazards List.....	6-12
6-4 Example External Events Hazards Screened Out	6-12
7-1 Example of Task Analysis	7-62
7-2 Example Probabilities of Errors of Commission in Operating Manual Controls	7-68
7-3 Types of Dependent Events Based on their Impact on Preclosure Safety of a Repository	7-78
7-4 A Guide to Unreliability of Various System Arrangements with Consideration of Dependent Failures	7-82
7-5 Generic Beta Factors	7-96
7-6 Sources of Facility-Specific and Operations-Specific Experience Information	7-102
7-7 Example of Generic Component Failure Rates Database	7-115
7-8 Crane Failure Demand Rates	7-133
8-1 Dose Criteria for Category 1 and Category 2 Event Sequences	8-2
8-2 Example of Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) Spent Nuclear Fuel (SNF) Radionuclide Inventories.....	8-3
8-3 Example of Category 1 Crud Source Term Calculations.....	8-6
8-4 Example of High-Level Radioactive Waste Activity (Curies Per Canister).....	8-8
8-5 Example of Annual Releases from the Subsurface Due to Normal Operations	8-12
8-6 Example of Calculating Annualized Cesium-137 Release for Category 1 Event Sequences.....	8-13
8-7 Example of Source Terms for GENII-S Computer Runs	8-14
8-8 Inhalation Dose Calculation Example	8-22
8-9 Submersion Dose Calculation Example.....	8-23
8-10 Example of Dose Summary Table	8-23
8-11 Example of CSNF Release Fractions in Air for Category 2 Event Sequences.....	8-26
9-1 Properties of the Mean of a Lognormal Distribution.....	9-10
10-1 Examples of Seismic Consequences of Roof Collapse onto Waste Forms (Hypothetical System)	10-9
10-2 Example Seismic Calculations for Seismic Failure in Hypothetical Assembly Transfer System	10-10
10-3 Example Seismic Classification of Structures, Systems, and Components for Hypothetical Assembly Transfer System.....	10-11
10-4 Example Maximum Estimated and Observed Wind Speeds near Yucca Mountain, Nevada	10-33

TABLES (Continued)

	Page
10-5 Design Basis Tornado Characteristics	10-34
10-6 Tornado Wind Speed (miles per hour) by Region	10-34
10-7 Example Tornado Wind Speed for 5-Degree Latitude and Longitude Box Containing Yucca Mountain, Nevada.....	10-35
10-8 Spectrum II Missiles	10-36
12-1 Development of a Preclosure Safety Analysis.....	12-4
12-2 Relative Risk Significance Based on 10 CFR Part 63	12-6
12-3 Updated Relative Risk Significance	12-8
12-4 Quality Levels Based on Risk Significance.....	12-9
12-5 Risk Significant Screening Criteria	12-11
12-6 Steps for Performing a Quality Assurance Classification Analysis of Structures, Systems, and Components Associated with Category 1	12-18

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACROYNMS	i
1. INTRODUCTION AND OVERVIEW	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-2
1.3 REFERENCES	1-3
1.3.1 Documents Cited	1-3
1.3.2 Codes, Standards, Regulations, and Procedures	1-3

ACRONYMS

CA	construction authorization
LA	license application
NRC	U.S. Nuclear Regulatory Commission
PSA	preclosure safety analysis
R&P	receive and possess (i.e., LA amendment to R&P high-level radioactive waste)
SSCs	structures, systems, and components
TSPA	total system performance assessment

INTENTIONALLY LEFT BLANK

1. INTRODUCTION AND OVERVIEW

A preclosure safety analysis (PSA) is a required element of the license application (LA) for a high-level radioactive waste repository. This document provides analysts and other Yucca Mountain Site Characterization Project personnel with standardized methods for developing and documenting a PSA.

A definition of the PSA is provided in 10 CFR 63.2, and more specific requirements for the PSA are provided in 10 CFR 63.112, as described in Sections 1.2 and 2.

The PSA requirements described in 10 CFR Part 63 were developed as risk-informed, performance-based regulations. These requirements must be met for the LA. The PSA addresses the safety of the geologic repository operations area for the preclosure period (i.e., the time up to permanent closure) in accordance with the radiological performance objectives of 10 CFR 63.111. Performance objectives for the repository, after permanent closure (described in 10 CFR 63.113), are not mentioned in the requirements for the PSA, and they are not considered in this guide. The methods described herein are expected to be in conformance with the review methods. The LA will be comprised of two phases: the LA for construction authorization (CA) and the LA amendment to receive and possess (R&P) waste. The PSA methods must support the safety analyses that will be based on the differing degrees of design detail in the two phases.

The methods described here combine elements of probabilistic risk assessment and deterministic analyses that comprise a risk-informed, performance-based safety analysis.

1.1 PURPOSE

The purpose of this desktop guide is to describe and standardize methods judged to be in conformance with NRC regulations and guidance for developing and documenting a PSA as part of the LA for a repository. In addition, this document provides approaches for obtaining:

- Uniformity in analyses
- Auditable analyses and databases
- A basis for training safety analysts
- Improved communications among the design and licensing groups and the U.S. Department of Energy
- A distinction in the analysis scope and approaches for the CA and R&P phases
- Preferred methods for analyzing and documenting preclosure safety.

The format of this desktop guide is flexible and sectioned to facilitate modifications. Changes may be motivated by requirements of the forthcoming NRC Yucca Mountain Review Plan, requests from the operating contractor, the U.S. Department of Energy, or the NRC.

1.2 SCOPE

This desktop guide is intended to be a complete guide for the preparation of a PSA for a repository in support of the LA. This guide provides analysts with relevant regulations, regulatory guidance, and licensing precedents, as well as instructions for performing each of the required analyses.

The document provides reference links for details and background information concerning methods and regulatory matters. The methods described are recommended for use on the Yucca Mountain Site Characterization Project. The methods generally are applicable to varying levels of design detail. Where important differences exist between analyses suitable for CA and those required for R&P, the initial issue of this document favors support of CA and may defer preparation of R&P-specific sections until needed.

The PSA is an iterative process that continues throughout the design and operational evolution of the repository design. The contents of the PSA are defined in 10 CFR 63.112(a) through (f). The analyses initially identify instances in which functions are required to prevent or to mitigate potential hazards and radiological releases. Prevention and mitigation functions are provided by SSCs important to safety that are identified and evaluated for reliability as part of the PSA process. The analyses also provide the risk-informed design bases (per 10 CFR 63.2) for developing design criteria (as described in 10 CFR 63.112(f)) that are incorporated in the project design criteria documents. The PSA supports the repository safety strategy (see Section 3) by identifying the event sequences and natural phenomena that define the design bases. In addition, the PSA demonstrates how the performance requirements of 10 CFR 63.111, the design criteria of 10 CFR 63.112(f), and the system reliability considerations of 10 CFR 63.112(e) are satisfied.

The PSA is independent and separate from the total system performance assessment (TSPA), which addresses postclosure safety. The PSA is concerned with events involving natural phenomena, active systems, and human actions that could occur within a time scale of 1 to several 100 years. The TSPA addresses events involving passive elements and natural processes that could occur over tens of thousands of years following permanent closure of the repository. Two areas of analysis have some similarity between PSA and TSPA: identifying natural phenomena hazards and calculating radiological consequences. Identifying and screening credible hazards from natural phenomena is performed in an External Events Hazards Analysis that provides input to the PSA. The TSPA has a separate procedure for identifying and screening features, events, and processes. The PSA will include a review of these features, events, and processes for their relevance as potential preclosure hazards. The PSA includes calculations of potential radiological consequences to workers and the public. Some of the methodology and biological dose conversion factors used in the PSA are similar to, or the same as, those used in the TSPA.

This guide is organized into modules; each module covers a limited range of subject matter.

- Section 1—Overview of the PSA process and the organization of this guide.

- Sections 2 through 4—Background information on regulatory requirements, the safety strategy used to define the goals of the safety analysis, and an overview of the PSA process to accomplish these goals.
- Section 5—Definition of the types of site and facility design information required as input to the PSA.
- Sections 6 through 9—Methods for performing hazards analyses, event sequence analyses, consequence analyses, and uncertainty analyses.
- Section 10—Methods for analyzing external events such as fires, earthquakes, and the loss of off-site power.
- Sections 11—Preclosure criticality.
- Sections 12 and 13—Definition of the processes for using PSA results to identify and classify SSCs important to safety in accordance with quality assurance classification methodology and to select 10 CFR 63.2 design bases for the SSCs important to safety.
- Section 14—Guidance on documenting PSA results and output of the processes described in Sections 2 through 13. This guidance includes comprehensive documentation of the analyses required to support a repository LA in accordance with the Yucca Mountain Review Plan.
- Appendix—Glossary.

1.3 REFERENCES

1.3.1 Documents Cited

None

1.3.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

INTENTIONALLY LEFT BLANK

CONTENTS

Page

2. REGULATORY REQUIREMENTS..... 2-1

INTENTIONALLY LEFT BLANK

2. REGULATORY REQUIREMENTS

[Information for this section is under development and will be provided later.]

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMS	ii
3. PRECLOSURE SAFETY STRATEGY	3-1
3.1 INTRODUCTION	3-1
3.2 GENERAL PRINCIPLES	3-1
3.3 PRECLOSURE SAFETY CASE.....	3-1
3.3.1 Preclosure Safety Analysis	3-2
3.3.2 Margin and Defense-in-Depth	3-2
3.3.3 Consequence Analysis of Very Low Probability Events and Event Sequences.....	3-3
3.3.4 Nuclear Industry Precedent and Experience	3-4
3.3.5 Evaluation Approach	3-5
3.3.6 Conservative or Bounding Approaches	3-5
3.3.7 Preferred Approach.....	3-5
3.3.8 Retrievability	3-6
3.3.9 License Specifications and Surveillances	3-6
3.3.10 Preclosure Testing.....	3-7
3.4 STRATEGY FOR PREVENTING OR MITIGATING PRECLOSURE OFFSITE RADIATION EXPOSURE.....	3-7
3.4.1 Identification of Important-to-Safety Features and Controls.....	3-7
3.4.2 Design Bases for Facilities and Limits on Operations.....	3-8
3.4.3 Safety Strategy for Repository Preclosure Operational Functions	3-8
3.5 REFERENCES	3-9
3.5.1 Documents Cited.....	3-9
3.5.2 Codes, Standards, Regulations, and Procedures	3-9

FIGURES

	Page
3-1 Margin For Dose Compliance.....	3-3

TABLES

	Page
3-1 Preclosure Safety Strategy	3-8

ACRONYMS

LA	license application
PSA	preclosure safety analysis
SNF	spent nuclear fuel
SSCs	structures, systems, and components

3. PRECLOSURE SAFETY STRATEGY

3.1 INTRODUCTION

This section describes the strategy that will be used to prevent or mitigate unacceptable preclosure radiological consequences for the high-level radioactive waste repository. The strategy focused on the offsite dose performance objectives presented in 10 CFR 63.111 and considered the preclosure activities that occur prior to the postclosure period. The strategy is a general plan that does not provide requirements for the repository.

3.2 GENERAL PRINCIPLES

When the license application (LA) is submitted, the safety case for the repository will be presented in a Safety Analysis Report. The safety case will address the logic, analyses, and calculations that describe how the repository systems, structures, and components (SSCs) meet performance objectives, and will include material incorporated by reference and other docketed material. This report will provide the basis for a U.S. Nuclear Regulatory Commission decision to authorize construction and eventually to license the repository. The preclosure safety case will be based on 10 CFR 63.2 SSC design bases (i.e., functions and controlling parameters) and the results of analyses and calculations presented in the preclosure safety analysis (PSA). The preclosure safety strategy is an approach that describes how a risk-informed design should be considered to facilitate compliance with 10 CFR Part 63 preclosure performance objectives.

3.3 PRECLOSURE SAFETY CASE

The preclosure period for evaluating event sequences will be consistent with the anticipated life of the repository. For simplicity, a 100-year preclosure period will be used in the PSA. A preclosure period of 100 years equates to a 1×10^{-2} per year event sequence probability cutoff for Category 1 event sequences, and it equates to a 1×10^{-6} per year event sequence probability cutoff for Category 2 event sequences. Using the 100-year period provides margin in evaluating event sequences for preclosure operations SSCs because the expected duration for emplacement activities is expected to be less than 50 years. The preclosure period must encompass the phases of preclosure operations preceding the time of permanent closure of the repository.

The *Design Basis Event Frequency and Dose Calculation for Site Recommendation* (BSC 2001b) assumed a 100-year operational phase for a higher-temperature operating mode. This operational period is valid for lower-temperature operating modes that have longer preclosure operational phases (BSC 2001a). However, if an operating mode is selected that extends the preclosure period of subsurface drift ventilation beyond 100 years, the effects on the event sequence probability cutoffs for subsurface events must be assessed. For ease of analysis, the preclosure period could be divided into two phases. Phase 1 would encompass the activities associated with emplacing waste in the subsurface facilities. This phase would include phased construction of the subsurface and potentially the surface facilities. Phase 2 would begin after emplacement activities are completed. If the flexible thermal design focuses on a lower-temperature operating mode, then cooling of the waste package could extend the Phase 2 preclosure period to 275 years after emplacement operations end. Because there is no expected movement of waste packages during the cooling period, the hazards to the waste package are

reduced. Furthermore, the resulting likelihood of Category 1 or Category 2 event sequences is reduced. Phase 2 may start when emplacement is completed (e.g., after 50 years of emplacement activities) and extend until permanent closure (the next 275 years for a total preclosure period of 325 years).

3.3.1 Preclosure Safety Analysis

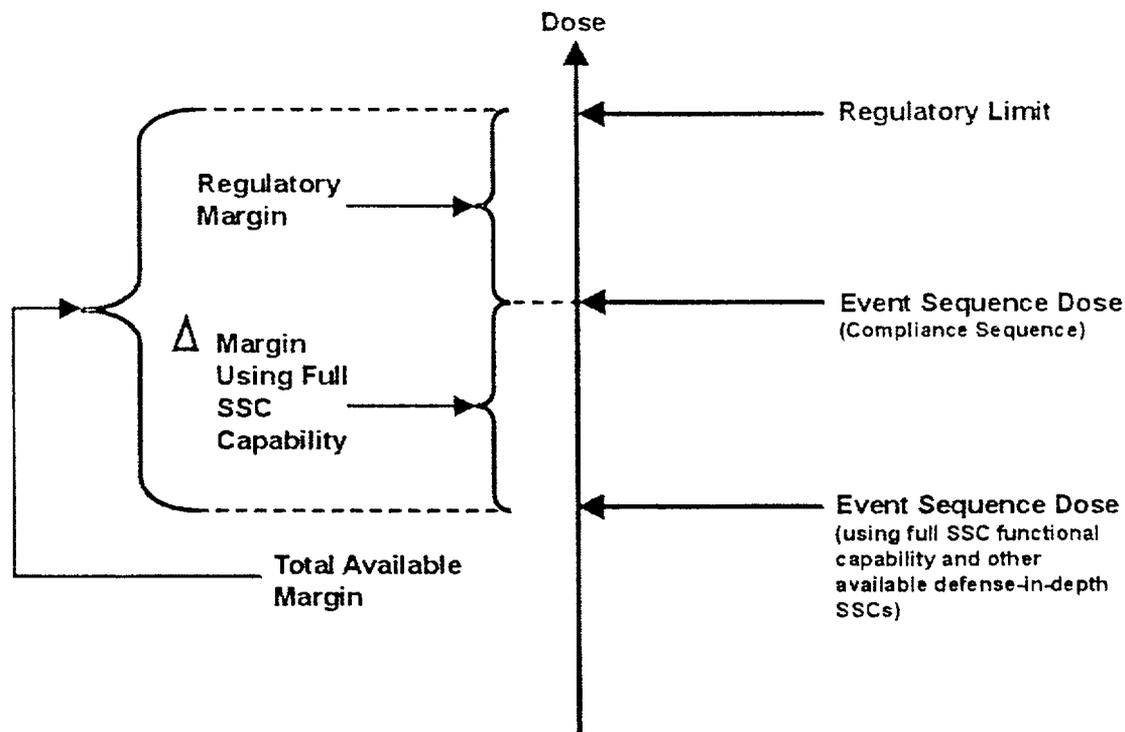
The purpose of the PSA will be to ensure that relevant internal and external hazards that could result in unacceptable consequences have been evaluated, and to ensure that preventive or mitigative features are included in the repository design such that the limits on radiation exposures specified in 10 CFR 63.111 will not be exceeded. The PSA will provide a framework for applying risk-informed, performance-based decision making to identifying SSCs important-to-safety, measures for providing defense-in-depth, license specifications, and surveillance intervals. The PSA will identify potential natural and operational hazards during the preclosure period, assess potential events and event sequences and their consequences, and identify SSCs and personnel activities that are intended to prevent or mitigate each accident sequence. Event sequence identification and analysis comprises an iterative process integrally tied to repository design. Consequently, the PSA and event sequence identification and analysis will continue to evolve with design maturation. Preliminary analyses based on the conceptual design should show large margins between expected performance and the regulatory limits. As the design matures, these margins will be reduced.

3.3.2 Margin and Defense-in-Depth

Margin, as used in this section, refers to the difference between calculated event sequence consequences and regulatory compliance limits (Figure 3-1). Margin is included in safety analyses for reasons that include analysis uncertainties, operational flexibility, and additional safety confidence.

The specific margin credited in the PSA will be the amount needed for defensibility of analyses and compliance with regulations. In specific cases, license specifications may be established to ensure that sufficient margin is maintained relating to the bounds of values related to the safety analyses. To accommodate potential changes to the design, data, or analyses that are in effect when the LA for construction authorization is submitted, one-half of the limits prescribed by the regulations will be used as a guideline for evaluating performance. The purpose of this guideline is to indicate the need for consideration of alternative features for prevention or mitigation of consequences resulting from potential design basis events. At the time of submittal of the LA amendment to receive and possess high-level radioactive waste, the acceptance criteria will be the regulatory dose limits with consideration of defensible uncertainties (see Section 9).

Defense-in-depth is the application of redundant or diverse physical and administrative barriers (or other protective measures) to mitigate unanticipated conditions, processes, and events such that failure of any one barrier or SSC does not result in failure of the entire system. Defense-in-depth ensures that safety is not wholly dependent on any single element of the design, construction, operation, or maintenance of the facility. The application of defense-in-depth will be risk-informed and will not be arbitrarily assigned. Facilities that include defense-in-depth should be more tolerant of failures and external challenges.



NOTE: Illustration of typical margin calculations for an event sequence. This event sequence takes credit for the 10 CFR 63.2 design bases functions. The dose calculation for the compliance event sequence is compared to the regulatory limit to provide a regulatory margin. Also shown is the dose calculation for the event sequence that credits the full design bases functional capabilities of the SSCs along with any additional defense-in-depth SSCs. The application of this SSC functional capability would provide additional margin to the regulatory limit that is under control of the Department of Energy.

Figure 3-1. Margin For Dose Compliance

3.3.3 Consequence Analysis of Very Low Probability Events and Event Sequences

The regulatory limit for event sequences that must be analyzed is greater than one chance in 10,000 for the preclosure period. Exceeding this threshold for the potential event sequences may be precluded by the design of SSCs. For example, the preclosure design bases for the repository will preclude a breach of a high-level radioactive waste or spent nuclear fuel (SNF) shipping cask, canister, or waste package resulting from a drop event (or other credible impacts) because that event sequence will have been demonstrated to have a frequency of less than 1×10^{-6} per year (see Section 3.5). If the event sequence has a frequency greater than 1×10^{-6} per year, the safety analysis must demonstrate that releases from a breached container will not result in site boundary doses above the regulatory limits.

The PSA will include evaluations of the consequences of selected sequences that are below the Category 2 threshold, using the best estimate of expected conditions, to provide confidence in the repository preclosure design. The purpose of this evaluation will be to ensure that an event sequence with high consequence levels is not arbitrarily excluded based on the low frequency of the event. Selected design features that maintain the event sequence frequency below 1×10^{-6} per year will be candidates for designation as important to safety. Features added to mitigate the consequences of such events would not be considered to be important-to-safety. These

consequence analyses will not be part of the safety case, but may provide additional confidence in the repository performance.

3.3.4 Nuclear Industry Precedent and Experience

The strategy for the preclosure operational period includes maximizing the use of proven technology and concepts that have been used for years in the commercial nuclear industry and in Department of Energy activities for safely handling radioactive wastes.

Precedents and experience from the commercial nuclear industry (and other nuclear fuel cycle facilities) will be used where appropriate in the design and analysis of the repository operational facilities. The use of precedent provides confidence in the PSA approach, and it provides data and lessons learned for incorporation into the hazards and consequence analyses.

The PSA will incorporate industry precedents that are appropriate for the repository. The use of precedent provides additional assurance that the processes used in the PSA are acceptable to the U.S. Nuclear Regulatory Commission, and it will allow them to focus on the application of processes. The use of precedents should also facilitate the review process. Industry precedent should be used (or adapted) when it results in compliance with regulatory requirements and it does not result in significant over-conservatism in the design development.

Regulation 10 CFR Part 63 is risk-informed and performance-based, and it requires identifying SSCs that are important to safety. This approach is a broader recognition of radiological risk than the traditional safety-related definition. Many industry and licensing precedents are based on traditional safety-related concepts with a more deterministic approach to safety analysis. The use of industry and licensing precedents should form the building blocks for the development of the PSA; however, in many cases, the intent and philosophy of the precedents should be used. For example, using regulatory guides that are based on the safety-related concept may be appropriate for the application to SSCs important-to-safety that have been classified as Quality Level-1, but they may be overly conservative for important-to-safety SSCs that are classified as Quality Level-2 or Quality Level-3 (quality assurance classifications are described in Section 12). However, for natural phenomena, the direct application of industry and licensing precedents may be appropriate (e.g., protection against floods or tornadoes).

When evaluating the applicability of industry and licensing precedents, the following will be considered:

- Differences in the regulatory basis or philosophy
- Regulatory definitions (e.g., event sequences, important to safety, safety-related)
- Performance objectives
- Licensing period.

Recent precedents related to risk-informed regulation will be used whenever appropriate. Using recent precedents will help to achieve the appropriate balance between using traditional industry and licensing precedents and using the current risk-informed regulatory philosophy.

3.3.5 Evaluation Approach

3.3.5.1 Risk-Informed Approach

A risk-informed approach, as discussed in this guide, is used to evaluate preclosure repository safety. As a result, deterministic precedents are not applied a priori. The risk-informed regulation results in balancing deterministic and probabilistic approaches. For example, the design of the preclosure facility to protect against external floods, extreme winds, tornado winds, and tornado missiles will primarily be deterministic and precedent-influenced. However, probabilistic analyses may provide insight into the appropriate intensity of site-specific hazards that the facility should withstand (e.g., magnitude of seismic events or tornadoes). In addition, selection of tornado missiles using a site-specific probabilistic method rather than through the use of a prescribed list may result in a more robust risk-informed design. Using probabilistic techniques to evaluate potential hazards is expected to be more appropriate for evaluating internal events. No arbitrary single-failures will be considered in the safety evaluation of event sequences. Failures will be based on a risk-informed approach as described in Section 4.

3.3.5.2 Mechanistic Evaluation

Mechanistic evaluations of the facility represent the preferred approach for evaluating event sequences. Mechanistic evaluations represent potential causes and effects of failures and actions. A non-mechanistic failure would be an arbitrary assumed failure of a component that is not linked to a cause (e.g., a breach of a transportation cask without a cause for the breach). In general, nonmechanistic failures are not assumed in the safety evaluation.

3.3.6 Conservative or Bounding Approaches

Reasonable values (e.g., mean frequencies and consequences; see Sections 7 and 8) and approaches will be used in evaluating the preclosure safety aspects of repository facilities. Simple bounding evaluations will be used when they do not overly constrain the design or the operations of the facility. For example, if a simple, conservative evaluation of an event sequence meets regulatory limits with existing SSCs and does not result in unusual quality assurance classification of an SSC (see Section 12) or the addition of SSCs to prevent or mitigate the event sequence, then the analysis is complete. However, if the bounding treatment of an event sequence results in the need for additional SSCs or the need for non-typical design and quality requirements to meet regulatory limits, then a more rigorous, less deterministic analysis may be warranted.

3.3.7 Preferred Approach

Many options are available for ensuring that event sequences are adequately prevented or mitigated. While the approaches to addressing event sequences may differ, a preferred strategy will govern how the repository event sequences are addressed:

- Design features are preferable to administrative features
- Passive features are preferable to active features

- Automatic features are preferable to manual features
- Separation is preferable to co-location.

Additionally, a risk informed approach should be used to determine acceptable preclosure 10 CFR 63.2 design bases (see Section 13). Protection will progress from a single component or system to redundant components and systems. Diverse components and systems will be included in the design if potentially important common-mode failures are identified. Developing a design that maximizes the implementation of these elements can result in a simple and transparent safety case, a facility with passive safety features, and less overall risk and minimal operational complexity.

3.3.8 Retrievability

Consistent with regulatory requirements, full retrieval of waste packages is not part of the LA acceptance criteria. However, waste package retrieval capability must be demonstrated in the design of the facility. The assessment of retrieval capability will demonstrate that the consequences of Category 1 and Category 2 event sequence will be within the performance objectives of 10 CFR Part 63 and that there are no Category 1 or Category 2 event sequences that could occur during retrieval that would preclude the capability to retrieve the waste packages.

An explicit analysis of full retrieval will not be included as part of the LA submittal. If full retrieval becomes necessary, an amendment to the Safety Analysis Report (with the design and operational modifications) will be submitted prior to commencing retrieval operations.

3.3.9 License Specifications and Surveillances

License specifications—License specifications are rules that establish when repository SSCs important-to-safety must be operable (including allowed outage times). They establish the limiting parameters for the operation of SSCs important-to-safety and the limits on the types and forms of waste to be received. These specifications provide additional assurance that the repository preclosure operations will be performed safely.

Licensing specifications will be derived from the PSA. Licensing conditions may include restrictions on the maximum annual throughput of transportation casks and waste packages; restrictions on the chemical form of radioactive waste; restrictions on waste package characteristics; requirements on testing, calibration, or inspection to ensure license conditions are observed; controls to restrict access to the site; preventative maintenance activities; and administrative controls related to management, procedures, record keeping, review, and audit. The licensing specifications will be developed to provide confidence that the facility will operate within the preclosure safety licensing conditions. Factors to consider in developing licensing specifications include the type and number of risks identified in the PSA, industry and regulatory precedents, and manufacturer specifications.

Surveillances are periodic (e.g., monthly, quarterly, or annually) operational tests of SSCs to demonstrate the ability of the SSCs to perform required safety functions. The frequency of surveillance and time constraints of action statements will be risk-informed.

Regulation 10 CFR 63.21(18) requires that license specifications, including the identification and justification for the selection of those variables, conditions, or other items that are determined to be probable subjects of license specifications, are included in the repository LA submittal.

3.3.10 Preclosure Testing

Testing activities that occur during the preclosure period will be evaluated in the PSA. Tests that need to be performed to demonstrate the operational readiness of the facility will be performed before startup and during the operating phase of the repository. These tests will demonstrate the adequacy of the facility to operate within the preclosure licensing basis.

3.4 STRATEGY FOR PREVENTING OR MITIGATING PRECLOSURE OFFSITE RADIATION EXPOSURE

3.4.1 Identification of Important-to-Safety Features and Controls

To ensure that radiation doses associated with Category 1 and Category 2 event sequences do not exceed the limits in 10 CFR 63.111(a)(2) and 63.111(b)(2), the repository design will incorporate a combination of prevention and mitigation features and controls. Prevention is the use of design features to reduce the postulated frequency of events that result in radiological release from the repository operations area to less than one chance in 10,000 of occurring before permanent closure. Mitigation is the use of design features and barriers to ensure that the consequences of a postulated radiological release event sequence are within the regulatory limits for doses to workers and the public. Mitigation includes features intended to reduce releases from the routine operations that are included in the Category 1 event sequence annual dose summation. The PSA is used to identify the preventive features, mitigative features, and operational controls that are required to demonstrate compliance with radiation dose limits.

This preclosure safety strategy requires using prevention features in the repository design wherever reasonable. Eliminating or minimizing the potential for radiological release events provides design and operational benefits. From an operations perspective, surveillance and maintenance of active safety features for mitigating the consequences of events have been demonstrated to add to nuclear facility operational complexity, and recovery from events has proved to be more challenging than anticipated. This strategy is implemented by performing the PSA as an integral part of the design process in a manner consistent with a performance-based, risk-informed philosophy. A risk-informed approach uses risk insights, engineering analysis and judgement, and equipment performance history to demonstrate the importance of the repository preclosure operational functions that have the most safety significance and to establish design criteria and management controls based upon these risk insights. This integral design approach ensures that the design features and operational controls important to safety are selected in a manner that assures safety while minimizing design and operational complexity through the use of proven technology.

3.4.2 Design Bases for Facilities and Limits on Operations

The preclosure safety strategy requires that SSCs important-to-safety must be designed, constructed, and operated in such a manner that they will survive credible external events and natural phenomena and that Category 1 and Category 2 event sequence dose limits will not be exceeded.

3.4.3 Safety Strategy for Repository Preclosure Operational Functions

The safety strategy for repository preclosure operational functions is based on the receiving waste, transferring waste into disposal containers, sealing disposal containers, transferring waste packages to emplacement drifts, and emplacing waste packages. These functions are based on site recommendation design features and illustrate the application of the preclosure safety strategy discussed in previous sections. The safety strategy for each of these functions is either prevention augmented by mitigation or mitigation augmented by prevention. Summary descriptions of the safety strategy for each of the five repository preclosure operations functions, and a potential list of safety strategies for each are summarized in Table 3-1.

Table 3-1. Preclosure Safety Strategy

Example Basic Operations	Canistered Fuel Safety Strategy	Uncanistered Fuel Safety Strategy
Receipt of Waste		
Survey Remove impact limiters Remove personal barriers Remove hold downs Upright cask Transfer cask to cart	Prevent events that could exceed shipping cask design basis (preclude breach)	Prevent events that could exceed shipping cask design basis (preclude breach)
Vent and Sample cask Unbolt cask cover Remove cover Remove materials from cask Install cover Bolt cask cover Store canistered waste Store SNF assemblies Decontaminate cask Remove DC cover Load DC Install DC cover Decontaminate DC	Prevent events that could exceed canister design basis (preclude breach)	Minimize the number of events that could result in uncanistered fuel drops; minimize radiation releases from drop events
Sealing the Disposal Container		
Weld DC Inspect DC welds Stress relieve DC welds	Prevent events that could exceed canister design basis (preclude breach)	Minimize the number of events that could result in disposal container drops; minimize radiation releases from drop events

Table 3-1. Repository Preclosure Safety Strategy (Continued)

Example Basic Operations	Canistered Fuel Safety Strategy	Uncanistered Fuel Safety Strategy
Transfer of the Waste Package (WP) to the Emplacement Drift		
Move WP and pallet to tunnel entrance Descent to drift entrance Park at drift entrance	Prevent events that could exceed WP design basis (preclude breach)	Prevent events that could exceed WP design basis (preclude breach)
Move WP and pallet to tunnel entrance Descent to drift entrance Park at drift entrance	Prevent events that could exceed WP design basis (preclude breach)	Prevent events that could exceed WP design basis (preclude breach)
Emplacement		
Move WP and pallet from tunnel entrance to permanent drift position	Prevent events that could exceed WP design basis (preclude breach)	Prevent events that could exceed WP design basis (preclude breach)

NOTE: DC = disposal container; WP = waste package

3.5 REFERENCES

3.5.1 Documents Cited

BSC (Bechtel SAIC Company) 2001a. *Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation*. TDR-MGR-SE-000009 REV 00 ICN 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20010705.0172.

BSC 2001b. *Design Basis Event Frequency and Dose Calculation for Site Recommendation*. CAL-WHS-SE-000001 REV 01 ICN 02. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20011211.0094.

3.5.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMS.....	ii
4. OVERVIEW OF PRECLOSURE SAFETY ANALYSIS ELEMENTS AND APPROACHES	4-1
4.1 INTRODUCTION	4-1
4.2 BACKGROUND	4-1
4.3 OVERVIEW OF PROCESS FOR PERFORMING A PRECLOSURE SAFETY ANALYSIS.....	4-2
4.3.1 Flow Diagram of Preclosure Safety Analysis Process.....	4-3
4.4 DEVELOPING AND DOCUMENTING THE PRECLOSURE SAFETY ANALYSIS IN THE LICENSE APPLICATION	4-9
4.4.1 Level of Design Detail in the License Application for Construction Authorization	4-9
4.4.2 Information Base for Preclosure Safety Analysis in Support of License Application for Construction Authorization	4-9
4.4.3 Preclosure Safety Analysis Based on Level of Design Detail Available at Time of License Application.....	4-11
4.5 ENSURING PERFORMANCE OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY.....	4-12
4.6 REFERENCES	4-15
4.6.1 Documents Cited.....	4-15
4.6.2 Codes, Standards, Regulations, and Procedures	4-15

FIGURES

	Page
4-1 Preclosure Safety Analysis	4-4
4-2 Process for Preclosure Safety Analysis Using Available Level of Design Detail.....	4-14

TABLES

	Page
4-1 Sample Approach for Demonstrating Compliance with 10 CFR 63.112(e).....	4-13

ACRONYMS

ALARA	as low as is reasonably achievable
CA	construction authorization
HEPA	high-efficiency particulate air
HVAC	heating, ventilation, and air-conditioning
LA	license application
LA-CA	license application for construction authorization
LA-R&P	license application to receive and possess
NRC	U.S. Nuclear Regulatory Commission
PSA	preclosure safety analysis
QA	quality assurance
R&P	receive and possess (i.e., LA amendment to R&P high-level radioactive waste)
SSCs	structures, systems, and components
YMP	Yucca Mountain Site Characterization Project

4. OVERVIEW OF PRECLOSURE SAFETY ANALYSIS ELEMENTS AND APPROACHES

4.1 INTRODUCTION

A high-level overview of how the preclosure safety analysis (PSA) will be performed for a repository at Yucca Mountain is presented in this section. The PSA comprises several kinds of analyses that must be integrated into a cohesive evaluation and documented. Further, the PSA process supports developing 10 CFR 63.2 design bases, design criteria, design requirements, structures, systems, and components (SSCs) classification, design evaluation, Q-List development, and the preclosure safety strategy in license application (LA) documentation.

The PSA process must support the LA for construction authorization (CA) as well as the LA amendment to receive and possess (R&P) high-level radioactive waste. The process must be sufficiently flexible and robust to support the LA given the level of design detail available for the SSCs of the geologic repository operations area at the time of the license application for construction authorization (LA-CA).

4.2 BACKGROUND

The requirements for performing and documenting a PSA for a repository, per the definition of 10 CFR 63.2 and the content defined in 10 CFR 63.112, are described in Section 2. The methods described are responsive to the U.S. Nuclear Regulatory Commission's (NRC's) methods and review acceptance criteria. The repository licensing process for waste emplacement consists of two steps: a CA and a license to R&P. A PSA is required to be provided in support of both licensing steps. Each of the licensing steps requires an NRC safety determination that is based on, respectively, the initial PSA for the CA, and the updated PSA for the license application to receive and possess (LA-R&P). The licensing plan is to submit the amount of design information in the LA that provides sufficient information for the NRC safety evaluation.

Because 10 CFR Part 63 was developed as a risk-informed, performance-based rule, the PSA is adapting a risk-informed, performance-based approach. While parts of the safety strategy (see Section 3) are based on deterministic principles and regulatory principles, a large portion of the safety evaluation for the preclosure operations apply elements of risk analysis. The methods described in this guide are consistent with NRC regulations and guidance. The methods are compatible with NRC guidelines (Milstein 2000, NRC 1983) for performing an integrated safety analysis (which was the term ascribed to the PSA prior to the promulgation of the Final Rule (10 CFR Part 63). The NRC guidelines permit the licensee to apply appropriate methods to produce results and documentation that are deemed suitably comprehensive by the NRC.

4.3 OVERVIEW OF PROCESS FOR PERFORMING A PRECLOSURE SAFETY ANALYSIS

The PSA applies elements of risk analysis that are imbedded in the hazards and event sequence analyses. The PSA comprises a structured, multi-tiered evaluation of hazards and event sequences. The PSA applies the risk-analysis triplet that asks the three questions:

- What can happen? (hazard identification and scenario development)
- How likely is it? (frequency or likelihood analysis)
- What are the consequences? (radiological doses or physical harm to workers or public)

The questions can be answered qualitatively, as well as quantitatively, and therefore, can be applied to deterministic, as well as probabilistic analyses.

These same three questions are applied over and over as the PSA progresses through the hazards analysis phase, event sequence analyses, consideration of safety-specific analyses, and as the design detail evolves. The PSA also includes elements of risk management by identifying means for preventing, reducing the likelihood of, or mitigating hazards.

The performance of a comprehensive hazards analysis and event sequence analyses in the preliminary stages of design requires the application of the knowledge and experience of a multi-disciplinary team comprised of personnel who are cognizant of one or more areas related to safety and design:

- Hazards analysis and event sequence analysis for radiological safety
- Design of mechanical systems for handling, opening, sealing, loading, and transporting waste forms
- Design of structural, electrical, and instrumentation and control systems
- Design of pool water-treatment and cooling systems (if needed)
- Design of heating, ventilation, and air-conditioning (HVAC) and high-efficiency particulate air (HEPA) filter systems for radioactive areas
- Design of disposal container and waste package
- Radiological consequence analyses
- Criticality safety
- Fire hazards and fire protection
- Design for radiation protection, shielding, and as low as is reasonably achievable (ALARA)

- Systems reliability modeling, including fault tree, failure modes and effects analysis, human factors, and common-cause failures
- Processing, packaging, and disposal of site-generated radiological and hazardous waste
- Licensing and regulations.

As needs dictate, other disciplines should be addressed. In addition to engaging multiple disciplines in the development of the PSA, the formal review of PSA products should engage cognizant personnel (subject matter experts) to ensure that the PSA is complete.

PSA activities and documentation will be Yucca Mountain Site Characterization Project (YMP) procedures.

4.3.1 Flow Diagram of Preclosure Safety Analysis Process

Figure 4-1 illustrates the PSA process that will be documented in the Safety Analysis Report. Individual sections of this desktop guide describe how each of the specific elements are performed and documented. Section 4.4.3 describes the process for performing a preliminary PSA with a limited amount of design detail. The three risk-analysis questions are addressed through the PSA process.

The elements of the PSA process, for the stages of design maturity, are described in the following paragraphs. (The bolded paragraph lead-ins refer to PSA elements shown in Figure 4-1.)

4.3.1.1 Hazards Analyses

Internal and External Hazard Identification—Hazards analysis is a systematic identification and evaluation of naturally occurring and human-induced hazards (see Section 6). To ensure completeness, the analysis begins with checklists of generic categories of hazards to identify which are applicable to a repository. The preclosure hazards at a geologic repository are not like those at a complex facility such as a nuclear power plant or petroleum refinery that contains and controls large amounts of thermal and chemical energy that can contribute to the initiation and magnitude of consequences should an accident occur. The high-level radioactive waste forms are contained in a series of physical barriers, including fuel rod cladding, canisters, transport casks, and waste packages. Thus, some form of energy must be imparted, generally from an external source, to a waste form to initiate some undesired sequence of events. Natural phenomena, such as earthquakes and tornadoes, are sources of energy, as well as the processes for lifting, moving, transporting, and welding that are inherent in repository operations. The role of the hazard analysis is to identify sources of energy that can have the potential to harmfully interact with a waste form. In the structured internal event hazards analysis, the forms of energy are categorized as Collision/Crushing, Chemical Contamination/Flooding, Explosion/Implosion, Fire, Radiation/Magnetic/Electrical/Fissile (i.e., potential criticality), or Thermal. The external events hazards analysis identifies credible natural phenomena such as earthquakes that could impart sufficient energy to the facilities to pose a hazard to a waste form.

The evaluation of hazards provides the technical bases for either including or excluding specific hazards from the PSA. Initially, qualitative evaluations are applied to screen out inapplicable or

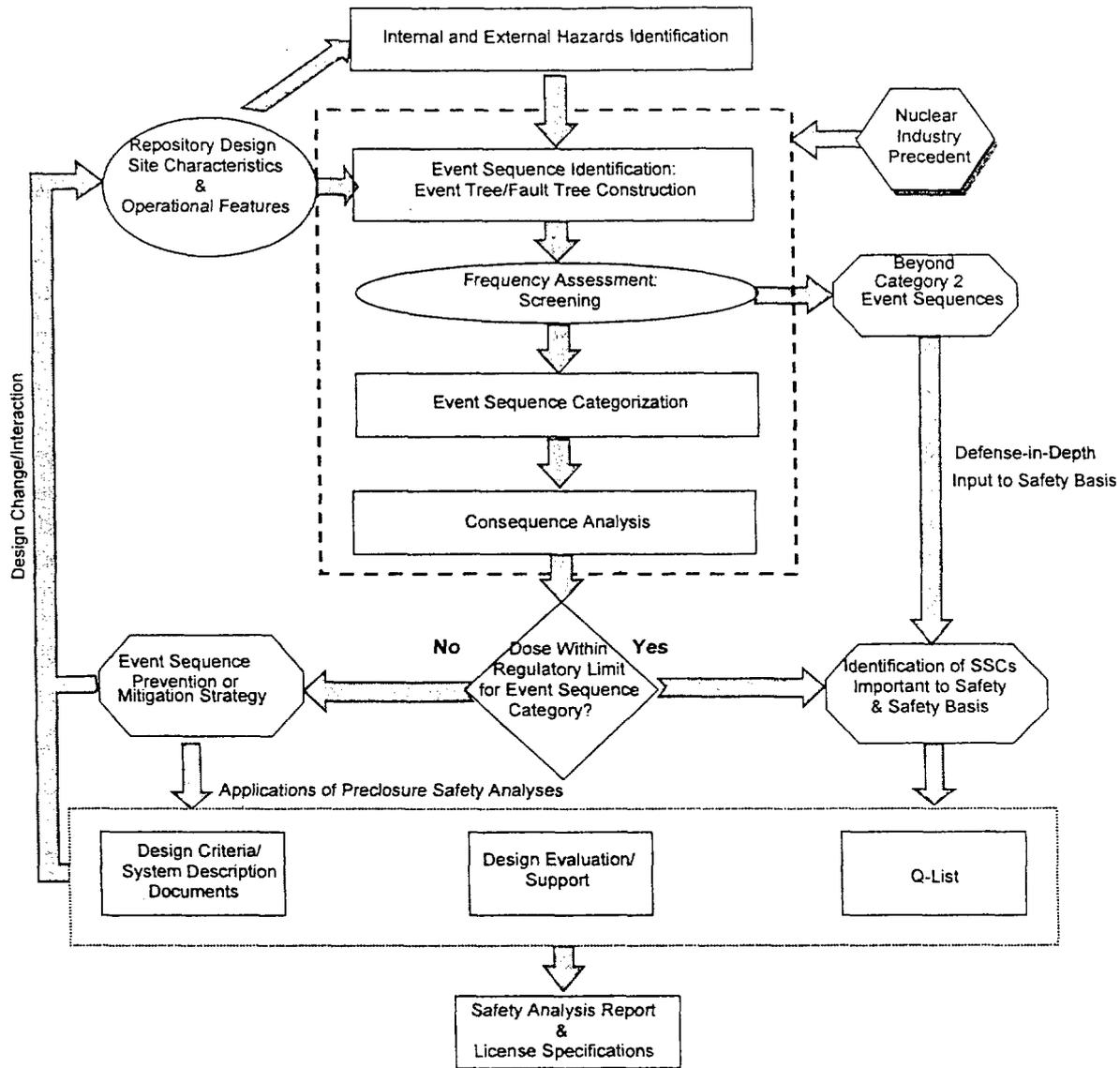


Figure 4-1. Preclosure Safety Analysis

incredible hazards, from hazards either internal or external to the repository facilities. External hazards include natural phenomena and human-induced events. Each credible hazard is considered as a potential initiator of event sequences that could lead to releases of radioactivity or radiological exposure of workers.

4.3.1.2 Event Sequence Analysis

The central box in Figure 4-1 contains several steps that comprise the PSA process. The analytic elements are described below, as they are applied in event sequence analysis for internal initiating events. The process applies several of the methods familiar to probabilistic risk

assessment. (Section 4.3.1.3 describes a variation on the process that is applied to external initiating event and natural phenomena, and which may invoke deterministic analysis or regulatory precedents.)

The qualitative screening of the internal events hazards analysis identifies credible events in each operational area that could potentially initiate an accident sequence. The internal event analysis identifies in more detail what events have to occur to result in a radiological accident and evaluates their credibility and potential consequences. The event sequence analysis incorporates analyses and design strategies from safety-specific disciplines (e.g., criticality and fire-protection) and across disciplines (e.g., criticality, fire, and radiological exposure).

Sequence Identification: Event Tree and Fault Tree Construction—The internal hazards are classified by potential energy sources, associated with each operation in the facility, that could directly or indirectly impact various radioactive waste forms. Energy sources include drops, collisions, tipovers and slapdowns, fires, explosions, flooding, criticality, chemical, radiation, thermal, and human interactions. Potential accident scenarios (or event sequences) may be displayed in the form of event trees that include an initiating event (from an identified hazard) and one or more enabling events that must occur to result in a release of radioactivity, a criticality, or an abnormal worker exposure. The event tree format provides a framework for estimating the likelihood of event sequences by displaying the frequency of the initiating event and the conditional probabilities of contributing (enabling) events.

Potential criticality event sequences are subjected to specialized analyses to demonstrate that sufficient design and operational controls are in place to ensure the probability of a criticality is below the threshold for credibility.

Frequency Assessment: Screening—The frequency (or annual probability of occurrence) is estimated with quantitative analyses for each event sequence that potentially results in a release of radioactivity or abnormal worker exposure. The framework of the event tree is used to display the frequency of the initiator and the conditional probabilities of each enabling event in a sequence. The frequency of each event sequence is calculated as the product of the initiator frequency and the probabilities of the enabling events.

The frequencies of initiating events for internal hazards are estimated from the annual frequency of each operation multiplied by the conditional probability of the initiating event per operation. For example, the frequency of a canister drop is estimated by the product of the frequency of canister lifts (i.e., the number per year) and the conditional probability of dropping the canister per lift. The annual frequencies of each operational step are determined from programmatic information that specifies the maximum number of transport casks, spent fuel assemblies, spent fuel canisters, high-level radioactive waste canisters, and waste packages that are expected to be processed each year during the preclosure operations. The conditional probability of each enabling event (usually a failure of some preventive or mitigative feature), such as a drop of a waste form, is estimated from generic data for similar operations. In many cases for the preliminary event sequence screening analyses, conservative probabilities are assumed for the conditional events (e.g., assuming a probability of 1.0 that all fuel rods breach in a drop sequence). This conservatism is warranted in most cases in the early screening because design criteria or design details are not in place. As noted below, one objective of the internal event

analysis is to define where prevention or mitigation controls are needed. Nevertheless, the event tree framework helps to display and keep track of the assumed probabilities and their bases.

The quantitative screening applies the 10 CFR 63.2 definition of event sequence to screen out event sequences whose estimated frequency results in a probability of less than one chance in 10,000 of occurring during the preclosure operations. Such event sequences are termed beyond Category 2 event sequences and are screened out as noted by the octagonal box in Figure 4-1. Because of uncertainties, the frequency screening is conservatively applied initially so that event sequences within a factor of 10 of the threshold are retained in a list of event sequences until they may be shown to be less than 10^{-6} per year.

Event Sequence Categorization—In this step of the analyses, the frequency of each event sequence that survived the frequency screening is categorized as Category 1 or Category 2 as defined by 10 CFR 63.2. This categorization is important because it establishes which portion of the performance objectives of 10 CFR 63.111 govern each sequence.

Consequence Analysis—In this portion of the analysis, the potential consequences of releases or exposures are calculated for Category 1 and Category 2 event sequences. In some cases, the release or exposure characteristics are similar for two or more event sequences permitting sequences to be grouped. For Category 1 event sequences, consequences are evaluated as potential contributors to chronic exposures and are aggregated for Category 1 event sequences. For Category 2 event sequences, consequences are evaluated for each Category 2 event sequence, individually, as an acute exposure. Consequence analyses are also performed to support prevention or mitigation strategies for external events, as described in Section 4.3.1.3.

The assessment of doses to the public and to workers for each event sequence is evaluated for credible exposure pathways.

Section 8 describes the dose pathways considered in more detail.

The output of the event sequence analysis is a tabulation of the event sequences by category and the consequences associated with each. Where appropriate, a bounding event sequence for each category is identified for each operational area. The characteristics of the bounding event sequence define the 10 CFR 63.2 design bases requirements for SSCs important to safety associated with that operational area.

Dose Within Regulatory Limit for Event Sequence Category?—This evaluation determines whether a specific repository design is licensable. If any deficiencies are noted wherein the respective performance objectives for Category 1 or Category 2 event sequences are not met (i.e., resulting in a “No”), the YMP develops an event prevention or mitigation solution to correct the deficiency. The solution may result in a design change or additional administrative control.

Ultimately, the answer must be “Yes” to be licensable. The SSCs that are to ensure that credible event sequences are in compliance with 10 CFR Part 63 are termed “important to safety.” This step is shown in Figure 4-1 as Identification of SSCs Important to Safety and Safety Basis. Section 4.5 describes the requirements for ensuring the performance of SSCs important to safety. Section 12 presents the approach of the quality level classification process.

As necessary through design evolutions, portions or all of the PSA steps are iterated until the performance objectives of 10 CFR 63.111 are met with the proposed design.

4.3.1.3 External Event Preclosure Safety Analysis

The event sequence analysis of external events involves some variations on the process used to evaluate internal hazards (see Section 10). In most instances, the safety strategy for external event initiators is prevention of sequence initiation or SSC survivability through design. Consequently, sequences that could result in releases or exposures would be expected to be beyond the Category 2 cutoff. As appropriate, however, potential event sequences are defined and their potential consequences are calculated and evaluated against the dose limits of 10 CFR 63.111. If prevention or mitigation is necessary to meet the regulations, the SSC(s) involved will be designed to withstand the effects of external events of prescribed intensity, either using NRC precedents or site-specific events. The following are portions of the external event analyses that are not illustrated explicitly in Figure 4-1.

External Event Hazards and Screening Analysis—Potentially credible hazards that survive the initial qualitative and quantitative screening of the external events hazards analysis, such as earthquakes, winds, tornado missiles, lightning, external fires, loss of offsite power, aircraft crashes, and industrial-military activities, are subjected to further analyses. Such analyses may include quantitative evaluation of their likelihood to determine if they can credibly occur during the preclosure operations, or credibly cause a radiological release.

Selection of Design Basis External Events—This is the outcome of the external events hazards and screening analysis, including the specification of the frequency and intensity of design basis earthquakes, tornadoes, loss of offsite power, and similar events. The external event sequences are considered in light of how undesired consequences (i.e., radiological, criticality, or fire and explosion) might be generated by interaction of the external event with operations or storage areas within the facility.

Event Sequence Prevention and Mitigation Strategy—This step produces design requirements such that event sequences initiated by external events cannot credibly result in an unacceptable release of or exposure to radioactivity. For example, cranes and similar devices may need to be designed to halt in a safe condition without dropping a waste form upon loss of offsite power. The buildings housing handling, packaging, and lag-storage of waste forms may need to be designed to withstand design basis earthquakes and other natural phenomena without initiating or failing to mitigate a release of or exposure to radioactivity and without initiating a criticality. This step is part of the activity, Identification of SSCs Important to Safety and Safety Basis, shown in Figure 4-1.

4.3.1.4 Applications of Preclosure Safety Analyses

Insights from the event tree analysis and associated consequence analysis help to define requirements for SSCs to prevent, or mitigate effects of, initiating events and contributing events. A given SSC may be significant to preventing an initiating event, preventing progression of an event sequence, or preventing or mitigating the release of radioactivity. Those SSCs that are necessary to prevent, reduce the likelihood, or mitigate consequences such that the Category 1

and 2 event sequences meet the performance requirements of 10 CFR 63.111 are designated as SSCs important to safety. The ultimate application of the PSA is support of the preclosure safety basis in the LA.

The following areas use results from the PSA:

- **Q-List**—Those SSCs designated as SSCs important to safety are included in the *Q-List* (YMP 2001). The classification is developed from results of safety analyses and classified as QL-1, QL-2, or QL-3 and placed on the Q-List (see Section 12).
- **10 CFR 63.2 Design Bases and YMP Design Criteria Documents**—Nuclear safety 10 CFR 63.2 design bases are developed for those SSCs designated as important to safety. The design bases ensure that the necessary preventive and mitigative functions identified for the SSC are included in the final design. The nuclear design bases are stated in the system description documents.
- **Design Evaluation and Support**—As the level of design detail evolves and design concepts are put forth, concurrent supplemental safety analyses are performed to evaluate whether or not the design basis are met, or to help the designers evaluate a proposed design. These analyses may be qualitative or quantitative. A qualitative evaluation, for example, might be used to demonstrate that the transportation cask handling operations can not result in a drop of a transport cask from a height greater than the cask design basis. A quantitative analysis might apply a fault tree model to demonstrate that the reliability of an SSC meets the probability criteria (e.g., to demonstrate that the HVAC system of the Waste Handling Building remains operational for a given time with a specified probability). Should the qualitative or quantitative analyses identify a deficiency or vulnerability in the proposed design, the designers would revise the design, operations, or both, accordingly.

In some instances, alternative design concepts for certain handling, packaging, or storage of waste may be under consideration by the design engineers. For example, alternatives for unloading a transportation cask may include dry (in air) or wet (under water) conditions. Similarly, design alternatives may include: remote vs. local control of operations; robotic vs. human control; handling only canistered spent nuclear fuel vs. a mixture of canistered and uncanistered spent nuclear fuel. Where decisions on such alternatives are pending at the time of submittal of LA-CA, the PSA explores the safety significance of each alternative (e.g., rates and concepts of handling, or characteristics of the waste forms). The PSA either presents the event sequence frequency and consequences for the bounding alternative of each operation, or the results for the baseline design with a discussion of the sensitivity of results to each of the alternatives.

As illustrated in Figure 4-1, the performance of the PSA is an iterative process incorporating site characteristics, design information, and safety strategies. The PSA process is performed and documented under YMP procedures. Excerpts and results of the respective analyses are incorporated into the Safety Analysis Report.

4.4 DEVELOPING AND DOCUMENTING THE PRECLOSURE SAFETY ANALYSIS IN THE LICENSE APPLICATION

In support of the LA-CA, the PSA process begins with information on conceptual design and operations, including application of a preclosure safety strategy, application of good practices from similar operations, industry codes and standards, and NRC regulatory precedents. A structured hazards analysis is performed to identify potential hazards, external and internal to the repository facilities, that initiate event sequences that could result in releases of radioactivity. Information on the natural phenomena and man-made hazards at the site and region should be well characterized. SSCs important to safety are identified from the analyses of hazards and event sequences. Design requirements derived from 10 CFR 63.2, design bases, that prevent or mitigate potential accidents are defined for the SSCs important to safety and are incorporated into the YMP design criteria document. As the 10 CFR 63.2 design bases are incorporated into the design, the PSA is updated to reflect the design commitments. For example, if a design feature eliminates a hazard or reduces the likelihood of an accident sequence, the PSA is revised.

4.4.1 Level of Design Detail in the License Application for Construction Authorization

The purpose of the LA is to present the safety case for a repository, and it must demonstrate that a repository will meet the postclosure and preclosure performance objectives. To demonstrate that a repository can meet postclosure performance objectives, a total system performance analysis is performed that is independent of the PSA. To demonstrate that a repository can meet the preclosure safety objectives, a PSA is performed. The PSA for the LA-CA must be at sufficient depth, commensurate with the available design detail, that provides sufficient assurance that the preclosure performance objectives of 10 CFR 63.111 will be met in the final design of a repository. A principal role of the preliminary PSA is defining the design bases that ensure that preclosure performance objectives can be met in the final design, in accordance with 10 CFR 63.112.

The LA should include a description of the systems that are required to protect the health and safety of the public and workers from Category 1 and Category 2 event sequences as defined in 10 CFR 63.2 for the preclosure period. The SSCs important to safety are identified as those required to meet preclosure performance objectives of 10 CFR 63.111. The LA should also include a description of systems that process radioactive waste and protect important to safety SSCs from interactions from other SSCs. In addition, the LA should identify design features that protect the health and safety of the worker during normal operations, including the proposed program for ensuring ALARA in a repository design. Further, the LA should define the design and operational strategies for addressing the safety-specific disciplines of criticality and fire-protection. The strategies, criteria, standards, and associated analyses for criticality and fire protection should be incorporated into the PSA.

4.4.2 Information Base for Preclosure Safety Analysis in Support of License Application for Construction Authorization

The premise of the PSA process is that sufficient information exists to (1) define the kinds of event sequences (scenarios) that can credibly occur in the kinds of operations that are known or expected to be necessary for receiving, handling, processing, packaging, transporting, and storing

waste forms, (2) estimate their frequency (likelihood), and (3) estimate their consequences. Section 5 states the requirements for descriptions of operating facilities and the site. At the time of the LA-CA, the hazards and event sequence analyses should be based on the information available that will consist of the following:

- Regulatory requirements per 10 CFR Part 63
- Site information (location, geography, geology, seismicity, and meteorology) that is well characterized by Exploratory Studies Facility, Nevada Test Site, and generally available information
- Industry codes and standards
- Regulatory and industry precedents for similar facilities
- Knowledge of good practices employed in similar operations that will be, or expected to be, adopted in a repository
- Experience and knowledge of members of multi-disciplinary PSA team
- Conceptual designs and principals of construction and operation.

Information on conceptual designs, construction, and operation should be derived from the general system descriptions provided in the project description document and system description documents. The information listed below provides a large portion of the bases for hazards analysis and event sequence development, such as:

1. Characterization of waste forms (age, thermal output, enrichment, burnup, radionuclide inventories) and their vulnerabilities to damage (e.g., physical form, cladding, allowable drop height)
2. Rate of waste receipt for each year of operation
3. Subsurface layout of drifts, positions of waste packages within the emplacement drifts, and installation of drip shields as defined by post-closure performance assessment considerations
4. Ground support, ventilation, and fire-protection systems of the subsurface facilities
5. Concepts for rescue, recovery, and decontamination of disabled transport and emplacement equipment
6. Concepts for waste package transport and emplacement in subsurface, including control, instrumentation, communication, and power supply system
7. Waste package design bases for potential accidental conditions (i.e., allowable drop heights, impacts, thermal or fire loading); criticality control features

8. Waste package sealing (welding or other); process for waste package remediation
9. Waste package radionuclide source terms for spent fuel assemblies, high-level defense waste
10. Preliminary surface facility layout, functional descriptions of operations for receiving, handling, packaging, staging, and transporting waste forms, including the rate of throughput
11. Surface facility construction concepts and commitments to NRC regulations, industrial codes and standards, including design for ventilation or filtration of radiological areas, seismic, tornadoes and winds, floods, and fire protection
12. Nuclear or radiological design bases and requirements (commitments) for surface and subsurface SSCs
13. Plan and schedule for concurrent construction (development) of the surface and subsurface facilities.

The documented basis for description of functions, operations, and features to be incorporated into the facility design should be derived from project documents.

4.4.3 Preclosure Safety Analysis Based on Level of Design Detail Available at Time of License Application

Figure 4-1 illustrates the overall PSA process. Figure 4-2 provides additional explanation for applying the PSA process as the design evolves. In the figure, the shaded boxes represent design processes and the open boxes represent portions of the PSA process.

The basic functional requirements of a repository are clearly defined and the basic operations required to carry out those functions can be defined, although design alternatives may exist to perform those functions. Design engineers initially focus on success and devise means to carry out each operation. The role of the hazards and safety analysts is to postulate potential failures and accident scenarios that could be associated with each functional area, including scenarios involving mechanical or hardware failures, software failures, human errors, and common-cause failures.

Various alternatives may be devised by designers for one or more operations to improve throughput (e.g., to achieve better reliability or improved maintainability), ensure licensability (e.g., a design meeting NRC guidelines), or reducing cost (e.g., a simpler design). Designers may also consider alternative designs that reduce the likelihood of accidents, either radiological or industrial, e.g., to implement the preclosure safety strategy. (Based on the results of the hazards and event sequence analyses of the PSA, design alternatives may be proposed to better meet regulatory requirements.)

Each of the functional operations requires suitable control and instrumentation systems, supporting systems such as AC and DC electrical power or fuel pool water supply, filtration, and cooling systems, and decontamination systems. Further, each of the functional operations

requires appropriate housing having an HVAC system, including HEPA filtration where necessary, and fire protection systems. The housing of the operations involving radioactive wastes will be designed, as appropriate, to withstand credible natural hazards such as earthquakes, tornadoes, and winds to preclude the initiation of event sequences.

Thus, even with limited design detail, the kinds of hazards and potential event sequences associated with the surface and subsurface operations can be identified and evaluated for their relative risk, and SSCs important to safety can be identified.

4.5 ENSURING PERFORMANCE OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY

The process described above results in the identification of SSCs important to safety based on function and provides insights into requirements for reliability of the SSCs and their support systems such as power supplies and associated instrumentation and controls. For other SSCs, the degree of mitigation may be identified, such as required filter efficiency for a HEPA filter. In some cases, the process identifies the need for a safety function that may not be in the evolving design drawings and facility descriptions within the design available at the time of LA-CA. In these instances, only the 10 CFR 63.2 design bases and design requirements for those safety functions which will be included in the system description documents.

Regulation 10 CFR 63.112(e) requires an analysis of the performance of the SSCs to identify those that are important to safety. This analysis should identify and describe the controls that are relied on to limit or prevent potential event sequences or mitigate their consequences. This analysis should also identify measures taken to ensure the availability of safety systems.

As stated in 10 CFR 63.112(e), the areas to be discussed include, but are not necessarily limited to, consideration of thirteen areas listed in Table 4-1. For each area, the table provides examples of programmatic strategies or controls that will be in place at the time of LA-CA.

Further, 10 CFR 63.112(f) requires a description and discussion of the design, both surface and subsurface, of the operations area, including the relationship between design criteria and the requirements specified by preclosure performance objectives (see 10 CFR 63.111(a) and (b)) and the design bases and their relationship to the design criteria.

As noted in Section 4.3, the LA-CA includes a description of the functions and operations of surface and subsurface facilities as the bases for the PSA. The PSA identifies the event sequences that could result in radiological exposures of the public or workers. In accordance with 10 CFR 63.112(f)(1), the design criteria of the SSCs important to safety are derived to ensure that the performance objectives of 10 CFR 63.111(a) and (b) are met, either as requirements to prevent or limit the likelihood of, or to mitigate the consequences of, the event sequences. The design requirements and criteria are incorporated into the system description documents of important to safety SSCs and which include the associated design bases. In accordance with 10 CFR 63.112(f)(2), the descriptions of a repository design and design bases provided in the LA-CA either demonstrate how the design bases are met or will be met at the time of the LA-R&P (Section 13 describes the process).

Table 4-1. Sample Approach for Demonstrating Compliance with 10 CFR 63.112(e)

Item	10 CFR 63.112(e) Requirement	Potential Approach for LA-CA
(1)	Means to limit concentration of radioactive material in air;	Radiation Protection Program strategy; Radiation confinement areas; Design criteria/bases for HVAC
(2)	Means to limit the time required to perform work in the vicinity of radioactive materials;	Radiation Protection Program strategy; Use of remote handling and maintenance equipment
(3)	Suitable shielding;	Radiation Protection Program strategy; Design bases for shielding; Preliminary shielding analysis of principal operations areas
(4)	Means to monitor and control the dispersal of radioactive contamination;	Radiation Protection Program strategy; Radiation confinement areas; Design bases for HVAC; Design criteria for Radiation Monitoring System
(5)	Means to control access to high radiation areas or airborne radioactivity area;	Radiation Protection Program strategy; Radiation confinement areas; Design bases for Radiation Monitoring System ; Design bases for interlocks and administrative controls
(6)	Means to prevent and control criticality;	Criticality safety strategy; Design bases for criticality controls of operational areas and waste packages
(7)	Radiation alarm system to warn of significant increases of radiation levels, concentrations of radioactive material in air, and increased radioactivity in effluents;	Radiation Protection Program strategy; Design bases for Radiation Monitoring System; Preliminary analyses of performance of Radiation Monitoring System
(8)	Ability of structures, systems, and components to perform their intended safety functions, assuming the occurrence of event sequences;	Design bases for SSCs including performance requirements derived from hazards and event sequence analyses, operating environments, and ability to withstand natural phenomena
(9)	Explosion and fire detection systems and appropriate suppression systems;	Fire Protection strategy; Preliminary fire hazards analyses
(10)	Means to control radioactive waste and radioactive effluents, and permit prompt termination of operations and evacuation of personnel during an emergency;	Radiation Protection Program strategy; Design bases for waste treatment building and systems; Design bases for Radiation Monitoring System including alarms; Preliminary emergency plans
(11)	Means to provide reliable and timely emergency power to instruments, utility service systems, and operating systems important to safety if there is a loss of primary electric power;	Design bases for primary and backup power sources for SSCs important to safety as appropriate to their safety function and need for continuing power or other support (e.g., radiation monitoring and continuation of cooling or air circulation) on loss of primary power source
(12)	Means to provide redundant systems necessary to maintain, with adequate capacity, the ability of utility services important to safety; and	Design bases for primary and redundant subsystems and power sources for SSCs important to safety as appropriate to their safety function and reliability requirements (e.g., to ensure sufficient small likelihood of an event sequence, or to ensure availability of mitigation function); Process flow, piping and instrumentation diagrams, and electrical one-line diagrams, as appropriate, to demonstrate the capability
(13)	Means to inspect, test, and maintain structures, systems, and components important to safety, as necessary, to ensure their continued functioning and readiness.	Design requirements to ensure that inspections, tests, and maintenance can be carried out; Preliminary commitments to administrative controls (e.g., preliminary licensing specifications) for carrying out periodic surveillance and tests to ensure availability of SSCs important to safety

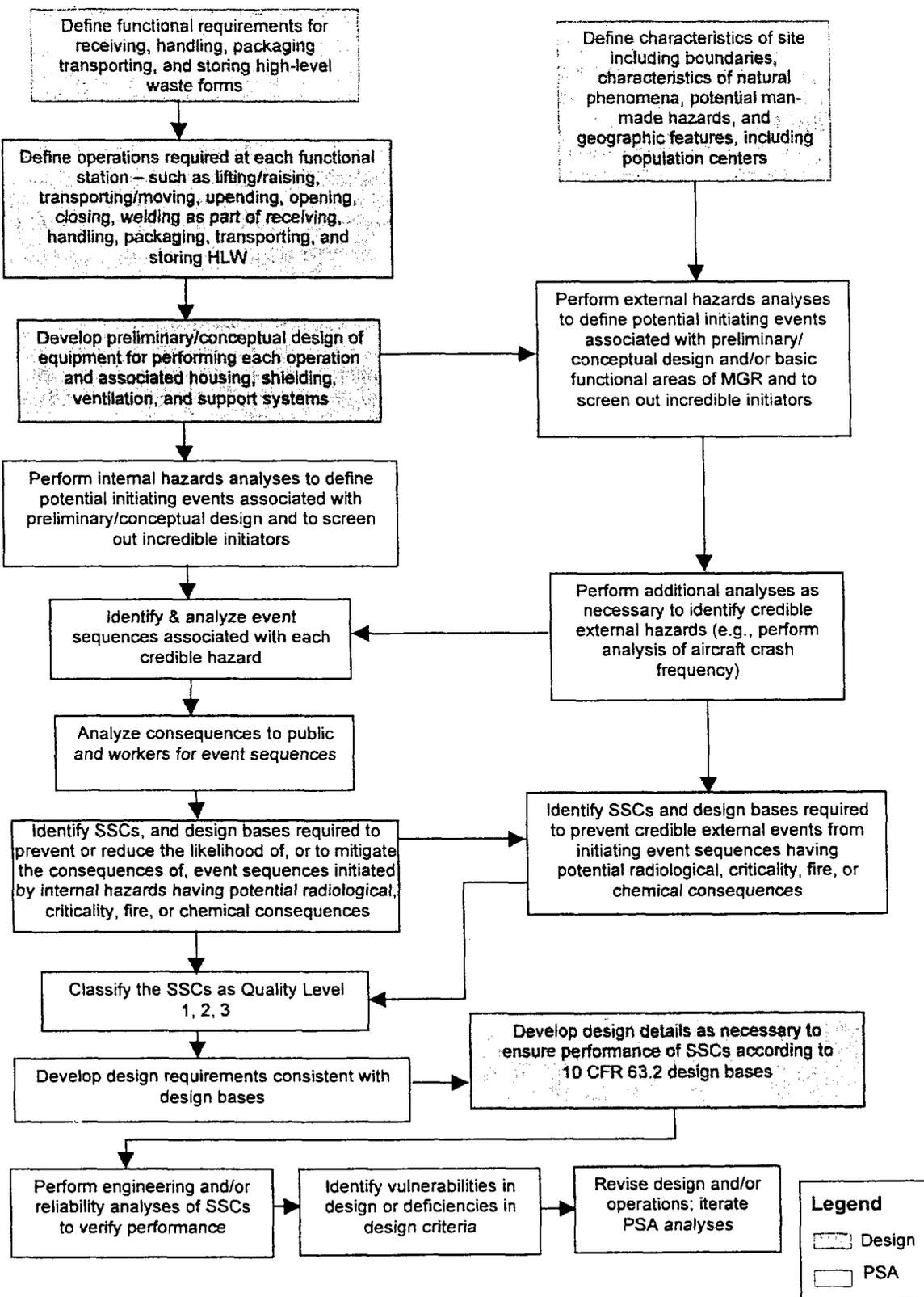


Figure 4-2. Process for Preclosure Safety Analysis Using Available Level of Design Detail

Even where the level of design detail is preliminary, the analyses included in the PSA processes identify the required safety functions, the design criteria for SSCs to achieve these safety functions, and commitments to ensure that the safety functions will be realized in the LA-R&P design. The PSA process will be updated as the design evolves to LA-R&P and the requirements of 10 CFR 63.112 (a) – (f) will be completely satisfied and documented.

4.6 REFERENCES

4.6.1 Documents Cited

Milstein, R. 2000. "Integrated Safety Analysis Guidance Document, Draft NUREG 1513." Attachment to SECY-00-0111: Final Rule to Amend 10 CFR Part 70, Domestic Licensing of Special Nuclear Material. Washington, D.C.: U.S. Nuclear Regulatory Commission. Accessed 07/25/2000. TIC: 247970. <http://www.nrc.gov/NRC/COMMISSION/SECYS/secy2000-0111/2000-0111scy.html>.

NRC (U.S. Nuclear Regulatory Commission) 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

YMP (Yucca Mountain Site Characterization Project) 2001. *Q-List*. YMP/90-55Q, Rev. 7. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.20010409.0366.

4.6.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMS.....	i
5. DESCRIPTION OF SITE, FACILITIES, AND OPERATIONS	5-1
5.1 INTRODUCTION	5-1
5.2 OVERVIEW OF APPROACH.....	5-1
5.3 REFERENCES	5-2
5.3.1 Documents Cited.....	5-2
5.3.2 Codes, Standards, Regulations, and Procedures	5-2

ACRONYMS

PSA preclosure safety analysis

INTENTIONALLY LEFT BLANK

5. DESCRIPTION OF SITE, FACILITIES, AND OPERATIONS

5.1 INTRODUCTION

The preclosure safety analysis (PSA) must include a general description of the structures, systems, and components, equipment, and process activities in the repository operations area. In addition, the PSA must provide a description of data pertaining to the repository site and surrounding region with sufficient detail to identify naturally occurring and human-induced hazards in the repository area (10 CFR 63.112).

Guidance for developing a description of the site characteristics, surface and subsurface facilities, and operations sufficient to support the hazards and event sequence analyses for preclosure radiological safety is presented in this section. A discussion of the applicable natural phenomena, external man-made hazards, and nearby facilities that could potentially affect the repository area is included. Site and facility characteristics applicable to repository postclosure safety are not discussed in this section.

5.2 OVERVIEW OF APPROACH

Material to be provided in support of the PSA will be contained in a brief summary section. Site and design features that are used in the hazards or event sequence analyses will be summarized with pointers to detailed sections of the license application submittal. No analytic methodology is required.

[Information for this section is under development and will be provided later.]

Information will be included that is relevant to performing preclosure hazards analyses, event sequence analyses, and consequence analyses. References will be provided to information sources and detailed descriptions found elsewhere in the license application submittal. A general description of the structures, systems, components, equipment, process (i.e., operational), and activities in the repository area will be provided (10 CFR 63.112(a), 10 CFR 63.112(f)).

As the basis of the safety analysis, brief descriptions of the site factors that could affect preclosure safety before permanent closure will be provided in the PSA, including:

- Site geography (location relative to prominent natural and man-made features such as mountains, rivers, airports, population centers, hazardous commercial facilities, and hazardous manufacturing facilities)
- Human populations (information based on recent census data)
- Natural phenomena and other external events sufficient to assess the likelihood of occurrence and to assess the impact on preclosure safety; discussion of relationship to features, events, and processes used in postclosure radiological analyses
- Meteorology (prevailing wind directions and speeds; discussion of data used in analyses of airborne releases for normal and postulated event sequences)

- Site boundaries (including a description and a map) and a description of methods for access control at the boundary.
- Operational and design factors that could affect radiological safety before permanent closure (i.e., the preclosure safety strategy, discussed in Section 3, and precedents from licensing of 10 CFR Part 50, 71, or 72 facilities).

5.3 REFERENCES

5.3.1 Documents Cited

None

5.3.2 Codes, Standards, Regulations, and Procedures

10 CFR 50. 1999. Energy: Domestic Licensing of Production and Utilization Facilities. Readily available.

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

10 CFR 71. 1999. Energy: Packaging and Transportation of Radioactive Material. Readily available.

10 CFR 72. Energy: Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-Level Radioactive Waste. Readily available.

CONTENTS

	Page
ACRONYMS	ii
6. HAZARDS ANALYSIS	6-1
6.1 EXTERNAL EVENTS HAZARDS ANALYSIS	6-1
6.1.1 Introduction.....	6-1
6.1.2 Overview of Approach.....	6-1
6.1.3 Details of Basic Approach to Screening with Examples	6-3
6.2 INTERNAL EVENTS HAZARDS ANALYSIS.....	6-20
6.2.1 Introduction.....	6-20
6.2.2 Overview of Basic Approach.....	6-21
6.2.3 Approach for Evaluating Applicability of Generic Internal Events to Repository Functional Areas.....	6-22
6.2.4 Examples of Evaluating the Applicability of Generic Events to Repository Function Areas	6-27
6.2.5 Internal Events Hazards List.....	6-36
6.3 REFERENCES	6-37
6.3.1 Documents Cited.....	6-37
6.3.2 Codes, Standards, Regulations, and Procedures	6-38
APPENDIX 6A BIBLIOGRAPHY FOR DOCUMENTS POTENTIALLY RELEVANT TO EXTERNAL EVENTS HAZARDS ANALYSIS	6A-1

TABLES

	Page
6-1 Generic External Events	6-4
6-2 Example Summary of External Events Hazards Analysis Screening	6-11
6-3 Example External Events Hazards List.....	6-12
6-4 Example External Events Hazards Screened Out	6-12

ACRONYMS

CPB	Carrier Preparation Building
DC	disposal container
DPC	dual purpose canisters
EEHA	external events hazards analysis
EEHL	external events hazards list
HLW	high-level radioactive waste
LA	license application
LLW	low-level radioactive waste
PSA	preclosure safety analysis
SNF	spent nuclear fuel
SSCs	structures, systems, and components
WHB	Waste Handling Building
WP	waste package

6. HAZARDS ANALYSIS

6.1 EXTERNAL EVENTS HAZARDS ANALYSIS

This section presents details of the methodology for the external event hazards analysis (EEHA) and the internal event hazards analysis portions of the Preclosure Safety Analysis (PSA).

6.1.1 Introduction

This section describes a method for performing an EEHA as part of the PSA to support the license application (LA) submittal. The EEHA provides a systematic method to identify and screen hazards stemming from natural phenomena and man-made activities that have the potential for initiating repository preclosure event sequences. A generic and comprehensive list of potential hazards is compiled in the EEHA. Qualitative and quantitative screening analyses are applied to reduce the number of potential hazards. The output of the screening process is a list of potential external hazards that must be evaluated as part of the repository design process or subjected to further evaluation to determine the credibility of the hazard and its potential radiological consequences. This list is called the external events hazards list (EEHL).

This section presents the methodology for performing an EEHA. External hazards include natural phenomena and man-made activities and facilities that are beyond the direct control of repository operations. Such hazards include onsite construction activities that may be concurrent with waste receipt, waste handling, and storage operations. Section 6.2 describes the approach for performing a counterpart analysis of hazards that are internal to the repository operations.

6.1.2 Overview of Approach

The PSA is a risk-informed, performance-based approach. As such, its purpose is to address these three questions:

1. What can happen? (What event sequences are possible?)
2. How likely is it? (What is the probability or frequency of the event sequence?)
3. What are the consequences? (What are the radiological releases and exposures? Intermediate consequences may be addressed to synthesize potential event sequences.)

This approach is similar to the methods used for Process Hazards Analysis, as described in *Guidelines for Hazard Evaluation Procedures* (AIChE 1992).

The first question is applied in the EEHA to hazards that are potential initiating events for radiological release event sequences. The “what” is defined at the first level by a list of generic events. The possibility of initiating an event sequence having radiological consequences (the third question) is implicit, but is not addressed initially. Instead, the EEHA addresses the second question (How likely is it?) to determine if a given hazard is a credible preclosure repository initiating event. A knowledge of the site characteristics is required to answer this question.

Potential intermediate consequence of the event sequences are considered to the extent that the direct consequences of an event sequence (e.g., landslide) could interact with the repository operational processes to induce a radiological release. A knowledge of the repository operations and the locations of radioactive material, as well as a conceptual layout of the facility, are required to determine the potential vulnerabilities to the respective external hazards. If a hazard category can be eliminated (screened out) it will not be necessary to consider potential event sequences, radiological consequences, or design solutions to withstand the hazard.

Screening Criteria—The question “How likely is it?” is addressed by performing the following series of qualitative and quantitative screening evaluations to determine whether or not:

1. The potential hazard exists at the repository site
2. The rate of the physical process of the hazard can produce sensible effects during the repository preclosure period (i.e., up to 325 years)
3. The consequences of the hazard are significant enough to affect operations or storage during the preclosure period
4. The event frequency is greater than 1×10^{-6} events per year.

The criteria are addressed sequentially so that when the answer to the query is negative, the analysis stops and the hazard is screened out and will not appear in the external events hazard list.

Documented rationale must be provided to support every response to the criteria. Such documentation must be in accordance with established procedures for documentation and categorization of data, if applicable.

Responses to the first, second, and fourth criteria are independent of the facility design. To the extent possible, the analysis should screen out those natural phenomena that are known to be impossible or non-existent in the region (e.g., ocean-front hazards such as a tsunami). The removal of these types of hazards may be accomplished through either a pre-screening to remove events from the (global) generic list of hazards or through the application of the same logic formally and repeatedly in the evaluation. In this guide, the latter method is used in the examples. Care must be taken to not screen out natural phenomena that may have site-specific applicability, such as flooding. Responses to the third criteria should be largely independent of the facility design. However, major changes in facility structures and operational concepts should be examined in light of the third screening criteria.

The product of this analysis is the EEHL, which contains the potentially credible external hazards that cannot be screened out. The hazards listed, however, will be categorized according to future actions and commitments. The hazards will be categorized according to the following criteria:

1. **Design Basis**—The hazard is included in the 10 CFR 63.2 design bases for preclosure safety (e.g., the requirements for items important to safety to withstand the specific natural phenomena).

2. **Analysis Required**—The hazard cannot be screened out without additional or corroborative analyses; the EEHL will be updated as such analyses are completed, with credible hazards re-categorized as initiating events for event sequences.

For ease of review, a companion table will list the hazards removed through the screening process and a summary statement detailing the basis for the removal.

6.1.3 Details of Basic Approach to Screening with Examples

This section illustrates the process for performing an EEHA through the application of the screening criteria previously discussed to a generic list of repository external hazards. The approach consists of the following steps:

1. Compile a comprehensive list of external hazards (natural phenomena and man-made) from generic sources (e.g., AIChE 1992).
2. Acquire information on the site and facility.
3. Apply the screening criteria, supported by analyses, where appropriate.
4. Produce a list of external hazards subject to design solutions (i.e., become event sequences) or to further analyses (e.g., event sequence modeling or consequence analysis).

The following subsections describe each of these steps.

6.1.3.1 Generic Events Checklist

The analysis begins with the development of a comprehensive list of events that could impact the repository operations areas and initiate an event sequence that results in a radioactive material release. The generic list is not project-specific, but provides a starting point for the systematic approach that is intended to identify potentially hazardous external events. The generic hazards list (Table 6-1) was synthesized from lists of external hazards developed by others (AIChE 1992). Its intent is to provide the most comprehensive list to ensure a thorough treatment of possible hazards. Should other potential external hazards be identified in the course of supporting LA submittal, these hazards should be subjected to the same screening analysis methodology and criteria as the generic hazards.

An event is considered a potential initiator of a radiological event sequence if, and only if, all of the screening criteria presented in Section 6.1.2 are determined to be applicable.

Table 6-1. Generic External Events

External Category	Hazard	Definition	Potential Concern for Preclosure Safety
1	Aircraft crash	Accidental impact of an aircraft on the site.	Penetration or loss of confinement of radioactivity; compounded by concurrent fire
2	Avalanche	A large mass of snow, ice, soil, or rock, or mixtures of these materials, falling, sliding, or flowing under the force of gravity.	Blockage of North Portal, burying of waste package transporter, collapse or distortion of structures housing radioactivity, disruption of electric power
3	Coastal erosion	The wearing away of soil and rock by waves and tidal action (see Erosion).	Not applicable
4	Dam failure	Failure of a large man-made barrier that creates and restrains a large body of water.	If possible, could invade surface structures, wash out bridges supporting waste transporter, disrupt power.
5	Debris avalanching	The sudden and rapid movement of debris (soil, vegetation and weathered rock) down steep slopes resulting from intensive rainfall.	Similar to Avalanche
6	Denudation	The sum of the processes that result in the wearing away or the progressive lowering of the surface of the earth by weathering, mass wasting, and transportation.	[And, so onanalyst to identify issues related to Preclosure Safety]
7	Dissolution	A process of chemical weathering by which mineral and rock material passes into solution.	
8	Eperogenic displacement	Geomorphic processes of uplift and subsidence that have produced the broader features of the continents and oceans.	
9	Erosion	The slow wearing-away of soil and rock by weathering, mass wasting, and the action of streams (denudation), glaciers, waves, wind.	
10	Extreme wind	Wind is a meteorological term for air that moves parallel to the surface of the earth. Extreme wind conditions for nuclear plants are defined in NUREG-0800 (NRC 1987) and ASCE 7-98 (ASCE 2000).	
11	Extreme weather fluctuations	Various types of weather fluctuations that exceed expected operational ranges of repository processes.	
12	Range fire	The combustion of natural vegetation external to the repository that propagates to combustible materials within the repository operations area.	
13	Flooding (storm, river diversion)	The covering or causing to be covered with water.	

Table 6-1. Generic External Events (Continued)

External Category	Hazard	Definition	Potential Concern for Preclosure Safety
14	Fungus, bacteria, and algae	Fungus and bacteria are part of a general class of microorganisms that may be present in the subsurface environment. Algae are aquatic plants that may be present in spent fuel storage and staging water-filled pools.	
15	Glacial erosion	Reduction of the surface of the earth as a result of grinding and scouring by glacier ice armed with rock fragments.	
16	Glaciation	The formation, movement, and recession of glaciers or ice sheets.	
17	High Lake Level	Any inland body of standing water occupying a depression in the surface of the earth, generally of appreciable size and too deep to permit vegetation to take root completely across the expanse of water with potential for overflow or flooding.	
18	High Tide	Tides are the rhythmic, alternate rise and fall of the surface of the ocean, and bodies of water connected with the ocean with the potential for flooding inland areas.	
19	High river stage	A river is a natural freshwater permanent or seasonal surface stream of considerable volume with a potential for flooding	
20	Hurricane	An intense cyclone that forms over the tropical oceans and ranges 100 to 1000 km in diameter.	
21	Inadvertent future intrusions (man-made)	Man-made inadvertent future intrusions with regard to the 100-year operational period involving undetected surface access into repository facilities.	
22	Industrial activity induced accident	An accident resulting from industrial or transportation activities unrelated to the repository.	
23	Intentional future intrusions (man-made)	Man-made intentional future intrusions with regard to preclosure involving undetected surface access or sabotage to repository facilities. Sabotage may also include events such as bombings and missile attacks.	
24	Landslides	A general term covering a wide variety of mass-movement land forms and processes involving the downslope transport, under gravitational influence, of soil and rock material.	
25	Lightning	The flashing of light produced by a discharge of atmospheric electricity between an electrically charged cloud and the earth.	
26	Loss of offsite or onsite power	The loss of electrical power either generated or controlled by persons outside of the repository site or a loss of power within the repository.	

Table 6-1. Generic External Events (Continued)

External Category	Hazard	Definition	Potential Concern for Preclosure Safety
27	Low lake level	A lake is any inland body of standing water occupying a depression in the surface of the earth, generally of appreciable size and too deep to permit surface vegetation to take root completely across the expanse of water where the lake level must be maintained for cooling purposes.	
28	Low river level	A river is a natural freshwater permanent or seasonal surface stream of considerable volume where river level must be maintained for cooling purposes.	
29	Meteorite impact	The impact of any meteoroid that has reached the surface of the earth without being completely vaporized.	
30	Military activity induced accident	An accident resulting from military activities on the Nevada Test Site or Nellis Air Force Range.	
31	Orogenic Diastrophism	Movement of the crust of the earth produced by tectonic processes in which structures within fold-belt mountainous areas were formed, including thrusting, folding, and faulting.	
32	Pipeline accident	Industrial pipeline containing hazardous materials (e.g., oil and gas).	
33	Rainstorm	A rainstorm of concern is one that produces the 100-year or greater maximum rainfall rate occurring for one day.	
34	Sandstorm	Extreme wind capable of transporting sand and other unconsolidated surficial materials.	
35	Sedimentation	The process of forming or accumulating sediment (solid fragmental material that originates from weathering of rocks) in layers.	
36	Seiche	A free or standing-wave oscillation of the surface of water in an enclosed or semi-enclosed basin (as a lake, bay, or harbor).	
37	Seismic activity, uplifting (tectonic)	A structurally high area in the crust, produced by positive movements over a long period of time that result in faults giving rise to the upthrust of rocks.	
38	Seismic activity, earthquake	Pertaining to earthquake or earth vibrations, including those that are artificially induced.	
39	Seismic activity, surface fault displacement	A fracture or a zone of fractures along which there is potential for displacement of the sides relative to one another parallel to the fracture.	
40	Seismic activity, subsurface fault displacement	A fracture or a zone of fractures along which there is potential for displacement of the sides relative to one another parallel to the fracture.	

Table 6-1. Generic External Events (Continued)

External Category	Hazard	Definition	Potential Concern for Preclosure Safety
41	Static Fracturing	Any break in a rock due to mechanical failure by stress (includes cracks, joints, and faults).	
42	Stream Erosion	The progressive removal, by a stream, of bedrock, overburden, soil, or other exposed matter, from the surface of its channel.	
43	Subsidence	The sudden sinking or gradual downward settling of the surface of the earth with little or no horizontal motion.	
44	Tomado	A small-scale cyclone generally less than 500 m in diameter and with very strong winds. Intense thunderstorms that are present in the desert southwest have the capability of producing tornadoes.	
45	Tsunami	A gravitational sea wave produced by a large-scale, short-duration disturbance on the ocean floor. Wave heights of up to 30 m may impact coastal regions.	
46	Undetected past intrusions (man-made)	Past intrusions involve mining activities where deep shafts, drill holes, or tunnels may have been excavated.	
47	Undetected Geologic features	Geologic features of concern to the 100-year operational period include natural event such as faults and volcanoes.	
48	Undetected Geologic processes	Geologic processes of concern to the 100-year operational period include natural events such as erosion, tectonic and seismic processes.	
49	Volcanic Eruption	The process by which magma and its associated gases rise into the crust and are extruded onto the surface of the earth and into the atmosphere.	
50	Volcanism, intrusive magmatic activity	The development and movement of magma and mobile rock material underground.	
51	Volcanism, ashflow (extrusive magmatic activity)	A highly heated mixture of volcanic gases, magma, mobile rock material, and ash traveling down the flank of a volcano or along the surface of the ground (silacic volcanism).	
52	Volcanism, ashfall	Airborne volcanic ash falling from an eruption cloud.	
53	Waves (aquatic)	An oscillatory movement of water manifested by alternating rise and fall of the water surface.	

6.1.3.2 General Description of the Repository Site

A site description should be prepared to establish a basis for screening natural phenomena. Section 5 of this guide provides guidance for gathering site-related information to support the EEHA (and the PSA). The EEHA analysts should advise the preparer of the PSA site description of the particular needs and degree of detail required to support the EEHA screening process. A summary of the relevant site description information should be provided in the EEHA documentation.

The site description should include summaries of pertinent information concerning site:

- Geography
- Demography
- Meteorology
- Hydrology
- Geology
- Nearby facilities (industrial and military)
- Transportation routes (public, industrial, and military).

An example of a site description summary is:

Yucca Mountain is located in southern Nevada approximately 100 miles (160 km) northwest of Las Vegas. The mountain is an irregularly shaped volcanic upland varying in elevation at its crest from 1,500 m to 1,930 m (4,921 ft to 6,332 ft) and characterized by approximately 650 m (2,132 ft) of relief. The area surrounding the site includes Nye, Lincoln, Esmeralda, and Clark counties in Nevada and Inyo County in California. The site occupies land controlled by three federal agencies: the U.S. Air Force (Nellis Air Force Range), DOE (Nevada Test Site), and the U.S. Bureau of Land Management (BLM). Nearly all the area surrounding Yucca Mountain is federally owned, and very little is developed or urban land. A large percentage of the land around Yucca Mountain is anticipated to remain federally owned or withheld from public use in the future.

The description should be as complete as necessary to support the PSA and the EEHA. Similarly, the description might continue with a summary of climatological and meteorological characteristics of the region and site to establish perspective for the screening analysis descriptions.

6.1.3.3 General Description of the Repository Facilities

The EEHA should provide a brief summary of the repository operational areas that are potentially vulnerable to external event hazards. This summary can be simplistic in describing the types and locations of radioactive materials (and operations involving those materials) that could be potentially vulnerable to a credible external event. This summary and the associated assumptions establish a portion of the bases for the evaluation of external hazards.

6.1.3.4 Application of Screening Criteria

A generic list of external hazards is presented in Table 6-1 with definitions sufficient to establish the potential impact on the repository based on site and facility descriptions. The screening criteria previously discussed can be applied sequentially with supporting rationale. Whenever the response to any criterion is negative, the analysis of that hazard ceases. Therefore, the rationale for negative responses must be defensible. As appropriate, qualitative arguments or calculations are provided to support the negative response. If the rationale is affected by a design-specific or site-specific assumption or condition, the rationale must document the source of the assumption or condition according to the procedures for documenting quality-affecting work.

If a hazard cannot be screened out through the application of screening criteria, it is retained on the EEHL for further disposition, either by including the hazard in the facility design criteria or by recommending the initiation of additional analyses of frequency or potential impact (consequences).

For clarity of presentation and to ensure completeness, the EEHA should be documented in a standard format to indicate the response to each criterion and to provide the supporting rationale, even if the rationale seems obvious. The analysis will establish a definition, establish the required conditions, will perform an evaluation, and will determine the applicability of each generic external event. The following format is used in Section 6.1.3.5 to document the screening analysis of each external event:

Definition—Establishes the explanation of the event to be analyzed.

Required Condition—State what has to occur for the event or events to exist and result in a potential release of radioactive material or exposure to radioactivity.

Evaluation—States what must occur for the event to be considered a potential initiator of a radiological release or exposure during the preclosure period.

Applicability—States the conclusion of the screening (i.e., whether the hazard is or is not applicable to the repository preclosure period).

If all of the above statements are applicable for any external event, then the event is considered applicable to the hazards list for the repository. If any statement is indeterminate (its validity cannot be determined at this time) then the hazard is not eliminated through the screening process.

If, for any external event, any one of the above statements is not applicable, then the event is not considered applicable to the hazards list for the repository and all the statements that follow are not applicable.

The following subsection provides several examples of application of the EEHA screening process that include various types of hazards and applications of the criteria. An event is considered to be a potential initiator of a radiological release event sequence if, and only if, all of the screening criteria presented in Section 6.1.2 are determined to be applicable.

The following notes provide conditions to be considered for the consideration of the criteria.

1. The potential hazard exists and is applicable to the repository site.

NOTE: If the event cannot exist in the Yucca Mountain region, e.g., because it pertains to an ocean or near-ocean phenomenon, then the statement is labeled as False. Similarly, if the event pertains to features that must exist in the immediate vicinity of the repository site to be considered a hazard, but do not actually exist at or near the repository, then the statement is also labeled as False.

2. The rate of the physical process of the hazard can produce sensible effects during the repository preclosure period (i.e., up to 325 years).

NOTE: Long-term phenomena are defined as those that require thousands of years for perceptible changes to take place. Potential hazards including Erosion, Glaciation, Glacial Erosion, Orogenic Diastrophism, Sedimentation, Seismic Activity Uplifting [Tectonic], and Stream Erosion are such phenomena. These phenomena are not applicable to the repository during the preclosure period even if it is extended to 325 years. Although supporting information may be included, the information is not required for disposition of the phenomena.

3. The consequences of the hazard are significant enough to affect operations or storage during the preclosure period.

NOTE: The response to this criterion must consider the characteristics of the repository operations that are potentially vulnerable to a release of, or exposure to, radioactivity as a consequence of the hazard interacting with the facility. This evaluation requires knowledge of the design of the facility, including the intended operations where radioactive material or potential fissile material are to be handled or stored. The facility information described in Section 5 of this guide is summarized in Section 6.1.3.3. This evaluation applies analysis elements similar to a "what if?" analysis or a Failure Modes and Effects Analysis to determine the manner in which direct or indirect consequences of the external hazards could potentially interact with the facility.

4. The event frequency is greater than 1×10^{-6} events per year.

NOTE: The event cutoff frequency of 1×10^{-6} events per year is based on a 100-year operational period. This screening criterion is stated in 10 CFR Part 63 as a chance of one in 10,000 in the period before permanent closure. If a different time period is appropriate (e.g., 30 years for surface operations or 325 years for preclosure subsurface operations and storage), then the frequency screening criteria will be adjusted appropriately to the hazard and the potentially vulnerable operations area.

The following subsection provides examples of how the screening analysis is applied to a range of hazard types.

6.1.3.5 Examples of Application of Screening Criteria

The following subsections are presented in a format that can be used to document the external event hazards screening process. The formatted material may be presented in a table if preferred.

These examples were selected from a previous EEHA (CRWMS M&O 1999) to include several various types of hazards and to represent the application of each of the primary screening criteria. Table 6-2 summarizes the application of the screening process for these examples. Table 6-3 illustrates the EEHL, which is the principal product of the EEHA. Table 6-4 lists the hazards that have been eliminated through the screening process.

Table 6-2. Example Summary of External Events Hazards Analysis Screening

External Hazard Name	Summary of Screening				
	1. Potential exists and the event is applicable to the repository site.	2. The rate of the hazard process is sufficient to affect the 100-year operational period.	3. Sensible consequences of the hazard are large enough to affect operations or storage during the preclosure period.	4. The event frequency is greater than 10^{-6} events per year.	Applicability (Included in EEHL?)
Aircraft crash	TRUE	TRUE	TRUE	TRUE	YES
Avalanche	FALSE	NA	NA	NA	NO
Coastal Erosion	FALSE	NA	NA	NA	NO
Dam Failure	FALSE	NA	NA	NA	NO
Eperogenic Displacement	TRUE	FALSE	NA	NA	NO
Extreme Wind	TRUE	TRUE	TRUE	TRUE	YES
Range Fire	TRUE	TRUE	TRUE	TRUE	YES
Inadvertent future intrusions (man-made)	TRUE	TRUE	TRUE	TRUE	YES
Loss of offsite or onsite power	TRUE	TRUE	TRUE	TRUE	YES
Meteorite Impact	TRUE	TRUE	TRUE	FALSE	NO
Seismic activity, earthquake	TRUE	TRUE	TRUE	TRUE	YES

NOTE: NA = Not applicable

Table 6-3. Example External Events Hazards List

External Hazard Name	Comments
Loss of offsite or onsite power	Design bases to mitigate release
Seismic activity, earthquake	Design bases to mitigate release
Aircraft crash	Probabilistic analysis required
Extreme Wind	Group with wind/tornado
Range Fire	Group with other fire analyses
Inadvertent future intrusions (man-made)	Additional analysis required

Table 6-4. Example External Events Hazards Screened Out

External Hazard Name	Principal Basis for Screening Out
Avalanche	1. Not present at site
Coastal Erosion	1. Not present at site
Dam Failure	1. Not present at site
Eperogenic Displacement	2. Process too slow to affect preclosure
Meteorite Impact	4. Frequency below 1×10^{-6} per year

External Hazard 1, Aircraft Crash

Definition—Accidental impact of an aircraft on the site.

Required Condition—Periodic presence of aircraft over or near the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—The statement is true because of the potential for commercial aircraft overflights and the proximity of the repository site to the flight path of military aircraft flying from Nellis Air Force Base to their practice range (CRWMS M&O 1999).

2. The rate of the process of the hazard is sufficient to affect the 100-year operational period. TRUE.

Rationale—The effect of an aircraft crash is immediate.

3. The consequences of the hazard are significant enough to affect operations or storage during the preclosure period. TRUE.

Rationale—Potential effects of aircraft crash are readily identified as potential direct impact on radioactive waste and an indirect impact on safety-related structures, as well as a source of fire initiation. If deemed necessary, available evidence or analyses can be referenced. For example, a prior EEHA (CRWMS M&O 1999) referred to an analysis of the potential consequences that was performed in 1990.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—Insufficient evidence exists to support a negative response without detailed analyses. Furthermore, the response to this criterion is subject to change if there are changes in site layout, site usage, or frequency and types of aircraft in the vicinity.

Applicability—Yes. This event is applicable to the EEHL for the repository site.

External Hazard 2, Avalanche

Definition—A large mass of snow, ice, soil, or rock, or mixtures of these materials, falling, sliding, or flowing under the force of gravity.

Required Condition—Steeply sloped terrain found in high mountain ranges must exist.

Evaluation—

1. Potential exists and is applicable to the repository site. FALSE.

Rationale—The required condition (high mountain ranges) does not exist. Therefore, it is not applicable on this basis alone.

It is also noteworthy that temperature and precipitation levels at the repository site do not support the build-up of large masses of snow, ice, or soil required to produce an avalanche (except, potentially, a debris avalanche). If deemed necessary, references may be provided to justify that historical evidence for temperatures and precipitation preclude this event.

Criteria 2 through 4 are not applicable because the analysis stops with first not applicable evaluation.

Applicability—No. This event is not applicable to the EEHL for the repository site.

External Hazard 3, Coastal Erosion

Definition—The wearing away of soil and rock by waves and tidal action (see Erosion).

Required Condition—A coastline must exist at the site.

Evaluation—

1. Potential exists and is applicable to the repository site. FALSE.

Rationale—This event requires a coastline, which does not exist at the repository; therefore, the event is eliminated from further consideration.

Criteria 2 through 4 are not applicable because the analysis stops with first negative evaluation.

Applicability—No. This event is not applicable to the EEHL for the Yucca Mountain site.

External Hazard 4, Dam Failure

Definition—Failure of a large man-made barrier that creates and restrains a large body of water.

Required Condition—A dam must exist in the vicinity of the site.

Evaluation—

1. Potential exists and is applicable to the repository site. FALSE.

Rationale—This event requires a dam of sufficient size and proximity to the repository site. Since the required condition does not exist in the vicinity of the repository site, this event is eliminated from further consideration.

Criteria 2 through 4 are not applicable because the analysis stops with first negative evaluation.

Applicability—No. This event is not applicable to the EEHL for the repository site.

External Hazard 8, Eperogenic Displacement (see Subsidence)

Definition—Geomorphic processes of uplift and subsidence that have produced the broader features of the continents and oceans.

Required Condition—Geomorphic processes must exist at the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—Cannot exclude geomorphic processes that are ubiquitous (see 2, below).

2. The rate of the process is sufficient to affect the 100-year operational period. FALSE.

Rationale—This event is defined as a long-term geologic process. Therefore, this phenomenon is not applicable to the repository during the preclosure operational period (approximately 325 years or less).

Criteria 3 and 4 are not applicable since analysis stops with first negative evaluation.

Applicability—No. This event is not applicable to the EEHL for the repository site.

External Hazard 10, Extreme Wind

Definition—Wind is a meteorological term for that component of air that moves parallel to the surface of the earth. In the *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants* (NRC 1987, Sections 2.3.1, 3.3.1, and 4.3) it is stated that the 100-year return period “fastest mile of wind” including vertical velocity

distribution and gust factor should be used and be based on the standard published by the American National Standards Institute with suitable corrections for local conditions. The current standard published by the American National Standards Institute is ANSI/ASCE 7-98, *Minimum Design Loads for Buildings and other Structures* (ASCE 7-98 2000, Section 4.3). The basic wind speed is defined as a 3 second gust with annual probability of 0.02 of being equaled or exceeded (for a 50 year mean recurrence interval) (ASCE 7-98 2000, p. 13).

Required Condition—Meteorological conditions conducive to wind generation must exist at the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—Extreme winds do occasionally occur in southern Nevada (Eglington and Dreicer 1984, Coats and Murray 1985), making this event applicable for consideration during the 100-year operational period.

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—The impact is immediate. Wind effects could initiate event sequences and cause collapse or failure of SSCs that house radioactive materials.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—Wind effects could initiate event sequences and cause collapse or failure of SSCs that house radioactive materials. However, without engineering analyses, this statement is viewed as indeterminate. Since the response to this criterion is indeterminate (i.e., its validity cannot be determined at this time), it is treated as equivalent to TRUE.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—Some credible extreme wind conditions exist for all sites. The design basis determination will establish the wind parameters for the repository facilities.

Applicability—Yes. This event is not applicable to the EEHL for the repository site.

External Hazard 12, Fire (Range)

Definition—The combustion of natural vegetation external to the repository that propagates to combustible materials within the repository operations area.

Required Condition—Combustible materials must exist on the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—Since vegetation is present and at least one source of range fires (see Lightning) then range fires are possible.

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—The impact is immediate. Range fire effects could initiate event sequences and cause failures of SSCs that house radioactive materials.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—Range fire effects could initiate event sequences and cause failures of SSCs that house radioactive materials. However, without engineering analyses of range fire hazards and system vulnerabilities, the response to this criterion is indeterminate. Since the response is indeterminate (i.e., its validity cannot be determined at this time), it is treated as equivalent to TRUE.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—Although it may be judged that the occurrence of range fires in the region is credible, additional engineering analyses are required to determine the credibility of range fires severe enough to impact the SSCs of the surface facilities. Since the response to this criterion is indeterminate (its validity cannot be determined at this time) it is treated as equivalent to true.

Applicability—Yes.

External Hazard 21, Inadvertent Future Intrusions (Man-Made)

Definition—Man-made inadvertent future intrusions (with regard to the 100-year operational period) involve undetected surface access into repository facilities.

Required Condition—Potential for human access to surface facilities must exist.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—The site borders the Nevada Test Site and highways exist in the area.

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—The effects of an intrusion could be immediate with respect to initiating an event (e.g., loss of offsite power). This event may include intrusion into an area that contains radioactive material. However, engineering and safeguard analyses are required to identify specific vulnerabilities. Therefore, the response to this criterion is indeterminate (its validity cannot be determined at this time), so it is treated as equivalent to TRUE.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—The effects of an intrusion could lead to an initiating event (e.g., loss of offsite power) or human exposure to radioactive material. However, engineering and safeguard analyses are required to identify specific vulnerabilities. Therefore, the response to this criterion is indeterminate (its validity cannot be determined at this time), and it is treated as equivalent to TRUE.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—Without a supporting safeguards analysis to state the contrary, the response to this criterion is indeterminate (its validity cannot be determined at this time), and it is treated as equivalent to TRUE.

Applicability—Yes. This event is applicable to the EEHL for the repository site.

External Hazard 26, Loss of Offsite or Onsite Power

Definition—This event includes the loss of electrical power either generated or controlled by persons outside the repository site as well as a loss of power within the repository.

Required Condition—The need and provision for electrical power at the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—The repository operations will rely primarily on offsite power from a commercial grid. Such grids are vulnerable to outages from many causes. As appropriate to sustain required safety functions, onsite power supplies will be provided for selected SSCs important to safety.

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—The impact is immediate. Loss of power effects could initiate event sequences.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—Loss of power effects could initiate event sequences. Design bases and event sequence analyses are required to evaluate this event. Because this statement is indeterminate (its validity cannot be determined at this time), the statement is treated as equivalent to true.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—The rate of occurrence of a loss of offsite power is known to be on the order of 0.1 per year for nuclear plants. Site-specific analysis is required for the repository offsite power supply reliability and design-specific reliability analysis of onsite safety-related power supplies are required as well. Because the response to this criterion is indeterminate (its validity cannot be determined at this time), it is treated as equivalent to TRUE.

Applicability—Yes. This event is applicable to the EEHL for the repository site.

External Hazard 29, Meteorite Impact

Definition—The impact of any meteoroid that has reached the surface of the earth without being completely vaporized.

Required Condition—Potential meteorite impact at the site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—Meteorites fall randomly throughout the surface of the earth (Solomon et al. 1975, p. 69).

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—Because this statement is indeterminate (its validity cannot be determined at this time) then the statement is treated as equivalent to TRUE.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—Because this statement is indeterminate (its validity cannot be determined at this time) then the statement is treated as equivalent to TRUE.

4. The event frequency is greater than 1×10^{-6} events per year. FALSE.

Rationale—A screening analysis has been performed. Areal strike frequency data was obtained (Solomon et al. 1975, Table 1, Column 5): the sum of the probabilities greater than one pound (> 0.001 ton) is approximately 1.5×10^{-8} per year per 105 ft² area. The facility footprint was conservatively estimated to be 624,235 ft² and

assumed to be vulnerable to release of radioactivity given a meteorite greater than one pound. The probability of impact on the repository footprint area is estimated to be 9.36×10^{-8} per year ($6.24 \times 1.5 \times 10^{-8}$). The 624,235-ft² footprint-area is conservative because all of the area is not completely filled with waste forms. The area would have to be ten times larger to increase the frequency to greater than 1×10^{-6} per year. Even during peak years, only a fraction of the area will be occupied by waste forms. Therefore, meteorite impact is not considered credible for consideration during the 100-year operational period. Other supporting rationale may be provided, such as noting that the American Nuclear Society guidelines for external hazards at nuclear plants also states that the probability of meteorite impact is less than 1×10^{-6} per year (ANSI/ANS-2.12-1978).

The bases for such quantitative screening analyses, such as meteorite areal strike frequency and site vulnerable area, must be documented as inputs or assumptions.

Applicability—No. This event is not applicable to the EEHL for the repository site.

External Hazard 38, Seismic Activity, Earthquake

Definition—This event pertains to earthquake or earth vibrations, including those that are artificially induced.

Required Condition—Natural seismic activity or man-induced events such as weapons testing on Nevada Test Site.

Evaluation—

1. Potential exists and is applicable to the repository site. TRUE.

Rationale—Earthquakes have occurred as recently as 1993 in the region (National Research Council 1995, p. 92), making this event applicable for consideration during the 100-year operational period. The *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain* (YMP 1997) describes the strategy for the 100-year operational period seismic design methodology. Note that nuclear weapon testing is no longer performed at the Nevada Test Site.

2. The rate of the hazard process is sufficient to affect the 100-year operational period. TRUE.

Rationale—The impact is immediate. Earthquake effects could initiate event sequences and cause collapse or failures of SSCs that house radioactive materials.

3. The consequences of the hazard are significant enough to affect the 100-year operational period. TRUE.

Rationale—Earthquake effects could initiate event sequences and cause collapse or failures of SSCs that house radioactive materials. Design criteria for selected SSCs will have to be defined to prevent adverse consequences. Without engineering

analyses, the response to this criterion is viewed as indeterminate and is treated as equivalent to TRUE.

4. The event frequency is greater than 1×10^{-6} events per year. TRUE.

Rationale—The repository will use mean annual probabilities of 1×10^{-3} and 1×10^{-4} as reference values in determining the frequency category 1 and frequency category 2 design basis vibratory ground motions (YMP 1997, p. iii). The SSCs important to safety will be designed to withstand a design basis earthquake (frequency category 1 or frequency category 2), as appropriate.

Applicability—Yes. This event is applicable to the EEHL for the repository site.

6.1.3.6 External Events Hazards List

The EEHA will summarize the process and the results. The EEHA process results in the EEHL. The EEHL is a listing of external hazards that will be addressed either as initiating events for event sequences, or otherwise dealt with. The EEHL will be accompanied by a summary table listing those events that have been eliminated for consideration through the screening process and a brief description of the principal basis for the elimination of the event.

Table 6-3 is an example of an EEHL using the examples presented in Section 6.1.3.5. The EEHL includes those events external to the control of repository operations that are potential candidates for initiating radiological event sequences during the preclosure (100-year) operational period.

In addition, the EEHA will provide a summary table of those hazards that were eliminated through the screening process, including a statement of the primary rationale for the elimination of the hazard. Table 6-4 illustrates these hazards, based on the examples in Section 6.1.3.5.

6.2 INTERNAL EVENTS HAZARDS ANALYSIS

6.2.1 Introduction

The purpose of this analysis is to identify and document the internal hazards and preliminary events as part of the PSA. Internal hazards are those hazards presented by operation of the facility and its associated processes. These hazards are in contrast to external hazards, which involve natural phenomena and external man-made hazards. The hazard analysis methodology used in this analysis provides a systematic means to identify facility hazards and associated event sequences that may result in adverse radiological consequences to the public and facility workers during the repository preclosure period. The events are documented in a preliminary internal event hazards list and are intended to be used as input to the repository initiating event selection process. It is expected that the results from this analysis will undergo further screening and analysis based on the criteria that apply to the performance of event sequence analyses for the preclosure period of repository operation. As the repository design progresses, this analysis will be reviewed to ensure that no new hazards are introduced and previously evaluated hazards have not increased in severity.

6.2.2 Overview of Basic Approach

This analysis is performed utilizing the hazard analysis methodologies described in the *System Safety Analysis Handbook* (Stephans and Talso, eds. 1997) and addresses the repository internal hazards and associated events that could result in radiological consequences to the public or facility workers during the preclosure period. The list of preliminary events is generated by applying a checklist of potential generic events (see Section 6.2.3.3) to each functional area within the repository. A description of the process steps is provided in the following sections.

6.2.2.1 Define Repository Functional Areas

To facilitate identification of repository hazards, the repository is divided into functional areas. These functional areas are defined by a specific function, physical boundaries of the facility, or both. Repository functional areas are listed in Section 6.2.3.1 and described in Section 6.2.4.

6.2.2.2 Define Repository Design Configuration and Operations

Following the definition of functional areas, facility design configuration and operations within those areas are established and documented prior to hazard identification activities. Functional area design configuration and operations are discussed in Sections 6.2.3.2 and 6.2.4.

6.2.2.3 Develop Generic Event Checklist

Once the repository functional areas, design configuration, and facility operations are defined, a list of generic internal events is developed that, if determined to be applicable, could result in adverse radiological consequences to the public or facility workers. This generic list is not project-specific and attempts to identify all potentially hazardous event sequences. A comprehensive list will ensure a thorough treatment of all possible events. The development of generic events will make maximum use of existing repository documents where similar work has been performed. A list of generic events is provided in Section 6.2.3.3.

6.2.2.4 Determine the Repository Applicability of Internal Events

This portion of the analysis includes a review of the repository functional areas, including facility design and operations, to determine the applicability of generic events that could potentially result in adverse radiological consequences.

Specific criteria will be developed for each of the generic events to support the applicability determination. If the criteria are satisfied, the generic event has the potential for adverse radiological consequence and specific preliminary events will then be identified. It should be noted that potential events producing adverse radiological consequences will not be identified in all functional areas.

A general review of previously performed safety evaluations of repository operations has been conducted to determine the preliminary events applicable to the repository. These evaluations included:

- *Preliminary Worst-Case Accident Analysis to Support the Conceptual Design of a Potential Repository in Tuff* (Jackson et al. 1984)
- *Site Characterization Plan Conceptual Design Report - Volume 4 Appendices F - O* (MacDougall et al. 1987)
- *Yucca Mountain Site Characterization Project Identification of Structures, Systems, and Components Important to Safety at the Potential Repository at Yucca Mountain* (Hartman and Miller 1991)
- *Preclosure Radiological Safety Analysis for Accident Conditions of the Potential Yucca Mountain Repository: Underground Facilities* (Ma et al. 1992)
- *Preclosure Radiological Safety Evaluation: Exploratory Studies Facility* (Schelling and Smith 1993).

The following approach should be used to document the analysis of preliminary events presented in Section 6.2.4.

- **Area Description**—Establishes the baseline description of the repository functional area. Information will be used to gain an understanding of the expected use of the area.
- **Generic Event Category Applicability**—Summarizes results from the applicability assessment for each of the following generic events:
 - Collision/Crushing
 - Chemical Contamination/Flooding
 - Explosion/Implosion
 - Fire
 - Radiation/Magnetic/Electrical/Fissile
 - Thermal.
- **Reference**—Identifies the source of the preliminary design data used to conduct the analysis.
- **Preliminary Events**—Identifies specific events based on the potential for interaction.

6.2.3 Approach for Evaluating Applicability of Generic Internal Events to Repository Functional Areas

The basic input used in the performance of this analysis consists of repository process and design information and includes system description documents, process flow diagrams, mechanical flow diagrams, and a conceptual description of repository operations. Additional design input to this analysis is described in the following sections.

6.2.3.1 Repository Functional Areas

The following functional areas have been defined to facilitate the identification of the repository hazards and events associated with preclosure operations. A description of each functional area is provided in Section 6.2.4.

- Waste Receipt and Carrier or Cask Transport
- Carrier Preparation
- Waste Handling - Carrier Bay
- Waste Handling - Canister Transfer
- Waste Handling - Assembly Transfer
- Waste Handling - Disposal Container Handling and Waste Package (WP) Remediation
- Subsurface Transport, Emplacement, and Monitoring
- Site-Generated Waste Treatment - Liquid LLW
- Site-Generated Waste Treatment - Solid LLW

6.2.3.2 Repository Design Configuration and Facility Operation

Prior to performing repository hazards analysis, facility design configuration and operations as well as the function of facility SSCs are established. This analysis is based upon the repository design and functions. A brief description of operations for each functional area is provided in Section 6.2.4.

6.2.3.3 Generic Internal Event Checklist

The development of the generic internal event checklist is based on the following hazard evaluation techniques:

- Energy Analysis (Stephans and Talso, eds. 1997, p. 3-77)
- Energy Trace Barrier Analysis (Stephans and Talso, eds. 1997, p. 3-79)
- Energy Trace Checklist (Stephans and Talso, eds. 1997, p. 3-85).

The generic list is based upon the lists provided in these three approaches that have been reorganized for convenience and applicability to repository preclosure operations. The resulting comprehensive checklist contains a series of questions for each generic hazard. Applicability to a functional area of design is determined by a positive response to all questions.

6.2.3.3.1 Collision/Crushing

A. Categories-

1. **Uncontrolled Mass/Force**-Examples include: excessive velocity or acceleration of mass, inadvertent operation of appendage, failure of primary or secondary structure, tumbling (or tipped-over) mass, uncontrolled robot, or uncontrolled fixed rotating equipment, falls, drops.

2. **Protrusions into Pathways**—Examples include: extended appendages, protruding structural elements, or improperly placed equipment.

B. **Applicability to Functional Area of Design**—

1. Is kinetic or potential energy present?
2. Can the kinetic or potential energy be released in an unplanned way?
3. Can the release of kinetic or potential energy interact with the waste form?

6.2.3.3.2 Chemical Contamination/Flooding (not normally a direct potential threat to the waste form—usually a contributing cause of another threat category)

A. **Categories**—

1. **Reactions**—Examples include: release of chemicals or materials that react with system materials causing system deterioration. The released materials could foster electrolytic, galvanic, or stress corrosion, or oxidation.
2. **Off-Gassing**—Example: release of volatile or condensable materials.
3. **Venting**—Examples include: leaking or venting of materials, gases, or liquids.
4. **Debris/Leaks**—Examples include: small loose or free parts, flaking, leaking fluids or flooding, or dirt and dust, oxidized materials (e.g., metal rust).
5. **Flooding**—Examples include: water, water leading to the potential for criticality.

B. **Applicability to Functional Area of Design**—

Category 1—Reactions:

1. Are corrosive or reactive chemicals or materials present?
2. Can these chemicals or materials be released?
3. Can the chemicals or materials interact with the waste form?

Category 2—Off-Gassing:

1. Are volatile or condensable materials present?
2. Can these materials be released?
3. Can these materials interact with the waste form?

Category 3–Venting:

1. Is there potential for venting materials in the area?
2. Can the materials interact with the waste form?

Category 4–Debris and Leaks:

1. Is there potential for debris or leaks in the area?
2. Can the debris or fluids interact with the waste form?

Category 5–Flooding:

1. Are sources of water present in the area?
2. Is there a potential to release the water?
3. Can the released water interact with the waste form with potential for criticality?

6.2.3.3.3 Explosion/Implosion (This event is normally accompanied by shrapnel or other high velocity debris.)

A. Categories–

1. **Pressure Energy Release**–Examples include: damage, failure, and rupture of pressurized containers or components and release of gases, or implosion of containers, vessels, or enclosed structural volume.
2. **Electrical Energy Release**–Examples include: faults, arcs, static charge, electrical component failure, battery overcharge or overdischarge, or out of phase source connection.
3. **Chemical Energy Release**–Examples include: chemical dissociation or reactions, fire internal to confined volumes, adiabatic detonation, or ignition of confined flammable gases.
4. **Mechanical Equipment**–For example: rotating equipment disintegration due to overspeed.

B. Applicability to Functional Area of Design–

1. Are pressure, electrical, chemical, or mechanical energy present?
2. Can an event occur that results in an explosion or implosion energy release?
3. Can the released energy impact the waste form directly?

6.2.3.3.4 Fire

Must have ignition, fuel, and oxidizer sources.

Ignition Sources—Examples include: electrical faults, shorts, arcs, chemical reactions, hot surfaces, small flames, or catalytic reaction (see Explosion/Implosion).

Fuel and Oxidizer Sources—Examples include: flammable materials (solids and liquids) and flammable atmospheres (gases), in addition to the presence of an oxidizing environment from ambient atmosphere or other chemical agents (see Contamination).

A. **Categories**—Not Applicable

B. **Applicability to Functional Area of Design**—

1. Are fuel, oxidizers, and ignition sources present?
2. Is there sufficient fuel and oxidizer to sustain fire?
3. Can fire interact with the waste form?

6.2.3.3.5 Radiation/Magnetic/Electrical/Fissile

A. **Categories**—

1. **Ionizing**—Examples include radioactive materials, x-rays, or high voltage radio frequency equipment.
2. **Non-Ionizing**—Examples include electromagnetic interference, radio frequency, or corona.
3. **Magnetic**—Examples include permanent magnets and electromagnetic devices.
4. **Nuclear Particles**—Examples include ion and electron beams or radioactive materials.
5. **Laser Light**—For example high energy laser beams and accompanying energy forms such as heat.
6. **Fissile Material**—Examples include uranium-233, uranium-235, and plutonium-239.

B. **Applicability to Functional Area of Design**—

1. Are radiation, magnetic, or electrical energy sources present external to the waste form? Is fissile material present?

2. Is a mechanism present to release radiation, magnetic, or electrical energy?
3. Can the release of radiation, magnetic, or electrical energy interact with the waste form?
4. Can fissile material be arranged in such a manner as to result in criticality?

6.2.3.3.6 Thermal (also see Fire)

A. Categories—

Heat—This category accommodates any thermal energy source with sufficient energy to have an impact on the waste form.

B. Applicability to Functional Area of Design—

1. Are external thermal energy sources present?
2. Can thermal energy be released?
3. Can the thermal energy affect the waste form?

6.2.4 Examples of Evaluating the Applicability of Generic Events to Repository Function Areas

6.2.4.1 Example 1: Waste Receipt and Carrier or Cask Transport

Area Description—Transportation casks containing spent nuclear fuel (SNF) and high-level radioactive waste (HLW) and associated carriers are received at the repository waste entry point or security gate. The SNF and HLW are contained in casks equipped with impact limiters and personnel barriers. At the security gate, the cask carrier and offsite prime mover are inspected for contraband, sabotage, and radioactive contamination. Following inspection, the offsite prime mover is decoupled and an onsite diesel-driven prime mover is used to transport the carrier or cask to the Carrier Preparation Building (CPB). Following preparation of the carrier or cask in the CPB, the system moves the carrier or cask to the carrier bay of the Waste Handling Building (WHB) for cask unloading.

This functional area is located on the surface at the north portal and consists of security inspection and radiation monitoring equipment, required road and rail systems, and onsite prime movers. The system also transports empty transportation casks and associated carriers from the WHB to the CPB for preparation and on to the repository security gate for dispatch from the site.

Generic Events Applicability—

Collision/Crushing—Yes

Chemical Contamination/Flooding—None identified

Explosion/Implosion—None identified

Fire—Yes - diesel fuel fire

Radiation/Magnetic/Electrical/Fissile–Yes - Radiation, Fissile
Thermal–Yes (see Fire)

Reference–Jackson et al. 1984, MacDougall et al. 1987, Hartman and Miller 1991, and applicable system description and design documents.

Preliminary Events–

Collision/Crushing–Cask collision, railcar derailment involving transportation cask, overturning of truck trailer involving transportation cask

Fire, Thermal–Diesel fuel fire

Radiation–Radiation exposure of facility worker

Fissile–Criticality associated with cask collision, railcar derailment, or overturned truck trailer and rearrangement of cask internals

6.2.4.2 Example 2: Carrier Preparation

Area Description–Transportation casks containing SNF and HLW and associated carriers are delivered to the CPB by the onsite diesel-driven prime mover. Within the CPB, carriers and casks are prepared for entering the carrier bay of the WHB. The primary operations include:

- Measure external carrier and cask radiation levels
- Remove and retract personnel barriers
- Inspect carriers and casks for radiation contamination
- Measure external cask temperature
- Remove and retract impact limiters.

The CPB material handling system also functions to prepare empty carriers and casks for dispatch from the repository. Specifically, the carriers and casks are inspected for radiation contamination and the impact limiters and personnel barriers are installed. The empty carriers and casks are removed from the CPB for dispatch by the offsite prime mover. The system performs these functions utilizing remotely operated cranes and manipulators; however, some local operator actions may be required.

Generic Events Applicability–

Collision/Crushing–Yes

Chemical Contamination/Flooding–None identified

Explosion/Implosion–None identified

Fire–Yes

Radiation/Magnetic/Electrical/Fissile–Yes, Radiation/Fissile

Thermal–Yes (see Fire).

Reference–Applicable system description and design documents.

Preliminary Events–

Collision/Crushing–Handling equipment drops on transportation cask, cask collision

Fire, Thermal–Diesel fuel fire

Radiation–Radiation exposure of facility worker

Fissile–Criticality associated with cask collision and rearrangement of cask internals.

6.2.4.3 Example 3: Waste Handling - Carrier Bay

Loaded transportation casks and associated carriers are transported from the CPB to the WHB carrier bay by the onsite diesel-driven prime mover (rail and road). Incoming carriers and casks are prepared for waste removal by upending the cask on the carrier, lifting the cask from the carrier and lowering the cask onto a cask transfer cart. The system also functions to load empty transportation casks and non-disposable canisters onto carriers for shipment from the repository. The system performs these functions utilizing remotely operated cranes and manipulators; however, some local operator actions may be required.

Generic Events Applicability–

Collision/Crushing–Yes

Chemical Contamination/Flooding–None identified

Explosion/Implosion–None identified

Fire–Yes

Radiation/Magnetic/Electrical/Fissile–Yes, Radiation/Fissile

Thermal–Yes (see Fire).

Reference–Applicable system description and design documents.

Preliminary Events–

Collision/Crushing–Transportation cask drop, transportation cask slap down, cask collision, isolation door closes on transportation cask, handling equipment drops on transportation cask

Fire, Thermal–Diesel fuel fire

Radiation–Radiation exposure of facility worker

Fissile–Criticality associated with cask collision or drop and rearrangement of cask internals.

6.2.4.4 Example 4: Waste Handling - Canister Transfer

Transportation casks containing large and small disposable canisters are transferred from the carrier bay to the canister transfer area by means of cask transfer carts. In the canister transfer area, canisters are unloaded from casks, stored as required, and loaded into disposal containers (DCs). Empty casks are also prepared for shipment from the repository. Cask unloading begins with cask inspection, sampling, and lid bolt removal operations. The cask lids are removed and

the canisters are unloaded. Small canisters are loaded directly into a DC, or are stored until enough canisters are available to fill a DC. Large canisters are loaded directly into a DC. Transportation casks and related components are decontaminated as required, and empty casks are prepared for shipment from the site.

Two independent and remotely operated canister transfer lines are provided in the WHB. The lines are operated independently to handle disposable canisters and load them into DCs. Each canister transfer line contains an airlock, cask preparation and decontamination area, and a canister transfer cell. Each cask preparation and decontamination area includes a cask preparation station and a cask decontamination station. Remote handling equipment consists of cask transfer carts, cask preparation manipulators, and equipment required to perform sampling, cask unbolting, lid removal, and decontamination. The canister transfer cells include a canister transfer station and DC transfer cart supported by remote handling equipment including a bridge crane (sized to handle the largest canisters), DC loading manipulator, and an array of large and small canister lifting fixtures. A canister staging rack is provided for the accumulation of small canisters in a shielded area.

Generic Events Applicability--

Collision/Crushing--Yes

Chemical Contamination/Flooding--None identified

Explosion/Implosion--None identified

Fire--None identified

Radiation/Magnetic/Electrical/Fissile--Yes, Radiation/Fissile

Thermal--None identified.

Reference--Applicable system description and design documents.

Preliminary Events--

Collision/Crushing--Transportation cask slapdown, DC slapdown, canister drop, canister slap down, canister collision, canister drops onto DC, canister drop on sharp object, canister drop onto another canister at small canister staging rack, shield door closes on transportation cask, shield door closes on DC, handling equipment drops on transportation cask, canister or DC

Radiation--Radiation exposure of facility worker

Fissile--Criticality associated with small canister staging rack, criticality associated with collision or drop of casks or canisters, and rearrangement of container internals.

6.2.4.5 Example 5: Waste Handling - Assembly Transfer

Area Description--Transportation casks containing uncanistered spent nuclear fuel (SNF) assemblies or Dual Purpose Canisters (DPCs) are transferred from the carrier bay to the assembly transfer area by means of cask transfer carts. Casks are lifted from the transfer cart and placed into a cask preparation pit. The cask interiors are sampled for radioactivity, vented, cooled down with compressed gas, and then filled with water. The cask lid bolts are then

detensioned and removed. The cask is lifted and placed in the cask unload pool, where the cask lid is removed and the assemblies are removed and placed directly into a transfer cart or a staging rack. Assemblies contained in a DPC involve the additional steps of removing the DPC from the cask and DPC opening prior to assembly removal. Following assembly removal, empty transportation casks and DPCs are removed from the pool and prepared for dispatch from the repository site.

Following removal from the cask or DPC, the SNF assemblies are transferred to the assembly cell (either directly or from the staging rack) by an inclined transfer cart. In the assembly cell, the SNF assemblies are placed in the assembly drying station for water removal and then transferred to DC. The DC is then fitted with a temporary seal, decontaminated, evacuated, and backfilled with nitrogen and moved to the DC cell for lid welding.

The system utilizes remotely operated equipment to perform these functions including, a bare fuel assembly transfer machine, fuel assembly grapples, container transfer carts, contamination barriers, inspection instruments, and low-level radioactive waste (LLW) removal subsystems.

Generic Events Applicability--

Collision/Crushing--Yes

Chemical Contamination/Flooding--Yes, Flooding

Explosion/Implosion--None identified

Fire--Yes

Radiation/Magnetic/Electrical/Fissile--Yes, Radiation/Fissile

Thermal--Yes.

Reference--Applicable system description and design documents.

Preliminary Events--

Collision/Crushing--Transportation cask drop, transportation cask slap down, cask collision, SNF assembly drop onto pool floor, SNF assembly drop onto SNF assembly staging rack, SNF assembly drop onto assembly cell floor, SNF assembly drop onto assembly dryer, SNF assembly drop onto DC, SNF assembly collision, loaded SNF assembly basket drop onto pool floor, loaded SNF assembly basket drop onto SNF assembly staging rack, loaded SNF assembly basket drop onto assembly cell floor, loaded SNF assembly basket drop onto assembly dryer, loaded SNF assembly basket collision, uncontrolled descent of loaded incline basket transfer cart

Flooding--Uncontrolled pool water draindown or filling resulting in flooding

Fire, Thermal--SNF overheating due to loss of pool water resulting in excessive clad temperature and possible zircaloy cladding fire, SNF overheating in an assembly transfer basket or dryer resulting in excessive clad temperature and possible zircaloy cladding fire

Radiation--Uncontrolled pool water draindown or filling resulting in flooding and radioactive contamination of adjoining WHB areas, increased radiation levels in the

assembly transfer area and potential uncovering of fuel assemblies, radiation exposure of facility worker

Fissile—Criticality associated with a cask collision or drop and the rearrangement of cask internals, criticality associated with SNF assembly staging rack, criticality associated with misload of assembly dryer, criticality associated with misload of disposal container.

6.2.4.6 Example 6: Waste Handling - Disposal Container Handling and Waste Package Remediation

Area Description—Within the DC handling area, empty DCs are prepared for loading, DCs are transferred to and from the assembly and canister transfer systems, the DC lids are welded, and WPs are temporarily stored. WPs are also loaded into the WP transporter and transferred to and from the WP remediation system. DCs consist of the container barriers, spacing structures or baskets, shielding integral to the container and packing contained with the container. The WP consists of the DC and waste form(s) after the outer lid welds are completed and accepted.

The process begins with empty DC preparation, which includes staging the DCs, installing collars, tilting the DC upright and outfitting the container, and transferring it to DC transfer operations. DC transfer operations include staging DC lids for the weld stations, and transferring the DCs to or from the assembly or canister transfer systems for loading and welding. The DC welding operation receives loaded DCs directly from the waste handling lines or from interim lag storage for welding. The welding operations include mounting the DC on a turntable, removing lid seals, and installing and welding the inner and outer lids. The weld process for each lid includes non-destructive examination. Following examination and weld acceptance, the container is called a WP and is either staged or transferred to a tilting station. At the tilting station, the WP is tilted to horizontal, the collars are removed, and the WP is transferred to WP transporter loading operations. The WP transporter loading operations include survey and decontamination, and lifting and loading the WP into the WP transporter. DCs that do not meet the welding examination criteria are transferred to the WP remediation system for inspection or repair.

The DC handling area is contained within the WHB and includes areas for empty DC preparation, welding, staging, loaded WP staging, WP transporter loading, and the associated operating galleries and required equipment maintenance areas. The empty DC preparation area is located in an unshielded structure.

Disposal container handling equipment includes a DC/WP bridge crane, tilting station, and transfer carts. The welding area includes DC/WP welders, staging stations, and a tilting station. Welding operations are supported by remotely operated equipment including transfer carts, a bridge crane and hoists, welder jib cranes, welding turntables, and manipulators. WP transfer includes a transfer, decontamination, and transporter load area. The operations are supported by a remotely operated horizontal lifting system, decontamination system, decontamination and inspection manipulator, and a WP horizontal transfer cart. All handling operations are supported by a suite of fixtures including yokes, lift beams, and lid attachments. Remote equipment is designed to facilitate decontamination and maintenance, and interchangeable components are provided where appropriate. Set-aside areas are included as required for fixtures and tooling to

support off-normal and recovery operations. Semi-automatic, manual, and backup control methods support normal, maintenance, and recovery operations.

Generic Events Applicability–

Collision/Crushing–Yes

Chemical Contamination/Flooding–None identified

Explosion/Implosion–None identified

Fire–Yes

Radiation/Magnetic/Electrical/Fissile–Yes, Radiation/Fissile

Thermal–Yes.

Reference–Applicable system description and design documents.

Preliminary Events–

Collision/Crushing–WP drop, WP slap down, WP drop onto sharp object, WP collision, equipment drops onto WP, DC drop, DC slap down, DC drop onto sharp object, DC collision, handling equipment drops on DC

Fire, Thermal–Fuel damage by burn through during welding process, SNF overheating in a DC resulting in excessive clad temperature and possible zircaloy cladding fire

Radiation–Radiation exposure of facility worker

Fissile–Criticality associated with the DC/WP staging area, criticality associated with collision or drop of DC/WP and rearrangement of container internals.

6.2.4.7 Example 7: Subsurface Transport, Emplacement, and Monitoring

Area Description–The waste emplacement system transports the loaded and sealed WP from the WHB to the subsurface emplacement area. This system operates on the surface between the north portal and the WHB, and in the underground ramps, access mains, and emplacement drifts. This system accepts the WP onto a reusable rail car, moves the WP into the shielded transporter, transports the WP to the emplacement area, and emplaces the WP in the emplacement drift. The operation cycle is completed when the transport equipment returns to the surface WHB to receive another WP.

Major items and sub-systems of the waste emplacement system consist of the following:

- A shielded transporter with a reusable rail car for the movement and transfer of the WPs. The transporter requires transport locomotives for movement.
- Transport locomotives for the transporter movement and control functions between the WHB and the subsurface repository.

- A remotely controlled emplacement gantry for the WP emplacement functions in the emplacement drifts. The gantry is self-powered through a direct current third rail system.
- A gantry carrier for gantry transfer between the emplacement drifts and the maintenance facilities. The gantry carrier requires a transport locomotive for the carrier movement and control functions.

The sequence of the subsurface WP handling process is described in the following paragraphs:

The WP, positioned on a reusable rail car, is moved into the shielded transporter at the WHB. A remotely controlled loading mechanism moves the rail car into and out of the transporter. The loading mechanism will be an integral part of the transporter.

A pair of transport locomotives is used to move the transporter from the WHB, into and down the north ramp, into the east or west main, and to the vicinity of the designated emplacement drift. At the pre-selected emplacement drift location, one locomotive is uncoupled to allow the transporter, with the transporter doors facing the drift entrance, to be pushed into the emplacement drift turnout. Before the transporter is pushed into the turnout, the locomotive operators leave the locomotive, and the following functions of the emplacement sequence are performed remotely. Once the transporter is partway in the turnout, the transporter doors and the drift isolation doors open remotely, then the transporter is pushed into contact with the subsurface emplacement transportation system drift transfer dock.

Once the transporter is docked, the unloading mechanism moves the reusable rail car with the WP out of the transporter and onto the rails located on the transfer dock. The emplacement gantry moves into position over the WP, it engages the WP by the skirts at both ends, and raises the WP off the reusable rail car. The gantry carries the WP into the emplacement drift, stopping at a pre-determined emplacement position. The WP is lowered onto permanently installed pedestals. The gantry disengages from the WP and moves back to its waiting position at the transfer dock. These operations are reversible to support moving an emplaced WP to another location.

The transporter retracts the reusable rail car, and is pulled away from the drift entrance doors by a locomotive. The transporter doors and the drift doors are then closed, and the transporter returns to the surface WHB for another transport and emplacement operation. The transporter may also receive a WP onto the reusable rail car from the emplacement gantry to support moving the WP to another emplacement drift or to the surface WHB.

Following emplacement, the WPs are monitored between the time the WP is emplaced and the time the repository is closed. Concurrent with the emplacement and monitoring of WPs, construction is underway on the development of additional emplacement drifts. Physical separation of emplacement and development activities is provided by isolation air locks. When a predetermined number of newly excavated emplacement drifts are ready for waste emplacement, the isolation airlocks are moved to include the newly developed drifts in the emplacement area.

Generic Events Applicability–

Collision/Crushing–Yes

Chemical Contamination/Flooding–Yes, Flooding

Explosion/Implosion–No

Fire–Yes

Radiation/Magnetic/Electrical/Fissile–Yes, Radiation/Fissile

Thermal–Yes, see Fire.

Reference–Jackson et al. 1984, MacDougall et al. 1987, Hartman and Miller 1991, Ma et al. 1992, Schelling and Smith 1993, and applicable system description and design documents.

Preliminary Events–

Collision/Crushing–Transporter derailment outdoors, transporter derailment on ramp or in main drift, transporter collision with other stationary or moving equipment, WP reusable rail car rolls out of transporter, runaway transporter, rockfall onto transporter, loaded emplacement gantry derailment, WP drop from emplacement gantry, WP or emplacement gantry collision with equipment or another WP, rockfall onto WP, steel set drop onto WP, failure of isolation air locks due to rockfall, equipment collision, or other impacts as a result of development operations

Flooding–Flooding from water pipe break originating on development or emplacement sides

Fire, Thermal–Fire associated with WP transporter, locomotive, or development equipment

Radiation–Radiation exposure of facility worker, early or juvenile WP failure and resultant release of radioactive material

Fissile–Criticality associated with collision or drop of WP and rearrangement of package internals.

6.2.4.8 Example 8: Site-Generated Waste Treatment - Liquid Low-Level Radioactive Waste

Area Description–Liquid LLW is piped to the waste treatment building for processing. Liquid waste is treated by filtration, evaporation, and ion exchange. Water meeting the requirements for reuse is recovered. Following pH adjustment, non-recyclable liquid is solidified and packaged in drums. The drums are temporarily stored awaiting offsite shipment for disposal.

Generic Events Applicability–

Collision/Crushing–Yes

Chemical Contamination/Flooding–Yes, Flooding

Explosion/Implosion–None identified

Fire—None identified
Radiation/Magnetic/Electrical/Fissile—Yes, Radiation
Thermal—None identified.

Reference—Applicable system description and design documents.

Preliminary Events—

Collision/Crushing—Handling equipment drops on liquid LLW
Flooding—Uncontrolled release of liquid LLW
Radiation—Operator exposure to radioactive material.

6.2.4.9 Example 9: Site-Generated Waste Treatment - Solid Low-Level Radioactive Waste

Area Description—Solid LLW is shipped to the waste treatment building in drums. The waste consists of combustible and noncombustible job control waste (e.g., protective clothing, rags, wood), ion exchange resin and discarded tools and equipment. The waste is treated by shredding, size reduction, compaction, or dewatering as applicable, packaged in drums with a solidification agent and temporarily stored awaiting offsite shipment for disposal.

Generic Events Applicability—

Collision/Crushing—Yes
Chemical Contamination/Flooding—None identified
Explosion/Implosion—None identified
Fire—Yes
Radiation/Magnetic/Electrical/Fissile—Yes, Radiation
Thermal—Yes (see Fire).

Reference—Applicable system description and design documents.

Preliminary Events—

Collision/Crushing—Solid LLW drop, handling equipment drops on solid LLW
Fire, Thermal—Fire involving combustible LLW
Radiation—Operator exposure to radioactive material.

6.2.5 Internal Events Hazards List

The product of this analysis is the Internal Events Hazards List. The Internal Events Hazards List contains the potentially credible internal hazards that cannot be screened out by the process described.

6.3 REFERENCES

The following documents are referenced directly in the methods or examples presented in Section 6.1 of the Guide. Appendix A presents a list of other documents that may prove useful in conducting an EEHA.

6.3.1 Documents Cited

AIChE (American Institute of Chemical Engineers) 1992. *Guidelines for Hazard Evaluation Procedures*. 2nd Edition with Worked Examples. New York, New York: American Institute of Chemical Engineers. TIC: 239050.

ANSI/ANS-2.12-1978. 1978. *Guidelines for Combining Natural and External Man-Made Hazards at Power Reactor Sites*. La Grange Park, Illinois: American Nuclear Society. TIC: 8767.

ASCE 7-98. 2000. *Minimum Design Loads for Buildings and Other Structures*. Revision of ANSI/ASCE 7-95. Reston, Virginia: American Society of Civil Engineers. TIC: 247427.

Coats, D.W. and Murray, R.C. 1985. *Natural Phenomena Hazards Modeling Project: Extreme Wind/Tornado Hazard Models for Department of Energy Sites*. UCRL-53526, Rev. 1. Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL.20010405.0048.

CRWMS M&O 1999. *MGR Design Basis Extreme Wind/Tornado Analysis*. ANL-MGR-SE-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19991215.0461.

Eglinton, T.W. and Dreicer, R.J. 1984. *Meteorological Design Parameters for the Candidate Site of a Radioactive-Waste Repository at Yucca Mountain, Nevada*. SAND84-0440/2. Albuquerque, New Mexico: Sandia National Laboratories. ACC: NNA.19870407.0048.

Hartman, D.J. and Miller, D.D. 1991. *Identification of Structures, Systems, and Components Important to Safety at the Potential Repository at Yucca Mountain*. SAND89-7024. Albuquerque, New Mexico: Sandia National Laboratories. TIC: 203536.

Jackson, J.L.; Gram, H.F.; Hong, K-J.; Ng, H.S.; and Pendergrass, A.M. 1984. *Preliminary Worst-Case Accident Analysis to Support the Conceptual Design of a Potential Repository in Tuff*. SAND83-1787C. Albuquerque, New Mexico: Sandia National Laboratories. TIC: 229295.

Ma, C.W.; Sit, R.C.; Zavoshy, S.J.; and Jardine, L.J. 1992. *Preclosure Radiological Safety Analysis for Accident Conditions of the Potential Yucca Mountain Repository: Underground Facilities*. SAND88-7061. Albuquerque, New Mexico: Sandia National Laboratories. ACC: NNA.19920522.0039.

MacDougall, H.R.; Scully, L.W.; and Tillerson, J.R., eds. 1987. *Nevada Nuclear Waste Storage Investigations Project, Site Characterization Plan Conceptual Design Report*. SAND84-2641. Volume 4, Appendices F-O. Albuquerque, New Mexico: Sandia National Laboratories. ACC: NN1.19880902.0017.

National Research Council 1995. *Technical Bases for Yucca Mountain Standards*. Washington, D.C.: National Academy Press. TIC: 217588.

NRC (U.S. Nuclear Regulatory Commission) 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

Schelling, F.J. and Smith, J.D. 1993. *Preclosure Radiological Safety Evaluation: Exploratory Studies Facility*. SAND92-2334. Albuquerque, New Mexico: Sandia National Laboratories. TIC: 207076.

Solomon, K.A.; Erdmann, R.C.; and Okrent, D. 1975. "Estimate of the Hazards to a Nuclear Reactor from the Random Impact of Meteorites." *Nuclear Technology*, 25, 68-71. La Grange Park, Illinois: American Nuclear Society. TIC: 241714.

Stephans, R.A. and Talso, W.W., eds. 1997. *System Safety Analysis Handbook*. 2nd Edition. Albuquerque, New Mexico: System Safety Society. TIC: 236411.

YMP (Yucca Mountain Site Characterization Project) 1997. *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain*. Topical Report YMP/TR-003-NP, Rev. 2. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19971009.0412.

6.3.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

APPENDIX 6A

BIBLIOGRAPHY FOR DOCUMENTS POTENTIALLY RELEVANT TO EXTERNAL EVENTS HAZARDS ANALYSIS

ANS 1988. *Design Criteria for an Independent Spent Fuel Storage Installation (Water Pool Type)*. ANSI/ANS 57.7-1988. La Grange Park, Illinois: American Nuclear Society. TIC: 238870.

ANS 1992. *Determining Design Basis Flooding at Power Reactor Sites, an American National Standard*. ANSI/ANS 2.8-92. La Grange Park, Illinois: American Nuclear Society. TIC: 236034.

Braithwaite, J.W. and Nimic, F.B. 1984. *Effect of Host-Rock Dissolution and Precipitation on Permeability in a Nuclear Waste Repository in Tuff*. SAND84-0192. Albuquerque, New Mexico: Sandia National Laboratories. ACC: MOL.19980622.0579.

Coats, D.W.; and Murray, R.C. 1985. *Natural Phenomena Hazards Modeling Project: Extreme Wind/Tornado Hazard Models for Department of Energy Sites*. UCRL-53526, Rev. 1. Livermore, California: Lawrence Livermore National Laboratory. TIC: 225881.

Coe, J.A.; Glancy, P.A.; and Whitney, J.W. 1995. *Volumetric Analysis and Hydrologic Characterization of a Modern Debris Flow Near Yucca Mountain, Nevada*. Denver, Colorado: U.S. Geological Survey. ACC: MOL.19950307.0140.

Crowe, B.; Perry, F.; Geissman, J.; McFadden, L.; Wells, S.; Murrell, M.; Poths, J.; Valentine, G.A.; Bowker, L.; and Finnegan, K. 1995. *Status of Volcanism Studies for the Yucca Mountain Site Characterization Project*. LA-12908-MS. Los Alamos, New Mexico: Los Alamos National Laboratory. ACC: HQO.19951115.0017.

CRWMS M&O (Civilian Radioactive Waste Management System Management and Operating Contractor) 1996. *Preliminary MGDS Hazards Analysis*. B00000000-01717-0200-00130 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19961230.0011.

CRWMS M&O 1996. *Probabilistic Volcanic Hazard Analysis for Yucca Mountain, Nevada*. BA0000000-01717-2200-00082 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19971201.0221.

CRWMS M&O 1997. *Engineering Design Climatology and Regional Meteorological Conditions Report*. B00000000-01717-5707-00066 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980304.0028.

CRWMS M&O 1997. *Final Report Waste Package Degradation Expert Elicitation Project*. Rev. 0. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980218.0231.

CRWMS M&O 1998. *Retrievability Strategy Report*. B00000000-01717-5705-00061 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980723.0039.

CRWMS M&O 1999. *MGR Aircraft Crash Frequency Analysis*. ANL-WHS-SE-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19981221.0203.6.2.6.

DOE (U.S. Department of Energy) 1988. *Site Characterization Plan, Yucca Mountain Site, Nevada Research and Development Area*. DOE/RW-0199. Eight volumes. Washington, D.C: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: HQO.19881201.0002.

Eglinton, T.W. and Dreicer, R.J. 1984. *Meteorological Design Parameters for the Candidate Site of a Radioactive-Waste Repository at Yucca Mountain, Nevada*. SAND84-0440/2. Albuquerque, New Mexico: Sandia National Laboratories. ACC: NNA.19870407.0048.

Lipman, P.W.; and Mullineaux, D.R. 1981. *The 1980 Eruptions of Mount St. Helens, Washington - Geological Survey Professional Paper 1250, Aerial Distribution, Thickness, Mass, Volume, and Grain Size of Air-fall Ash From the Six Major Eruptions of 1980*. Denver, Colorado: U.S. Geological Survey. TIC: 218260.

Ma, C.W.; Sit, R.C.; Zavoshy, S.J.; and Jardine, L.J. 1992. *Preclosure Radiological Safety Analysis for Accident Conditions of the Potential Yucca Mountain Site Repository: Underground Facilities*. SAND88-7061. Albuquerque, New Mexico: Sandia National Laboratories. ACC: NNA.19920522.0039.

Ma, C.W.; Zavoshy, S.J.; Jardine, L.J.; and Kiciman, O.K. 1991. *An Analysis of Scenarios and Potential Radiological Consequences Associated with U.S. Military Aircraft Crashes for The Yucca Mountain Site Repository*. SAND 90-7051. Albuquerque, New Mexico: Sandia National Laboratories. TIC: 222207.

NRC (U.S. Nuclear Regulatory Commission) 1974. *Design Basis Tornado for Nuclear Power Plants*. Regulatory Guide 1.76. Washington, D.C: U.S. Nuclear Regulatory Commission. TIC: 2717.

NRC 1988. *Evaluation of Station Blackout Accidents at Nuclear Power Plants*. NUREG-1032. Washington, D.C: U.S. Nuclear Regulatory Commission. TIC: 225880.

Perry, F.V. and Crowe, B.M. 1987. *Preclosure Volcanic Effects: Evaluations for a Potential Repository Site at Yucca Mountain, Nevada*. Los Alamos, New Mexico: Los Alamos National Laboratory. ACC: NNA.19900112.0341.

Squires, R.R.; and Young, R.L. 1984. *Flood Potential of Fortymile Wash and its Principal Southwestern Tributaries, Nevada Test Site, Southern Nevada*. Water-Resources Investigations Report 83-4001. Carson City, Nevada: U.S. Geological Survey. ACC: HQS.19880517.1933.

Uniform Building Code 1997, Volume 2, *Structural Engineering Design Provisions*. International Conference of Building Officials (ICBO), Whittier, California. TIC: 233818.

YMP (Yucca Mountain Site Characterization Project) 1993. *Evaluation of the Potentially Adverse Condition "Evidence of Extreme Erosion During the Quaternary Period" at Yucca*

Mountain, Nevada. YMP/92-41-TPR. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: NNA.19930316.0208.

YMP 1995. *Site Atlas* 1995. Deliverable OE10. Two volumes. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19960311.0262.

YMP 1995. *Technical Basis Report for Surface Characteristics, Preclosure Hydrology, and Erosion.* YMP/TBR-0001, Rev. 0. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19951201.0049.

YMP 1997. *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain.* YMP/TR-003-NP, Rev. 2. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19971009.0412.

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMS.....	iv
7. EVENT SEQUENCE (DESIGN BASIS EVENT) FREQUENCY ANALYSIS	7-1
7.1 EVENT TREE ANALYSIS.....	7-1
7.1.1 Purpose.....	7-1
7.1.2 Scope.....	7-1
7.1.3 Overview of Approach.....	7-1
7.1.4 Details of Approach.....	7-8
7.1.5 Examples of Applications of Event Tree Analysis.....	7-16
7.2 FAULT TREE ANALYSIS.....	7-28
7.2.1 Introduction.....	7-28
7.2.2 Overview of Approach.....	7-28
7.2.3 Details of Approach.....	7-31
7.2.4 Examples of Application	7-45
7.3 HUMAN RELIABILITY ANALYSIS.....	7-52
7.3.1 Purpose.....	7-52
7.3.2 Scope.....	7-52
7.3.3 Overview of Approach.....	7-52
7.3.4 Details of Approach.....	7-53
7.3.5 Examples.....	7-74
7.4 COMMON-CAUSE AND DEPENDENT FAILURES ANALYSIS.....	7-75
7.4.1 Purpose.....	7-75
7.4.2 Scope.....	7-75
7.4.3 Overview of Approach.....	7-75
7.4.4 Details of Approach.....	7-81
7.4.5 Steps in Performing Dependent Failure Analysis for a Repository.....	7-92
7.4.6 Examples of Application	7-95
7.5 TECHNICAL INFORMATION.....	7-99
7.5.1 Introduction.....	7-99
7.5.2 Overview of Approach.....	7-99
7.5.3 Details of Approach.....	7-101
7.6 EVENT SEQUENCE FREQUENCY BINNING.....	7-135
7.6.1 Purpose.....	7-135
7.6.2 Scope.....	7-135
7.6.3 Overview of Approach.....	7-135
7.6.4 Details of Approach.....	7-136
7.6.5 Examples of Application	7-138
7.7 REFERENCES	7-139
7.7.1 Documents Cited.....	7-139
7.7.2 Codes, Standards, Regulations, and Procedures.....	7-141
APPENDIX 7A - BIBLIOGRAPHY OF INFORMATION SOURCES.....	7A-1

FIGURES

	Page
7-1	Example of a Fork Style Event Tree for a Hypothetical Waste Handling System..... 7-3
7-2	Example of a Stair-Step Style Event Tree for a Hypothetical Waste Handling System..... 7-5
7-3	Step in Event Tree Construction..... 7-10
7-4	Event Tree for Hypothetical Uncontrolled Descent Due to Random-Failure Initiator..... 7-17
7-5	Simplified Event Tree for Hypothetical Uncontrolled Descent (First Example) 7-24
7-6	Simplified Event Tree for Hypothetical Uncontrolled Descent (Second Example) 7-25
7-7	Event Tree for Hypothetical Fire Initiated Uncontrolled Descent..... 7-26
7-8	Event Tree for Hypothetical Human Error Initiated Uncontrolled Descent..... 7-29
7-9	Standard Fault-Tree Symbols 7-33
7-10	Illustration of Fault Tree Development..... 7-40
7-11	Pressure Tank System 7-46
7-12	Fault Tree Example for Pressure Tank Rupture 7-49
7-13	Simplified Fault Tree for Pressure Tank Example 7-51
7-14	Example of Fault Tree Containing Type A Human Actions 7-57
7-15	Example of Fault Tree Containing Type B Human Actions..... 7-58
7-16	Example of Event Tree with Type C Human Action in Event Headings 7-59
7-17	Operator Action Tree: A Generalized Representation of Type C HAs 7-70
7-18	Example of Human Reliability Analysis Tree 7-73
7-19	Physical Elements of Dependent Events..... 7-81
7-20A	Baseline Event Tree Without CCFs..... 7-85
7-20B	Event Tree with Fire-Initiated Common-Cause Failure of a Heating, Ventilation, and Air-Conditioning, and High-Efficiency Particulate Air Filter System. 7-85
7-21	Illustration of Logic Models for Independent Failures 7-90
7-22	Illustration of Logic Models for Common Cause Failures 7-91
7-23	Exponential Probability of Failure..... 7-104
7-24	Unavailability with Inspection and Test 7-105
7-25	Probability of Restoration – Exponential Repair Model..... 7-106

TABLES

	Page
7-1 Example of Task Analysis	7-62
7-2 Example Probabilities of Errors of Commission in Operating Manual Controls	7-68
7-3 Types of Dependent Events Based on their Impact on Preclosure Safety of a Repository	7-78
7-4 A Guide to Unreliability of Various System Arrangements with Consideration of Dependent Failures	7-82
7-5 Generic Beta Factors	7-96
7-6 Sources of Facility-Specific and Operations-Specific Experience Information	7-102
7-7 Example of Generic Component Failure Rates Database	7-115
7-8 Crane Failure Demand Rates	7-133

ACRONYMS

AC	alternating current [electrical power]
BC2	beyond Category 2 [event sequence]
CA	construction authorization
CCF	common-cause failure
CDF	cumulative distribution function
EF	error factor
EMF	electromagnetic force
ESF	Exploratory Studies Facility
ET	event tree
ETA	event tree analysis
FC	frequency category
FT	fault tree
FTA	fault tree analysis
HA	human action
HEP	human error probability
HEPA	high-efficiency particulate air
HFE	human failure event
HRA	human reliability analysis
HVAC	heating, ventilation, and air-conditioning
IE	initiating event
LA	license application
LN	lognormal
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
OAT	operator action tree
PDF	probability distribution function
PRA	probabilistic risk analysis
PSA	preclosure safety analysis
SNF	spend nuclear fuel
SSCs	structures, systems, and components
T&M	test and maintenance
WP	waste package

7. EVENT SEQUENCE (DESIGN BASIS EVENT) FREQUENCY ANALYSIS

This section presents details of the methodology for using sequence analyses in the Preclosure Safety Analysis (PSA).

7.1 EVENT TREE ANALYSIS

7.1.1 Purpose

This section defines the bases and methodology for the construction and use of event tree analysis (ETA) in support of the PSA. This analysis technique is applied when 1) identifying and structuring sequences of events that could potentially result in radiological releases or exposures, 2) identifying and quantifying dependencies between events in a sequence, 3) identifying the degree or magnitude of system failure or damage that correlates to the magnitude of potential releases and exposures, 4) quantifying the frequency (or annual probability) of various event sequences by combining probabilities of initiating and enabling events, and 5) providing a structure for including and propagating uncertainty factors in sequence quantification.

7.1.2 Scope

This section is a cursory, focused guide to the construction, application, and evaluation of event trees (ETs). While some concepts are universal to all ETA, the applications in this Section are focused on the support of the PSA. This section is not meant to be a textbook or exhaustive in scope. Where appropriate, reference is made to literature for additional information.

7.1.3 Overview of Approach

An ET is a graphical logic model that identifies the possible outcomes following an initiating event (IE). ETs are similar to decision trees in depicting the manner in which a chain of alternative outcomes can occur.

Potential accident scenarios (or event sequences) may be displayed in the form of ETs. ETs include an IE (from an identified hazard) and one or more enabling events that must occur to result in a release of radioactivity, a criticality, or an abnormal radiological exposure of the public or a worker. The ET format may also be used to analyze scenarios involving chemical exposures, fires, or explosions (see AIChE 1989, Figure 3.10). The enabling events generally represent the success or failure of some safety features that mitigate the effects of the IE alone or in combination with other events. The enabling events may also represent specific human actions (HAs) or physical conditions that could affect the progression of an event sequence (or scenario).

The ET format provides a framework for estimating the likelihood of event sequences by displaying the frequency of the IE and the conditional probabilities of contributing (enabling) events.

An ET generally represents a chronological sequence of events. However, in many cases an ET can be simplified (i.e., have fewer limbs or branches) by rearranging events such that the more likely or more significant events are addressed first.

ETs can be used in deterministic and qualitative analyses to display alternative possible sequences, to examine the levels of protection that are present in a design concept, or both.

Further, an ET may be simplified by assuming that some events will occur with a probability of one (e.g., all fuel cladding breaches in a dropped fuel assembly). This assumption may be appropriate if insufficient data exist to quantify the probability of a failure, if a conservative analysis is being performed, or if regulatory policy demands it.

The construction of ETs in the PSA will build, primarily, on the IEs or event categories identified in the internal events hazards analysis (see Section 6.2). In addition, ETs may be constructed as required for the events identified by the External Events Hazards Analysis (see Section 6.1). The following discussion primarily addresses the application of ETA for internal events. Section 10.1 describes the use of ETA for seismic event sequences.

IEs are identified in the internal events hazards analysis for each repository surface and subsurface operation that could directly or indirectly impact the various radioactive waste forms. IEs in a given operation may include one or more opportunities for drops, collisions, tipovers/slapdowns, fires, explosions, flooding, criticality; exposure to chemical, radiation, thermal effects; or HAs. In general, system design and good practices will provide features (one or more structures, systems, or components [SSCs]), administrative controls, or human intervention) that will serve as physical or functional barriers that prevent or mitigate the release of radioactivity or the exposure of individuals. The proper functioning and availability of such features provide success paths such that an IE does not lead to an undesired consequence. Depending on the number of features that are unavailable when challenged by the occurrence of a given IE, undesirable event sequences can be described that represent failure paths, abnormal occurrences, or accidents that are usually differentiated by the degree of undesired consequences that characterize the end state of a given failure path. The ET is a useful tool to define the manner in which failure paths may occur, as well as a framework for quantifying the frequencies of the various success and failure paths.

7.1.3.1 Example of Event Tree

Figure 7-1 shows an example of a simple ET structure for a hypothetical sequence of events associated with the handling of a canister containing radioactive waste. The ET was designed to display several of the types of events and dependencies that may come to play in realistic situations. Section 7.1.4 describes the processes for developing ETs and provides a more complex, hypothetical example for instructional purposes. Section 10.1 describes applications of ETs in seismic sequences.

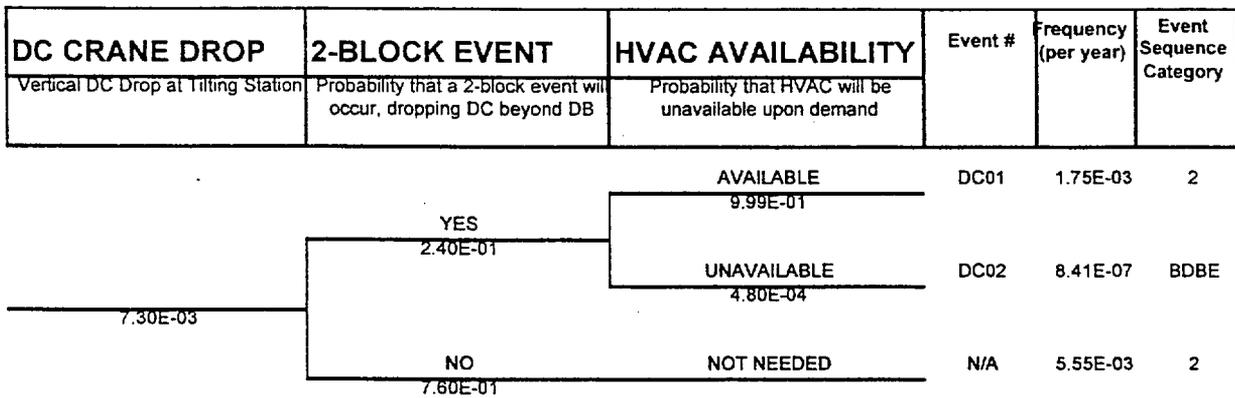


Figure 7-1. Example of a Fork Style Event Tree for a Hypothetical Waste Handling System

The ET in Figure 7-1 includes three events spaced across the top of the Figure. The event labels are known as the event headings. This logic diagram depicts a single line for the IE, but allows for (generally) two branches under each of the contributing (or enabling) event headings. The definitions in the event headings are carefully defined to describe a success. The upward branch above the IE represents a successful (yes or TRUE) IE. The downward branch below the IE represents a FALSE (no) event (e.g., the function fails or is unavailable). The success (or failure) criteria for each safety function must be precisely defined so that the meaning of the “no” branch is unambiguous. In binary logic, partial successes or failures are not permitted. The format for displaying the branches is termed the fork style because the TRUE and FALSE branches diverge from the incoming part. This style of ET is used by SAPHIRE (Russel et al. 1994). By contrast, Figure 7-2 illustrates an ET in the stair-step style. This style is easier to generate by hand (e.g., using the Microsoft Excel spreadsheet program).

Tracing through the branches in Figure 7-2, a particular path defines an event sequence that ends at an End State. Each End State represents the severity of the consequences associated with a particular event sequence (or scenario) expressed as the absence of, or the release of, radioactivity to the environment. The following describe the events represented in the figure, and the results:

- The IE is Drop of Waste Form (onto an unyielding surface). The cause of the drop may be a mechanical failure or human error. As shown in Note 1, the frequency of the IE is estimated from generic crane data for drops-per-lift (14 drops per 1,000,000 lifts) and the handling rate of the hypothetical operation (524 lifts per year). The IE frequency for drops of the waste form is estimated to be 7.3×10^{-3} per year.
- The first enabling event heading is titled “Waste Form Maintains Containment.” Since the waste form container will be designed to sustain certain handling stresses and impacts (i.e., those within its design basis, most or all of the possible drop heights could be within the design basis of the waste form and no release of radioactivity would occur). Unless there is absolutely no possible physical means for the operation to result in a breach of the waste form, there is a finite probability that a breach may occur. In the example of Figure 7-2, it is estimated that there is a rather high probability per lift of 0.25 (i.e., one chance in four) that if a drop occurs, it will exceed the design basis of the

waste form. This probability value could represent the experience data from commercial nuclear power plants (NPPs), independent fuel storage facilities, or other cranes where cases of two-blocking may have occurred. Two-blocking is a term used to describe situation in which lifting continues to a maximum allowable travel height until the strain against a dead pull results in a drop from a high point. The probability value of 0.25 per lift would represent all causes of drops, including hardware failure, software failure, and human errors. It is expected that repository design and operations will not allow such a large conditional probability. In this example, the conditional probability of the NO branch is, therefore, 0.25 and the probability of the YES branch is 0.75. The sum of probabilities for each branch point under each heading must equal 1.0.

- The second enabling event heading is titled “HVAC/HEPA Filter Available.” Since there are two exit paths from the event “Waste Form Maintains Containment,” the probability of the heating, ventilation, and air-conditioning (HVAC) and high-efficiency particulate air (HEPA) filter being available is conditioned on the need, operational conditions, or both, that are present in each path. In the case of the YES branch for “Waste Form Maintains Containment,” there is no need for the HVAC/HEPA filter and a single path labeled “Not Needed” is shown under the heading “HVAC/HEPA Filter Available.” For quantification purposes described below, a conditional probability of success of 1.0 is ascribed to dependent events that are not needed. By contrast, a conditional probability of failure of 1.0 is ascribed for dependent or deterministic events that are guaranteed failure.

In the case of the NO branch exiting event titled “Waste Form Maintains Containment,” however, there is a need to mitigate the amount of radioactivity that can escape from the operations building. A reliability analysis (e.g., a fault tree analysis; FTA) may show that the conditional probability of 5×10^{-4} of the HVAC/HEPA filter failing during a certain mission time (for example, 24 hours). The probability that the system is available (i.e., the system does not fail during the 24-hour mission time) is 0.9995 (i.e., $1 - 5 \times 10^{-4}$). Note that the success criteria for the HVAC/HEPA filter branch must include conditions such as: effectively remove 99 percent of particular matter greater than 0.3 microns for a period not less than 24 hours, when called upon. Recall the sum of probabilities at each branch point under each heading must equal 1.0.

- The structure of the ET now provides the means of identifying various event sequences, the means to quantify the frequency of each sequence, and a means of classifying the degree of damage, or amount of release, associated with each sequence.

The path from the IE, through YES on containment, and NOT NEEDED for the HVAC/HEPA filter is a success path. It is identified in Figure 7-2 as Sequence No. 1. The End States for the example in Figure 7-2 represent the source term (labeled Release Severity) associated with each event sequence. Success paths may be labeled “OK” (as is typical in ETA) or “N/A” (for not applicable). The non-success event sequences result in some releases is described qualitatively in the column labeled Release Severity.

DROP OF WASTE FORM	WASTE FORM MAINTAINS CONTAINMENT	HVAC/HEPA AVAILABLE	Sequence Identifier	Frequency (per year)	Release Severity
Drop of Waste Form onto Unyielding Surface	Cond. Probability: drop height within design basis of Waste Form Container	Probability that HVAC/HEPA is available upon demand			
Initiating Event ⁽¹⁾ 7.3E-03	YES ⁽²⁾ 0.75	NOT NEEDED	1	5.5E-3	OK (or N/A)
	NO ⁽³⁾ 0.25	YES 9.99E-01	2	1.8E-3	Low, gases
		NO ⁽⁴⁾ 4.8E-04	3	8.8E-7	Moderate gases & solids

- Notes:
- (1) Initiating event is due to unspecified failure in the lifting crane. From generic data, the frequency of initiating event is estimated to be 524 lifts/yr x 14 drops/million lifts
 - (2) Drop from normal height or less than design basis.
 - (3) Drop exceeds design basis due to 2-block event. Conditional probability of 2-block event is assumed to be 0.25 for this illustration.
 - (4) Unavailability of HVAC/HEPA derived from fault-tree analysis of HVAC/HEPA system.

Figure 7-2. Example of a Stair-Step Style Event Tree for a Hypothetical Waste Handling System

The frequency (or annual probability of occurrence) is estimated for each event sequence that results in a release of radioactivity or abnormal worker exposure. The framework of the ET is used to display the frequency of the initiator and the conditional probabilities of each enabling event in a sequence. The frequency of each event sequence is calculated as the product of the initiator frequency and the probabilities of all success and failure branches that comprise a given event sequence. The ET permits display of dependencies between the IE and enabling events, dependencies between enabling events, or both. Therefore, if there are sequence-dependent couplings between events, different sequences could have different probability values assigned to any given enabling event.

7.1.3.2 Quantification of Event Probabilities and Sequence Frequencies

The frequencies of IEs for internal hazards are estimated from the annual frequency of each operation multiplied by the probability per opportunity (or per operation) that the IE occurs. For example, the frequency of a canister drop is estimated by the product of the frequency of canister lifts (i.e., the number per year) and the conditional probability of dropping the canister per lift. The annual frequencies of each operational step are determined from programmatic information regarding the number of transport casks, spent fuel assemblies, spent fuel canisters, high-level radioactive waste canisters, and waste packages (WPs) that are expected to be processed each year during the preclosure operations.

The conditional probability of each enabling event (usually a failure of some preventive or mitigative feature), such as a drop of a waste form, is estimated from facility-specific data (if available) or generic data for similar operations. Section 7.5 describes the sources and techniques for defining appropriate event probabilities and their uncertainties for use in the PSA. Section 9 describes how uncertainties are applied and propagated. In many cases for the

preliminary event sequence screening analyses, conservative probabilities are assumed for the conditional events (e.g., assuming a probability of 1.0 that all fuel rods breach in a drop sequence). This conservatism is warranted in most cases in early screening analyses because complete design criteria and design details are not available.

A quantitative screening analysis applies the 10 CFR 63.2 definition of Category 2 Event Sequence to screen out event sequences whose estimated frequency results in a probability of less than one chance in 10,000 of occurring during the preclosure operations. Such event sequences are termed beyond Category 2 (BC2) Event Sequences and are screened out (see Section 4, Figure 4-1). Because of uncertainties, the frequency screening is conservatively applied initially so that event sequences within an order of magnitude of the threshold are considered as potential event sequences until additional design or phenomenological data, or detailed analyses including quantitative treatment of uncertainties, demonstrate that the event sequences have frequencies that are BC2. In the preliminary binning, frequencies of IEs and probabilities of enabling events are conservatively estimated and multiplied to estimate the frequencies of event sequences. The conservatisms are thereby stacked. Similarly, event sequences having frequencies within an order of magnitude of the Category 1 lower limit are considered Category 1 until more refined analysis shows otherwise.

In the refined analyses, probability distributions are defined for the IE frequencies and event probabilities to represent uncertainties and are propagated to derive probability distributions for sequence frequencies. The mean value of frequencies of event sequences will be used for binning the results as Category 1 or Category 2 event sequences. The mean value must be less than the frequency of the respective thresholds for Category 1 or 2, as appropriate, to provide the desired level of confidence (see Section 7.6).

7.1.3.3 Alternative Forms and Analysis of Event Trees

It is not feasible to list, by inspection, the important event sequences for a complex nuclear or chemical facility. The ET format provides a systematic and orderly approach to understand and accommodate the many factors that could influence the course of potential accidents. For simpler operations, such as many of the repository operations, the ET display may not be necessary; however, it does provide a powerful and convenient communication tool.

As described in the *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants* (NRC 1983), there are two main analytical formats for using ET and fault trees (FTs) in accident sequence delineation: small ET/large FT versus large ET/small FT. For repository preclosure safety analyses, the small ET/large FT technique is recommended for virtually all of the ETA and is described in the remainder of this Section. The large ET method is summarized for future reference.

Small ET quantification employs the use of FT linking. In this technique individual FTs that represent the respective event headings in the ET are linked through a sequence FT. Each of the function or system FTs is modeled to represent various basic events and dependencies on support systems. Evaluation of interdependencies between the heading events, such as common support systems or common HAs, is accommodated via the boolean algebra in the analysis of the sequence FT.

In the large ET method, by contrast, all of the dependencies and system boundary conditions are explicitly represented in the many headings and branches of the ET. The supporting FTs are small because they represent very specific conditions on the systems or HAs that are represented in the ET headings. In some cases, it is not necessary to use an FT per se, and tabulated probabilities suffice.

There is considerable latitude in the definition of event headings, even in the small ET approach. The same tree may use headings that represent functions, systems, components, and HAs. ET headings may also be used to establish conditions that could ameliorate or exacerbate potential sequences (e.g., the presence of an extreme ambient temperature or the presence of an oversized and overweight load on a lifting device).

Thus, the ET format can be used in two methods to describe potential accident sequence evolution:

- The first method is described in the *PRA Procedures Guide* (NRC 1983) for analyzing potential alternative responses of a complex system to a given IE. This method is sometimes referred to as a pre-incident (or pre-accident) analysis because it models sequences up to the point of having undesired damage states or releases (see AIChE 1989). In this application, a particular IE is postulated and an ET is constructed by listing across the top of the ET the various event possibilities that represent the safety functions or systems that are necessary to mitigate the potential consequences following the IE. For example, in a typical nuclear reactor ET, the IE is a loss of coolant accident and the functions listed across the top of ET would include reactor subcritical, containment overpressurization, and core cooling.

This type of application is appropriate for dealing with repository operational event sequences. This approach is appropriate for either initiators from internal or external events (including natural phenomena) that are directly associated with the repository operations (e.g., random failures of lifting devices) or those events that are tightly coupled to those operations (e.g., earthquake directly shakes the lifting device).

- The second method for using an ET is similar to the first method, but instead demonstrates how other possible events or conditions could exacerbate the potential accident (see AIChE 1989). Such ETs are sometimes termed post-incident (or post-accident) analyses to identify incident outcomes. For example, an ET developed for a large leakage of pressurized flammable material from an isolated liquid propane gas storage tank might include event headings such as immediate ignition, delayed ignition, flash fire, ignited jet point at liquid propane gas tank, and wind to populated area. Similarly, phenomenological ETs are used to describe the possible modes of containment behavior in the post-core-damage phase of nuclear reactor plants.

This type of application is appropriate for dealing with potential event sequences initiated by events originating offsite or outside of the repository operational areas such as range fires, toxic releases from transportation accidents, military or industrial hazards, or aircraft crashes that are not tightly coupled to the repository operational functions.

The first part of the ETA involves the probability that a harmful agent interacts with the facility or repository operational equipment.

The remaining discussion applies the pre-incident style of ETs as the primary application in the PSA.

The placement of events across the top of the ET can represent either the time sequence in which the events occur, proceeding left to right, or some other logical order reflecting operational dependencies (or conditions, as noted previously). Initially, the events can be ordered by temporal, functional, or hardware relationships, but the analyst may iterate to determine the best order to simplify the analysis or to clarify the presentation. Typically, a temporal ordering is used initially based on a process flow diagram, an operational description, or a pre-analysis such as an Event Sequence Diagram (see Section 10.1). However, functional or hardware dependencies should be considered, as in cases in which a given failure mode may imply the guaranteed failure of one or more other events in the headings.

For a given IE, the analyst must identify the safety functions that must be performed to control the sources of energy and radiation hazards in the facility. Such safety functions can be provided by active systems through automatic or manual actuation, by passive systems that provide barriers or containment, or from the natural or inherent feedback in the facility. As noted, the success criteria for each function must be unambiguously defined.

Starting with the IE, the analyst must postulate the success or failure of each function or system in the context of boundary conditions established by the states of the functions or systems in the ET headings. As noted, an event heading may connote the presence or absence of an enabling condition (e.g., temperature exceeds normal operating range or operator by-passes interlock). When the analyst considers a succeeding event, such as crane prevents lift beyond prescribed height, the probability of failure may depend on the operating temperature (i.e., one probability of failure based on random hardware failures or human error is used when temperatures are normal, but perhaps a higher probability is assigned when the temperature is abnormally high). This method models the dependency on prior conditions. For conservatism an ET may be constructed such that the abnormal temperature guarantees failure (i.e., has a probability of 1.0 that the crane lift height exceeds the limit).

7.1.4 Details of Approach

7.1.4.1 Constructing an Event Tree

Figure 7-3 summarizes the tasks in required to construct and evaluate an ET. The steps are described in Section 7.1.4.2.

ETs can be constructed at both a functional level and a system level.

Functional level ETs are developed at a relatively high level and serve to order and depict the safety functions according to the mitigating requirements of a given IE. The functional ET can also be used to depict contingent events that may result only if a precursor or conditioning event occurs (e.g., fire occurs after waste form is dropped). Functional ETs are generally simple or short, but each event heading in the functional ET can be supported by a complex FT.

FT linking is used to quantify the sequence frequencies. Dependencies between functions, or their supporting systems, are flushed out when the minimal cutsets are determined (see Section 7.2) for the sequence FT.

If there are potential dependencies between the functional event headings (e.g., two or more functional events depend on the same source of electrical power or the same HA), then a system level ET may be required to understand the dependencies. A complete system heading ET that depicts all of the conditional probabilities and dependencies can be very complex or long.

One or more functional ETs should be developed for each credible IE that has been selected for analysis from the respective Internal or External Events Hazards Analysis. The ET is a primary tool for defining potential accident sequences. As noted, for some complex operations it may be necessary to draw an intermediate diagram known as an Event Sequence Diagram (see Section 10.1) to help simplify the ET.

As noted in Figure 7-3, before starting an ET, the analyst must know the system. This familiarization should be done with the help of personnel from design and operations, radiological consequence analysts, a radiation protection program, and safety-specific analyses (e.g., fire hazards, or criticality). The description and results of the Internal (or External) Events Hazards Analysis are a starting place. If more design or operational details are available, such as plan and elevation drawings and concept of operations, the functional ET should go beyond the discussion of potential events and consequences that may be speculative in the hazards analysis.

If necessary to understand the operations and how potential accidents could evolve, the ET analyst must acquire or draw a process flow diagram that shows each operation that interacts with the waste form (e.g., lifts, moves, and lowers). If necessary, an Event Sequence Diagram should be completed (see Section 10.1) to indicate success paths in the operations and how various event sequences may develop:

- For each operation in the system whose malfunction could impact the waste form, define an IE (e.g., crane drops waste form; shield door closes on waste form)
- From an inspection of the flow diagram, system layout, or event sequence diagram, list and order all of the subsequent events that could possibly happen after the IE has occurred. Since the event sequences that lead to release of radioactive material to the environment are the events of importance to the repository PSA, the analyst must consider all possibilities. Subsequent screening and analyses will filter out impossible, incredible, or insignificant event. Some events that may come to play in one or more sequences at the repository include:
 - Waste form containment is breached
 - Fire occurs concurrently
 - Waste form releases mass of radioactive material (amount may differ with or without concurrent fire).

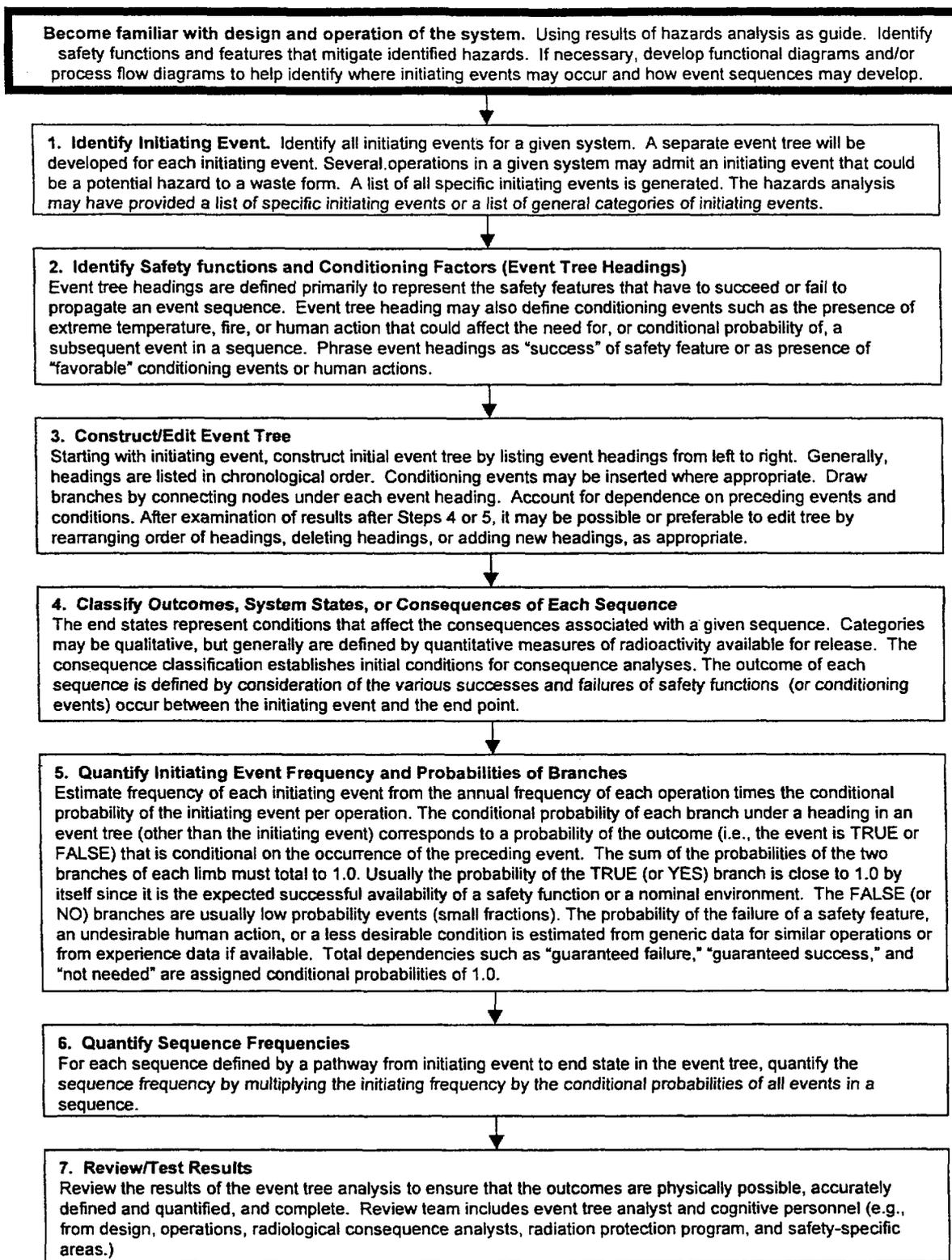


Figure 7-3. Step in Event Tree Construction

The graphical development of the ET may be constructed by hand (using pencil and paper), as a spreadsheet program (e.g., Microsoft Excel), or semi-automatically using special-purpose software such as a probabilistic risk analysis (PRA) workstation (e.g., SAPHIRE). Pencil and paper are recommended for initial conceptualization and ET simplification. A more refined ET can be constructed in a spreadsheet format that can also be used for quantifying sequences involving simple or moderately complex cases. If FT linking is to be used, then the final ET has to be constructed and quantified using a computer program such as SAPHIRE (Russel et al. 1994).

7.1.4.2 Steps in ET Construction

7.1.4.2.1 Identify the Initiating Event

The IE for each ET should be identified from a hazards analysis as an event that has the possibility of leading to an exposure to, or release of, radioactivity. In addition, the event must have been quantitatively screened in (found credible) in the hazards analysis. The IE will usually be an internal event that can impact energy or damage a waste form, such as crane drops [spent nuclear fuel] SNF canister. The IE could also be a fire (external or internal) or another external event (man-made or natural phenomena) such as loss of offsite power, aircraft crashes into waste handling building, or earthquake at waste handling building site.

In general, it is necessary at the outset to define the specific purpose of the ET analysis since concerns associated with the possible outcomes (e.g., public doses versus worker exposures) will influence the event headings, success criteria, and structure of the tree.

7.1.4.2.2 Identify Safety Functions and Conditioning Factors (ET Headings)

For each particular IE that is postulated to occur in a given operational area, an ET is constructed by listing the event headings across the top of the page. Event headings primarily represent the various event possibilities that represent the safety functions or systems that are necessary to mitigate the potential consequences following the IE. Such event headings may represent passive barriers, automatic safety systems, or alarms to alert operators. Thus, in the case of crane drops SNF canister, maintaining the integrity of the canister provides the safety function of containment of radioactivity. The ET heading could be canister is not breached (conditional on being dropped). Another safety function could be HVAC/HEPA filters exhaust air.

However, the headings may also represent conditioning events such as "building containment intact," which, when placed ahead (to the left) of "HVAC/HEPA filters exhaust air," provide a structure for conditioning the probability of failure of "HVAC/HEPA filters exhaust air." That is, if the event titled "building containment intact" is false (NO branch), then the conditional probability is 1.0 (guaranteed failure) that "HVAC/HEPA filters exhaust air" is false. Otherwise, when "building containment intact" is true (YES branch), then the probability that "HVAC/HEPA filters exhaust air" is false depends on the reliability of the HVAC/HEPA filter system. Other conditioning events may represent environmental factors such as temperature anomalies caused by an upstream event or consequential fire.

In some systems there may be a mutual dependence of all active safety functions on a single support active system, such as an onsite power supply. The ET for such a situation should use

the conditioning event “electric power available” early in the event headings. The FALSE branch would then result in a series of guaranteed failures and a simplified ET. Otherwise, the vulnerability posed by the power supply may not be realized until after the FT linking and boolean reduction is performed. If the safety functions and support systems have been designated a priori to be highly-reliable, single-failure proof, or both, then the event heading titled “electric power available” need not be included in the ET since the combinations of dependent failures may be too complex and best handled through FT linking.

The event heading may also represent a HA such as an explicit kind of conditioning event such as “operator installs proper lifting yoke” or an operational condition such as “operator maintains air seals on building containment.”

7.1.4.2.3 Construct or Edit the Event Tree

An ET is constructed conventionally left to right, beginning with the IE. Under each event heading, one or more sequence branch points (or nodes) are included to represent the two alternative pathways. Some ETs may use multiple branches, but multiple branches are not discussed here. The branch points may be drawn with two-pronged forks at each node, as illustrated in Figure 7-1, or as stair-steps, as illustrated in Figure 7-2.

The labels for the event headings are conventionally phrased such that an upward branch in the fork style (the convention to be used herein with the SAPHIRE computer software) represents that the heading is TRUE (branch labeled YES) indicates that the function is successful. For conditioning events, the upward branch represents (usually) the more favorable condition, tending toward successful mitigation or reduced consequences. The downward branch (labeled NO) represents the complementary situation (and probability) that is defined in the event heading, thus representing failure of the function or presence of the less desirable condition.

Although the example shown in Figure 7-1 was created with Microsoft Excel, the fork style is difficult to create by hand because changes and branching requires much re-drawing and re-positioning of lines on a page. However, fork-style ETs are very easily created and edited with a computer program such as SAPHIRE.

In the stair-step format (which is easy to implement in the Microsoft Excel spreadsheet program), the YES paths are represented by horizontal lines and the NO paths branch downward (see Figure 7-2).

One advantage of the fork style is the clearer depiction of dependent events (e.g., “guaranteed failure” or “not needed” are shown as horizontal paths that pass through a node without branching up or down). By contrast, in the stair-step style, dependent events resemble success branches unless they are labeled as “guaranteed failure” or “not needed,” or are depicted by a dotted line rather than a solid line.

In some instances, the analyst may restructure the headings of the ET to better represent dependencies on conditional or precursor events, or to simplify the ET. This process may occur iteratively after Step 4 in Figure 7-3 is performed.

If the outcomes (i.e., system states, or amounts of material released) of several sequences are the same or nearly the same, some event headings may be seen to be irrelevant to understanding and quantifying the risk. Even though the headings may introduce branching and extra sequences that could occur, the overall frequency of an exposure or release of a given magnitude would be the sum over these sequences. If some of the headings are deleted or subsumed in other headings, a simpler, but sufficient representation of the risk is achieved (see examples in Section 7.1.5).

7.1.4.2.4 Classify the Outcomes, System States, or Consequences of Each Sequence

The endpoint of each event sequence represents a potential state of the system. In ETs for nuclear reactor plants, the end points of the system analysis (i.e., the level 1 PRA) are called plant damage states. For the repository PSA, the endpoints will be termed system states or consequence categories. The end states represent conditions that affect the consequences associated with a given sequence.

For example, for an ET that addresses potential releases to the public, categories of consequences can be very qualitative in preliminary or scoping analyses (e.g., no release, small release – gases only, and small release – gases and particulates). Alternatively, the qualitative consequence categories can be more explicitly tied to the material at risk (e.g., no release, one fuel assembly breached, and basket of 8 fuel assemblies breached). The end states that result in no consequences of interest are usually labeled OK as shorthand.

The outcome of each sequence is defined by consideration of the various successes and failures of safety functions (or conditioning events) that must occur between the IE and the end point. For example, in a sequence where one spent fuel assembly has dropped and breached and the conditioning event “building containment intact” is FALSE, the release of radioactivity (gases, volatiles, and particulates) can escape to the atmosphere unimpeded and without the benefit of being filtered or released from an elevated stack. In a different sequence in which one spent fuel assembly has dropped and breached, the conditioning event “building containment intact” is TRUE and the “HVAC/HEPA filters exhaust air” is TRUE.

The consequence classification establishes initial conditions for the consequence analyses described in Section 8. The source terms, leak path factors, and atmospheric dispersion factors, including credit for stack height (appropriate to the consequence category) are used in the consequence analyses.

7.1.4.2.5 Quantify Initiating Event Frequency and Probabilities of Branches

The frequencies of IEs for internal hazards are estimated from the product of the annual frequency of each operation and the conditional probability of the IE per operation. For example, the frequency of a canister drop is estimated by the product of the frequency of canister lifts (i.e., the number per year) and the conditional probability of dropping the canister per lift. The annual frequencies of each operational step are determined from programmatic information that quantifies the number of transport casks, spent fuel assemblies, spent fuel canisters, high-level radioactive waste canisters, and WPs that are expected to be processed each year during the

preclosure operations. Per 10 CFR 63.112, the PSA will assume maximum throughput rate in these analyses.

Unless the ET is to be quantified using FT linking, branch point probabilities must be specified directly in the ET to aid in sequence quantification (see Step 6 in Figure 7-3).

The conditional probability of each enabling event (usually a failure of some preventive or mitigative feature such as a drop of a waste form) is estimated from the failure rates and repair times applicable to the event represented in the heading. Since little, or no, repository-specific data on equipment reliability is available, the ET and FT analyses will use generic data for similar operations. In many cases for the preliminary event sequence screening analyses, conservative probabilities are assumed for the conditional events (e.g., assuming a probability of 1.0 that all fuel rods breach in a drop sequence). This conservatism may be warranted in the early screening process because design criteria or design details are not in place.

Each branch under a heading in an ET (other than the IE) corresponds to a probability of the outcome (i.e., the event is TRUE or FALSE) that is conditional on the occurrence of the preceding event. The sum of the probabilities of the branches under each event heading in a given event sequence must total to 1.0. Usually the probability of the YES (or TRUE) branch is close to 1.0 by itself since it is expected to be available to successfully perform a safety function or to ensure a nominal operating environment. The FALSE (or NO) branches are usually low probability events (small fractions).

The branch-point probability values may be developed from databases of experience data) from qualified estimates of similar systems or events (see Section 7.5), from human reliability analysis (HRA, as described in Section 7.3), or from FT analyses (FTA, as described in Section 7.2). If the probabilities are independent of the preceding event, the application of data or analyses is relatively straightforward. If the probabilities are dependent (conditional) on the outcome of the preceding event, then appropriate adjustments must be made.

In FTA, adjustments are made within the structure of the FT as boundary conditions (e.g., house events; see Section 7.2). If experience data or estimates from similar systems are available for the specific condition, the analysis is straightforward. However, it may be necessary for the analyst to make reasoned estimates of the effects of previous events on the probability of interest. In such cases, the analyst must provide justification for the adjustment. For HRA, outcomes of previous events represent different performance shaping factors and the adjustments are accounted for in the quantification. For example, in the aftermath of an earthquake, repository operators may experience extra emotional stress that may lead to a higher probability of human error (see Section 7.3).

Some event branching may represent split fractions of highly likely events (e.g., 0.5 and 0.5 for equally likely conditions or 0.75 and 0.25 for cases where one branch is more likely than the other branch). For example, a conditioning event might represent the mix of waste forms being processed that possess different source term characteristics. In this example, 75 percent of the canisters may contain intact spent fuel assemblies and 25 percent of the canisters may contain fuel-rod segments. Depending on what these conditions imply, the event heading "canister contains intact assemblies" might be found late or early in the tree. If the condition affects only

the final consequence, then the event would be placed late and the number of release sequences would double. If the condition could affect the likelihood of a breach given a drop (e.g., the canisters containing fuel rod segments may be designed to withstand all credible drops without a breach), then the event heading would be placed earlier in the tree.

7.1.4.2.6 Quantify Sequence Frequencies

Unless FT linking is used, then the frequency of each sequence on the ET is determined by the multiplication of the frequency of the IE times all of the conditional probabilities appearing in the sequence of events. This method of ET quantification is typically referred to as "Large Event Tree Methodology" irrespective of the actual size of the trees. For example, if the frequency of the IE is 2×10^{-2} per year, the conditional probability of breach is 0.01, and the conditional probability of the HVAC/HEPA filter being unavailable is 0.001, the frequency of a sequence involving the release of gases, volatiles, and particulates is 2×10^{-7} per year (i.e., $2 \times 10^{-2} \times 0.01 \times 0.001$). The frequency of a sequence involving a drop, a breach, and a release of gases and volatiles through the HVAC/HEPA filter is event is 1.99×10^{-4} per year (i.e., $2 \times 10^{-2} \times 0.01 \times 0.999$). The frequency of a sequence involving a drop, no breach, and, therefore, no release is 1.98×10^{-2} per year (i.e., $2 \times 10^{-2} \times 0.99 \times 1.00$). Note that the sum of the frequencies of all of the event sequences equals the IE frequency: $2 \times 10^{-7} + 1.99 \times 10^{-4} + 1.98 \times 10^{-2} = 2 \times 10^{-2}$.

Unless FT linking is used, the event sequence frequencies may be calculated by hand using a calculator or with spreadsheet formulas (e.g., the Microsoft Excel spreadsheet program), or through the use of a computer software routine in a PRA workstation (e.g., SAPHIRE).

A separate FT is created for each event sequence if FT linking is used. These FTs are created internally using PRA software such as SAPHIRE. The ET headings that make up each sequence are inputs into a single AND gate. The single AND gate is the top event of the FT (see Section 7.2). The sequence FT is created by linking all of the event-heading FTs into a single FT. The sequence frequency is quantified by solving the FT using a computer program like SAPHIRE. The boolean algebra routine reduces a complex sequence expression to a table of minimal cutsets (see Section 7.2). Any dependencies between basic events modeled in the respective FTs for the event headings are revealed in the minimal cutsets. Because the ETs and systems used in the preclosure operations are not complex, FT linking is unlikely to be necessary in the repository PSA, particularly in the application for construction authorization (CA). When more design details are available, FT linking may be necessary to quantify event sequences and to support other analyses such as importance or sensitivity studies.

The results of the event sequence frequency analysis are used to classify event sequences as Category 1, Category 2, or BC2 Event Sequences (see Section 7.6). The ET page layout can be expanded to include a column that indicates the category of each event sequence in the tree.

7.1.4.2.7 Review of Test Results

The ET analyst and cognitive associates should review the results of the analysis to ensure that the outcomes are physically possible, accurately defined and quantified, and complete (this is an ideal, but omissions should be noted even if done deliberately for modeling purposes). As with

FT analysis, poor input data or erroneous information will lead to wrong and usually worthless ETs. The review team should include an ET analyst and cognizant personnel (e.g., personnel from design, operations, radiological consequence analysis, radiation protection programs, and safety-specific areas).

7.1.5 Examples of Applications of Event Tree Analysis

This section presents a series of ETs that were developed for instructional purposes. The three example ETs described each involve a hypothetical uncontrolled descent of a WP transporter train. The example variations between the three trees are constructed to illustrate one or more of the factors to be considered.

The hypothetical situation involves the transport of a WP from the surface facilities to the subsurface repository. The WP is enclosed in a shielded transporter car and hauled by one or more locomotives. The locomotives and transporter car are equipped with one or more brake systems, control and actuation systems that monitor and control the speed, and automatic and manual actuation systems for the brakes. During a trip down the North Ramp, an uncontrolled descent is initiated.

For illustration purposes, cases are illustrated for three different IEs. In the first case an undefined random failure in a mechanical, electrical, electronic, or software system causes the initiation of the event. In the second instance, an on-board fire on the controlling locomotive is assumed to result in an uncontrolled descent. In the third case, a human error is assumed to initiate the sequence of events leading to an uncontrolled descent.

7.1.5.1 Example 1: Random Event Initiates Uncontrolled Descent

Figure 7-4 illustrates how a hypothetical sequence of events, initiated by a random failure, can lead to or exacerbate the release of radioactive material. The event headings shown in the figure are essentially self-explanatory, but are elaborated as necessary. Recall that definitions of event headings must include unambiguous success criteria.

7.1.5.1.1 Event Tree Construction

The event headings in Figure 7-4 are arranged essentially in chronological order. They represent safety functions and conditioning events, as will be explained below. For completeness, one or more of the event headings could be defined to represent the successful operation of the mechanical, air, or hydraulic equipment of the brake system(s). For simplicity, it is assumed that these failure modes are included in the two headings that involve stopping the train. Alternatively, it may have been shown in a preliminary scoping analysis that the probability of a brake system failure is very small and only contributes to an incredible sequence. Therefore, the revised tree is simplified.

- **Uncontrolled Descent Initiated**—A random failure in a mechanical, electrical, electronic, or software system on-board the controlling locomotive causes the train to speed up.

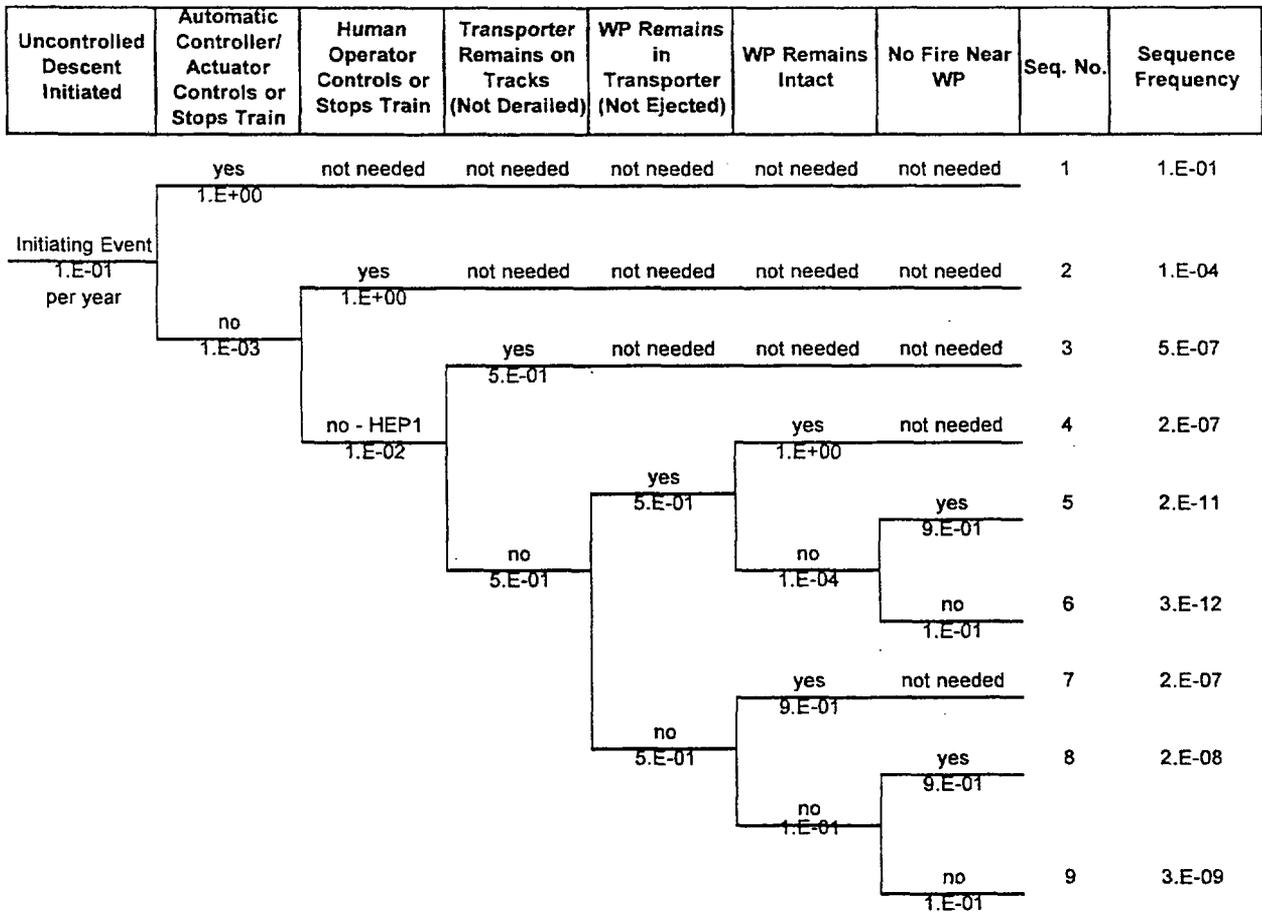


Figure 7-4. Event Tree for Hypothetical Uncontrolled Descent Due to Random-Failure Initiator

- Automatic Controller/Actuator Controls or Stops Train**–In this example it is assumed that the initiating failure has not disabled the automatic control system that monitors speed and sends signals to slow down or to apply emergency brakes when needed. This heading represents a safety function.
- Human Operator Controls or Stops Train**–In this example, it is assumed that the initiating failure has not disabled the manual control system that permits a human operator, as a backup to the automatic system, to decrease the train speed or to apply emergency brakes. This heading represents a safety function.
- Transporter Remains on Tracks (not derailed)**–There is a curve in the track at the bottom of the North Ramp. If the runaway train attains sufficient speed, it will be expected to derail and hit the tunnel walls. If the transporter train remains on the track (even at high speed) it will eventually slow down and will not experience any hard impacts. This heading represents a conditioning event.
- Waste Package Remains in Transporter (not ejected)**–The WP will be restrained inside the transporter. In the event of a derailment during the runaway, the impact on the WP is expected to be reduced by energy absorption by the transporter car. If the WP

is ejected, however, it could impinge on ground support structures, track rails, rock protrusions, and other items, and all of the kinetic energy would be imparted to the WP. This heading represents a conditioning event. The response to this heading affects the probability of breaching the WP. Although not developed in this example, the response to this heading could also affect the assumed source term if the number of fuel rods breached is correlated to the impact energy.

- **Waste Package Remains Intact**—This is the key event heading with respect to a radioactive release. If the WP is not breached, no radioactivity is assumed to be released. Otherwise, depending on the degree of breaching, varying amounts of radioactivity may be released.

The WP is designed to withstand credible impacts. The repository safety strategy is to demonstrate that impact on a WP from an uncontrolled transporter is incredible. The event analysis will provide support to that conclusion.

Nevertheless, it is possible for the WP involved in the derailment to have a manufacturing defect or out-of-specification welded lid seal. At some probability, such defective WPs may breach in an impact that is within the design basis of the WP.

- **No Fire Near Waste Package**—This heading is included in this example to illustrate the modeling of a post-accident environment that could exacerbate consequences. In the example the heading is applied only to sequences where the WP is already breached. The presence of a fire near the WP might increase the fraction of radionuclides that are released from the spent fuel rods inside the breached WP. The source of the fire is not defined in this example, but could result from an electrical fire initiated when the transporter crashes into an electrical supply cabinet. In other ET development involving intense fires, it may be appropriate to order the fire event ahead of the WP Remains Intact event to enable the fire to be a cause of the WP breach as well as a mechanism for exacerbating the release.

The ET is constructed with consideration given to dependencies and conditioning events. The construction leads to the defining of the nine sequences, as labeled in “Seq. No.” in Figure 7-4. The sequence numbers are used to describe the bases for the construction.

- Sequence 1—The automatic system responds correctly to the IE. None of the other event headings come into play and are labeled “not needed.” There is no radioactive material released in this sequence.
- Sequence 2—After the automatic system fails to respond to the IE, the train operator correctly intervenes. None of the remaining event headings come into play in mitigating the event sequence and are labeled “not needed.” There is no radioactive material released in this sequence.
- Sequence 3—After the automatic system and the train operator fail to respond to the IE, the train descends uncontrolled to the bottom of the North Ramp without

derailing. Because no impact results, the remaining event headings do not come into play and are labeled “not needed.” There is no radioactive material released in this sequence.

- Sequence 4–The transporter derails and impacts the tunnel walls. The WP remains inside the transporter and is not breached. The fire issue is not relevant (see the previous discussion) and is labeled “not needed.” There is no radioactive material released in this sequence.
- Sequences 5 and 6–The transporter derails and impacts the tunnel walls. The WP remains inside the transporter and is breached. In Sequence 5 no fire is present; Sequence 6 includes a fire. Both sequences result in a release. Because of the fire, the amount of radioactive material released in Sequence 6 may be greater than the amount released in Sequence 5.
- Sequence 7–The transporter derails and impacts the tunnel walls. The WP is ejected from the transporter and may impact walls, rails, or other items, but is not breached. The fire issue is not relevant (see the previous discussion) and is labeled “not needed.” There is no radioactive material released in this sequence.
- Sequences 8 and 9–The transporter derails and impacts the tunnel walls. The WP is ejected from the transporter and may impact walls, rails, or other items, but is not breached. In Sequence 8 no fire is present; Sequence 9 includes a fire. Both sequences result in a release of radioactive material. Because of the fire, the amount of radioactive material released in Sequence 6 may be greater than the amount released in Sequence 5.

After constructing the ET, the analyst proceeds with sequence frequency quantification, as described in the following Section.

7.1.5.1.2 Event Tree Quantification

For illustration purposes arbitrary values are assigned to the IE and the branch points in Figure 7-4. Rationale statements are provided for the parameters used in the example.

The values provided in the Figure use scientific notation with one significant digit. Therefore, the probabilities of most of the success branches are shown as 1×10^0 . The value of each success branch is actually the complement of the probability of the failure branch (i.e., if $p(\text{failure}) = 1 \times 10^{-3}$, then the $p(\text{success}) = [1 - p(\text{failure})] = [1 - (1 \times 10^{-3})] = 9.99 \times 10^{-1}$ [which is rounded to 1×10^0]).

Note that if more than one branch appears under a given event heading, the values of the probabilities may be different in the respective branches to reflect dependencies or conditions occurring earlier in the tree. Specific instances are described in the following paragraphs.

- **Uncontrolled Descent Initiated**–A frequency of 1×10^{-1} per year is assigned. The emplacement rate for WPs is assumed to be approximately 500 per year. Based on

actuarial data (if available) or analysis (such as FT), if it is determined that an uncontrolled descent could be initiated 2 times in 10,000 trips; the probability would be 2×10^{-4} per demand. Therefore, the assumed frequency is calculated as the product of 500 per year and 2×10^{-4} per demand, or 1×10^{-1} per year.

- **Automatic Controller/Actuator Controls or Stops Train**—Based on actuarial data (if available) or analysis (such as FT), it is determined that the failure rate of the control system is 1×10^{-3} . The complementary probability is $(1 - 1 \times 10^{-3}) = 9.99 \times 10^{-1}$ (which is rounded to 1×10^0).
- **Human Operator Controls or Stops Train**—Using HRA (see Section 7.3) that take into consideration the situational factors (performance shaping factors) that account for such factors as available instrumentation, control layout, and time pressure on the human, the human error probability (HEP), labeled HEP1, is estimated to be 1×10^{-2} per demand. The complementary probability is $(1 - 1 \times 10^{-2}) = 9.9 \times 10^{-1}$ (which is rounded to 1×10^0).
- **Transporter Remains on Tracks (not derailed)**—Calculations (hypothetical) indicate that the train may achieve the critical speed for derailling near the middle of the curve if the runaway starts more than halfway up the ramp. Therefore, a probability of derailment of 0.5 is assumed.

The complementary probability is $(1 - 0.5) = 0.5$.

- **Waste Package Remains in Transporter (not ejected)**—No analyses are available for the response of the transporter car and WP to a crash into a tunnel wall. Therefore, it is assumed that there is equal chance of success and failure. Therefore, a probability of WP ejection of 0.5 is assumed and a probability of derailment of 0.5 is assumed. The complementary probability is $(1 - 0.5) = 0.5$.
- **Waste Package Remains Intact**—The WP is designed to withstand credible impacts. It is possible for the WP involved in the derailment to have a manufacturing defect or out-of-specification welded lid seal. These weak WPs may breach in an impact that is within the WP design basis. The probability of WP breach is assumed to be correlated with the relative impacts of the WP ejection and non-ejection cases.

The probability of WP breach when the WP remains in the transporter is assumed to be 1×10^{-4} per demand. The complementary probability is $(1 - 1 \times 10^{-4}) = 9.999 \times 10^{-1}$ (which is rounded to 1×10^0).

The probability of WP breach when the WP is ejected from the transporter is assumed to be 1×10^{-1} per demand. The complementary probability is $(1 - 1 \times 10^{-1}) = 9.9 \times 10^{-1}$ (which is rounded to 1×10^0).

- **No Fire Near Waste Package**—No analysis is available to evaluate whether or not the construction material in the transporter car, or other sources, will ignite on impact with the wall. It is assumed that the probability is 1×10^{-1} per demand. The complementary probability is $(1 - 1 \times 10^{-1}) = 9.9 \times 10^{-1}$ (which is rounded to 1×10^0).

Using the (hypothetical) values described above, and presented in Figure 7-4, each sequence is quantified by multiplying the frequency of the IE and the probabilities of each event that occurs in that sequence. For example, the frequency of Sequence 1 is simply the product of the probability of the IE (1×10^{-1} per year) and the probability that the automatic control system functions (approximately 1.0). The result is 1×10^{-1} per year.

The frequency of Sequence 9 is more complex, involving the product of the IE frequency and six probability values.

The example in Figure 7-4 was constructed and quantified using the Microsoft Excel spreadsheet program.

Note that the values used for preliminary ET analyses may be viewed as point estimates and are generally assumed to be the median values. As described in Section 9, median values propagate through multiplication; thus, the sequence frequencies shown in Figure 7-4 are median values. For sequence frequency binning, however, the mean value of frequencies will be used. To obtain the mean values, uncertainties are quantified as described in Section 9. The IE frequency and each probability value will have a probability distribution function (PDF) assigned to it; usually a log normal distribution defined by its median value and an error factor (EF). The PDFs are then combined analytically (if simple) or using a Monte Carlo routine (for more complex problems).

7.1.5.1.3 Interpretation of Event Tree

The sequences of interest are those having “yes” in the Release column of Figure 7-3 (i.e., sequences 5, 6, 8, and 9). None of these sequences have a median frequency greater than 1×10^{-6} per year, so all of the examples have frequencies that are BC2. If it were desired to show margins to regulatory limits, consequence analyses would be performed for these sequences using methods described in Section 8.

7.1.5.1.4 Simplification of Event Trees

Consequence Binning—Consequence analyses may indicate that the release fractions from a breached WP do not vary significantly, regardless of whether or not a credible fire is present. A credible fire, in this case, is defined as one that could be initiated as a result of the runaway rather than an independent fire initiated by petroleum-based fuels. If this is the case, the ET heading “No Fire Near WP” can be eliminated because the resulting dose consequences are not different enough to warrant carrying the distinction forward in the ET. In this situation, Sequences 5 and 6 would merge into one sequence (labeled as 5A) and Sequences 8 and 9 would merge (labeled as 8A). The frequency of Sequence 5A is essentially the same as the former Sequence 5 and the frequency of Sequence 8A is essentially the same as that for Sequence 8. The ET would now have only 7 outcome sequences and only two sequences that have radioactive material releases. The modified tree is not shown.

This simplification is applied in the other examples presented in Sections 7.1.5.2 and 7.1.5.3.

Event Heading Definitions/Success Criteria—In this situation the design criteria for the WP will not withstand the potential maximum impact during the runaway. Here one or more branches under the heading “WP Remains Intact” may be candidates for simplification or deletion. The discussion of this situation starts with the original ET presented in Figure 7-4.

In one case the WP may breach whenever it is ejected from the transporter at the runaway speed. In this case the “yes” branch is eliminated (eliminates Sequence 7 in Figure 7-4) and the probability of the “no” branch becomes 1.0 (dependent failure guaranteed by the ejection). This modification would increase the frequencies of Sequences 8 and 9 by a factor of 10 (the inverse of 1×10^{-1} per demand). The probability of WP failure when it remains in the transporter might also be increased (e.g., to 1×10^{-2} per demand), thus affecting the frequencies of Sequences 5 and 6. This modified (simplified) ET is presented in Figure 7-5.

In another case, where it is shown or assumed that it does not matter whether or not the WP is ejected from the transporter, the heading “WP Remains in Transporter (not ejected)” is irrelevant and can be deleted from the tree. Therefore, Sequences 4 through 7 are eliminated from the original ET. The frequencies of the releases in Sequences 8 and 9 increase. The heading “WP Remains Intact” could be merged with “Transporter Remains on Tracks (not derailed)” to further simplify the analysis (under these circumstances any derailment results in a release) or the headings could be retained to enhance communication of the events in the sequence and gain insights. This modified (simplified) ET is presented in Figure 7-6.

7.1.5.2 Example 2: On-board Fire Initiates Uncontrolled Descent

This example is presented to illustrate how a previously developed ET may be modified to represent other initiators. In particular, this example illustrates how the ET for the uncontrolled transporter descent, initiated by a random failure internal to its operational systems, can be modified to represent potential events initiated by a fire. Figure 7-7 illustrates this example.

7.1.5.2.1 Event Tree Construction

The ET depicted in Figure 7-4 and the event descriptions in Section 7.1.5.1.1 are used with modifications, as described in the following text. The ET is initially simplified by assuming that the event heading “No Fire Near WP” is irrelevant (see Section 7.1.5.1.1). The IE titled “Uncontrolled Descent Initiated” is not shown explicitly in this ET; it is a potential consequence of subsequent failure events.

The following event headings are used:

- **Fire Initiated in Transporter Locomotive**—This IE represents a fire that could occur in any of the electrical components and wiring in the controlling locomotive.
- **Fire Suppression System Extinguishes Fire**—The transporter locomotives will be equipped with automatic fire-suppression systems in accordance with the need defined through a fire hazards analysis. The successful operation of this system influences dependent events, as described below.

- **Automatic Controller/Actuator Controls or Stops Train**—In this example, two different pre-conditions are modeled. In the first case, shown in the upper portion of Figure 7-7, the fire suppression system is successful in extinguishing the fire before it causes failure of the automatic control system. However, the automatic control system could subsequently fail for other independent causes. Should such a failure occur, given that a runaway was initiated by the initial fire, the “no” branch is developed in the same manner as that depicted in Figure 7-4.

In the case where “Fire Suppression System Extinguishes Fire” is unsuccessful (the no branch), it is assumed that there is a dependent failure; that is, a common-cause failure (CCF) of the function titled “Automatic Controller/Actuator Controls or Stops Train.” This failure is given as “GF (CCF/Fire)” in Figure 7-7 to indicate a guaranteed failure due to the CCF.

- **Human Operator Controls or Stops Train**—For illustration it is assumed in this example that the human-actuated controls are not failed by the fire; however, the probability of human error is affected. In the upper portion of the ET depicted in Figure 7-7, following the independent failure of the automatic control system, the probability of human error is assumed to be the same as in Figure 7-4 (labeled as HEP1). In the lower portion of the ET, in the aftermath of the fire that progresses far enough to cause failure of the automatic control system, the operator may react with lower reliability because of the extra distractions and stresses. This probability is labeled as HEP2 in Figure 7-7.
- **Transporter Remains on Tracks (not derailed)**—Same as in Section 7.1.5.1.1.
- **Waste Package Remains in Transporter (not ejected)**—Same as in Section 7.1.5.1.1.
- **Waste Package Remains Intact**—Same as in Section 7.1.5.1.1.

7.1.5.2.2 Event Tree Quantification

This example will discuss the features of Figure 7-7 that are different than Figure 7-4.

- **Fire Initiated in Transporter Locomotive**—For illustration, an arbitrary frequency of 1×10^{-1} per year is specified. An actual analysis would apply actuarial data for electric locomotives.
- **Fire Suppression System Extinguishes Fire**—An estimate of the failure probability is developed from FT analysis or from actuarial data, supported by a fire-propagation analysis.
- **Automatic Controller/Actuator Controls or Stops Train**—If the fire suppression system is successful in extinguishing the fire before it causes failure of the automatic control system, the same value for independent failure from Figure 7-4 is used (i.e., 1×10^{-3} per demand).

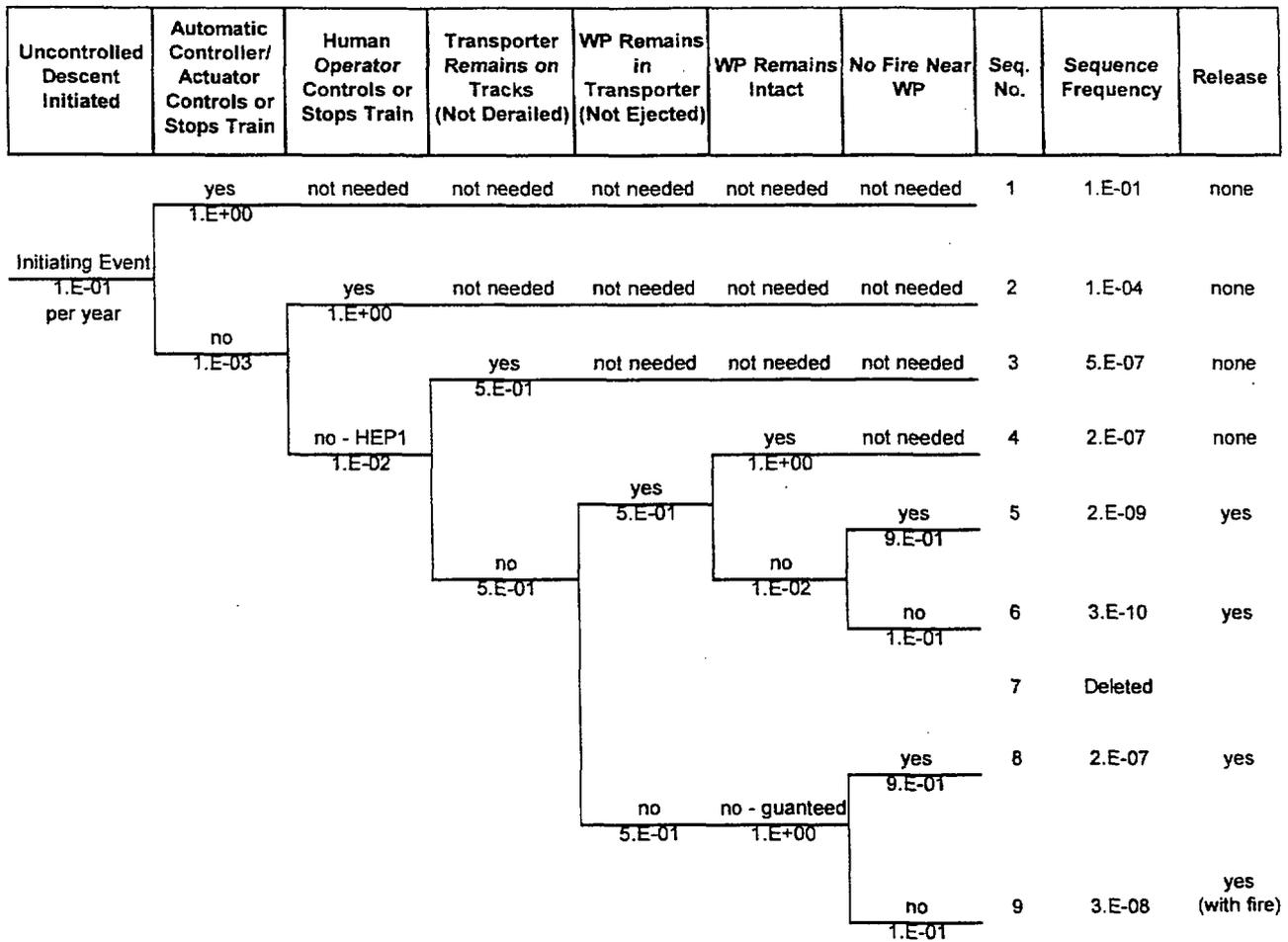


Figure 7-5. Simplified Event Tree for Hypothetical Uncontrolled Descent (First Example)

In the case where “Fire Suppression System Extinguishes Fire” is unsuccessful, the automatic system fails due to a CCF. This is given as “GF (CCF/Fire)” in Figure 7-7, and the conditional probability is 1.0.

- **Human Operator Controls or Stops Train**—In the upper portion of the tree (Figure 7-7) following the independent failure of the automatic control system, the probability of human error is assumed to be same as in Figure 7-4, labeled as HEP1. It is quantified as 1×10^{-2} per demand.

In the lower portion of the tree, in the aftermath of the fire that progresses far enough to cause failure of the automatic control system, the operator may react with lower reliability because of extra distractions and stresses. This probability is labeled HEP2 (Figure 7-7). Using HRA (see Section 7.3) that accounts for the situational factors (performance shaping factors) that account for such factors as available instrumentation, control layout, and time pressure on the human, the HEP, labeled HEP2, is estimated to be higher by an order of magnitude (i.e., 1×10^{-1} per demand).

The quantification of the remaining events in Figure 7-7 are the same as in Figure 7-4.

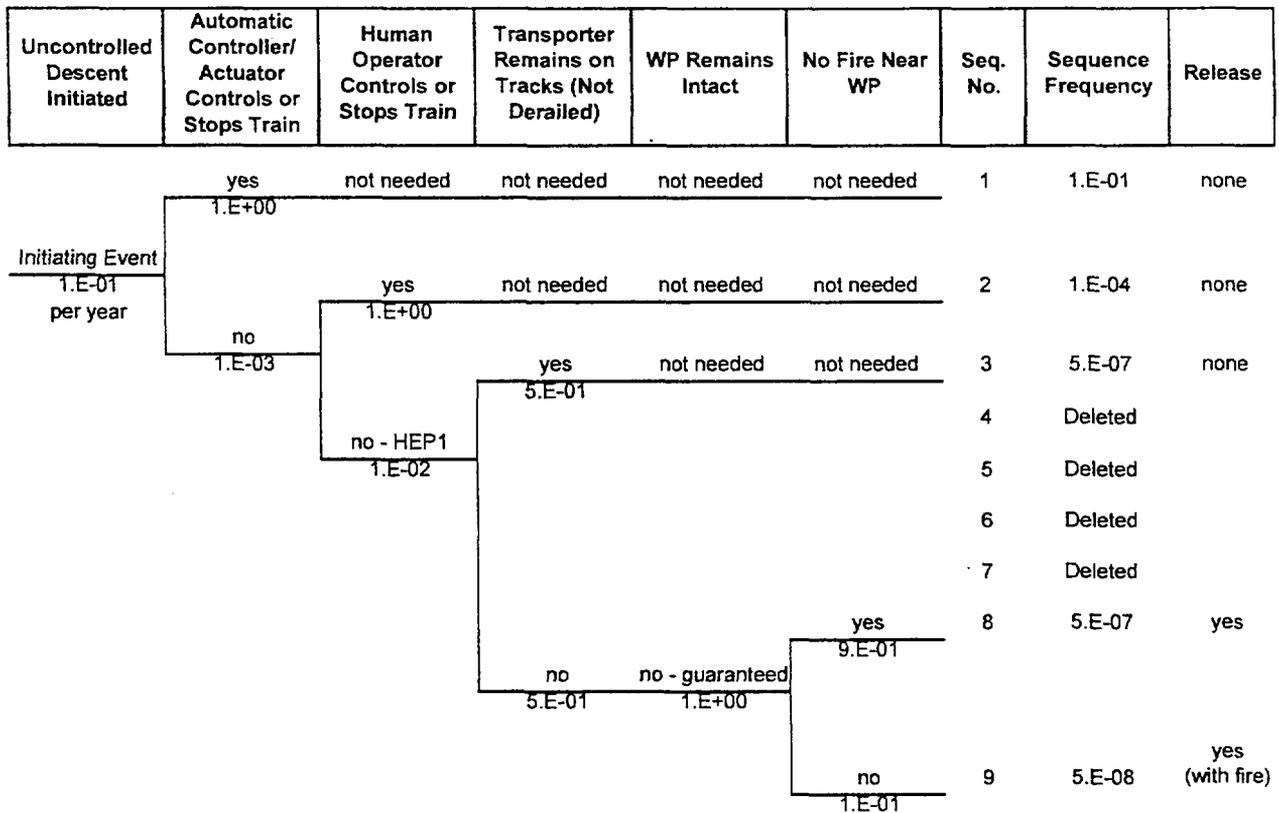


Figure 7-6. Simplified Event Tree for Hypothetical Uncontrolled Descent (Second Example)

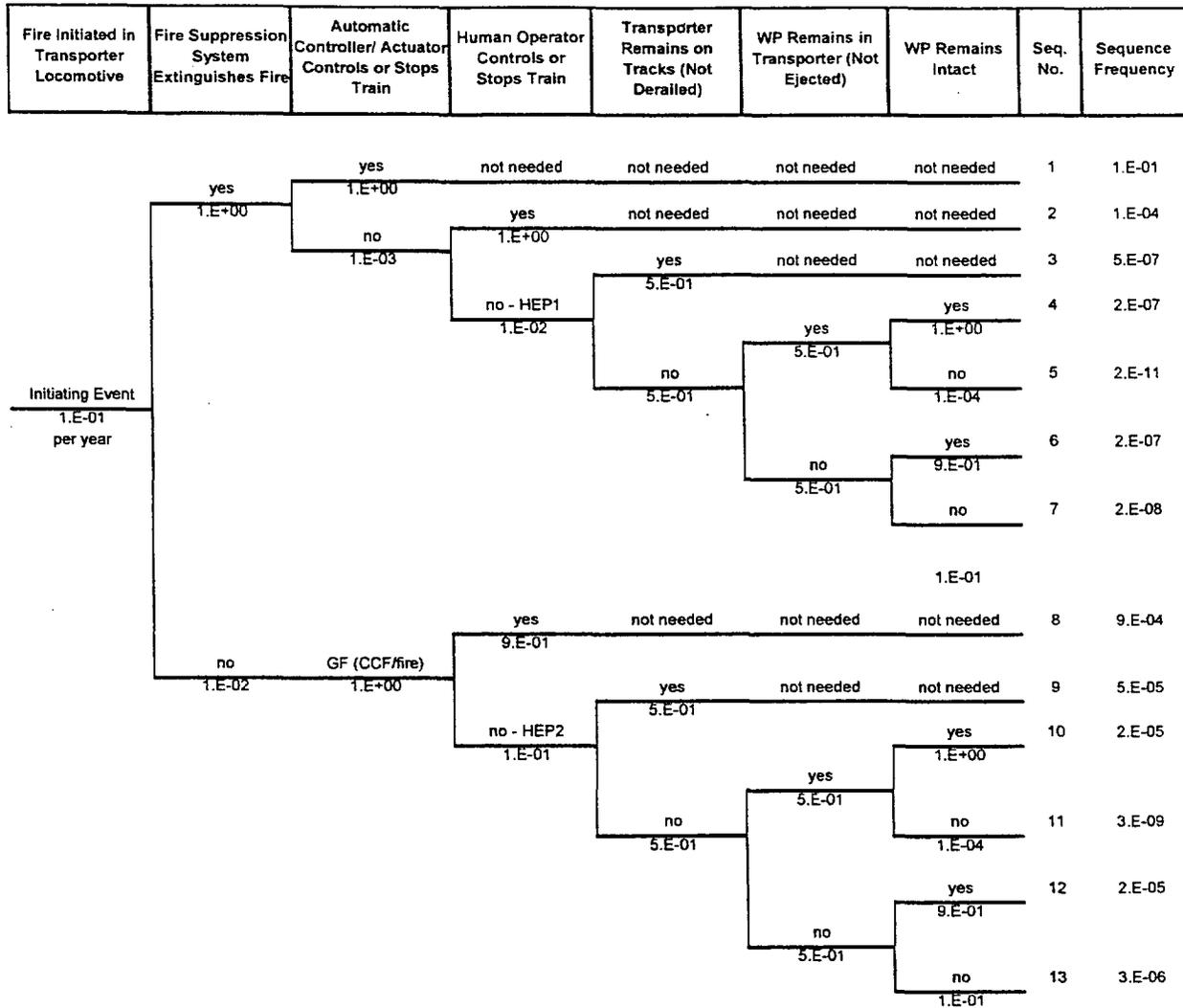
- **Transporter Remains on Tracks (not derailed)**—Same as in Section 7.1.5.1.2.
- **Waste Package Remains in Transporter (not ejected)**—Same as in Section 7.1.5.1.2.
- **Waste Package Remains Intact**—Same as in Section 7.1.5.1.2.

The quantification of sequence frequencies proceeds the same as described in Section 7.1.5.1.2, using the Microsoft Excel spreadsheet program.

7.1.5.3 Example 3: Human Operator Initiates Uncontrolled Descent

This example is presented to further illustrate how dependent events affect the construction and quantification of ETs.

In this example, it is assumed that an operator on the control locomotive or in a central control room commits an erroneous action that not only initiates an uncontrolled descent, but also disables all of the systems that can be used to control the speed or apply emergency brakes.



NOTE: GF = guaranteed fault.

Figure 7-7. Event Tree for Hypothetical Fire Initiated Uncontrolled Descent

7.1.5.3.1 Event Tree Construction

The example ET is shown in Figure 7-8. The event descriptions in Section 7.1.5.1.1 are used, with modifications as described in the following paragraphs. The tree is simplified by assuming that the event heading “No Fire Near WP” is irrelevant (see Section 7.1.5.1.1). The IE titled “Uncontrolled Descent Initiated” is not shown explicitly in this tree; it is a potential consequence of subsequent failure events.

The following event headings are used.

- **Uncontrolled Descent Initiated by Operator Error**—An operator on the control locomotive or in a central control room, commits an erroneous action that initiates an uncontrolled descent.

The event frequency is estimated to be 1×10^{-3} per year based on actuarial data or HRA.

- **Automatic Controller/Actuator Controls or Stops Train**—In this example, it is assumed that the initial operator error also causes a dependent (common-cause) failure of the automatic controller. This dependent, guaranteed failure deletes the chance for a success (yes) branch under this event heading. It is labeled “GF (CCF)” in Figure 7-8.

The conditional failure probability is 1.0.

- **Human Operator Controls or Stops Train**—This event may be considered to be the same event as the IE and could be deleted from the tree structure. However, it could also be a true dependency where the initial operator error disables the system that an operator (not necessarily the same one) would attempt to use as an emergency action.

For this example, a CCF is assumed, and no success branch is shown. The “no” branch is labeled “GF (CCF)” in Figure 7-8 with a conditional failure probability is 1.0.

In other constructions, the probability of operator recovery might be included to generate a success branch under this event.

The definitions and quantification of the remaining events in Figure 7-8 are the same as in Figure 7-4.

- **Transporter Remains on Tracks (not derailed)**—Same as in Section 7.1.5.1.1.
- **Waste Package Remains in Transporter (not ejected)**—Same as in Section 7.1.5.1.1.
- **Waste Package Remains Intact**—Same as in Section 7.1.5.1.1.

7.1.5.3.2 Quantification

The quantification of sequence frequencies proceeds the same as described in Section 7.1.5.1.2, using the Microsoft Excel spreadsheet program.

7.2 FAULT TREE ANALYSIS

7.2.1 Introduction

This section defines the bases and methodology for the construction and use of FTA in support of the PSA. Logic models of physical system are applied in FTA for the purpose of quantifying the probabilities of top events based on combinations of basic events that represent mechanical failures or human error. The use of FTA has application in 1) quantifying the frequency of IEs as well as the conditional probability of enabling events that contribute to event sequences, 2) explicit modeling and quantifying of dependencies between primary (front-line) safety systems and support systems, 3) top-down modeling of combinations of events that lead to an undesired outcome, including development of master logic diagrams, 4) defining how operation-specific controls and management measures can be used to prevent or mitigate releases of radioactivity, and 5) providing a structure for propagating uncertainties in basic events to the top event.

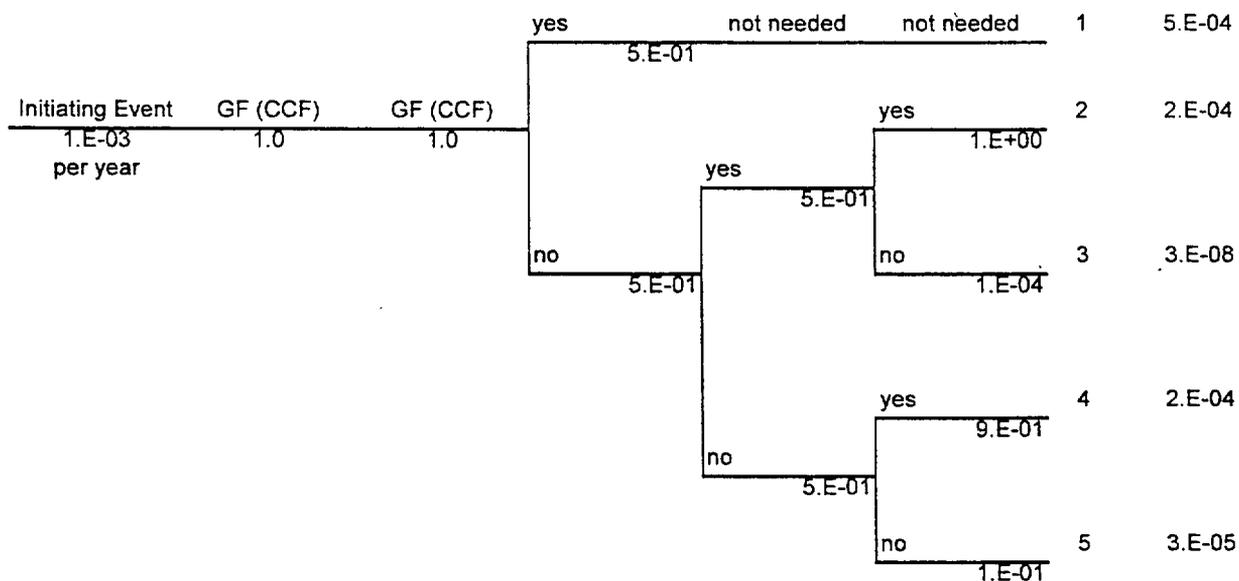
This section provides a cursory, focused guide to the construction, application, and evaluation (both qualitative and quantitative) of FT models. While some concepts are universal to all FTAs, the applications in this section are focused on support of the PSA for a repository. The guide is not meant to be a textbook or exhaustive. Where appropriate, reference is made to literature for additional information.

7.2.2 Overview of Approach

The use of FTAs is a special branch of systems analysis. The goal of FTA, similar to other systems analysis, is to effect a structured analysis of complex systems using abstractions and approximations to support decision-making in safety and engineering. FTA is used to synthesize information from which to infer potential vulnerabilities as well as to estimate the probabilities of undesired events.

General Description—An FT model maps physical systems into a logic model based on deductive logic. The deductive model begins at some undesired event (or consequence), such as release of radioactivity from surface facility, and identifies (deduces) all of the causes of the undesired event. The undesired event is termed the top event in FTA and must be defined precisely. The model is developed downward from the top event through the various levels of assembly and usually stops at the basic event level. That is, an FTA for the top event, “release of radioactivity from surface facility,” would proceed from facility to building to operation to system to subsystem to the basic events that are failures in specific hardware components, software, electronic control or logic elements, human errors, or loss of essential support functions, such as loss alternating current (AC) electrical power. The FT can include the loss of, or circumvention of, design and administrative controls. The basic events for a given component, therefore, may represent independent failures, CCFs, or dependent failures (see Section 7.5 for more information on CCFs and dependent failures).

Uncontrolled Descent Initiated by Operator Error	Automatic Controller/ Actuator Controls or Stops Train	Human Operator Controls or Stops Train	Transporter Remains on Tracks (Not Derailed)	WP Remains in Transporter (Not Ejected)	WP Remains Intact	Seq. No.	Sequence Frequency
--------------------------------------------------	--------------------------------------------------------	----------------------------------------	----------------------------------------------	-----------------------------------------	-------------------	----------	--------------------



NOTE: GF = guaranteed fault.

Figure 7-8. Event Tree for Hypothetical Human Error Initiated Uncontrolled Descent

Master Logic Diagram—An FT developed for a top event such as “release of radioactivity from surface facility” is sometimes termed a master logic diagram as a framework for identifying and organizing all of the hazards at a given facility. In this application, the top event is defined broadly but explicitly. The causes and probability of a given accident or class of accidents for a specific facility are also analyzed with FT logic. In this application, the top event might be “release of radioactivity from transport cask unloading facility resulting in dose greater than 5 rem at site boundary.” The FT logic is applied to identify all of the fault combinations that must occur to result in the defined top event. Various paths from the top event down to the fundamental or basic events (e.g., human errors, equipment failures, and earthquakes) comprise alternative event sequences (or accident scenarios). Thus, the FT logic will usually capture the same scenarios as identified in ET analysis. However, individual sequences of events may be difficult to define in complex FTs.

System Analyses/ET Headings—Most applications of FTA, however, involve evaluations of the vulnerabilities within a given system or of the unreliability (or unavailability) of that system. The system unavailabilities are needed, for example, to quantify the probabilities of event headings in ETs and support quantification of event sequence frequencies. For example, an ET for the waste handling building might have an event heading “HVAC/HEPA filter starts and runs for 24 hours,” expressed as a success criterion. An FTA of the HVAC/HEPA filter system is

developed to reveal how failures of the system may occur (the vulnerabilities), and to estimate the probability of the failure branch under that ET heading.

Selection of Top Event and Success Criteria—The FT top event for a system is generally defined as a complete, or catastrophic, failure of the system resulting in the unavailability of the desired function. It is important to be careful in choosing the top event and its success criterion. If the definition is too general, the analysis will be unmanageable. The analysis will not provide a sufficiently wide view of the system and its interfaces if the top event is too specific.

Qualitative Evaluation/Cutset Generation—The FT model is solved qualitatively using the rules of boolean algebra to reveal the number of combinations of basic events that can result in the occurrence of the top event. Section 7.2.4.1 presents basic boolean algebra as background material for the FT analyst. A summary of boolean algebra is presented in Section VII of the *Fault Tree Handbook* (Vesely et al. 1981). The combinations of events that lead to the top event are termed cutsets. Through complete boolean reduction, the least number of unique cutsets are determined and are termed the minimal cutsets. The occurrence of at least one of the minimal cutsets will result in the occurrence of the top event. The probability that the top event will occur is the union (or OR logic, or arithmetic sum) of the probabilities represented by the minimal cutsets.

The results of a qualitative FTA provide insights into potential system vulnerabilities that may, in some cases, be prevented or reduced in probability through design or operational modifications. For example, if the cutset analysis reveals that the system is very vulnerable to a human error by the facility operator (e.g., to ensure building air-tightness) then an interlock switch could be introduced into the design such that the system failure requires the concurrent failure of the interlock and the operator error.

Stated another way, qualitative FTA also serves to demonstrate the defense-in-depth of a system. A simple FT can determine if a potential accident condition or a system performance is defended against a single failure (or single contingency). A hand-drawn FT also can be a useful tool for the safety analyst.

In applications of an FTA program such as SAPHIRE (Russel et al. 1994), the analyst can truncate the qualitative analysis by specifying the maximum order of cutsets to be generated. The order is the number of concurrent basic events to be included in a minimal cutset. A singlet cutset includes one basic event (i.e., it represents a single-point failure) and may include a known and unlikely passive failure such as the collapse of a shield wall or may reveal the key human error, as discussed previously. A doublet cutset represents the concurrent occurrence, or intersection (or AND logic, or arithmetic product) of two basic events. In the previous example, a design modification that added an interlock to prevent the human error single point failure would produce a doublet in a revised FTA: the human error is ANDed with failure of the interlock. The cutset ordering continues through triplet, quadruplet, and so forth. In practical terms, it is seldom necessary to go beyond doublets or triplets unless the system is very complex.

Quantitative Evaluation/Top Event Probability—The FT model may be solved quantitatively after the minimal cutsets have been derived. The probability of the top event is represented by the union (or OR logic, or arithmetic sum) of all of the minimal cutsets. Quantitative

probabilities are inserted for all of the basic events that appear in the minimal cutsets. The symbolic boolean operations of intersection (AND) is replaced with the arithmetic operation of multiplication and the union (OR) is replaced by summation. The basic event probabilities are derived as described in Sections 7.3, 7.4, and 7.5. Quantitative FTA is used in the quantification of event sequence frequencies (i.e., by direct or indirect linking to ETs) and categorization of event sequences.

The probability of each minimal cutset is quantified by the multiplication of the probabilities of all of the basic events appearing in it. The top event probability is calculated by adding the probabilities of all of the minimal cutsets.

The results of a quantitative FTA provide a different degree of insight into potential system vulnerabilities than is provided by the qualitative FTA. For example, by maintaining the discrete probabilities of individual cutsets, it is revealing to rank their contribution to the top event probability. This methodology provides visual insights into the dominant contributors as well as a means for formal importance ranking. Knowledge of the relative importance of various cutsets and the basic events that contribute to the top event (e.g., hardware failures, software failures, human errors, and CCFs) can be used to prioritize design alternatives, importance to safety classifications, and other risk-informed analyses.

The analyst can truncate the quantitative analysis by specifying the minimum cutset probability to be generated in an FTA application program such as SAPHIRE. Thus, if the analyst is interested in finding the dominant contributors to a total system unavailability that is on the order of 10^{-3} per demand, a minimum cutset probability of perhaps 10^{-4} to 10^{-5} might be specified since 10 to 100 cutsets are required to produce the top event probability range. On the other hand, if a top event probability of 10^{-6} is needed, the cutoff probability for individual cutsets might be set at 10^{-8} to 10^{-9} , at least initially, to ensure that all significant contributors are accounted for. Several iterations are usually required to settle in at an appropriate cutoff probability for a given system.

7.2.3 Details of Approach

This section presents a brief introduction to the fundamental elements of FTA. The PSA analyst should consult the *Fault Tree Handbook* (Vesely et al. 1981), the *PRA Procedures Guide* (NRC 1983), and the SAPHIRE Users' Manual (Russell et al. 1994) for more information.

7.2.3.1 Essential Boolean Algebra

It is not necessary for the FT analyst to understand boolean algebra unless it is required to solve an FT by hand. The FT programs such as SAPHIRE (Russell et al. 1994) provide all of the manipulations of boolean expressions for the analyst. In many cases, simple FTs can be solved by hand using the rudimentary elements of boolean algebra. The following discussion presents the boolean operations, their arithmetic (engineering) equivalent notations, and their corresponding probability expressions. The examples represent the occurrence of event C after operating on events A and B, and their respective probabilities (i.e., $p(A)$, $p(B)$, and $p(C)$).

Union [OR logic, sum of event probabilities]	$C = A \cup B; C = A \text{ OR } B; p(C) = p(A) + p(B) - [p(A) p(B)]$	(Eq. 7-1)
Intersection [AND logic, multiplication of event probabilities]	$C = A \cap B; C = A \text{ AND } B; p(C) = p(A)p(B)$	(Eq. 7-2)
Absorption (reduce condition for TRUE expression to minimum), for example,	$C1 = A \cup (A \cap B) = A; C1 = A \text{ OR } (A \text{ AND } B) = A; p(C1) = p(A) + (p(A) p(B)) = p(A)$ $C2 = A \cap (A \cup B) = A; C2 = A \text{ AND } (A \text{ OR } B) = A; p(C1) = p(A) (p(A) + p(B)) = p(A)$ Note that if A is TRUE then C is TRUE no matter whether B is TRUE or FALSE. The sub-expressions involving B has been absorbed by those expressions involving A.	(Eq. 7-3) (Eq. 7-4)
Complementation [Event NOT A (or \bar{A} , or A') is the complement of event A]	$C3 = A \cup \bar{A} = 1; C3 = A + \bar{A} = 1; p(C3) = p(A) + p(\bar{A}) = 1$ $C4 = A \cap \bar{A} = \phi [\text{null}]; C4 = A \bar{A} = 0; p(C4) = p(A)p(\bar{A}) = 0$	(Eq. 7-5) (Eq. 7-6)

The boolean logic of AND and OR form the basic building blocks of an FT structure. Specialized adaptations of the AND logic have been introduced into FT symbology as described below. The rule of boolean logic, especially ABSORPTION and COMPLEMENTATION are used in solving an FT (i.e., finding the minimal cutsets among all the possible combinations of basic events).

7.2.3.2 Fault Tree Symbols

The symbols used in FT construction are illustrated in Figure 7-9. These symbols have been standardized and have been incorporated into the graphics and logic of programs such as SAPHIRE. It is unlikely that FTA performed for preclosure safety will use all of the symbols and their associated logic, but all are presented for completeness.

7.2.3.2.1 Top Events and Intermediate Events

A rectangle used to enclose the precise statement about the top event or an intermediate event. The event described in the rectangle represents a fault event that occurs because of the occurrence of one or more antecedent events acting through logic gates. A rectangle is usually opened by specifying a logic gate (an AND or OR gate) as a place to enter the textual description of the top or intermediate event in a program such as SAPHIRE. But, intermediate event descriptions are often included in rectangles in a tree structure as clarifying descriptions with pass through logic (i.e., no AND or OR).

Several symbols are used to indicate the types of primary or fundamental events that act as antecedents or conditioning events for faults higher in a tree.

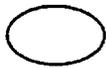
7.2.3.2.2 Primary Events

Basic Event—A basic event is a fault that requires no further development; it is represented by a circle. The circle signifies that the appropriate limit of resolution has been reached. It signifies that the stopping rule for the analysis scope has been satisfied. A basic event may be a component failure, a system failure, software

PRIMARY EVENT SYMBOLS



BASIC EVENT — A basic initiating fault requiring no further development



CONDITIONING EVENT — Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

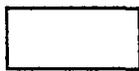


UNDEVELOPED EVENT — An event which is not further developed either because it is of insufficient consequence or because information is unavailable



EXTERNAL EVENT — An event which is normally expected to occur

INTERMEDIATE EVENT SYMBOLS



INTERMEDIATE EVENT — A fault event that occurs because of one or more antecedent causes acting through logic gates

GATE SYMBOLS



AND — Output fault occurs if all of the input faults occur



OR — Output fault occurs if at least one of the input faults occurs



EXCLUSIVE OR — Output fault occurs if exactly one of the input faults occurs



PRIORITY AND — Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)



INHIBIT — Output fault occurs if the single fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

TRANSFER SYMBOLS



TRANSFER IN — Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)



TRANSFER OUT — Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

Figure 7-9. Standard Fault-Tree Symbols

failures, a human error, or a CCF. The probability or failure rate of a basic event, along with its uncertainty distribution, represents the fundamental input to a quantitative FTA.

- **Undeveloped Event**—An undeveloped event is represented by a diamond. This symbol represents an event that could be developed further toward basic events. However, it is not further developed because it does not cause significant consequences, sufficient information is not available to warrant decomposition, information is available for faults at the higher level, or the analyst wants a placeholder. For example, an event titled “loss of AC power supply ‘Train A’ to HVAC/HEPA filters” might be shown as a diamond on an FT as an input to “HVAC/HEPA filter fails to start and run for 24 hours.” The analyst may either quantify the probability of the loss of AC “Train A” or later change the diamond to a TRANSFER (definition to follow) to a detailed FT for the AC power system.
- **Conditioning Event**—A conditioning event is represented by an ellipse (oval). This symbol represents a restriction or condition that can be applied to any logic gate but is used primarily with PRIORITY and INHIBIT gates. For example, an FT for a potential criticality event might have a conditioning event titled “moderator is present” as an input to an AND gate that also includes “misload of WP” and “neutron absorber omitted from WP.”
- **External Event**—An external event is represented by a house. This symbol does not represent a fault; it represents an event that is expected to occur. It may play the role of a conditioning event or a contingency event. For example, an FT might model an event such as “AC applied to motor startup sequencer” due to an out-of-sequence relay operation whose primary fault be “relay contacts fail closed.” An EXTERNAL EVENT titled “AC power available to motor start sequencer” would show the need for the presence of the additional event or condition before the fault could occur.

7.2.3.2.3 Gate Symbols

The gate symbols and the logic they represent provide the backbone of an FT structure. The operational aspect of a gate is to define whether the output of the gate is TRUE or FALSE depending on the status of several inputs to the gate. When the output of a gate is TRUE in an FT, the fault described in the event box occurs (exists). The logical operation of each kind of gate is described as follows:

- **AND**—The AND gate is represented by a flat-bottomed arch (or mailbox). The OUTPUT fault occurs if, and only if, all of the input events or faults occur.
- **OR**—The OR gate is represented by an arch-bottomed barn roof (or bishop’s hat). The OUTPUT fault occurs if at least one of the input events or fault occurs. This gate is sometimes called the INCLUSIVE OR to distinguish it from the EXCLUSIVE OR (description to follow). However, most FTAs encountered in the PSA for the repository will use the basic (or inclusive) OR (see discussion of EXCLUSIVE OR).

- **Exclusive OR**—The exclusive OR is represented by a modified OR symbol that has an arch-bottomed triangle inside the “barn,” or “rafters” from the peak of the barn to the bottom. The output fault occurs if exactly one of the input events or faults occurs. Alternatively, this logic could be represented by an OR gate with a conditioning event specifying a required order of the inputs or exclusion statement “A not B, or B not A.” It is noted in the *Fault Tree Handbook* (Vesely et al. 1981) that the quantitative difference between the inclusive and exclusive OR events is generally insignificant.
- **Priority AND**—Priority AND is represented by an AND gate with an inscribed triangle (caution: it looks similar to the exclusive OR gate but has a flat bottom). The output fault occurs only if all of the inputs occur (like the AND gate) in the prescribed sequence order. If A, B, and C are three inputs to the PRIORITY AND, read left to right, the output occurs only if A occurs before B, B occurs before C, and C occurs. Alternatively, this logic could be represented by an AND gate with a CONDITIONING EVENT specifying the required order of the inputs (as “A before B, B before C”).
- **Inhibit**—An INHIBIT is represented by a hexagon. The INHIBIT is a special kind of AND gate that propagates a fault in the presence of an enabling condition. The single input fault is shown as the only input into the bottom apex of the hexagon and the enabling condition as a CONDITIONING EVENT connected to the side of the hexagon. For example, an INHIBIT event might be defined as “fire protection system fails to prevent control system failure” with the only input fault being “fire protection system fails” while the conditioning event is “fire greater than Z degrees occurs in control area.” There is little distinction in this example between the fires as conditioning events, rather than external (house) event, except in the specificity of fire severity.
- **K-out-of-N**—K-out-of-N is represented by an OR gate with an attached oval. This gate symbol states the condition for occurrence of the intermediate event, which requires failure of K components out of N total to cause the described intermediate fault event. This gate symbol is a shortcut for the actual boolean logic, which is a combination of AND gates with combinations of the basic events as inputs. Here the AND gates are input to the OR gate of the intermediate event. This gate symbol is often used in modeling the failure logic of safety-related instrumentation and control systems in which safety is balanced against trip avoidance. It is unlikely that instrumentation and control systems for a repository will use such logic; however, other systems having multiple levels of redundancy, such as the HVAC system of a waste-handling building, may use this type of gate.

7.2.3.2.4 Transfer Symbols

The transfer symbols serve several purposes:

- Assist the analyst in controlling the complexity and graphic scale of an FT so text remains legible (e.g., to put a complex tree on multiple pages),

- Allow modularization to direct the flow of fault to repeated elements without redrawing portions of the FT (e.g., a fault in a motor-control center may be a common input to several fans in a complex HVAC system), and
- Permit linking of trees of main systems to subsystems or to support systems (e.g., the main HVAC FT may link to subsystems in primary and secondary isolation zones to portions of an AC power supply system).

The TRANSFER IN and TRANSFER OUT symbols work together, often as pairs. For each TRANSFER IN, there must be a corresponding TRANSFER OUT in another page of the FT or in an FT for the corresponding subsystem or support system. Note that it is possible for multiple TRANSFER INs to be linked to a single TRANSFER OUT.

A TRANSFER IN is indicated by a triangle with a connection from its top apex to an EVENT BOX. The TRANSFER IN indicates that the event defined is developed further at the occurrence of the corresponding TRANSFER OUT. For example, two inputs to the event “HVAC/HEPA filter system fails to start and run for 24 hours” through an AND gate might be “Train A of HVAC/HEPA filter system fails to start and run for 24 hours” and “Train B of HVAC/HEPA filter system fails to start and run for 24 hours.” Each of the latter events could be shown as a TRANSFER IN events. The corresponding TRANSFER OUT events would be attached to the top events of FTs representing, respectively, “Train A ...” and “Train B ...”

A TRANSFER OUT is indicated by a triangle with connection out of its side to an EVENT BOX. The TRANSFER OUT symbol indicates that the tree structure represented below the top event is effectively a part of one or more other FTs that have faults at higher levels of assembly.

The application of the various symbols will be described later in several examples.

7.2.3.3 Guidance on Fault Tree Construction

This section describes how FT models are constructed using deductive logic. The discussion is oriented toward logic modeling to support the PSA of a repository at relatively high level of design detail.

Actual applications of FTA to the repository PSA are provided in Subsurface Transporter Safety Systems Analysis (CRWMS M&O 2000) based on FT models developed in Application of Logic Diagrams and Common-Cause Failures to Design Basis Events (CRWMS M&O 1997). The logic models were based on a limited amount of design detail but were quite extensive in defining the potential human errors and CCFs that lead to the undesired top event. Portions of this application were used as examples in the following discussion.

The necessary ingredients in FT construction include an understanding of the systems and an understanding of how things may go wrong. The Fault Tree Handbook (Vesely et al. 1981) has attempted to make FT construction more systematic, by developing rules for FT construction. The analyst is referred to Chapter V of the Fault Tree Handbook (Vesely et al. 1981) for a discussion on the fundamentals of FT analysis of complex systems. The following material is provided as background information and terminology that is useful in helping the PSA team gain experience as FT analysts.

Each event in an FT has a name and a description. The name is an abbreviated set of letters, numbers, or characters that is used as a unique label on graphics, in databases, and reports. The name is generally recognizable by key letters, although not in complex trees or if system-specific identification tags are used. The description may be a verbose, full definition of the event that may be tabulated with the event name, or it may be an abbreviated version that fits conveniently into the graphic displays and printouts.

This section adapts several of the rules of the *Fault Tree Handbook* (Vesely et al. 1981) in examples that are more appropriate to the PSA.

Rule 1 - Top Event Definition—The top event is defined as precisely as it can be expressed. It is an undesired event (e.g., an entire accident sequence) or a description of specific events that contribute to an accident sequence (e.g., the IE, the failure of a specific safety function or system, or a particular human error). The FTs will represent the failure or unavailability of an event defined in an ET model of potential accident sequences in most cases. As noted, the headings of an ET are defined in terms of specific success criteria that must be achieved to take credit for the safety function. The corresponding FT models the complement of the event heading success criteria; that is, the top event of the FT represents the probability that the success criteria are not met.

For any events described in an FT model, precision is the key factor to proper logic development. The statements entered in the top event (and other event boxes) are expressed as a fault (or a failure). The fault (WHAT condition) and when it occurs (WHEN condition) should be precisely stated. The WHAT condition describes the relevant failed (or undesired operating) state of the function, structure, system, or component. The WHEN condition describes the condition of the system that makes the WHAT condition a fault. The analyst should be as verbose as necessary to precisely define the fault condition. The event box in the tree diagram should not dictate the event description. Words, but not ideas, should be abbreviated if necessary.

An example undesired event sequence involves a runaway transporter train on the North Ramp during a descent to emplace a WP. After the occurrence of an event that initiates a runaway, automatic systems and HAs are called upon to arrest the runaway before a derailment or impact on the WP occurs. The success criteria would be “runaway is controlled before train attains derailment speed on the North Ramp (during descent of the North Ramp).” The first part of the description defines the WHAT condition, and the phrase in parentheses defines the WHEN condition. The phrase in parentheses might be omitted for brevity in the FT, but must be clearly stated in the definition of the condition of interest. The corresponding top event of an FT model would be “failure to control runaway before train achieves derailment speed during descent of the North Ramp,” as illustrated in Figure 7-10. The name given to the top event is CONTRUN.

The specification of the WHEN condition during descent of the North Ramp may serve to identify the event, by contrast, to a similar event (e.g., during an ascent or the North Ramp, or during the descent of a different portion of the main tunnel, such as a North Ramp Extension). The WHEN condition may also assist in the definition of a specific time span, or mission time, during which success is required.

Deductive logic is then applied successively at lower and lower levels of decomposition until the model is sufficient to support the analysis or has reached the lowest level of detail (e.g., at the component level).

Rule 2 - Development of Immediate Cause—The next step in FT development is to define the immediate, necessary, and sufficient causes for the top event. These causes are not the basic causes, but are immediate causes or immediate mechanisms. If all of the immediate causes are independent of each other and each fit definition of immediate, necessary, and sufficient to result in the top event, the top event is developed as an OR gate. If the top event occurs only if two or more causal events occur concurrently, then the top event is developed as an AND gate. The top event is often developed as an AND gate to represent some conditioning event that must be present for the fault to occur.

In the example “failure to control runaway before train achieves derailment speed during descent of the North Ramp,” the immediate causes might be identified as “human operators fail to apply brakes in timely manner” and “failure of brake system to apply sufficient braking force upon demand.” Since the occurrence of either event will result in the occurrence of the top event, the two events are input through an OR gate to the top event. At this stage of FT development, the definition of the immediate cause can be general or universal and does not require specific design details.

The development can be made more general, or inclusive, by replacing the causal event “human operators fail to apply brakes in timely manner” with “failure to detect runaway initiation and failure to apply brakes in a timely manner,” which is illustrated in Figure 7-10 by the event named DETAPPL. This definition allows for flexibility in further development if it is not known, or decided at the time of the analysis, whether human operators or automatic systems will be the primary means of detecting an initiation of runaway and actuating brakes. One application of the FTA is to assist in the determination of the design requirements needed to achieve the necessary functional reliability. The event DETAPPL is depicted as an undeveloped event by the use of a diamond under the event description box.

The timely manner phrase is a reminder that restrictions may be placed on the definitions of the causal events that correspond to the WHEN portion of the top event criteria. The mission-time parameters can be used in the event descriptions if they are known. For example, if the rate of acceleration and distance to the “point of no return” are known, a minimal response time can be specified (e.g., 30 seconds). The causal event might then be defined as “failure to detect runaway initiation and failure to apply brakes within 30 seconds.” The probability of failing to respond could potentially be calculated from a time-dependent reliability model for the respective electronic and human systems and the required response time of 30 seconds.

The name BRKFORC is given to the event titled “failure of brake system to apply sufficient braking force upon demand,” as illustrated in Figure 7-10. The event titled BRKFORC is depicted as an undeveloped event by the use of a diamond under the event description box. An explicit mission time could also be applied to the causal event titled BRKFORC. In this case, however, the mission time is defined as the “time on the ramp” during each descent operation (e.g., 30 minutes). The probability of failure on demand may be estimated from the system

failure rate and the potential exposure time of 30 minutes. These matters are described further in the discussion of basic event quantification in Section 7.2.4.5.

All descriptive (causal) events located below the top event are termed Intermediate Events.

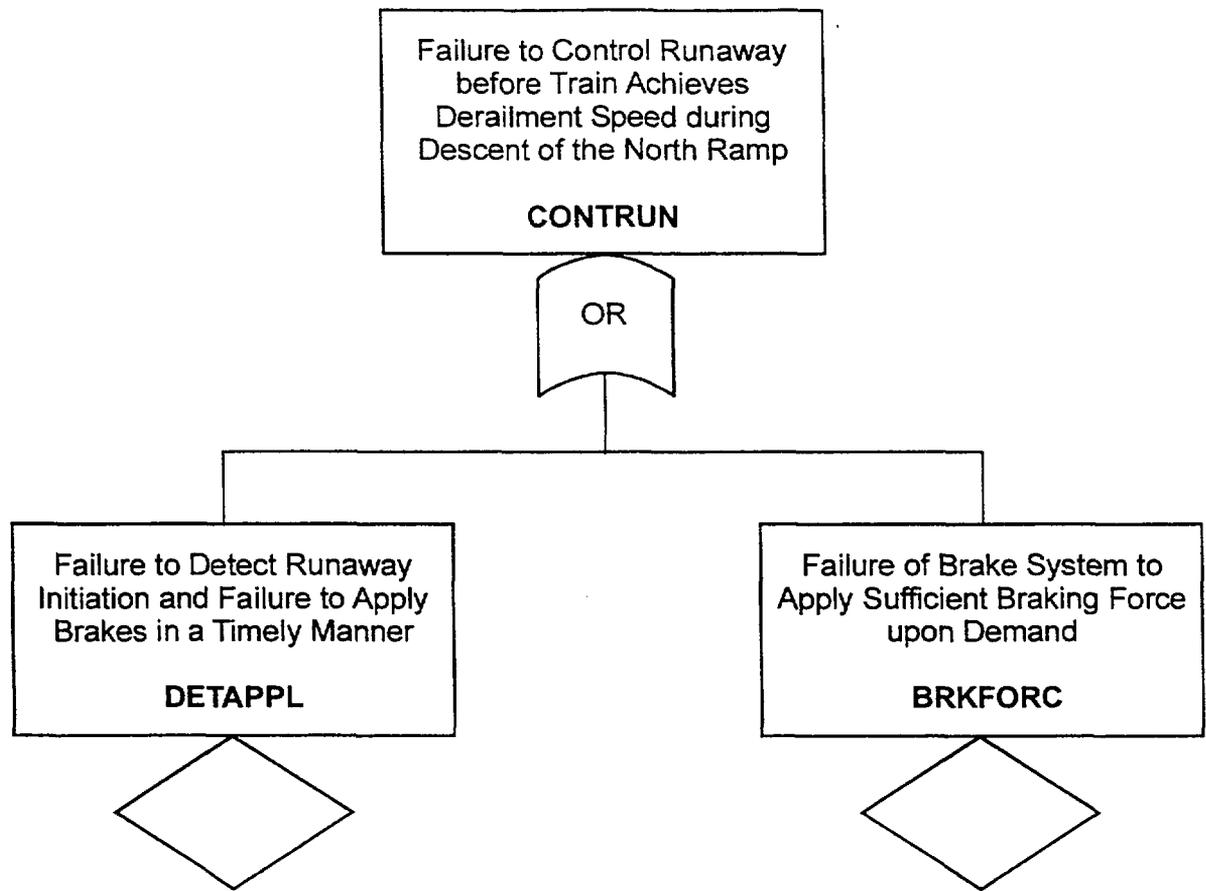
Rule 3 - Complete the Gate—All inputs to a particular gate (i.e., a boxed event description with an event name) should be completely defined before any of them are analyzed (decomposed) further. This rule is important for maintaining discipline in the deductive logic decomposition of a top event down to lower level events. All of the causal (input) events must be precisely defined, as described previously.

Rule 4 - No Miracles—The logical development of causal events is based on the occurrence of faults or failures in which the normal or expected functions do not take place. A corollary to this logical development is the No Miracles rule, as defined in the *Fault Tree Handbook* (Vesely et al. 1981). That is, if the normal functioning of a system, component or human actions propagate a fault sequence, it is assumed that the normal function occurs (i.e., there is no miraculous interdiction of the fault propagation). By contrast, if the normal functioning of a component blocks the fault propagation, then faults must be introduced into the tree to defeat the blocking function. This situation usually results in the introduction of an AND-gate: primary fault sequences are propagated upward in the tree and connected with the failure of the fault blocking function with an AND gate.

Rule 5 - Development of Intermediate Events—The immediate causes of the top event are each, in turn, treated like a top event and the immediate, necessary, and sufficient causes for each event are defined. This process is essentially a sequential application of Rule 2 that is continued down through the levels of assembly, continually transferring the point of view from failure mode (result) to the failure mechanism (cause). The process stops when the lowest level of resolution is reached, usually at the failure mode level of individual components or subsystems.

This discussion continues with the example shown in Figure 7-10.

If it is possible in the system design for either a human or an electronic system to detect the need for applying brakes, and then to apply them, an event named DETAPPL is developed as an AND gate with two inputs. These inputs are titled AUTOSPD (the failure of autospeed controller to detect overspeed and apply brakes) and HASPEED (the failure of operator to detect overspeed and apply brakes), which is not illustrated in Figure 7-10.



7.2-2.CDR.PSA GUIDE/2-5-02

Figure 7-10. Illustration of Fault Tree Development

The event BRKFORC is developed as an OR gate since (in this hypothetical example) a failure of either a brake control system (the event titled BRKCONT) or a failure of the brake mechanisms (the event titled BRKMECH) will result in the event titled BRKFORC, which is not illustrated in Figure 7-10).

Rule 6 - Identify Potential Dependent or Common Cause Failures—Note that the *Fault Tree Handbook* does not have a rule to explicitly identify and model common-cause or dependent failures. For emphasis, this PSA Guide adds this rule to ensure that the PSA analyst does not overlook these important mechanisms.

7.2.3.4 Basic Event Quantification

Quantitative data are input at the lowest level of resolution of each branch of an FT. The analyst must ensure that the data are appropriate to the precise definition of the basic event. In the analysis of system reliability, the lowest level is usually the failure probability for a specific failure mode of a component. For example, in an FT for a fluid system, one or more branches would terminate in basic events such as “pump A fails to start,” “pump A fails to run for 8 hours,” or “pump A out of service for maintenance.”

If the top event is quantified as a probability (e.g., probability that system fails to supply adequate cooling flow for 24 hours), then all input data must be expressed as probabilities (as unitless or per demand).

If the top event is quantified as a frequency of an undesired event (e.g., radioactive release from canister transfer system), however, then input data must be a mixture of probabilities and event frequencies or rates that become joined through AND gate(s). For example, there may be two scenarios that lead to the top event (filtered release and unfiltered release). The top event is shown as an OR gate. Under each of the intermediate events titled "filtered release" and "unfiltered release," respectively, there would be an AND gate. One input to each AND gate would be an IE (such as crane drops canister a distance further than design height) quantified as a frequency or rate of occurrence (i.e., per unit time) and an event representing the conditional probability of a "radioactive release given drop of canister further than design height" (unitless as per demand or per opportunity).

If the top event is quantified as a failure rate (e.g., "the system fails to supply adequate cooling flow" at a rate of λ [e.g., failures per million hours]), then the basic input data generally are expressed as failure rates (units of inverse time). However, if the top event requires combinations of failures of subsystem or components (i.e., using AND gates), then all but one of the inputs to each AND gate must be expressed as a conditional probability (i.e., probability per demand, given the occurrence of the first, or triggering, event).

The product of a frequency and one or more probability terms is a frequency. It is never appropriate to multiple a frequency (or rate) by another frequency (or rate) because the resulting units are not physical (i.e., units of hours⁻² have no meaning).

Section 7.5 provides guidance on developing input information for preclosure safety analyses. This section provides a brief discussion for continuity.

All available historical (actuarial) event data for the actual SSCs of a repository should be used to define the quantitative probabilities and frequencies used in FTA and ETA. Since there will be no repository operational data prior to the license application (LA) submittal, other sources of information are needed. Again, when available, performance data for SSCs of the same design and operational environment as that intended for each operation in a repository should be used. The analysis must otherwise proceed with the best available data for SSCs that closest resemble those to be used in the repository design, such as data from other fuel handling facilities. In many cases, especially for the CA submittal, it will be necessary to use generic tabulated data (e.g., electrical data, electronic data, and various mechanical systems and components data used in many PRAs). In other cases, it will be necessary to use surrogate data (i.e., railroad accident statistics) to estimate the probabilities of events during WP transport. Except for direct data from repository operations, it may be necessary to modify the probabilities to account for conditions at the repository that are different from those for which the data represent. In some instances, the probabilities may be higher (e.g., a more severe operating environment). However, these probabilities may be smaller in other cases (e.g., additional quality assurance or administrative controls preclude some of the events in the surrogate database). See Section 7.5 for an additional discussion on this process.

Basic event probabilities or failure rates are derived from experience data, as described in the following section:

7.2.3.4.1 Basic Event Probability

An event probability is a pure number ranging from 0 to 1.0. As a probability, it is physically unitless. Component faults are characterized as one of the following probabilities:

- Failure on demand – the probability of a failure per demand
- Standby failure – the probability of a failure on demand after a given non-operational period, usually given as time-between-inspections
- Operational failure – the probability of failing to run or operate (provide required function) during a specified time period (i.e., the mission time).

The symbol used for the probability in discussions, tables, or qualitative FTA is very often a “p.” However, in many cases the symbol “q” is used to connote the probability of failure (per demand), or unavailability (i.e., the probability of being unavailable when called upon for the time required).

The value of q may be derived directly from demand-based experience data, or indirectly from rate (or frequency) based experience data, as described in the following definitions.

Demand-Based Experience Data—K failures are observed in N challenges (demands) on components in records or test data. Demand-based data analysis would estimate the failure rate (or probability per demand), also termed the component unavailability, to be:

$$q = K/N \text{ failures per demand} \quad (\text{Eq. 7-7})$$

When a component or system failure probability is needed for quantifying an input to a basic event in an FT, q has the proper characteristic.

Rate Based Experience Data—M failures are observed in exposure (operational or test) time T for components in records or test data. Rate-based data analysis would estimate the failure rate (in units of numbers of failures per unit time), also termed the component failure frequency, to be:

$$\lambda = M/T \text{ failures per hour} \quad (\text{Eq. 7-8})$$

When a component or system failure rate is needed for quantifying an input to a basic event in an FT, λ has the proper rate-based characteristic.

If the probability of failure (unavailability) of a component or system is needed, however, the rate data must be used to calculate an appropriate unavailability factor.

Operational Unavailability (No-repair Model)—The unavailability of a component or system in the exponential reliability model without repair is calculated as:

$$q = 1 - \exp(-\lambda * t_M) \quad (\text{Eq. 7-9})$$

Where t_M is the mission time and q is the probability that the component or system will not perform its safety function for at least a time t_M when it is needed. The expression for q is usually approximated as

$$q \approx \lambda * t_M \quad (\text{Eq. 7-10})$$

when λ , t_M , or both are small values.

Standby Unavailability (with-repair or renewal)—The average unavailability of a system that is on standby but is periodically inspected at a time interval (t_I) and repaired, if necessary, is given by

$$q \approx (\lambda * t_I)/2 \quad (\text{Eq. 7-11})$$

where it is assumed that the component or system is as good-as-new after inspection or repair.

Common Cause Failures—A more complete discussion of dependent failures and CCFs is presented in Section 7.4.

In developing FT models that include redundant components or subsystems, it is generally recognized that the joint probability of concurrent failure of two or more redundant components may not be the product of independent failure probabilities. That is, the failures of the individual components or subsystems may be dependent (i.e., coupled). This possibility is modeled in the FT when the construction rules are applied.

The probabilities of the CCFs are quantified using demand-based or rate-based parameters, as appropriate, for the event being quantified. In FTA for repository preclosure safety, it is expected that most CCF quantifications will apply the beta factor method (see Section 7.5) in a repository preclosure safety FTA.

7.2.3.4.2 Initiating Event Frequency

When the purpose of an FTA is to quantify the frequency of an event sequence (or accident scenario), the frequency of the IE must be scaled to match the operational load of the system. For example, the IE definition may be “crane drops SNF canister” and the quantification required would be “ F_D drops per year.” The operational throughput of the system may be Z canisters per year. Demand-based and rate-based data can be used to calculate the frequency of the IE, as explained in the following examples:

Demand Based: Experience data could show that the probability of dropping any given canister during a lift is Q_D drops per lift (i.e., more precisely defined as the probability of a canister drop per lifting operation). If the frequency of lifting the canisters is Z per year, then the frequency of the postulated IE is:

$$F_D = Z * Q_D \text{ (drops per year)} \quad (\text{Eq. 7-12})$$

Rate Based: Experience data could show that the rate of dropping any given canister during operational time is λ_D drops per hour (e.g., this rate might be derived from related information such as a crane failure rate). In this situation, the exposure time (or mission time) must be defined for each lift operation to derive the probability of drop per lift. The estimated time that each canister is suspended in a vulnerable condition during each operation is T_L minutes. The probability of canister drop per lift is calculated as

$$Q_D = \lambda_D * T_L \text{ (drops per lift)} \quad (\text{Eq. 7-13})$$

The time units must be converted, as appropriate, in these examples.

Proceeding in the same manner as for the demand-based case, the frequency of the postulated IE is calculated as:

$$F_D = Z * Q_D \text{ (drops per year)} \quad (\text{Eq. 7-14})$$

7.2.3.4.3 Human Error Probabilities or Rates

Many basic events in FTs may represent human errors in operations or maintenance. Special techniques have been developed for estimating the probabilities of various types of human errors. The events are sometimes called HAs to include the positive effects (recoveries or interventions) as well as to recognize that the basic causes of an undesired event involving a human may be situational and not a true human error. An HRA is the process of analyzing situations where human errors (or human recovery actions) may occur and the process of quantifying the probability of those actions. Section 7.3 describes the recommended approach for the support of the PSA HRAs for the respective phases of LA submittals. This section provides a brief guide to their application in FTA.

Quantification is often described as HEP, which is usually quantified in terms of the probability per opportunity (or exposure). The HA event is treated in FT logic as a command fault; that is, as a mode of failure for a given component or system. It is sometimes helpful to examine each situation to identify the potential errors of commission, in which a human acts improperly (spuriously or induced by the contextual situation) to initiate an unwanted state or response of the system. It is also helpful to identify potential errors of omission in which the human fails to perform a required act that would prevent an unwanted state or response of the system. Such HAs may occur during maintenance activities (including test, inspection, and calibration), leaving a system or component in an unavailable or failed state. They also may occur during on-line maintenance (initiating an unwanted event sequence) or during operations (as IEs of unwanted sequences, or when failing to respond to, and recover from, unwarranted conditions).

The probability (for use in FT quantification) that a given component is unavailable when called upon because of maintenance errors is termed Q_{HM} . The frequency of maintenance of the component is F_M per year. The probability of a human error that leaves the component unavailable is quantified as HEP_{HM} (per opportunity; i.e., per each maintenance on the component).

Note that there is also a term for the time that the component or system is unavailable during (error free) maintenance; this term represents the time that the system is offline.

7.2.4 Examples of Application

This section provides an example of the process for creating an FT logic model for the specific failure mode of a relatively simple system. The example is derived from the *Fault Tree Handbook* (Vesely et al. 1981, Section VIII) for the Pressure Tank System (Figure 7-11). The system is not necessarily similar to any repository systems.

7.2.4.1 System Familiarization

The first step in any PSA is to define the system and understand how it functions. This step is the necessary prerequisite for FT analyses as well as for hazards analyses, common cause failure analyses, and ET analyses.

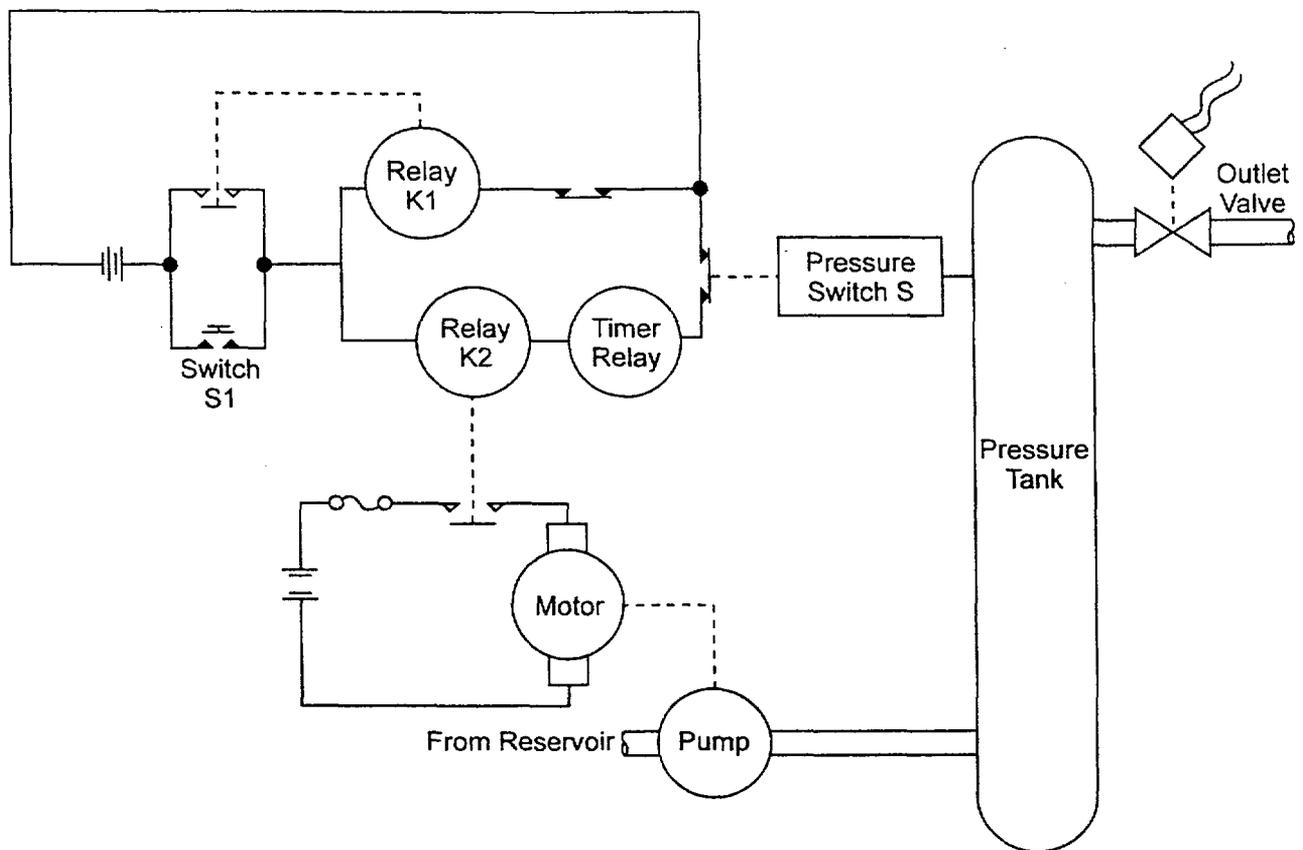
Several operating modes are possible for the system configuration:

- Dormant mode
- Pumping mode
- Ready mode
- Emergency shutdown.

The function of each component of the system varies according to the operating mode. The function of the control system is to regulate operation of the pump. The pump brings in fluid from an infinite reservoir. Ten seconds are normally required to pressurize the tank.

The pressure switch contacts are closed when the tank is empty but open when the threshold pressure is reached. The opening of the pressure switch contacts de-energize the coil of relay K2, whose contacts then open to stop the power to the pump and cease pumping. The tank is fitted with an outlet valve that drains the tank; however, there is no pressure relief valve on the tank. When the tank is emptied, the pressure switch closes, thereby energizing relay K2 and the pump to repeat the cycle.

Switch S1 contacts are open in the dormant state, which de-energizes the coils of relays K1 and K2 and, thereby, opens the contacts of both relays. Relay K1 is self-latching and closes, and remains closed, after switch S1 is pressed momentarily to startup the system. The timer contacts remain closed in the dormant state (and during system startup) for up to 60 seconds of continuous energization. The timer is reset every time the power to the timer is interrupted by the opening of the pressure switch contacts. The timer provides an emergency shutdown function in case the pressure switch fails. If the pressure switch fails to break the pump control



Source: modified from Vesely et al. (1981, Figure VIII-1).

Figure 7-11. Pressure Tank System

circuit, the timer contacts open to de-energize relay K2, whose contacts then open to stop the power to the pump.

This system description is applied to an example of FT construction using the rules and definitions in the *Fault Tree Handbook* (Vesely et al. 1981). A skilled FT analyst may not go through the steps mechanically but would use such rules intrinsically.

7.2.4.2 Fault Tree Construction for Pressure Tank Example

It was decided in this example to resolve the FT down to the component level.

The first step in the FT construction is to define the top event as a precise statement of the undesired system effect and a system failure mode of interest. This is an application of Rule 1.

Write a statement in the top event box as a fault. State precisely WHAT the fault is and WHEN it occurs.

For the example, the top event is defined as: Rupture of Pressure Tank After the Start of Pumping. The next step is application of Rule 2 and the immediate cause principle. The analyst identifies three immediate and necessary causes for the top event and adds an OR gate below the

top event. One cause is identified as “Tank Rupture (Primary Failure)” to indicate the possibility of a random failure of a tank operating under normal, expected environmental conditions. This fault is shown on the FT diagram as a circle (i.e., a basic event).

Two other immediate faults are identified. The first is named “tank ruptures due to improper selection or installation,” which disqualifies the tank for the operating conditions. This fault is shown in the FT diagram as a diamond to indicate that it will remain undeveloped. As noted in the *Fault Tree Handbook* (Vesely et al. 1981), under the ground rules set for the analysis, this fault may be introduced for completeness and then immediately pruned from the tree as being outside the scope of the analysis. It is noted that the potential mechanisms are potentially related to human error in this example.

The other secondary fault is simply identified as such (i.e., tank ruptures (secondary failure)) to acknowledge that there may be several fault paths that can cause the top event by creating an environment or operating condition that is beyond the qualification basis of the tank.

Rule 3 is applied to complete the gate by explicitly diagramming the three faults under the top event.

Rule 2 is now applied to the event titled “tank ruptures (secondary failure).” Because this is a component fault, an OR gate is added under the event box and immediate causes are identified. In the example, two faults are identified. One is an undeveloped event titled “Secondary Tank Failure from Other Out-of-Tolerance Conditions (Thermal, mechanical);” the other input fault is titled “Tank Rupture due to Over Pressure Caused by Continuous Pump Operation > 60 sec.” This fault description is seen to be a precise statement of a fault that addresses the fault effect, mode, and mechanism in a single statement. It is concluded that this is not a component fault and therefore must be a system fault. The input to a system fault event box may be an OR gate, an AND gate, an INHIBIT gate, or no gate at all. In this case, motor running is a normal condition and results in a fault mechanism for the tank only if it runs for more than 60 seconds. Therefore, the fault is represented as an INHIBIT gate in which the input event is “pump operates continuously for > 60 sec” and the conditioning event is “if pump runs > 60 sec tank will rupture (probability = 1.0).” The conditioning event is not developed further; it is a statement of the condition or assumption.

The event titled “pump operates continuously for > 60 sec” is developed further to identify the basic causal faults. The application of Rule 2 (principle of immediate cause), the analyst cannot identify the need for a gate because there is a unique event titled “pump motor runs for > 60 sec” that is tightly coupled to the pump impeller. An application of Rule 3 (No Miracles) indicates that it cannot be assumed that the pump shaft will break or that the motor winding will burn out to avoid the undesired pumping time. The event titled “pump motor runs for > 60 sec” is coupled directly to the event titled “power applied to pump motor > 60 sec.” There are no miracles to interrupt the power; therefore, a “no gate” input is appropriate.

Applying Rule 5, the process is repeated for the event titled “power applied to pump motor > 60 sec.” Using Rule 2 indicates that the immediate cause is “K2 relay contacts remain closed > 60 sec.” Thus, the FT structure below the INHIBIT gate input to “Tank Rupture due to Over Pressure Caused by Continuous Pump Operation > 60 sec” appears as a series of intermediate

events without any gates. This structure is typical of initial FT construction. As will be described later, the series of pass through fault descriptions do not contribute to FT evaluations either in qualitative or quantitative analyses. This series is usually collapsed into as few fault statements as possible without losing information.

Rule 2 is next applied to the fault titled "K2 relay contacts remain closed > 60 sec." This component fault requires the addition of an OR-gate. Three faults are defined as immediate causes. The fault "K2 relay contacts fail to open" is a primary failure. It is implied in the primary failure that all other portions of the relay unit are functioning properly; however, the relays do not open (perhaps because of corroded contacts or broken springs if the contacts are to open when the coil is de-energized). The secondary failure titled "K2 relay (secondary failure)" is included for completeness, but is not developed further. The command fault is titled "EMF [electromagnetic force] applied to K2 relay coil > 60 sec;" it is developed further for defining the basic causes.

An examination of the control circuit indicates that the immediate cause is a condition that requires the concurrence of two events: "Pressure switch contacts closed > 60 sec" AND "EMF remains on pressure switch when pressure switch closed > 60 sec." An AND gate is added below "K2 relay contacts remain closed > 60 sec" and the event boxes for the two input events are also added.

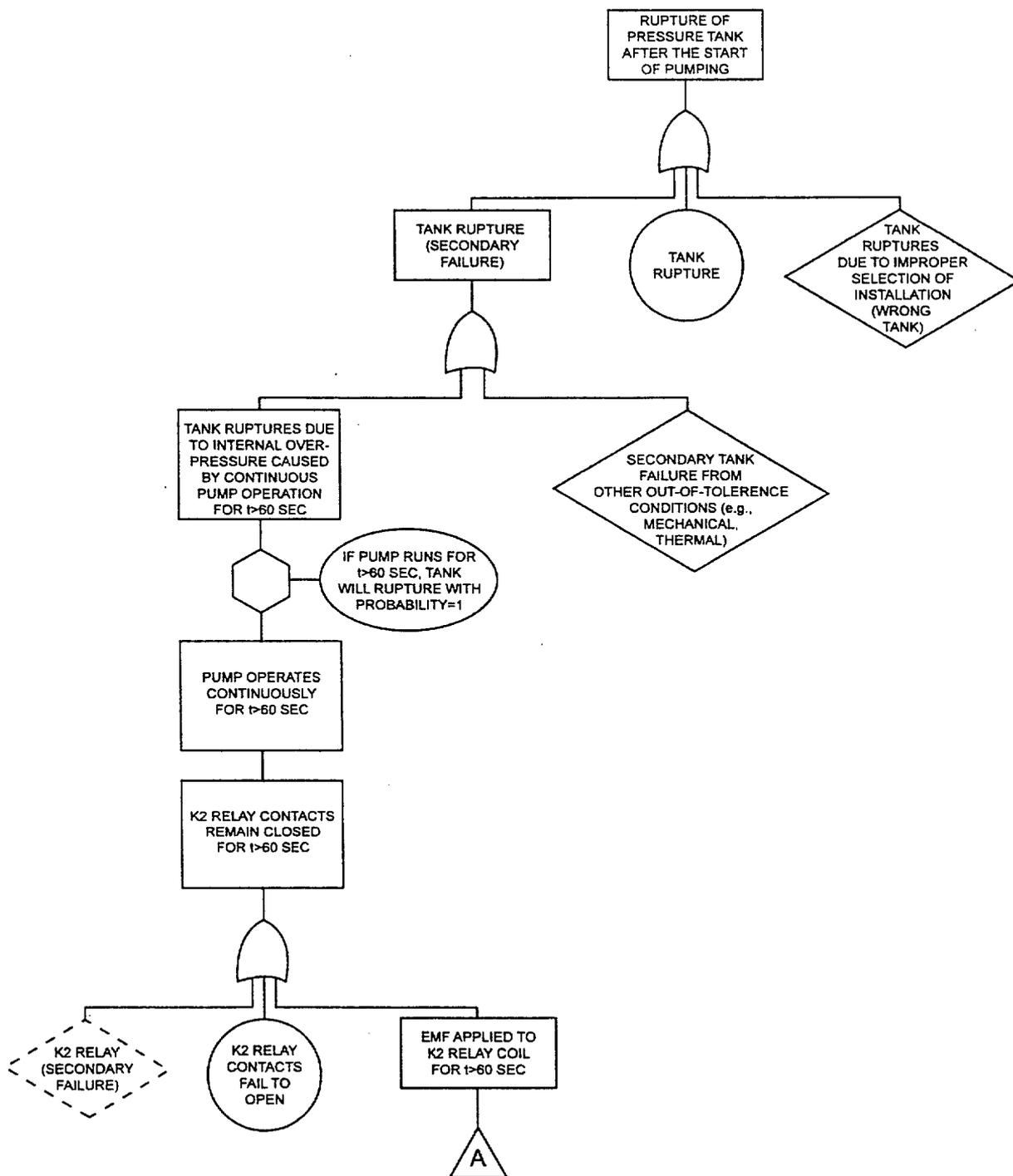
The development of the event titled "EMF remains on pressure switch when pressure switch closed > 60 sec" proceeds in a similar manner. The development continued per Rule 5. The discussion of this example is terminated, however, because the process is repeated until every path down the tree from the top event is terminated at primary or secondary faults of components or command faults that are not developed further. The complete FT for the example is presented in Figure 7-12. The reader should consult the *Fault Tree Handbook* (Vesely et al. 1981, Section VIII) for the full description of the development of this FT example for the pressure tank system, as well as other examples.

Rule 6 should now be applied to examine the system for potential dependent or common-cause failures. Since the example system has nonredundant components, there are no common-cause failures to include. The FTA could be expanded to show explicit dependence on an external electric power supply.

The complete tree should be examined and simplified if it is too complete (i.e., contains events that do not contribute to the understanding of the basic causal factors or do not contribute to the analysis of minimal cutsets or quantification). The *Fault Tree Handbook* (Vesely et al. 1981), for example, deletes many of the secondary faults. As noted previously, many of the intermediate events can be deleted or merged with other event descriptions. The simplified FT, illustrated in Figure 7-13 terminates with primary failures. The primary failures are indicated by circles and are, therefore, treated as basic events in the FT structure.

Simplification of an FT is not necessary when using a program such as SAPHIRE to solve the FT for the minimal cutsets or for quantification. However, it may be advisable to simplify a complex FT for reporting. Documentation of complex trees may run from 10 to 50 pages if legible font sizes are desired. Such a presentation adds numerous TRANSFER IN and

TRANSFER OUT symbols to the FT, making the FT very difficult to follow, especially for readers not familiar with FTs. Detailed trees are appropriate for documenting the analysis. However, simplification of an FT to a few (one to four) pages is recommended for summary reports, including those supporting an LA submittal.



Source: modified from *Fault Tree Handbook* (Vesely et al. 1981, Section VIII).

Figure 7-12. Fault Tree Example for Pressure Tank Rupture

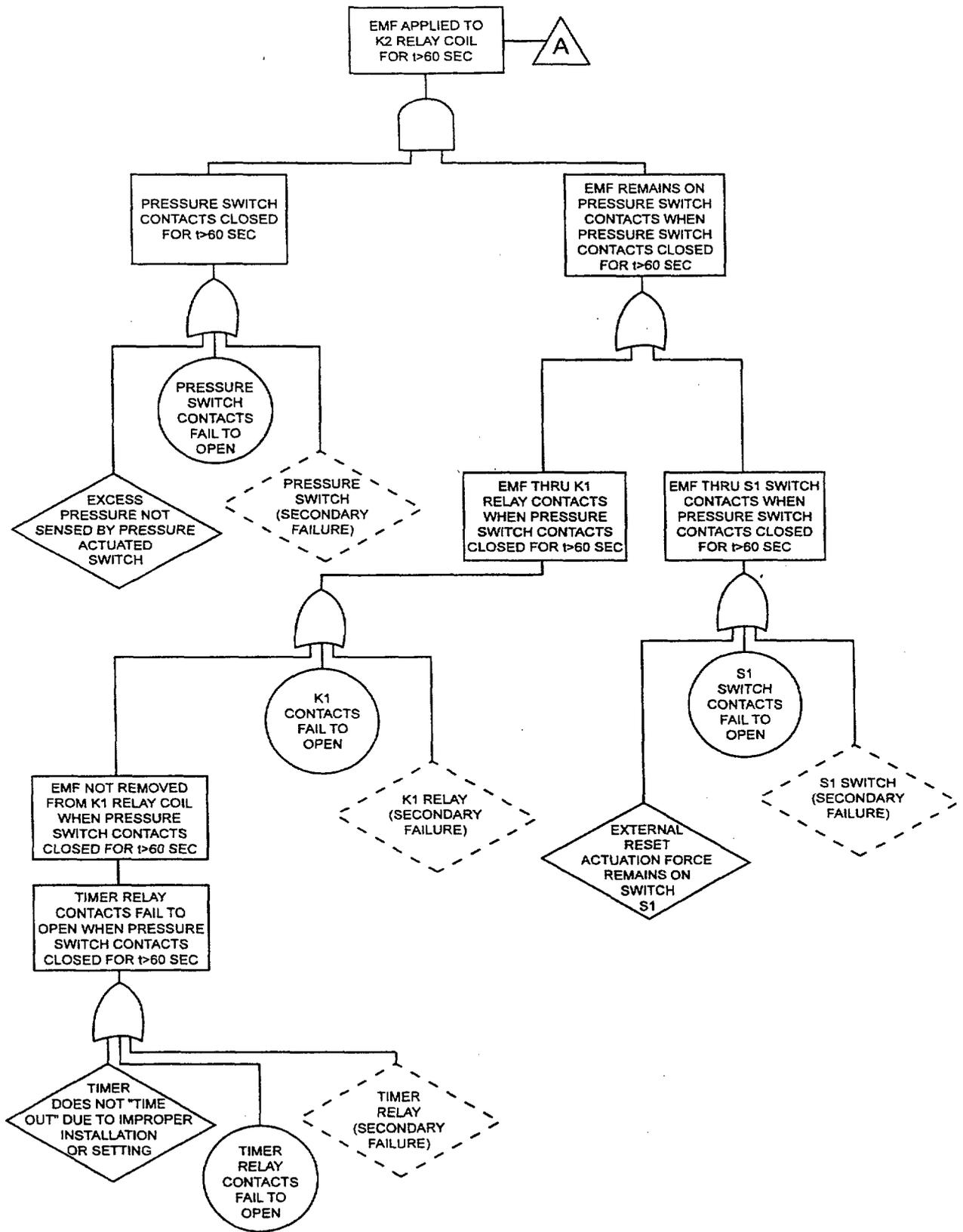
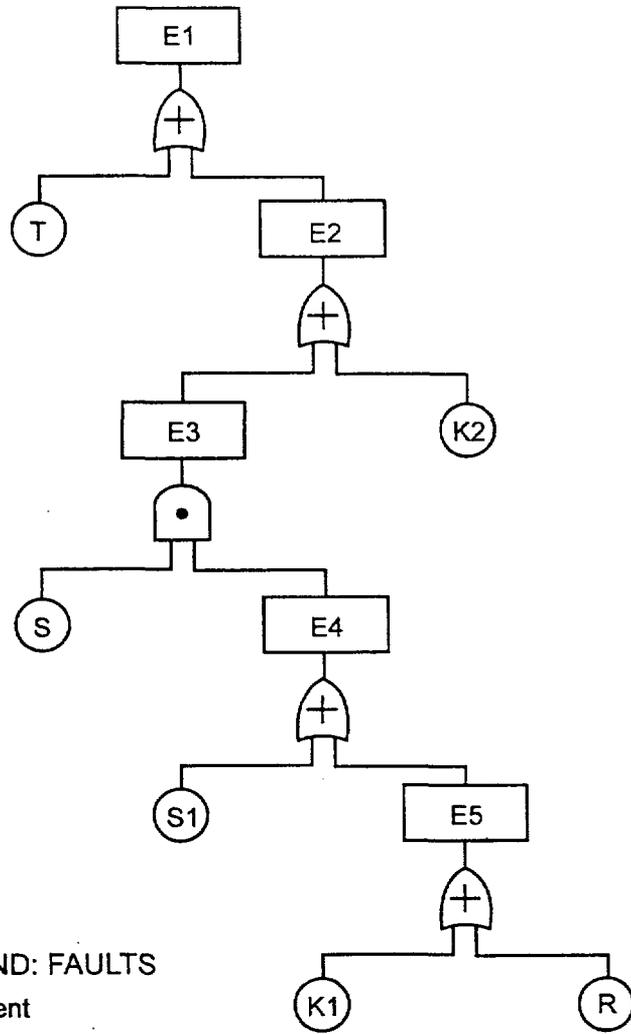


Figure 7-12. Fault Tree Example for Pressure Tank Rupture (Continued)



- LEGEND: FAULTS**
- E1 Top Event
 - E2, E3, E4, E5 Intermediate Fault Events
 - R Primary Failure of Timer Relay
 - S Primary Failure of Pressure Switch
 - S1 Primary Failure of Switch S1
 - K1 Primary Failure of Relay K1
 - K2 Primary Failure of Relay K2
 - T Primary Failure of Pressure Tank

Figure 7-13. Simplified Fault Tree for Pressure Tank Example

7.3 HUMAN RELIABILITY ANALYSIS

7.3.1 Purpose

This section defines the bases and methods for the application of HRA in support of the PSA for a repository. The section defines the methodology for the treatment of HAs in operational, administrative, and maintenance activities that are explicitly incorporated into the ET or FT logic models for the PSA.

7.3.2 Scope

This section presents a cursory, focused guide to the construction, application, and evaluation (both qualitative and quantitative) of HRA models. While some concepts are universal to all HRAs, the application in this section is focused on the support of the repository PSA. This section is not meant to be a textbook or exhaustive in scope. Where appropriate, reference is made to literature for additional information.

The HRA methods presented in this section provide a systematic process for identifying HAs that can affect the risk associated with preclosure operations of a repository and quantifying their probabilities.

7.3.3 Overview of Approach

An HRA is primarily an engineering discipline developed in support of PRA activities, but may involve a multi-disciplinary team. The topic of HRA is frequently called human factors in PRAs or safety reports. While HRA is related to, and works in concert with, the disciplines of Human Factors and Ergonomic Engineering, there are important differences. Human Factors analysts, who are often educated in the field of behavioral science, are engaged to provide work situations that reduce the likelihood of errors qualitatively by providing unambiguous instrumentation, logical arrangements of controls, ease of access, and ease of communications. The human reliability analyst is usually an engineer or system safety analyst who can identify potential human events that can affect safety. The human reliability analyst identifies where and how human interactions can influence the progression of event sequences, estimates the probability that a particular HA will be performed correctly and in a timely manner, and evaluates the effect on the frequencies of alternative event sequences. The HRA analyst can often estimate the probability of incorrect HAs using generic or surrogate information. In more complex instances, the human reliability analyst may be assisted by a Human Factors Specialist to identify and quantify the effects of performance shaping factors and error-forcing conditions or to prepare a detailed task analysis as a framework for quantifying the probability of performing the task correctly and timely.

The HAs of interest to PSA are operational, maintenance, or administrative actions that can ameliorate or exacerbate the probability of an unwanted event sequences. The HAs of interest are identified through the process of ET construction and the supporting FT construction. Significant HAs may be modeled as event headings in ET construction.

This section presents a discussion of the HRA techniques that are to be applied in the PSA.

7.3.4 Details of Approach

Background—Advances in HRA were initiated as part of the evolution of PRA methodology. Early PRA studies during the 1970s (e.g., the Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants [NRC 1975]) demonstrated the uses of ET and FT modeling of accident sequences for complex nuclear reactor power plants, and identified instances in which human interactions with the plant systems could hinder (exacerbate) or help (ameliorate) the initiation or propagation of event sequences. The Reactor Safety Study (NRC 1975) was supported by an early version of the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations (Swain and Guttmann 1983). The early PRAs also served to identify areas where HRA methodology was weak and in need of improvement to adequately model the interactions and to quantify the probability of such actions.

During the past 30 years, research and data-gathering operations sponsored by the U.S. Nuclear Regulatory Commission (NRC), the Electric Power Research Institute, the Institute of Nuclear Power Operations, and others have produced many insights into the underlying causes of undesired HAs (unsafe acts) and several methods for representing and quantifying human failure events (HFEs). The most recent attempt to improve upon HRA methodology is the ATHEANA study (NRC 2000).

Much of the HRA methodology has been developed to support PRAs for complex systems represented by NPPs, chemical process plants, and the piloting of aircraft. Although the operations of a repository are not as potentially challenging to human operators as one of the more complex systems, and as not as susceptible to catastrophic results in the event of unsafe acts, most of the HRA methods can be applied to the PSA, albeit with some simplifications.

Anatomy of an Accident—Post-event evaluations of many industrial accidents have shown that a high proportion can be attributed to some form of HFEs. Such evaluations have shown that the type of HFEs involved in many catastrophes are caused by faulty diagnosis, flawed or missing communications, failure to perceive a signal or warning, decisions taken too late, and violations of procedure or rule. Hidden (latent) HFEs (e.g., faulty maintenance, or failure to return a system or component to service) can contribute to the progression or severity of an accident.

By comparing accidents across industries and performing an evaluation of their root causes, various authors (e.g., Joksimovich et al. 1993) have defined the anatomy of an accident in terms of “the four Ms:”

- **Machine**—The system design with basic flaws, control characteristics, and operator friendliness
- **Milieux (Media)**—Operating conditions (context), commercial and regulatory pressures, natural phenomena
- **Man**—Operator reliability in preventing accidents and controlling systems in emergency conditions; maintenance reliability

- **Management**—Flaws in safety culture, organizational influences, quality of procedures, training, and resources provided; reactions to political and regulatory pressures.

The evolution of PRA methodology has addressed each of the four Ms sequentially. Early PRAs concentrated on the effects associated with non-human influences (i.e., Man and Milieux). The HRA research conducted over the past two decades concentrated on the human influences; first at the individual (Man) level, and most recently, on the organizational influences (Management) level.

As noted, the most recent attempt to improve upon HRA methodology was the ATHEANA study (NRC 2000). The term HFE (i.e., human failure event) was introduced in that to eliminate the element of blame, which is viewed as implicit in the older term of human error. The basic premise of ATHEANA was that many HFEs are caused by contextual, or situational, conditions that virtually guarantee that the human operator will make the wrong decision or perform an unsafe act that results in a desired plant state. While the ATHEANA study provides a framework for identifying the causal factors that underlie an HFE, it does not provide a specific representation. Instead, the study adapts some of the older techniques. Further, the ATHEANA study is oriented toward the post-accident responses of NPP operators. Such risk-significant emergency responses are not relevant to a repository.

This section describes the methods that are appropriate to the PSA.

HRA Process and Structure—The processes of HRA may be addressed (via the risk triplet) by asking: what can happen, what are the consequences, and how likely is it? These questions are applied at any point in the development of an ET or FT whenever there is a known or potential human interaction with the systems or processes. Several methods have been developed to provide a structured process for addressing these questions. This section will adapt principal elements of the SHARP process, as presented in Section 7.3.4.1.

The answers to “what can happen?” identify where potential errors of commission can initiate or exacerbate an event sequence, where errors of omission can potentially occur (in which a human fails to take appropriate action to mitigate the sequence), or where the human can ameliorate the effects of prior human errors or equipment failures by performing a recovery action. Refinements of this identification process take into account the operational context (e.g., the availability of instrumentation, the occurrence of a precursor event such as equipment failure, or prior HAs). This evaluation is similar to the dependency analysis for events in an event sequence as described in Section 7.1.

The answers to “what are the consequences?” require the knowledge of the likely system response given the HA. If a human closes a switch in the wrong system, or in the right system at the wrong time, how does the facility respond? Does this action require rapid recovery to avoid a significant release of radioactivity, or is it benign? If the consequences are deemed significant in quantifying the frequencies or radiological consequences of event sequences, then the third question will be addressed.

The answer to “how likely is it?” may be easy to answer for some well-known, generic HAs or could involve an extensive analysis. In some applications, it is efficient to perform a

conservative quantitative screening by assigning a high probability to the event, such as 1.0. If the HA is not revealed as a significant contributor to the FT top event probability, or a sequence frequency, then the HA can be eliminated through the screening process and not subjected to a detailed analysis.

There are several different methods for representation and quantification of probabilities of human errors. Many of these methods are aimed at particular types of HAs. As part of the structured approach to HRA, potential human interactions are categorized as one of three types:

- **Type A**—Type A characterizes human events that occur before the IE of an event sequence. Type A HAs are typically related to testing and maintenance (T&M) wherein a system is left in a state of unavailability or under-capacity. Errors of commission and errors of omission can occur. This type of human interaction may be termed latent because its effect on the progression of an accident is unrevealed until the system is called upon. The potential effects of Type A human interactions on system unavailability are usually modeled in FTs.
- **Type B**—Type B characterizes human events that are caused by or contribute to an IE. Such events are not usually analyzed in PRAs for nuclear plants for which experience data exist for IEs. The human-related causes are considered to be implicit in the historical data. This implicitness also may be true for some IEs for a repository. In general, Type B events should be considered for first-of-a-kind facilities such as a repository. Such human events are usually errors of commission. Type B events are modeled in FTs to quantify the likelihood of an IE.
- **Type C**—Type C characterizes human events that occur after an IE as part of the process of mitigating an event sequence. Errors of commission and errors of omission can occur. The influence of Type C events on event sequences is modeled primarily in ETs. For some HRA quantification, it is appropriate to sub-divide Type C into:
 - **Type CP**—This subtype refers to human interactions that are procedurally driven by formal procedures (written emergency operating) or by informal procedures (learned training) that guide the human operator in performing a series of steps
 - **Type CR**—This subtype refers to recoveries of unavailable systems and of prior human errors. Such HAs may not be part of a procedure, but they rely on the knowledge of the operating crew.

This guide recommends techniques deemed appropriate for the PSA for each category.

7.3.4.1 Structured and Systematic Approach for Incorporating Human Reliability Analysis into Preclosure Safety Analysis

One approach for structuring the responses to the risk-triplet questions is termed SHARP (Hannaman and Spurgin 1984). The SHARP1 process (Wakefield et al. 1992) enhances SHARP, but this effort primarily is a rebundling of the seven steps into the first two of four

stages (the other two stages are recovery analysis and internal review). These enhancements are not deemed relevant to the purposes of this guide.

The SHARP process defined seven steps for a structured, systematic approach for incorporating HRA into a PRA. It was developed originally as a means to augment an existing PRA so as to improve its treatment of HRA. Pre-existing ETs and FTs are examined for human interaction. For the PSA of a repository, however, HAs will be addressed as part of iterative development of ETs and FTs as the design details evolve. Much of the SHARP guidance fits well. Since all PSA analyses, including HRA, will be performed and documented according to Yucca Mountain Project procedures, the SHARP Step 7 - Documentation is not addressed in this section.

Therefore, a six-step SHARP process is used as the framework for conducting the HRA portion of the PSA. The following sections define the activities of each of the following steps:

1. Identification and Logic Modeling
2. Screening
3. Task Analyses
4. Representation and Models
5. Quantification of HA Probabilities
6. Quantification of the ET or FT

7.3.4.2 Identification and Logic Modeling (Step 1)

This step may be regarded as integral to the development ET or FT logic models as described in Sections 7.1 and 7.2, respectively. In general, Type A and B human interactions will be modeled in FTs as basic events that contribute to the top event expression for SSC unavailability (Type A) or as an IE (Type B). Figure 7-14 illustrates the manner in which a Type A HA is incorporated into a system FT. Figure 7-15 illustrates the use of a Type B human interaction as a contributor to an IE. The shaded boxes in the respective figures indicate the HAs.

A Type C human interaction (after an IE) will usually be modeled in ETs, but could be modeled in an FT in the same manner as a Type A human interaction. As noted in Section 7.1, HAs may be included as one of the event headings that define the logic structure of the tree. Potential dependencies between the HA and a precursor event can be identified as described in Section 7.1. Figure 7-16 illustrates how a Type C human interaction is included in an ET. The shaded event heading in the figure indicates the HA.

Step 1 also covers situations where preliminary ET or FTs have to be modified to include HAs. For example, preliminary logic models may be high-level or functional. After design decisions are made regarding the selection of specific types of equipment to accomplish the functions (the selection of, for example, manual versus automatic controls), there will be a better understanding of where and how humans can interact with the operational systems. The logic models will be updated accordingly.

The output of Step 1 is a comprehensive list of all of the potential human interactions that affect the event sequences.

The quantification of the conditional probability of the HFE uses an appropriate method, as described in section 7.3.4.

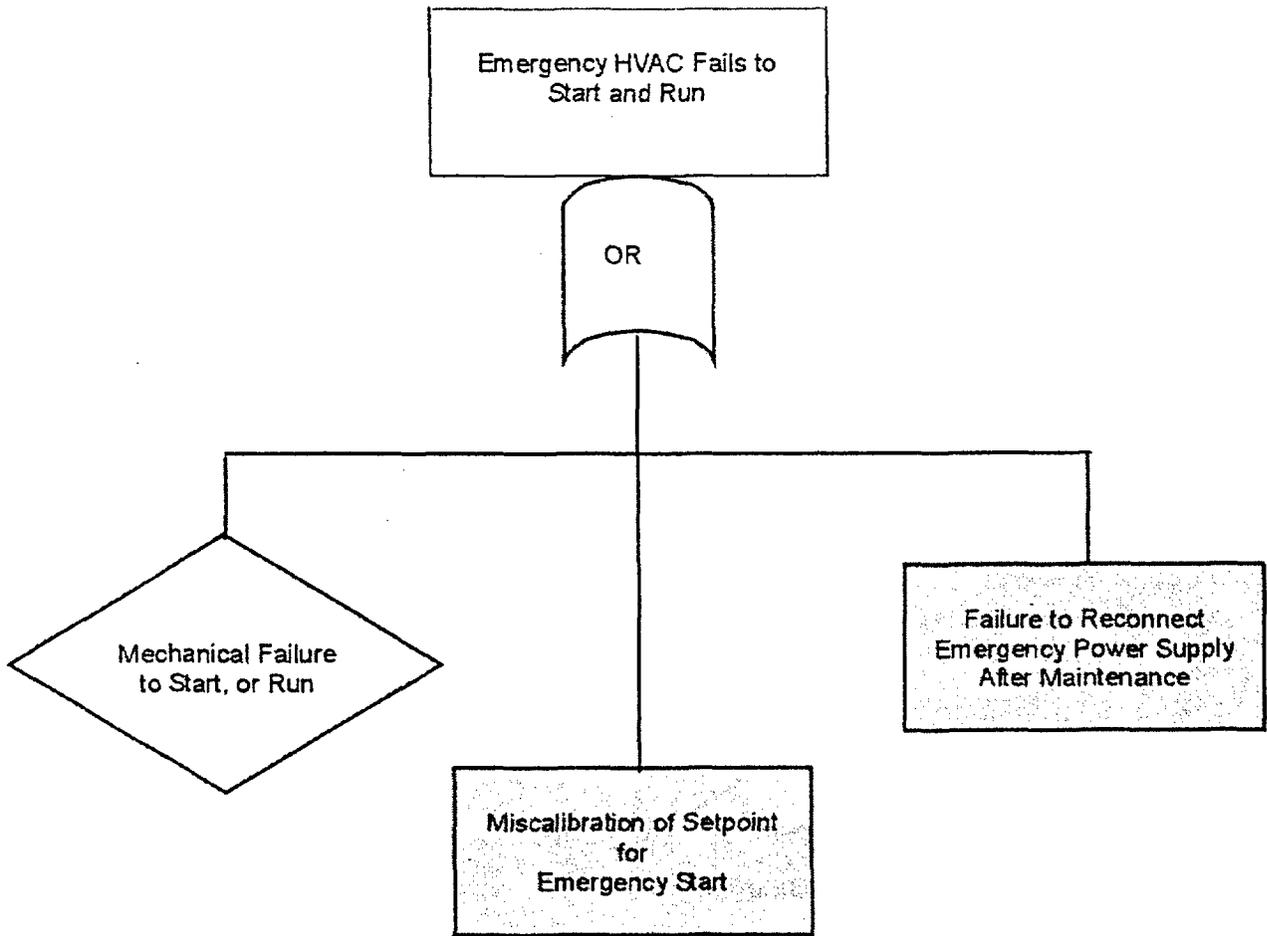


Figure 7-14. Example of Fault Tree Containing Type A Human Actions

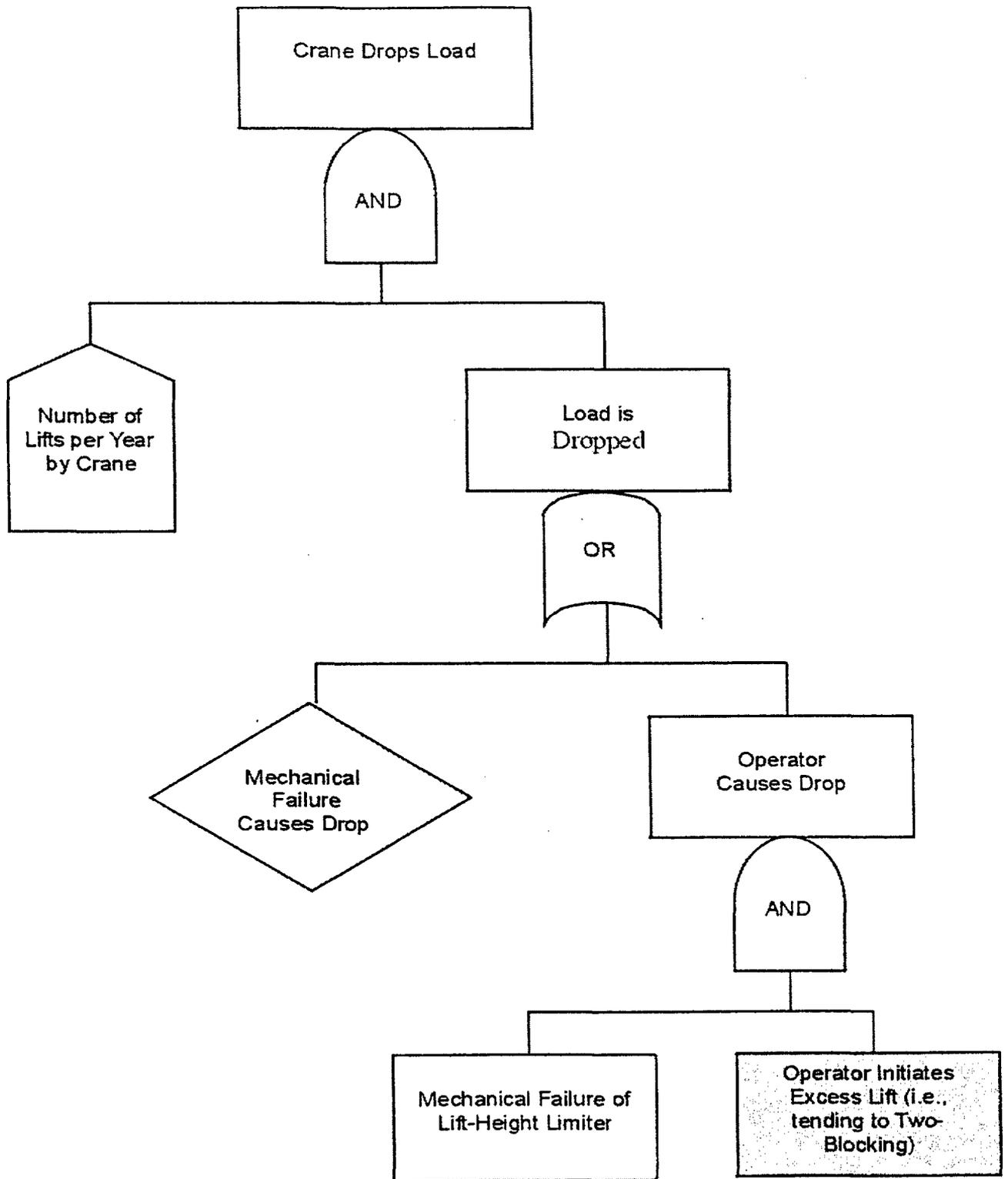


Figure 7-15. Example of Fault Tree Containing Type B Human Actions

Example of Event Tree with Human Action in Event Headings

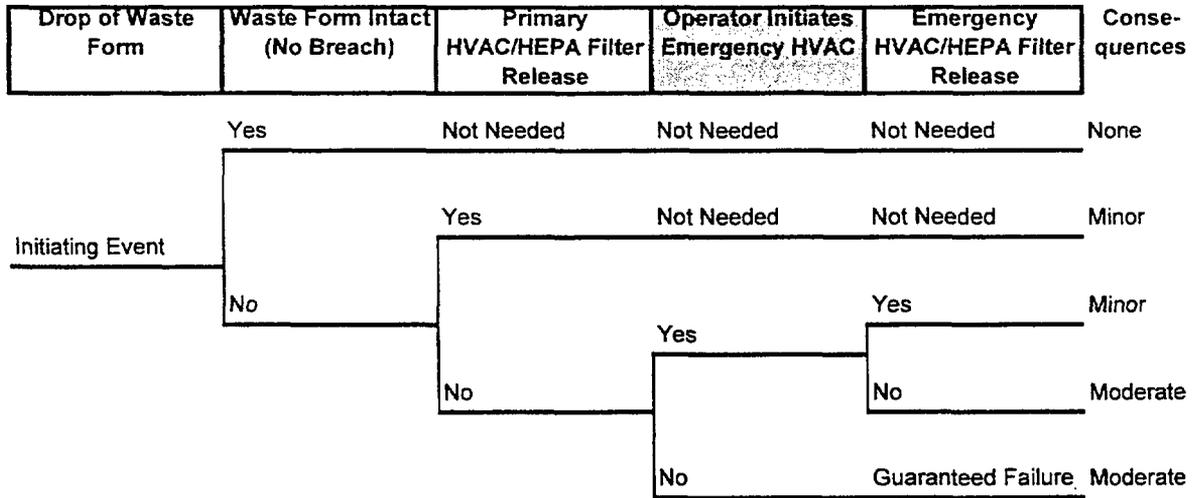


Figure 7-16. Example of Event Tree with Type C Human Action in Event Headings

7.3.4.3 Screening (Step 2)

The purpose of Step 2 is to reduce the number of HAs that require a detailed HRA. If few HAs are identified, the screening process may not be very important. Nevertheless, it is useful to survey the list of HAs to identify those of potential importance.

Screening may be performed qualitatively or quantitatively on the basis of either frequency (probability) or radiological consequences.

Qualitative screening rules are to be developed to fit the purpose of the PSA. The screening rules must be tailored to fit the safety function and the system characteristics. Examples of qualitative screening rules for Type A (pre-IE) or Type B (part of IE) human interactions include:

- Analyze (retain) miscalibration events because of potential CCFs
- Eliminate from consideration mis-alignment events where there is
 - Automatic realignment on demand signal
 - Interlocks to prevent operation with mis-alignment
 - System status indicated in control panel

Examples of qualitative screening rules for Type C human interactions include:

- Eliminate the interaction if the success or failure of the action has no influence on progression of event sequence
- Retain HAs that change the state of equipment that is required to respond to (mitigate) sequence progression
- Eliminate the interaction if physical limitations prevent action (e.g., requires access to radioactive or hostile environment, or if the time required is too short for a realistic HA).

Quantitative screening is performed as a pre-test to determine the potential significance of a given HA to the unavailability of an SSC or to event sequence frequencies. Quantitative screening should be applied to Type A human interactions because these events compete with hardware and software failures in system logic models and may only serve as backups to automatic actions. A coarse screening is performed in such cases by setting the probability of the human failure alternatively to 1.0 and 0.0 (or by using a nominal value such as 0.01 or 0.001 based on similar HAs) and comparing the top event probabilities in the two cases. If the difference is judged insignificant, then that HA does not need detailed analysis.

Quantitative screening of a HA in Type B human interactions is similar to that of Type A. If non-human initiated causes dominate the initiator, then the particular Type B HA does not require detailed analysis.

Since a Type C HA is judged important enough to explicitly model in ET headings, a probability screening may not rule out the need for a detailed analysis. On the other hand, the radiological consequences of performing a particular HA (e.g., restoring offsite power within X hours) may be insignificant. In this case, that HA may also be excluded from a detailed analysis.

7.3.4.4 Task Analyses (Step 3)

This step is the initial step of detailed HRA. In the SHARP methodology (Hannaman and Spurgin 1984), this step is termed Breakdown. The objective of this step is to identify as specifically as possible the level of available detail, the tasks or actions that the particular human is required to perform, including any time restrictions. The human may be, for example, an equipment operator, a central control room operator, a T&M technician, a health physicist, or a supervisor.

There may be detailed procedures for the specific task in mature designs. In earlier stages of design, the HR analyst will have to consult with the design and operations staff to define the principle tasks to be performed, the time restraints, and the man-machine interface that will be used (including the types and locations of controls, instrumentation, or other source of information).

A human-factors evaluation is then performed to identify the conditions and contextual environment associated with each task. The conditions and context are then used to identify the specific performance shaping factors and error-forcing conditions that will be used in the representation and quantification steps.

Table 7-1 presents an example of a task analysis for a hypothetical transfer of an SNF assembly that affects the IE and the emergency response.

It may be possible to identify and take credit for recovery actions to reduce the importance of the initial HFE as part of this step or after the quantification of the FT or ET.

7.3.4.5 Representation and Models (Step 4)

The representation is the method (or logical framework) for organizing the information developed in Step 3. Selection of a representation method for a particular HA depends on the quantification method used for the Type A, B, or C human interactions. The model is the equation(s) that result from the representation. Quantification (Step 5) is the process of assigning values to the parameters used in the model.

- Representation methods include:
 - Simple success-failure
 - HRA ET
 - HRA FT
 - Operator action tree (OAT).

Quantification methods are discussed in the Step 5.

The representation and models recommended for the PSA are described in the following sections.

7.3.4.5.1 Type A

Type A HAs are typically T&M errors (leaving an SSC in an unavailable or degraded state), calibration errors (resulting in failure to actuate automatic safety functions when the conditions require), or the failure of items such as interlocks or limit switches. The methods described in Swain and Guttman (1983) are applicable to a repository.

Figure 7-14 illustrates a simple FT that includes two Type A HAs (the FT is developed as part of Step 1). The top event is titled “Emergency HVAC Fails to Start and Run.” Three causes of the top event are shown as inputs to an OR gate. One input is titled “Mechanical Failure to Start or Run.” This event is shown as diamond indicating that the logic is undeveloped (see Section 7.2). One Type A HA is titled “Miscalibration of Setpoint for Emergency Start,” and the other is titled “Failure to Reconnect Emergency Power Supply After Maintenance.” The top event describes a probability to start or run, q_{SR} , which is termed the unavailability of the HVAC in the sequence frequency quantification. Therefore, all of the input events must be represented as probabilities.

Table 7-1. Example of Task Analysis

Part A: Task Description and Context

Task Number	Task Description	Subtask Description	Location and Environment	Indications	Time Factor	Other Factors
1	Transport block to pickup location	Move bridge, trolley, or both into position	Control Room and Manual Control	Visual – coarse position; CRT – computer-aided positioning	Normal speed for throughput	Procedures for entire operation cycle; extensive training
2	Lower block to height for engaging load			CRT – computer aided		
3	Engage load	Operate remote grapple to mate with lifting lugs on load		Panel lights for limit-switch position		Faulty lifting lugs on package may prevent full mating
4	Raise block to transport height (e.g., so bottom of load is six inches above floor)			Visual – coarse position; CRT – computer-aided height monitor		
5	Transport load (supported by cable and block) to transfer location (move bridge, trolley, or both into position)					
6	Lower block until load is supported by target location					
7	Disengage load	Operate remote grapple to release lifting lugs on load		Panel lights for limit-switch position		Faulty lifting lugs on package may prevent release
8	Raise block to transport height (repeat cycle)					

Table 7-1. Example of Task Analysis (Continued)

Part B: Identification of Influence Factors and Potential Unsafe Acts

Task Number	Task Description	Potential Influence Factors	Potential Mistakes/Slips	Consequences of Mistake/Slip	Recovery Potential
1	Transport block to pickup location	Computer positioning miscalibrated	Mis-alignment of grapple with lifting lugs	No engagement (not a safety problem)	Manual- halt operation to calibrate computer
2	Lower block to height for engaging load				
3	Engage load	Faulty lifting lugs; failure of engagement indicators, interlocks, or both	Inadequate engagement of lugs	Uneven load; single lug engaged; slap-down of load	
4	Raise block to transport height (e.g., so bottom of load is six inches above floor)	Operator distracted – too routine; computer aided height control fails or not used	Raises load higher than procedure calls for	Potential damage to load - Contingent upon subsequent drop	Lower back to normal
5	Transport load (supported by cable and block) to transfer location (move bridge, trolley, or both into position)	Operator distracted – too routine; computer aided position and speed control fails or not used			
6	Lower block until load is supported by target location				
7	Disengage load				
8	Raise block to transport height (repeat cycle)				

Note: CRT = cathode ray tube (i.e., a computer monitor).

A representation of system or component unavailability due to a Type A maintenance or calibration error accounts for several factors:

- Initial HEP (E_i)
- Probability of non-recovery of initial error by self, crew, or supervisor (R)
- Single component or multiple components
- Whether or not the system or component availability is checked or monitored between T&M intervals (announced versus unannounced unavailability)
- The fractional time that the component or system is out-of-service (or miscalibrated) between periodic T&M.

The generalized model for Type A HAs is:

$$q_{SR} = (p_{HE} * d)/T \quad (\text{Eq. 7-15})$$

$$p_{HE} = E_i * R \quad (\text{Eq. 7-16})$$

where

d = mean equipment downtime (or time in a miscalibrated state), in hours, between scheduled T&M with regular interval (T) hours; E_i and R are defined above.

If the equipment outage or miscalibration is not checked or monitored between scheduled T&M, the mean downtime is equal to the T&M interval, and

$$d = T \quad (\text{Eq. 7-17})$$

and

$$q_{SR} = p_{HE} = E_i * R \quad (\text{Eq. 7-18})$$

If the equipment outage or miscalibration is checked or monitored between scheduled T&M, the mean downtime is a function of the efficiency of the checking (monitoring) function. Here efficiency is defined as the probability (C_i) of detecting a prior error during the i^{th} check that occurs at an interval (H_i) within the interval (T). In this case, the mean outage (miscalibration) of the system or component is represented as

$$d = H_1 + C_1 * H_2 + C_2 * H_3 + C_1 C_2 * H_3 + \dots \quad (\text{Eq. 7-19})$$

Values for E_i , R , and C_i are estimated from experience data (if available) or from Swain and Guttman (1983). Table 7-2 presents examples of the form of information contained in Swain and Guttman (1983).

The initial error, E_i , may be either an error of commission or an error of omission. Estimates of the parameters account for factors affecting the quality of T&M, such as:

- T&M procedures
- training
- use of independent checkers
- tagging system (e.g., to avoid T&M and calibration of wrong equipment)
- administrative controls
- safety culture.

The presence and quality of these factors will have to be assumed and documented for the PSA. The application in the quantification (Step 5) accounts for these factors.

7.3.4.5.2 Type B

Type B HAs are typically operational or T&M errors that cause a system or component to change state, and thereby initiate an abnormal operating condition that could propagate to a sequence of events leading to release or exposure to radioactivity.

Figure 7-15 illustrates a simple FT that includes a Type B HA (the FT is developed as part of Step 1). The top event is titled "Crane Drops Load" in a FT representation to estimate the frequency of the event. The house event represents the frequency of opportunities for the operator to err; it is titled "Number of Lift per Year."

Two causes of the intermediate event titled "Load is Dropped" are shown as inputs to an OR gate. One input is titled "Mechanical Failure Causes Drop." This event is shown as a diamond indicating that the logic is undeveloped (see Section 7.2). The other intermediate event is titled "Operator Causes Drop." These two events will be quantified as probabilities per lift.

The event titled "Operator Causes Drop" is developed through an AND gate to represent that the event can happen only if both input events occur (i.e., that "Operator Initiates Lift > Normal Height" and "Mechanical Failure of Lift-Height Limiter" occur).

A representation for the HA titled "Operator Causes Drop" is illustrated next. The information from Step 2, Table 7-1, indicates that the operation is manually controlled. Table 7-1 defines the tasks to be performed by the operator:

- Transport the block to the pickup location (move the bridge, trolley, or both into position)
- Lower the block to the height for engaging the load
- Engage the load (e.g., operate the remote grapple to mate with the lifting lugs on the load)
- Raise the block to the transport height (e.g., so that the bottom of load is six inches above the floor)

- Transport the load (supported by a cable and block) to the transfer location (move the bridge, trolley, or both into position)
- Lower the block until the load is supported by the target location
- Disengage the load (e.g., operate the remote grapple to release the lifting lugs on load)
- Raise the block to the transport height (repeat the cycle).

The analyst now asks “what can happen?” with respect to dropping the load; that is, what erroneous actions could the operator take to cause the load to drop. While there may be several opportunities for the operator to cause the drop, this illustration will examine the task titled “Raise block to transport height.” This task has the potential for causing a two-blocking event that can result in the overstressing and breaking of the lifting cable(s), resulting in a load drop from a height exceeding the normal transport height.

The operator is trained to raise the load only to the normal transport height (e.g., six inches) but the controller permits the operator to raise it higher, subject to a control interruption by an interlock that prevents the raising of the load to the two-blocking height. Each time that the operator performs the routine lift (that has been performed hundreds of times previously) a probability exists that the attention of the operator can be diverted. An initial error of commission is committed by holding the lift control too long and raising the load too high.

If the operator or other crew member realizes the commission of the initial error in a timely manner, the event can be recovered (i.e., the lift can be stopped and the load lowered). If there is no height-limiting device and no recovery, then the initial error will result in two-blocking event followed by a load drop.

The FT (Figure 7-15) leads to the following model (i.e., the boolean expression for the FT events) for estimating the frequency of the IE:

$$f_{OD} = f_{LL} * q_{HL} * E_O * R \quad (\text{Eq. 7-20})$$

where

f_{OD} = frequency that load drops are initiated by operator error, drops per year

f_{LL} = frequency of load lifts using crane (calculated from throughput), lifts per year

q_{HL} = probability that lift-height limiter fails on demand, probability per demand

E_O = probability of initial error that the operator attempts to raise the load to excessive height probability per opportunity (probability per routine lifting operation)

R = probability that the operator fails to recover from the initial error

As in the case of a Type A HA, the parameters E_O , and R are estimated from experience data (if available) or from Swain and Guttmann (1983). Table 7-2 presents examples of the form of

information contained in Swain and Guttmann. Estimates of the hardware unavailability (q_{HL}) are obtained from experience (see Section 7.5) or through FTA (see Section 7.2).

7.3.4.5.3 Type C

Type C HAs are actions taken by an operator in response to an IE or another event. The HAs of interest are those taken to prevent an event sequence from progressing toward a worse state, actions taken to mitigate the consequences of an event sequence, or actions taken that worsen the situation. Generally, such HAs are included in the heading of the ET for a given IE. It is particularly important to show the HA in the ET headings if there are dependencies between the success of the HA and prior events in the ET or if the success or failure of the HA represents a significant turning point in the evolution of event sequences (see Section 7.1).

For example, an ET heading titled "Operator Starts Emergency HVAC" might be an important action that would prevent a significant release of radioactivity following the drop and breach of a waste form, followed by an event titled "Loss of normal HVAC." This action warrants its inclusion in an ET heading. The operator may be prompted early in the sequence to initiate the action by an alarm (e.g., radiation alarm, or loss of normal HVAC alarm), an operator, or (later) by secondary indications (e.g., radiation alarms in stack monitors). In addition there may be no secondary prompt; instead, the indication may rely solely on the attentiveness of the operator (and other staff). The success or failure of the alarm or prompts to alert the operator represent alternative conditions that affect the probability of the success or failure of the operator performing the HA. Thus, the representation of the probability of human failure must account for the dependency on the prompt.

In other cases, a Type C HA may be modeled as part of an FT for a system failure event that is represented in an ET heading. This is the case, for example, for a backup operator action to manually actuate a system that is supposed to start automatically. The ET heading represents the operation of the system; for example, a heading titled "Emergency AC power is available." The system is supposed to start automatically on the loss of voltage of the primary power supply. The system FT for the failure event titled "Emergency AC power is unavailable" would include events representing the failure of components, including the failure of the actuation function. The backup operator action titled "Operator fails to actuate emergency AC power" would be ANDed with the automatic actuation event in the FT.

The following sections present representations for the respective cases of Type C HAs.

7.3.4.5.3.1 Type C HAs in Event Tree Headings

This type of Type C HA has been the subject of a considerable amount of research and development, as well as the subject of a considerable amount of controversy.

The principal research on this HA has been directed toward a better understanding, representation, and quantification of the reliability of the operators of NPPs in preventing and mitigating severe accidents. Severe accidents for NPPs are event sequences that progress to undesired plant damage states that exceed the design basis accidents; namely, core damage and, possibly, loss of secondary containment. Because the probability of human error involves cognitive processes, this research has involved various multi-disciplinary teams of system-safety

and PRA practitioners, behavioral scientists, human-factors specialist, NPP operators and operations supervisors, and operator training personnel.

Table 7-2. Example Probabilities of Errors of Commission in Operating Manual Controls

Item	Potential Errors	HEP ^a	Error Factor
	Select wrong control on a panel from an array of similar-appearing controls: ^b		
(2)	identified by labels only	0.003	3
(3)	arranged in well-defined functional groups	0.001	3
(4)	which are part of a well-defined mimic layout	0.0005	10
	Turn rotary control in wrong direction (for two-position switches, see item 8):		
(5)	when there is no violation of population stereotypes	0.0005	10
(6)	when design violates a strong population stereotype and operating conditions are normal	0.05	5
(7)	when design violates a strong population stereotype and operation is under high stress	0.5	5
(8)	Turn a two-position switch in wrong direction or leave it in the wrong setting	^c	

Source: Modified from Swain and Guttman (1983, Table 20-12)

NOTES: ^a The HEPs are for errors of commission only and do not include any error of decision as to which controls to activate.

^b If controls or circuit breakers are to be restored and are tagged, adjust the tabled HEPs according to Swain and Guttman (1983, Table 20-15).

^c Divide HEPs for rotary controls (Items 5 through 7) by 5 (use same EFs).

The HAs of most interest to NPP risk assessment are, typically, time-critical and are performed when the operators are under extreme stress because they understand the severity of the evolving situation. There are other Type C HAs, however, that are risk-significant for NPPs that are not as time-critical. These differences have led to different types of representations for the two classes of Type C HAs.

The hazards and operations associated with a repository do not pose demands on the operators with the severity of those associated with NPPs. In addition, the risk profile of a repository is not expected to be very sensitive to operator reliability for Type C HAs. Nevertheless, the efforts of the past three decades have led to advances in the understanding and development of alternative methods for the representation and quantification that can be applied in the PSA, where appropriate, to Type C HAs.

7.3.4.5.3.2 Operator Action Tree

The operator action tree (OAT) shown in Figure 7-17 is a generalized representation of Type C HAs. The OAT is an ET. There are two main phases of operator response that are indicated across the top of the figure: detection, diagnosis, and decision phase, as well as Manual Action. The OAT, as shown, represents both time critical and non-time critical HAs. Two ET headings comprise the detection, diagnosis, and decision phase: Cognitive Processing/Procedural Mistakes and Failure to Process Information in a Timely Manner.

The event heading titled “Cognitive Processing/Procedural Mistakes” covers all of the information gathering and diagnosis that the operator performs (e.g., through the instrumentation or through phone calls from local operators) that make the operator aware of an off-normal situation. The indications are symptoms that are indicative of an event. Operators are trained to use the symptoms to diagnose the event and initiate appropriate actions.

As shown in the OAT, the failure to diagnose the event leads to a failure to perform the Type C HA, as indicated by the “F” at the endstate. The probability of this failure is shown as p_1 in the figure. The representation, modeling, and quantification of p_1 have been the principal subjects of HRA research. Most recently, it was the primary motivation for the ATHEANA project (NRC 2000). Methods for quantifying p_1 are discussed in a following section.

The event heading titled “Failure to Process Information in a Timely Manner” means that there is a finite time window within which the manual action must be started; if not, the action is performed too late. This non-action results in a failure to perform the Type C HA, as indicated by the “F” at the endstate. The probability of this failure is shown as p_2 in the figure. Representation, modeling, and quantification of p_2 have also been subjects of HRA research (e.g., Moieni et al. 1993). If the particular HA is not time-critical, this event heading, sequence branch, and endstate are deleted from the OAT.

The event heading in the Manual Action phase of the OAT is labeled “Manipulative Slips.” The term slips is used to denote that at this point, the operator knows what to do and moves to the appropriate control to execute the desired action. For various reasons, including poor ergonomic design, the operator selects the wrong control or moves it to the wrong position. In addition, p_3 includes the probability that all steps in a control action are not completed, or not completed within a required time window. The result is a failure to perform the Type C HA, as indicated by the “F” in the endstate. The probability of the slip is indicated by p_3 in the figure.

The probabilities, p_1 and p_3 , (Figure 7-17) represent non-recovered mistakes and slips. For some of the Type A and Type B HAs, the final probability represents a product

$$p_i = E_i * R_i \quad (\text{Eq. 7-21})$$

where

- E_i = probability of initial mistake (or slip) i
- R_i = probability of non-recovery of initial mistake (slip) i

The probability, p_2 , includes an implicit failure to recover.

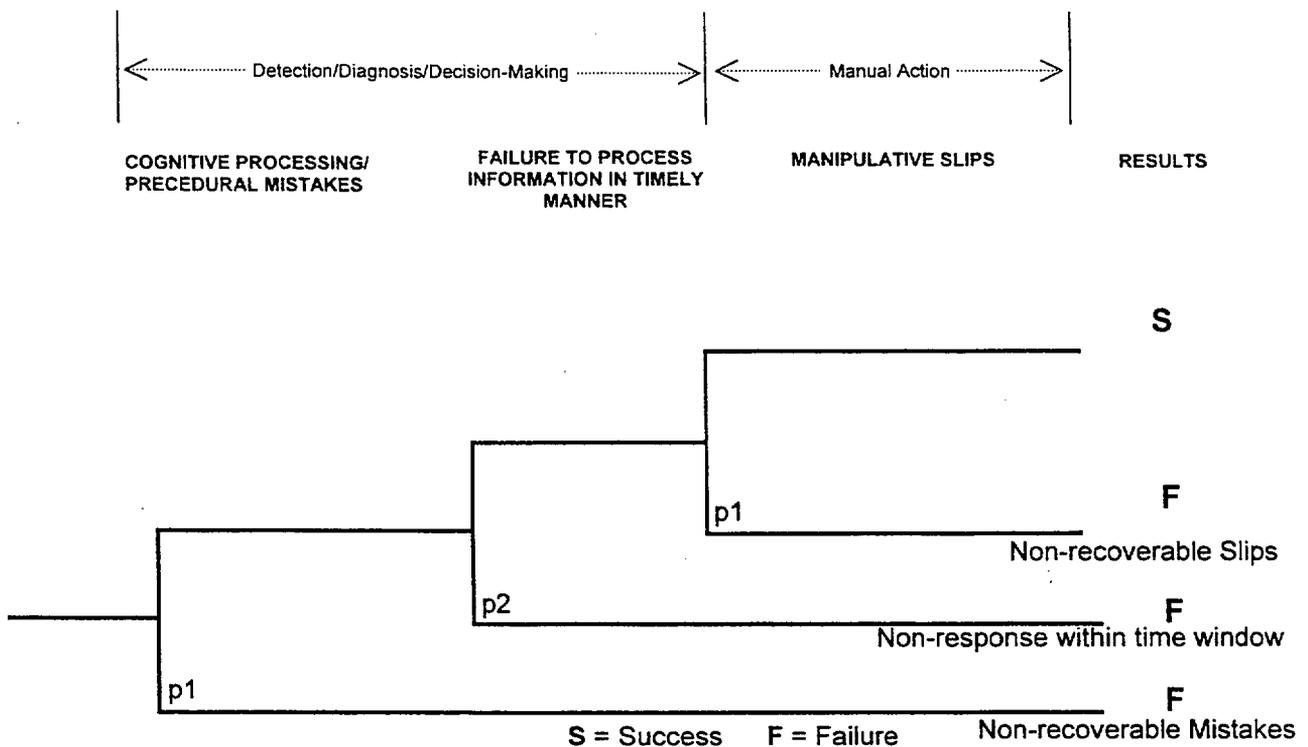


Figure 7-17. Operator Action Tree: A Generalized Representation of Type C HAs

The probability of failing to perform the particular Type C HA is the sum of the three failure branches of the OAT (labeled F):

$$P_{HA} = p_1 + p_2 + p_3 \quad (\text{Eq. 7-22})$$

The following sections describe the representations and models for the respective probabilities (p_1 , p_2 , and p_3). This is an elaboration of Step 4. These sections also describe the bases for quantifying the probabilities, which is Step 5.

7.3.4.5.3.3 Representation, Modeling, and Quantifying p_1

Several methods have been developed for defining p_1 for NPP applications (e.g., Moieni et al. 1993). This portion of the detection, diagnosis, and decision phase for NPPs typically involves the use of emergency operating procedures that the operators follow to diagnose and respond to the event. Currently, NPPs use symptom-based emergency operating procedures that support decision making with cascading IF-THEN statements. While a repository will have emergency operating procedures, it is unlikely that they will be as complex as those of NPPs.

All of the methods provide some means of identifying and quantifying the effects of causal factors (or error forcing conditions) and Performance Shaping Factors that affect the probability. Typical causal factors might be:

- Erroneous or incomplete procedures (e.g., have inadequate validation and verification)
- Inadequate training to help diagnose, or apply procedures

- Inadequate instrumentation or alarms
- Miscommunication among crew members

Alternative approaches for p_1 include:

- Swain and Guttman (1983, Chapter 20)
- Decision tree (Moieni et al. 1993)
- ATHEANA (NRC 2000)

Most of the approaches for p_1 appear to be too complex, inappropriate, or both, for the types of operator actions expected in a repository. These alternative methods will be reviewed and adapted as appropriate to the PSA

7.3.4.5.3.4 Representation, Modeling, and Quantifying p_2

[Information for this section is under development and will be provided later.]

7.3.4.5.3.5 Representation, Models, and Quantification of p_3

The p_3 probability represents the chance of a non-recovered slip by control operators or the probability of not completing all steps in a control action within the required time window. This type of HA is generally viewed as non-cognitive and the requirements are well known to the trained operator.

Alternative representations of p_3 depend on the complexity of the manual actions to be performed. If the action is simple, such as changing the position of a single switch or controller, then a binary, success or failure, representation suffices. If the action requires multiple steps then either a HR FT or Swain and Guttman HRA tree can be used to delineate the various steps and the conditional probabilities of the sequential steps. These representations include dependencies between steps.

The representation, modeling, and quantification must include the effects of performance shaping factors (e.g., quality of ergonomic interface of indicators, controls, communications, training, and the complexity of task) for all of the representations.

The basic source of information on quantification is the *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations* (Swain and Guttman 1983). This handbook has extensive tables of generic error types. For example, the error titled "Select wrong control on a panel from an array of similar-appearing controls" (Swain and Guttman 1983, Table 20-12; see also Section 7.2) and the recommended values for the HEP and EF for lognormal (LN) distribution are presented. See Section 7.6 and Section 9 for discussions of uncertainties and EFs.

The HEP values and EFs are given for various configurations and operating conditions. For the example previously quoted, the HEP and EF are 0.003 and 3, respectively, if controls are identified by labels only. If the control is part of a panel where controls are arranged in a well-delineated functional groups, then the HEP is given as 0.001 with an EF of 3. Further, several ancillary tables provide adjustments for various performance-shaping factors and operating

conditions. Again, for the example quoted, a footnote reads “if controls ... are to be restored and are tagged, adjust the tabled HEPs according to Table 20-15.”

For a single step HA, such as an HA titled “Start emergency HVAC with Switch No. 1234,” located in a well-delineated functional group with no performance shaping factors outside the nominal range, the representation and quantification are given as:

$$\begin{aligned} p_3 &= \text{HEP (tabulated for conditions, adjusted for performance} \\ &\quad \text{shaping factors) with EF} && \text{(Eq. 7-23)} \\ &= 0.001 \text{ (EF = 3)} \end{aligned}$$

The representation for multiple-step HAs is a compounding of the single action case with consideration of dependencies. That is, if the operator slips on the first action without recovery, the execution of the second and subsequent actions may be missed because the operator is executing a practiced, but erroneous, series of manipulations. The representation is an HRA tree or an HR FT, depending on the HA to be modeled.

As an example, a HRA tree is illustrated in Figure 7-18. The control action consists of two steps: “Start emergency HVAC with Switch No. 1234,” which is located in a well-delineated functional group; and “Close HVAC damper between Zones 2 and 3 with switch D56.” This action requires that the switch be held in the closed position until the damper completely closes. Swain and Guttman (1983, Table 20-12, Item 10) gives this HEP as 0.003 (EF = 3).

Figure 7-18 illustrates an HRA tree for this HA. Following the convention of Swain and Guttman (1983), the branches labeled with capital letters represent failure to execute and small letters are the success branches. If there are no recoveries, the representation for p_3 is:

$$p_3 = A + B \quad \text{(Eq. 7-24)}$$

and the quantification is:

$$\begin{aligned} p_3 &= \text{HEP}_A + \text{HEP}_B \text{ (with composite EF)} && \text{(Eq. 7-25)} \\ &= 0.001 + 0.003 = 0.004 \text{ (EF > 3)} \end{aligned}$$

Where HEP_A and HEP_B are the human error probabilities for actions A and B, respectively.

If recoveries are possible at Step 1 or Step 2 (illustrated by dashed lines in Figure 7-18), the probabilities of non-recovery (R_A and R_B) are inserted into the representation as follows:

$$p_3 = \text{HEP}_A * R_A + \text{HEP}_B * R_B \text{ (with composite EF)} \quad \text{(Eq. 7-26)}$$

For example, if $R_A = 0.1$ and $R_B = 1$ (non-recoverable) the quantification becomes:

$$p_3 = (0.001)*(0.1) + (0.003) * (1.0) = 0.0031 \text{ (with composite EF)} \quad \text{(Eq. 7-27)}$$

The representation must also consider if the order of execution is important because of potential dependencies. For example, suppose the HVAC damper has to be fully closed before the emergency HVAC can be started (i.e., an interlock prohibits starting the HVAC). In this

particular example, the representation is further complicated by the dependency on the reliability of the hardware (interlock) as well as the human reliability:

$$p_3 = HEP_B + HEP_A * (1 - q_{IL}) + q_{IL}, \text{ (no recovery)} \quad (\text{Eq. 7-28})$$

where

q_{IL} = probability of failure of interlock, failures per demand

If $q_{IF} = 0.0001$, for example, p_3 is quantified as:

$$\begin{aligned} p_3 &= 0.003 + 0.001 * (1 - 0.0001) + 0.0001 \\ &= 0.0032 \end{aligned}$$

7.3.4.6 Quantification of Human Action Probabilities (Step 5)

[Information for this section is under development and will be provided later.]

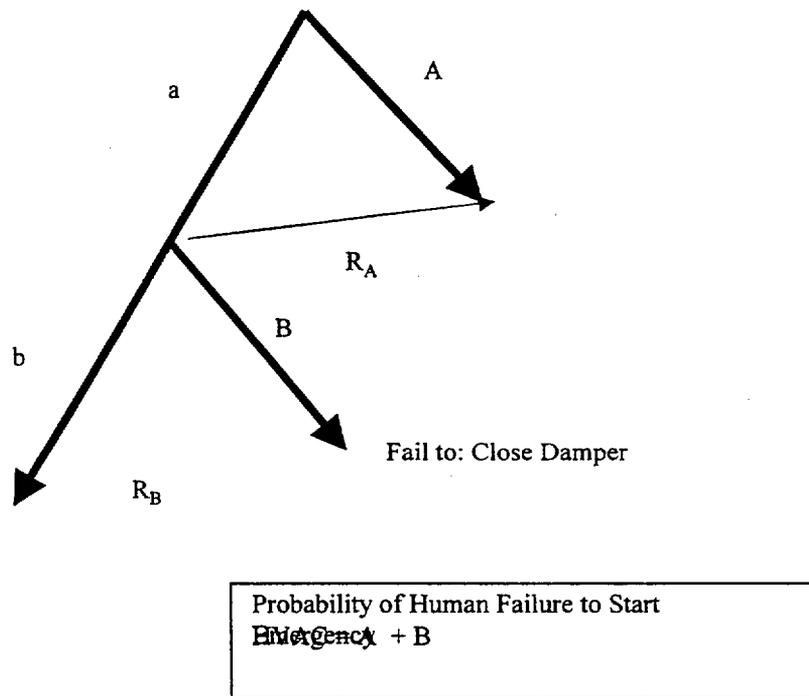


Figure 7-18. Example of Human Reliability Analysis Tree

7.3.4.7 Quantification of Event Tree/Fault Tree (Step 6)

This step is just a re-statement of the outputs of Sections 7.1 and 7.2, respectively. When all of the HA probabilities (and uncertainties) have been quantified, they are incorporated into the logic models. Quantification of the FT top event gives SSC unavailabilities, or IE frequencies, with the effects of HA. Quantification of event sequence frequencies illustrate the influence of HAs and any recovery actions that have been quantified.

7.3.5 Examples

[Information for this section is under development and will be provided later.]

7.4 COMMON-CAUSE AND DEPENDENT FAILURES ANALYSIS

7.4.1 Purpose

This guide defines the bases and methods for identifying and analyzing common-cause and dependent failures in support of the PSA. These common-cause failures (CCFs) and dependent failure analyses support event sequence analyses through applications in ETA and FTA. In addition, this section provides a link to HRA, which is an important contributor to CCFs and dependent failures.

7.4.2 Scope

This section is a guide to the identification and analysis of common-cause and dependent failures. While some concepts and methods are universal to safety and risk analyses of nuclear, chemical, and other facilities, the approaches and examples are focused on the support of a repository PSA. The guide provides methods that are expected to be acceptable to the NRC. The guide is not meant to be a textbook or exhaustive. Where appropriate, reference is made to literature for additional information. Examples of CCF applications are described in the discussions of ETA (Section 7.1), FTA (Section 7.2), and Seismic Analysis (Section 10.1).

In particular, this section will provide guidance in the following areas:

- Method(s) used to identify and screen important dependent failures in SSCs that affect preclosure safety
- Application of qualitative versus quantitative evaluations, where qualitative analysis is used to postulate, identify, and eliminate potential dependent failures through a screening process
- Quantitative methods for use when evaluating FTs, ETs, and event sequence frequencies
- Data requirements and sources
- Treatment of external events as potential common-cause IEs and how dependent failures of SSCs are conditionally linked to external hazard frequency
- Differences in approach and level of design detail and operational detail considered for the LA submittal for CA in contrast to the LA submittal to receive and possess nuclear materials
- Application of software packages (e.g., SAPHIRE, and the Microsoft Excel spreadsheet program)

7.4.3 Overview of Approach

The term common cause events refers to a specific class of dependent events that must be considered in reliability analyses of safety systems in support of a PSA or PRA. Common cause

failures are encountered when considering the causes of, and probabilities of, basic events at the component level in system logic models (e.g., FTs).

“Explicit” dependent failure is used to define those dependent events that can be directly attributed to physical phenomena and identifiable causal factors. Causal factors include inter-system dependencies that are hard-wired inter-connections; physical interactions between components or systems, such as missiles or sprays; environmental factors such as extreme temperatures or humidity; and human actions, including miscalibration of instruments or test and maintenance. The probabilities of such dependent events are quantified with appropriate equipment failure rates, test and maintenance intervals, and human-error probabilities. In some cases, physical interaction probabilities can be explicitly calculated, such as the probability of a spray or missile from the first failed component causing a failure in two or more additional components in the same or different systems.

System analysts include the explicit dependent failures in the system or plant logic models. That is, functional dependencies can be indicated in ETs to impose boundary conditions on event probabilities for events that occur later in the ET. In addition, functional dependencies of front line systems on support system are directly modeled in FTs as either basic (or undeveloped) events or as a transfer to the FT model of the support system. Likewise, cascading or propagating failures and operator actions to respond to events are modeled explicitly. Identified maintenance errors are modeled directly in the FTs.

By contrast, “implicit” dependent failures is used to define the potential occurrence of unidentified specific causal factors that can defeat the independence between redundant systems or components. Such dependencies are modeled in ET and FT logic as basic events as “pseudo-components” that are not physically present in the system design. The probabilities of such events are quantified using “implicit” or “parametric” analyses in which the failure rate information for various components is partitioned into independent and dependent rates.

Initially the plant or system logic model (e.g., FT) is developed with the basic events considered to be independent failures. Explicit intersystem dependencies are modeled as described above. Potential dependencies among components (basic events) that have not been explicitly modeled in the logic model are identified and modeled as pseudo-events in the FT models to represent CCFs. The probabilities of the CCFs are quantified with methods described in NUREG/CR-4780 (Mosleh et al. 1988). Only a brief acknowledgement of alternative methods is provided here since the simplest model for CCF analysis, the beta factor model, suffices for most preclosure safety analyses of a repository. The methods for the LA submittal for CA are presented. If deemed appropriate, this desktop guide can be revised to include more advanced methods of treating CCFs.

7.4.3.1 Definitions

The following are definitions (NUREG/CR-4780 [Mosleh et al. 1988]) of the principal terms that are used in this section.

Independent Event—This is an event in which a component state occurs causally unrelated to any other component state. Two events, A and B, are independent if and only if:

$$p(A|B) = p(A), \text{ and } p(B|A) = p(B) \quad (\text{Eq. 7-29a})$$

such that

$$p(A \text{ and } B) = p(A) * p(B) \quad (\text{Eq. 7-29b})$$

where

$p(x|y)$ = probability of occurrence of event x given the occurrence of event y, and

$p(x)$ = probability of occurrence of event x.

Dependent Event—This event does not satisfy the definition of an independent event. Two events, A and B, are dependent if and only if:

$$p(A \text{ and } B) = p(A) * p(B|A) = p(B)*p(A|B) \neq p(A) * p(B) \quad (\text{Eq. 7-30})$$

and more importantly

$$p(A \text{ and } B) > p(A) * p(B) \quad (\text{Eq. 7-31})$$

Common Cause Event—In the context of system modeling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time or in a short time interval and are a direct result of a shared cause. NUREG/CR-4780 (Mosleh et al. 1988) does not attempt to provide a clear and unambiguous definition of common cause events for all purposes. It is implied that the shared cause is not another component state because such cascading failures are modeled explicitly in the system models. The common cause is termed a root cause applied at the component level.

Root Causes—Root causes ideally can be traced to an event that occurred at some prior time. There are four general types of root causes:

- Hardware and software—inherent defects
- Human errors—operations, T&M, design, construction
- Environmental—events external to the equipment but internal to the facility or operation that result in abnormal stresses in the equipment
- External—events external to the facility that result in abnormal stresses in the equipment

Coupling Mechanism—A coupling mechanism is a means by which a root cause propagates to involve multiple components or subsystems. Three broad categories of coupling mechanisms are identified:

- Functional Couplings
- Spatial Couplings
- Human Couplings

Table 7-3 describes some examples of each of these coupling mechanisms.

Table 7-3. Types of Dependent Events Based on their Impact on Preclosure Safety of a Repository

Dependent Event Type	Characteristics	Subtypes (Coupling Mechanism)	Examples
1. Common Cause IE	Causes challenge to facility design or operations, and concurrently increases likelihood that one or more prevention or mitigation SSCs will fail	Functional Spatial Human	Loss of Offsite Power Earthquake or fire Maintenance error in main control room
2. Intersystem Dependency	Causes a dependency in a joint event probability involving two or more systems	Functional Spatial Human	Two trains of instrumentation and control fail because electric power supply fails Fire in one instrument cluster causes failure in others in proximity Operator error causes loss of two or more systems
3. Intercomponent (Intrasystem) Dependency	Causes a dependency in a joint event probability involving two or more components	Functional Spatial Human	Crane cable(s) break after two-block prevention features fail Failure of one of two crane cables allows rigging to tilt and sever second cable Installation of wrong lifting fixture permits crane two blocking and break of cables

Source: Modified from NUREG/CR-4780 (Mosleh et al. 1988, Table 2-1)

Common Cause Component Group—This is a group of components (usually similar) that are considered to have a high potential of failing due to the same cause.

Defensive Strategy—A defensive strategy is a measure taken to diminish the probability and consequences of common cause failures. Operations, maintenance, design, and surveillance are areas where defensive strategies can be applied.

Explicit Analyses—Explicit analyses of dependent or CCF failures are identified from specific potential root causes and coupling mechanisms. Inter-component or inter-system dependencies are shown explicitly in logic models (e.g., ETs and FTs). Conditional probabilities of dependent events are evaluated from consideration of vulnerabilities in the target component or system and opportunities for the coupling mechanism to link the root cause (triggering event) to failure of the target.

Implicit (or Parametric) Analyses—Implicit analyses of dependent or CCF failures are used when the possibility of dependent failure is known (or suspected) to exist but specific root causes and coupling mechanisms cannot be identified or quantified. Inter-component or inter-system dependencies are shown explicitly in the system logic models (principally FTs) to represent implicit events. Conditional probabilities of dependent failure are estimated using various parametric approaches such as the beta factor method.

Parametric Analyses—See the definition of implicit analyses).

Primary (Front-Line) System—A primary system is one that provides a direct function in the handling, packaging, or transporting a high-level radioactive waste form. Of particular importance are the front-line systems important to safety that prevent or mitigate potential unwanted sequences of events. Such front-line safety systems may be slated for single-failure-proof-, or fail-safe, design principles. The HVAC/HEPA filter system in the waste handling building of the surface facility is an example of an important front-line system. Analyses of dependent and CCFs can help to provide assurance that such systems perform their intended safety functions with adequate reliability.

Support (Secondary) System—A support system is one that provides an indirect function in the handling, packaging, or transporting of a high-level radioactive waste form by providing essential support to the front-line systems. An important support system for the safety of repository operations is the electrical supply system. Virtually every operation in a repository is dependent on electric power. Although many devices can be designed to halt in a safe mode on the loss of a power supply, other devices (i.e., HVAC/HEPA filters, instrumentation, or control systems) cannot. Thus, there is an explicit coupling (dependency) between the front-line system and the support system.

7.4.3.2 Background Discussion

The analysis of common-cause and dependent failures is a subtopic of PSAs.

A CCF (sometimes called common-mode failure, although there is a distinction) can be considered to be a special case of dependent failures. Dependent failures, as a class, are so-named to distinguish them from independent failures. Independent failures are sometimes termed random failures, but this is a misnomer since dependent failures can also occur randomly in time.

Common-cause and dependent failures are important considerations in the analysis of SSCs that are intended to be highly reliable in preventing or mitigating the effects of potential hazards. Considerations of common-cause and dependent failures are important whenever redundant components or subsystems (or alternative success paths) have been provided for safety and reliability. The treatment of common-cause and dependent failures contrasts with traditional reliability analyses and single-failure-proof design approaches that implicitly assume that only independent failures can occur among two or more redundant components or subsystems.

Dependent failures result from the coexistence of two factors: a susceptibility for components to fail or be unavailable from a particular root cause and a coupling mechanism.

For example, two components located in the same room might be susceptible to failure if the humidity exceeds some level. An event such as a rupture of a hot-water or steam pipe would result in extreme humidity and induce a dependent failure of the two components. High humidity from the steam break would be the root cause of the component failure. The fact that the components are situated in the same room where there is a source of water or steam is the coupling mechanism.

Design errors can also result in dependent failures. For example, the redundant safety injection system at one NPP failed because the motor-operated valves in both of the redundant pump trains were undersized and unable to open against the pressure. The root cause was the design process and the coupling mechanism was the use of identical valves and common demand conditions in addition to the lack of adequate surveillance tests. An analogous situation could occur in a repository. For example, if the braking power of each of two redundant and diverse brake systems on the emplacement transporter was designed to be inadequate, then the effect of having a redundant backup system might be negligible. Or, the design might be such that the primary brake system fails in such a way to cause a spray or missile to induce failure of the backup system. Generally, CCFs due to system design flaws are eliminated through design reviews, including fault tree analysis and quality assurance. As the design of a repository evolves, PSA specialists can help in design reviews to eliminate potential common cause failures. Potential design flaws must be evaluated implicitly as one of the non-specific common causes during the preliminary design phases.

Figure 7-19 (based on Mosleh et al. 1988) illustrates the general model for consideration of dependent failures or CCFs. A root cause interacts with each of the multiple components labeled A through N by the means of a coupling mechanism. A defense strategy may be employed to prevent dependent failures or reduce their likelihood. A defense strategy attacks any or all of the elements in the figure by eliminating or reducing the root cause, eliminating or reducing the coupling mechanism, or by making each component less susceptible to the root cause or the coupling mechanism (one means of achieving the latter might be to use diverse components). Table 7-3 illustrates several typical root causes and coupling mechanisms.

A dependent failure of two or more redundant SSCs can occur when there is a coupling mechanism that links a causal agent to the failure of the multiple SSCs. In some cases (usually termed physical interaction dependencies), the failure of one component may cause a domino effect, such that a missile, spray, excess stress, water hammer, or other mechanism induces the failure of two (or more) of the redundant components. Design and operational features can be provided to eliminate such physical interactions, once identified.

Another type of dependent failure among redundant SSCs occurs when two or more components or subsystems are dependent on the same support system. For example, if all of the fan motors in a HVAC/HEPA filter system are connected to the same power bus, all fans will fail to run if the power system fails. Design features can eliminate such dependencies or displace them a lower level (e.g., by providing redundant offsite and onsite power distribution systems).

Source: modified from NRC (1987)

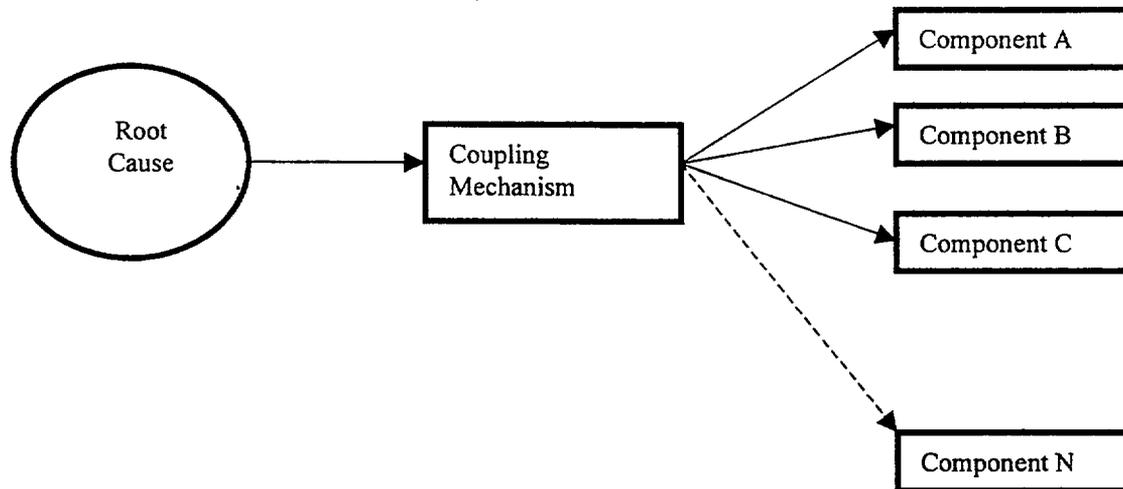


Figure 7-19. Physical Elements of Dependent Events

A CCF of two or more redundant SSCs, as noted, is a special designation for dependent failures that are caused by coupling mechanisms other than physical interactions or systemic dependencies. Such CCFs may arise from common maintenance errors, common calibration errors, inadequate design (capacity), abnormal loads, or other situations that result in multiple components (or systems) failing in response to a given demand or during a given mission time.

Insights from the PRAs of nuclear plants and quantitative risk analysis of chemical process plants, as well as events such as the Three Mile Island incident and Challenger explosion, have revealed the significance of CCFs in potential accidents. The identification and elimination of potential CCFs are now part of safety design and operations.

In addition, studies have shown that CCFs (identified or unidentified) limit the practical reliability that is achievable in engineered systems. Even with the use of redundant and diverse channels (trains), there appear to be limits on the lowest probability of failure that can be achieved. Table 7-4 summarizes a commentary in Watson (1987) on the reliability achievable with various system configurations employing varying degrees of redundancy and diversity. It is noted that the lowest limit for fully diverse and redundant systems is approximately 10^{-6} per demand. Therefore, any system analysis for active repository systems that yields a failure probability less than 10^{-6} should be challenged and reviewed to ensure that all potential causes of CCF and dependent failures have been identified. In most cases, failure causes deemed unimportant at the beginning of modeling or design evolution become dominant after all other identified causes have been defended against or designed out. This does not mean that lower probabilities are to be categorically dismissed, but only that the analysis is subject to scrutiny if major safety decisions are based on such analyses.

7.4.4 Details of Approach

The analysis of CCFs and dependent failures may take many forms. In explicit analyses, potential dependent or CCF failure models are identified from specific potential root causes and probabilities of common-cause events are evaluated from a consideration of vulnerabilities and

opportunities for coupling via spatial, functional, environmental, or human interactions. In implicit analyses (also termed parametric modeling), it is assumed that a small fraction of the total failure probability of a component or system is attributed to CCFs of indeterminate or non-specific causes. The small fraction of CCFs is included in system reliability models though parameters derived from experience data or through judgement. The well-known beta-factor method is an example of an implicit or parametric model.

Table 7-4. A Guide to Unreliability of Various System Arrangements with Consideration of Dependent Failures

System Arrangement ^a	Description and Features	Range of Unreliability Factors ^b
Single Channel System	The simplest form of a system having a single input module and single processor or output module. The lower limit of probability of failure is about 10^{-2} . Adding a redundant channel can improve the reliability to about 10^{-4} if only independent failures can occur. But the effects of CCF become apparent.	0.2 to 10^{-2}
Partly Redundant System	A system having redundancy in its input channels only might have a failure probability in a range of 5×10^{-2} to 10^{-3} . The inference is that the most significant contributors to system failure have been determined to be in the input, although redundancy could be extended to other modules for further reduction in failure probability. CCF	5×10^{-2} to 10^{-3}
Partly Diverse System	The logical development in the quest for higher system reliability is to reduce the CCF probability by introducing diversity into those parts of the system where redundancy was previously considered, as in the Partly Redundant System, and to introduce redundancy where there was none previously. In this example, the input modules apply diverse designs while the processor or output applies redundant modules. One arrangement could be isolated channels where the channel fails if either its input or its processor or output fails. Alternatively, cross ties may be included to permit either input channel to connect to either process/output channel. It is cautioned that such cross ties may themselves introduce other CCF paths. The Partly Diverse System is capable of a failure probability in a range of 10^{-2} to 10^{-4} .	10^{-2} to 10^{-4}
Fully Diverse System	For further reduction in system failure probability, the independence between redundant channels must be improved by using diverse designs for input modules and for processor/output modules, and eliminating any cross ties between the channels. Systems have evolved to provide a failure probability in a range from 10^{-3} to less than 10^{-5} .	10^{-3} to $< 10^{-5}$
Two Diverse, Redundant Systems	The final stage in this example of system design evolution is to provide diverse input channels each being two-fold redundant in addition to redundant and diverse processor/output modules (i.e., four input channels, two each connected to one of two redundant and diverse processor/output modules). For practical reasons it is unlikely that more than two-fold redundancy can be applied to each subsystem. There are, therefore, completely diverse and separate systems throughout and would be expected to provide an overall system failure probability in a range of 10^{-4} to 10^{-6} .	10^{-4} to 10^{-6}

Source: Modified from Watson (1987, Figure 9)

NOTES: ^a Examples are primarily active electronic systems that have input, and processing/output modules.

^b Per Watson (1987, Figure 10).

7.4.4.1 Explicit Modeling of Dependent Failures in Event Trees and Fault Trees

When specific mechanisms or linkages can be identified among components, subsystems, or systems, dependent failures can, and should be, modeled explicitly in ETs or FTs. More details on how such dependencies are modeled are provided in Sections 7.1, 7.2, and 10.1. An overview is presented in the following paragraphs.

Table 7-3 lists types of dependent events, their characteristics, principal coupling mechanisms, and examples relevant to repository operations.

7.4.4.1.1 Explicit Dependencies in Event Trees

The framework of the ET is used to display the frequency of the initiator and the conditional probabilities of each enabling event in a sequence. The frequency of each event sequence is calculated as the product of the initiator frequency and the probabilities of branch nodes that appear in the event sequence. The ET permits analysis of the dependencies between the IE and enabling events, dependencies between enabling events, or both. This means that if there are sequence-dependent couplings between events, there may be different probability values for a given enabling event in different sequences.

A dependent event in an ET has to be inserted into the tree after (to the right of) a precursor event upon which it is dependent. In extreme cases of dependency, the occurrence of the precursor event may guarantee the occurrence of the dependent event; that is, there is complete dependence between the events.

Figure 7-20A and 20B illustrate how dependent failures can alter the structure of ETs and affect the outcomes of event sequences. Figure 7-20A illustrates a simple (baseline) ET containing only independent events. The IE is a drop of a waste form that causes a release inside the hot cell. When the HVAC/HEPA filter system functions properly, the filtered release is small. This is indicated by a "Yes" under the event heading titled "HVAC/HEPA Filters Release" leading to Sequence No. 2. If the HVAC/HEPA filter fails (by independent failure), as represented by the "No" branch, the release is large, as represented by Sequence No. 3. Because this failure is independent of the IE, the frequency of Sequence No. 3 is equal to the frequency of the IE multiplied by the independent failure probability of the HVAC/HEPA filter.

Figure 7-20B, by contrast, illustrates the case in which the initiator is a fire inside the hot cell. In this example, it is assumed that there is a dependency between the initiating event (fire) and the HVAC/HEPA filter system. In this case, there is no "Yes" (or success) branch under the heading titled "HVAC/HEPA Filters Release," which leads to Sequence No. 3 and a large release. Note that the sequence numbers are different in Figures 7-20A and 20B.

The origin of the fire is not defined in this example. In addition, the probability of success or failure of a fire suppression system is not modeled in this example. See Section 10.1 for a discussion of such ETs.

Such a fire could induce a drop of a load as another type of dependent failure that could occur together with the dependent failure of the HVAC/HEPA filter. This event sequence would result in a simpler ET and a higher frequency of release.

Similarly, events may be dependent on the availability of a support system. In an ET having an IE titled "loss of offsite power," an event heading might be titled "backup power system is available." Subsequent events that are dependent on having AC or DC electrical power are shown in various event headings. For example, the HVAC/HEPA filter requires AC power for its fan motors, but the control and instrumentation systems may require DC electric power to perform their safety functions. Unless provided with fail-safe features, devices such as cranes, manipulators, and transport vehicles may be dependent on the availability of electric power.

In a loss-of-offsite-power ET, in the “no” branch after the heading titled “backup power system is available,” no branching node would be shown under the event heading titled “HVAC/HEPA filter operates” to indicate a “guaranteed failure” because the HVAC/HEPA filter is dependent on the AC and DC power. In the “yes” branch, by contrast, a branching node would be included to represent the independent failure of the HVAC/HEPA filter system when AC and DC power are available. The other examples would be similarly modeled.

Dependencies on key HAs can be modeled in an ET in the same manner. If an operator is supposed to take an action to prevent or mitigate a potentially unsafe situation (e.g., activate a filtration system, a backup power supply, or close an isolation barrier), the branching nodes under the event headings in the ET are developed to show these dependencies. The dependencies may be complete, giving a guaranteed failure (as in the examples previously mentioned), or result in conditional probabilities that are higher than the independent failure probability for the heading event.

The analyst must justify the conditional probabilities assigned in such circumstance.

7.4.4.1.2 Explicit Dependencies in Fault Trees

To a certain degree, accounting for explicit dependencies in FT modeling is almost automatic if the analyst is thorough. The top-down decomposition of the top event to subsystems, components, and basic events leads to the identification of virtually all of the explicit dependencies.

For example, in an FT for a multi-train HVAC/HEPA filter system, the analyst resolves the failure of one of the trains (an event titled “HVAC/HEPA filter Train A fails to start and run”) through an OR gate that includes as inputs: failure of the motor to start and run, failure of HEPA filter element, and failure of the fan. These inputs represent failures within the hardware of the primary system. Other events that could cause Train A to be unavailable (e.g., Train A out of service for maintenance, No electric power available to Train A, or Operator fails to actuate Train A) must be included to complete the FT. These inputs are examples of explicit dependencies that are incorporated into the logic model for the system.

In a multi-train system (such as the HVAC/HEPA filter system in the example), several of the modeled dependencies may be found to be CCFs. For example, if Train A and Train B (and other trains) all depend on a single train of electric power, then loss of the power supply would result in a loss of all HVAC/HEPA filters. In FT analyses, such dependencies might be identified through inspection in a simple system. Otherwise, in the determination of the minimal cutsets for the system failure, the singlet representing the failure of the electric power supply would be identified automatically through the boolean algebra.

7.4.4.1.3 Common-Cause Initiating Events

The IEs such as earthquakes, floods, fires, and loss of offsite power (previously discussed) can be important contributors to the risk of a facility unless design provisions prevent dependent failures. These topics are addressed in more detail in their respective sections of this guide. This section provides an overview of IEs and dependent failures using an earthquake as an example. Section 10.1 Seismic Analysis, illustrates the applications of seismic ETs that account for

Baseline Event Tree

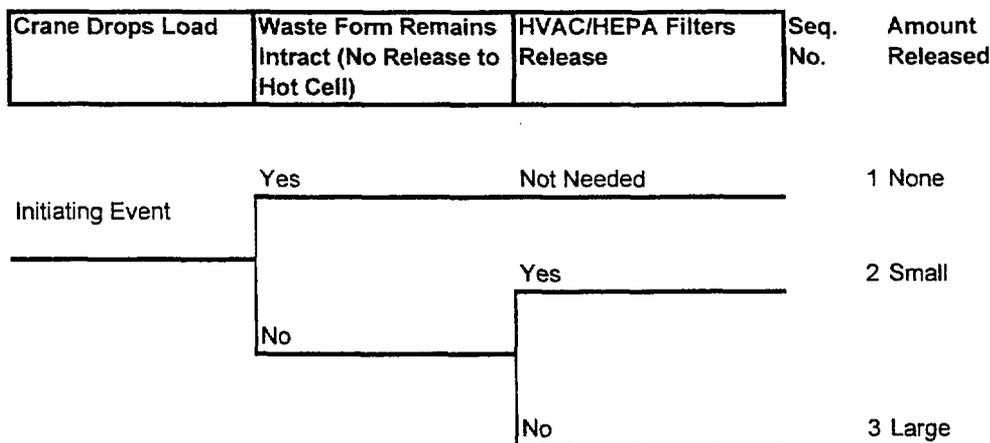


Figure 7-20A. Baseline Event Tree Without CCFs

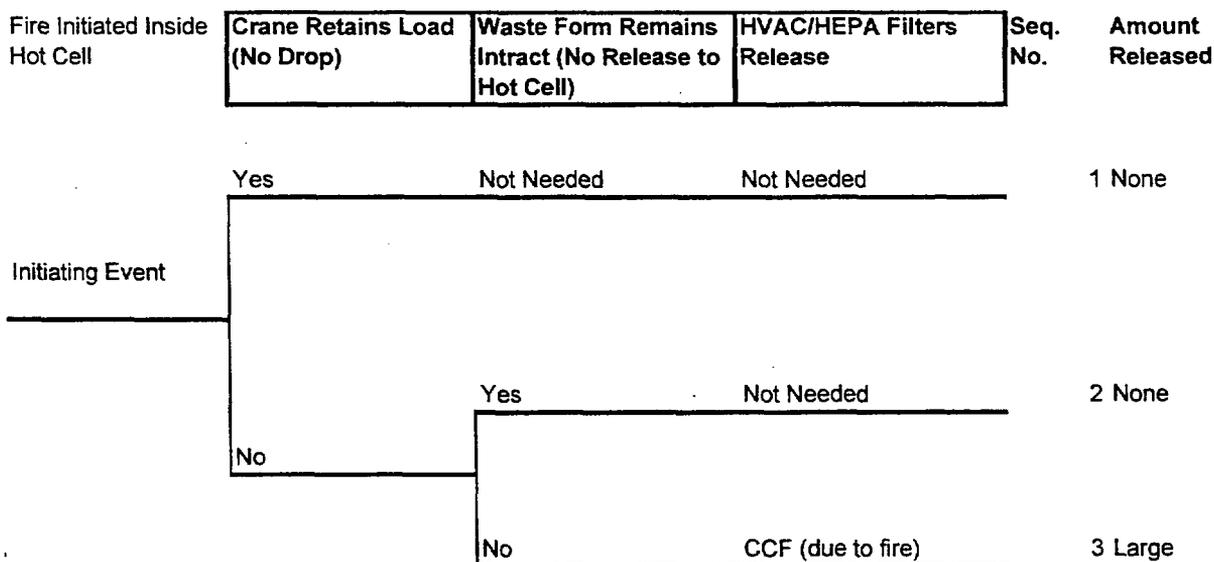


Figure 7-20B. Event Tree with Fire-Initiated Common-Cause Failure of a Heating, Ventilation, and Air-Conditioning, and High-Efficiency Particulate Air Filter System

dependent failures after a common-cause initiator (i.e., an earthquake that exceeds the seismic design criteria of the SSC).

An initial model of a seismic ET for a fuel handling facility, for example, could include headings that represent all of the undesirable interactions and consequences that might occur as a result of an earthquake of any unspecified magnitude. The IE would be labeled “strong earthquake occurs at site.” Consequently, potentially dependent events that could be included as ET headings

include crane drops transport cask, manipulator drops fuel assembly, crane falls onto spent fuel racks, hot cell walls are breached, hot cell walls collapse, or HVAC/HEPA filter fails to function. An ET would be used to display the possible event sequences that might occur unless design features prevent some or all sequences from being credible. The seismic ET can be used for qualitative analyses or applied further in deterministic or probabilistic evaluations (see Section 10.1).

In a deterministic analysis, the seismic ET would be modified to account for success criteria and design features that withstand design-basis earthquakes up to a given magnitude. Two design basis earthquakes have been defined for a repository: the Frequency Category 1 (FC-1) earthquake (1×10^{-3} per year with a magnitude to be specified) and a Frequency Category 2 (FC-2) earthquake (1×10^{-4} per year with magnitude greater than that of FC-1).

Two new ETs are created by modifying the initial tree. One tree (the FC-2 ET) would define the IE as “earthquake of magnitude greater than FC-1 but less than FC-2 occurs.” The other tree would label the IE as “earthquake less than FC-1 occurs.”

All of the event headings that represent an SSC that is designed to withstand the FC-2 earthquake without a loss of a safety function would have branches representing the independent failure of the SSC in a deterministic application of the FC-2 ET. By contrast, all of the event headings that represent an SSC that is designed to withstand only the FC-1 earthquake would not have branching nodes, thus representing guaranteed failure. The ET thus eliminates many of the possible sequences from the initial ET.

All of the event headings that represent an SSC that is designed to withstand the FC-2 earthquake without loss of safety function would be considered to be a guaranteed success with respect to the seismically induced failures in a deterministic application of the FC-1 earthquake ET. In this ET, however, all of the event headings that represent an SSC that is designed to withstand either the FC-1 earthquake or those designed for the FC-2 earthquake would have branching nodes representing potential independent failures. Any SSC not designed to withstand at least the FC-1 earthquake is assumed to be a guaranteed failure without any branching nodes.

Finally, a third ET is created that has the IE titled “earthquake exceeding design basis occurs at site.” All of the possible seismic-induced failures of SSCs would be treated as guaranteed dependent failures in a deterministic application. The number of event sequences would be significantly reduced, perhaps collapsing the tree to one sequence: a severe earthquake occurs and all SSCs fail dependently.

Section 10.1 also describes the application of seismic ETs with CCFs in probabilistic analyses such as seismic PRA or seismic margins analysis.

7.4.4.2 Use of Software

Dependent events and CCFs are readily handled in both ETs and FTs with computer programs such as SAPHIRE. A Microsoft Excel spreadsheet can be used to draw ETs that include dependent events and can be used to quantify event sequences. The ETs and CCFs of basic events can be handled with an FT computer program such as CAFTA.

7.4.4.3 Implicit (or Parametric) Modeling and Quantification of Common-Cause Failure

A CCF analysis can be applied to systems containing several levels of redundancy and diversity, including systems having various success criteria (e.g., 1 out of 2, 2 out of 3, and so on).

The simplest example for introducing CCF analyses is illustrated in Figure 7-21A. This figure presents a reliability block diagram for a system having two-fold redundancy. The success criterion is one out of two: if either component A or B is available, the system safety function is achieved. Figure 7-21B illustrates the FT logic model for the system assuming that all failures of A and B are independent. The top event (failure of safety function) will occur when A and B fail, as represented by the AND gate. The probability of the top event is given as:

$$P_S = P_A * P_B \quad (\text{Eq. 7-32})$$

If $P_A = P_B = 0.01$ (Eq. 7-33)

then $P_S = 0.01 * 0.01 = 0.0001$ (Eq. 7-33)

The potential for CCF is introduced into the reliability block diagram by inserting a pseudo-component that is in series with the representations of the physical components (or systems), A and B, as shown in Figure 7-22A. The pseudo component is labeled CCF_{AB} . Figure 7-22B illustrates the FT logic model for the system in the reliability block diagram. The top event (failure of safety function) will occur when A and B fail independently OR if they fail by a CCF. The top event is resolved into an OR gate having event CCF_{AB} as one input and the event titled "independent failures of A and B" as the other input. The probability of the top event is given as:

$$P_S = P_{A,I} * P_{B,I} + P_{CCF} \quad (\text{Eq. 7-35})$$

where $P_{A,I}$ and $P_{B,I}$ are the probabilities of independent failures of A and B, respectively.

The expression in Equation 7-35 is valid for any appropriate values of the parameters $P_{A,I}$, $P_{B,I}$, and P_{CCF} . A determination of the value of P_{CCF} is required, but not easily achieved.

The beta-factor method is applied here to quantify the probability of the top event to illustrate the basic approach that is recommended for the PSA.

7.4.4.3.1 Beta Factor Approach

The beta factor method assumes that a fraction β of the reported failures of components is due to CCFs with the remainder due to independent failures.

If

$$P_A = P_B = P_{Tot} \quad (\text{Eq. 7-36})$$

where p_{Tot} is the total failure probability of either component A or B, taken alone, then the probability of both components failing due to CCF is defined as

$$p_{CCF} = \beta * p_{Tot} \quad (\text{Eq. 7-37})$$

and the probability of independent failure is

$$p_{A,I} = p_{B,I} = (1 - \beta) * p_{Tot} \quad (\text{Eq. 7-38})$$

A typical value (e.g., a rule of thumb often used in screening analyses) is to assume $\beta = 0.1$. Using this value in the example gives the following equations:

$$p_{CCF} = \beta * p_{Tot} = 0.1 * 0.01 = 0.001$$

$$p_{A,I} = p_{B,I} = (1 - \beta) * p_{Tot} = (1 - 0.1) * 0.01 = 0.9 * 0.01 = 0.009$$

$$p_S = p_{A,I} * p_{B,I} + p_{CCF} = 0.009 * 0.009 + 0.001 = 0.000081 + 0.001$$

The contribution from the CCFs dominates the system failure probability. This is a typical result from the beta factor approach when β is 0.1 or higher. For the two-fold redundancy case, it may be shown that CCFs dominate the system failure probability until $\beta \approx p_{Tot}$. In this example, if $\beta \rightarrow 0.01$, then the factor $\beta p_{Tot} \approx 0.0001$ and is approximately equal to the term $p_{A,I} * p_{B,I}$ for the probability of independent failures. In other cases, if the independent component $p_{A,I} = p_{B,I} = 0.001$, then a $\beta = 0.01$ would dominate the system failure probability. It should be noted that the beta factor method gives essentially the same numerical result for any redundancy of two or higher. More complex, multi-parameter models may be used, as described in Section 7.4.4.3.7.

The beta factor method is perhaps the most useful technique for including CCFs in the PSA, especially for the LA submittal for CA, when complete design detail is not yet available. Moreover, the beta factor is suitable when only two-fold redundancy is used. The value chosen for beta may be less than, or more than, the generic beta of 0.1. The analyst must determine whether design, operational controls, and environmental controls affect the susceptibility and opportunity for CCFs and justify an appropriate beta factor or factors.

7.4.4.3.2 Using the Beta Factor with Component Failure Rate and Event Frequencies

The development of the methodology in Sections 7.4.3 and 7.4.3.1 used the probability of a system or component failure as the parameter of interest. The same development can be based on a failure rate using the beta factor. The original development of the beta factor was based on component failure rates because experience data (from which beta is derived) are expressed in terms of failure rate (either in units of time or per demand).

These results demonstrate that even a small contribution from CCFs can seriously degrade the reliability of a safety system. Designer and safety analysts must be cautioned against overconfidence and complacency when redundancy or single-failure proof designs are specified. The CCFs associated with these designs must be controlled.

Experience data are expressed in one of the following forms:

Demand Based—K failures are observed in N challenges (demands) on components in records or test data. In this basis, data analysis would estimate the failure rate (or probability per demand). The failure rate, also termed the component unavailability, is calculated as:

$$q = K/N \text{ failures per demand} \quad (\text{Eq. 7-39})$$

CCF Contribution, Beta Factor Estimation:

The analysts examine the database(s) to identify what fraction of all recorded failures can be attributed to CCFs. It is determined that a portion k_{CCF} of the K failures are attributed to CCFs. This defines the beta factor as:

$$\beta_q = k_{CCF}/K \quad (\text{Eq. 7-40})$$

So that
$$q_I = (1 - \beta_q) q \quad (\text{Eq. 7-41})$$

$$Q_{CCF} = \beta_q q \quad (\text{Eq. 7-42})$$

where

q_I = probability of independent failures, per demand

Q_{CCF} = Probability of CCF failure, per demand

In the demand-based case, q is a probability; therefore, the development in Sections 7.4.3 and 7.4.3.1 apply directly.

CCF Contribution, Beta Factor Estimation:

The analysts examine the database(s) to identify the fraction of all recorded failures that can be attributed to CCFs. It is determined that a portion m_{CCF} of the M failures are attributed to CCFs. This defines beta as:

$$\beta_\lambda = m_{CCF}/M \quad (\text{Eq. 7-44})$$

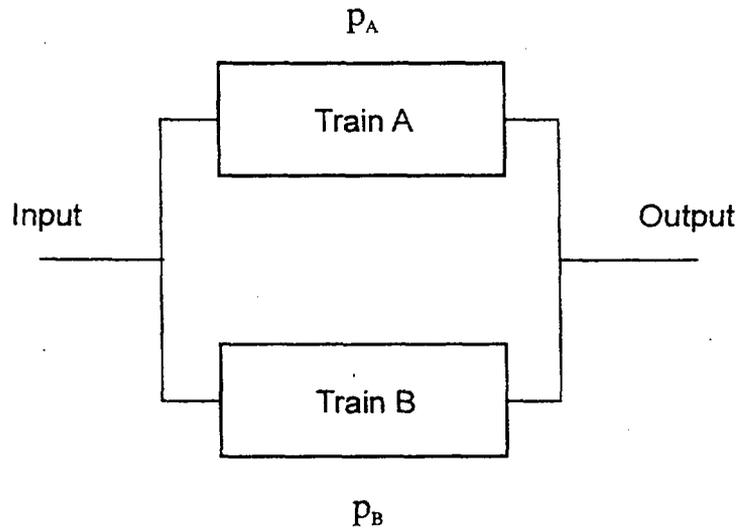
The failure rate for independent failures becomes:

$$\lambda_I = (1 - \beta_\lambda) \lambda \quad (\text{Eq. 7-45})$$

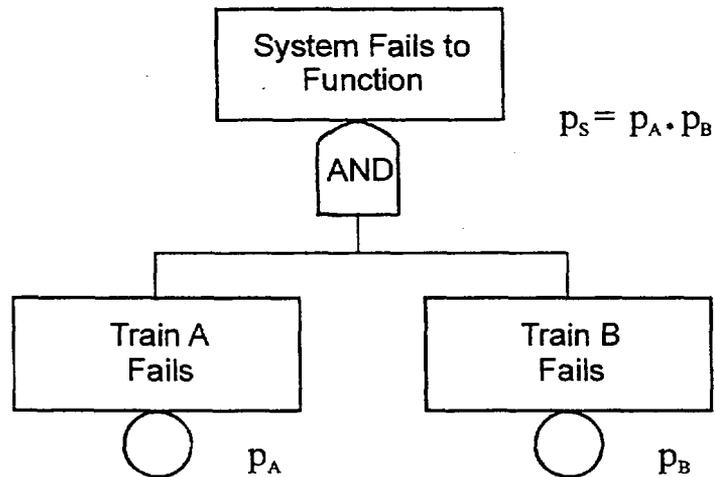
and the expression for the failure rate for CCFs is:

$$\lambda_{CCF} = \beta_\lambda \lambda \quad (\text{Eq. 7-46})$$

A. Reliability Block Diagram of Redundant System



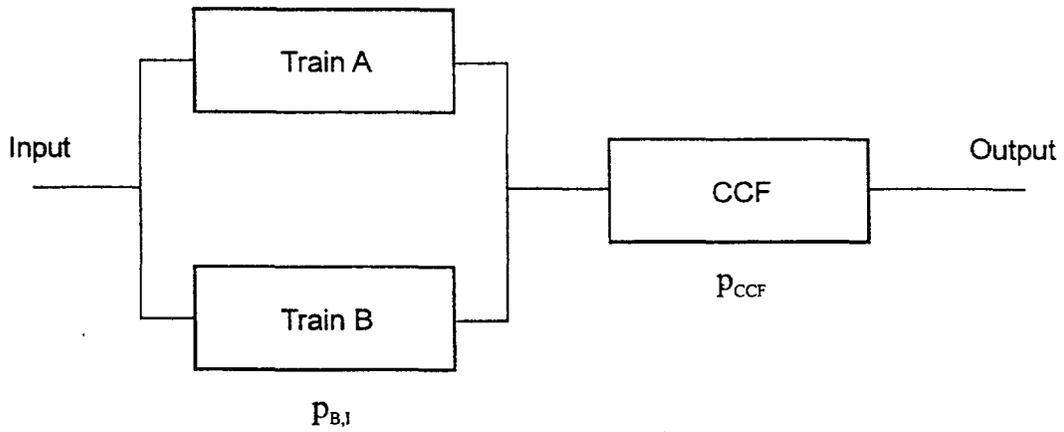
B. Fault Tree Logic Model of Redundant System



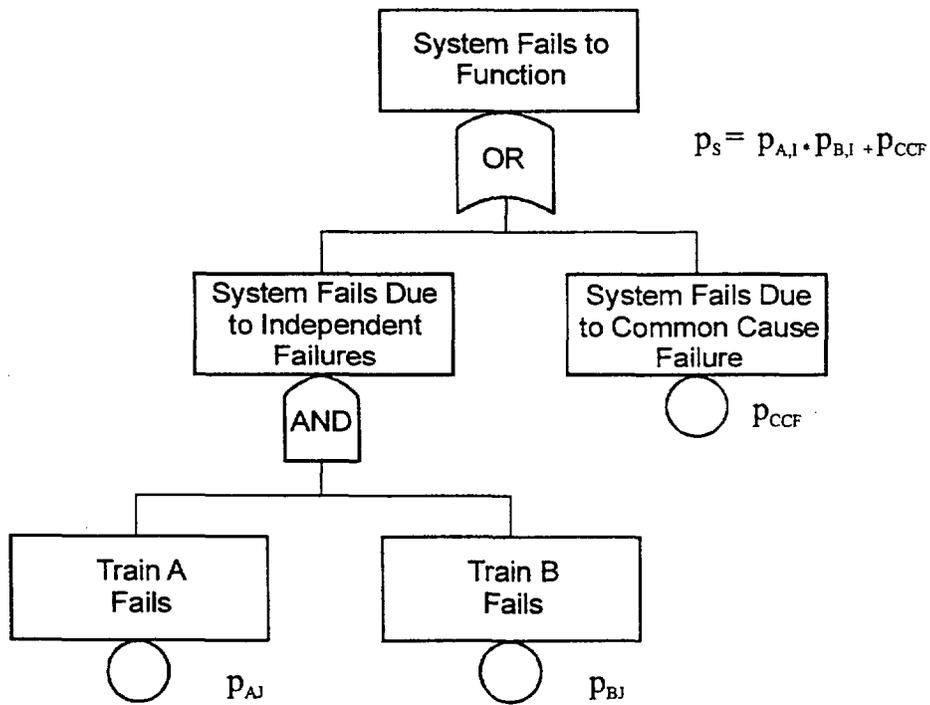
7.4-3.CDR.PSA GUIDE/2-5-02

Figure 7-21. Illustration of Logic Models for Independent Failures

A. Reliability Block Diagram of Redundant System with Pseudo Series Element CCF



B. Fault Tree Logic Model with CCF of Redundant System



7.4-4.CDR.PSA GUIDE/2-5-02

Figure 7-22. Illustration of Logic Models for Common Cause Failures

The unavailability of a component or system in the exponential reliability model is expressed as:

$$P_F = 1 - \exp(-\lambda t_M) \quad (\text{Eq. 7-47})$$

Here t_M is the mission time and P_F is the probability that that the component or system will not perform its safety function for at least a time t_M when it is needed. The expression for P_F is usually approximated as

$$P_F \approx \lambda t_M \quad (\text{Eq. 7-48})$$

and P_F is the probability of failure for all causes (i.e., the total of independent and common cause failures) for the mission time, t_M .

The independent failure and CCF contributions to the component or system unavailability can be separated using Equations 7-45 and 7-46.

The probability of independent failure is

$$P_{F_I} \approx \lambda_I t_M \approx (1 - \beta_\lambda) \lambda t_M \approx (1 - \beta_\lambda) P_F \quad (\text{Eq. 7-49})$$

and the probability of CCF is:

$$P_{F_{CCF}} \approx \lambda_{CCF} * t_M \approx \beta_\lambda t_M \approx \beta_\lambda * P_F \quad (\text{Eq. 7-50})$$

Rate Based— M failures are observed in exposure (operational or test) time T for components in records or test data. In this basis, data analysis would estimate the failure rate (in units of numbers of failures per unit time, also termed the component failure frequency) as:

$$\lambda = M/T \text{ failures per hour} \quad (\text{Eq. 7-43})$$

7.4.4.3.3 Other Methods for Common-Cause Failure quantification

When diversity is also present in addition to redundancy and in cases where three-fold or higher redundancy is used, other methods such as the Multiple Greek Letter or the alpha factor should be used. If the need arises, the analyst should consult a source such as NUREG/CR-4780 for instructions.

7.4.5 Steps in Performing Dependent Failure Analysis for a Repository

The following steps are presented to guide the analyst. The steps are based on those presented in NUREG/CR-4780 (Mosleh et al. 1988) but are less detailed since some of the steps are not relevant to the preclosure safety of a repository. The first two steps are general systems analysis tasks that are performed in conjunction with ET and FT analyses.

7.4.5.1 Step 1—System Logic Model Development

System Familiarization—The specific system or operation of a repository is examined for preclosure safety issues. The analyst becomes familiar with the design, environment, and

operational characteristics of the system. This step is a common starting point and common activity for the entire PSA. For dependent failure analysis, attention must be given to the following points:

- The results of external and internal event hazards analyses are used to develop event sequence descriptions (e.g., using ET logic models) and FT logic models of SSCs that are relied upon for prevention or mitigation of particular sequences of events.
- The analyst must understand the intended function of each front-line SSC, what it is composed of (i.e., construction, kinds of components), what kinds of procedures will govern its operation, and its requirements for T&M.
- The analyst must also understand which support systems are required for proper functioning of each frontline SSC (i.e., does it require electrical power, cooling water or air, temperature or humidity control?).
- The analyst should consider the location of each SSC in relation to other operations that may pose hazards of spatial interaction.

Problem Definition—In this step, the analyst translates information from the familiarization step into specific considerations and constraints that will influence the logic model development. Particular points to be considered include:

- Specific success (performance) criteria that are defined for each SSC that prevents or mitigates an undesired sequence
- Boundaries of the specific system being considered (i.e., what it includes and what it does not)
- Dependencies between frontline (primary) system and support systems or functions (for complex systems, a support matrix may be constructed to define direct and indirect dependencies between primary, secondary, and tertiary systems and components or HAs)
- Ground rules imposed on the analyses to focus on the problems of interest (e.g., coarse modeling and conservative rules might be applied to preliminary analyses, and then more detailed modeling and more realistic rules might be applied in later analyses)
- Identify those root causes of dependent failures that will be explicitly modeled (e.g., earthquakes, fires, T&M, human errors).

The last point is important; in later modeling of implicit (parametric) dependencies care must be taken to not introduce double counting.

Logic Model Development—Explicit dependencies are incorporated into ET or FT logic models. Implicit (or parametric) dependencies are treated in FT models that permit the analyst to relate (decompose) a system state (such as HVAC/HEPA filter system is unavailable) to lower,

component level states. The dependent failure events are then treated as one cause of component failure alongside independent component failure events.

7.4.5.2 Step 2—Identification and Screening of Common-Cause Failure Component Groups

The objectives of this step include qualitative and quantitative screening to:

- Identify the groups (or types) of components to be included in, or excluded from, the CCF analysis
- Prioritize the groups to allocate resources and time
- Provide engineering arguments to aid data analysis
- Provide engineering insights for later formulation of CCF defense alternatives

Qualitative Analysis—The analyst searches for common attributes and mechanisms of failure that can lead to common cause events. This step relies on past experience and an understanding of system and component behavior in the intended operational environment for signs of potential dependence among redundant components as well as consideration of defenses that may be included in the design. If necessary, a root-cause analysis is performed to substantiate and improve the initial identification of potential CCFs.

Quantitative Screening—This step is applied in the CCF analysis of complex systems to identify dominant contributors to system unavailability or event sequence frequencies. In this step, conservative values are assigned to each basic event in the system FT for both independent and CCF modes. If several potential CCFs are associated with a given system, this step will help to identify the dominant contributors and to prioritize further analyses.

7.4.5.3 Step 3—Common Cause Modeling and Data Analysis

A CCF model that best fits the situation being modeled is then selected. NUREG/CR-4780 (Mosleh et al. 1988) several methods are presented. For most repository analyses that involve two-fold redundancy, the beta-factor method is the recommended approach. However, the appropriate beta factor must be applied.

The analysis of appropriate CCF factors is similar to the general problem of parameter estimation and selection, as discussed in Section 7.4. If information sources are available for systems or components similar to those of a repository and are located in an environment similar to a repository application, the analyst should attempt to extract CCF factors. Otherwise a generic beta factor should be used. Although a beta factor of 0.1 is a good value for use in preliminary analyses of high quality components, the analyst should consider whether a smaller or larger value is more suitable for the quality of component, the environment, and the degree of uncertainty in the root causes and coupling mechanisms for the CCFs.

Table 7-5 (based on Table 3-7 of NUREG/CR-4780 [Mosleh et al. 1988]) lists generic beta factors for several components used in nuclear reactor plants. The generic factor ranges from

0.03 for various pumps to 0.22 for various safety and relief valves. The average value is 0.1 for all components.

7.4.5.4 Step 4—System Quantification, Sensitivity Analysis, and Interpretation of Results

After all of the CCF elements in the system logic model have been assigned appropriate CCF parameters (e.g., an appropriate beta factor) and parameters have been assigned to all independent failure modes and explicit dependencies (such as human error probabilities or T&M unavailability), the probability of system failure is quantified (e.g., using the SAPHIRE code). This step identifies the key contributors to system unavailability. These contributors are expected to be one or more CCF events. The initial results may point to potential recovery actions that can reduce the impact of the CCFs and identify defenses against the CCFs.

At this stage, it may be desirable to perform a sensitivity analysis by varying the beta factors in the various CCF elements to gain insight into the significance of uncertainty in the CCF parameters.

The analyst should also perform a review of the results at this point to determine if the system unavailability factor appears to be extraordinarily small or large.

7.4.5.5 Step 5—Reporting/Documentation

Although the dependent failure/CCF analysis is an integral part of the event sequence analyses, it is important that the analyst clearly document this portion of the analyses with respect to assumptions, modeling approximations, and parameter selection.

NUREG/CR-4780 (Mosleh et al. 1988, Section 3) presents a detailed explanation of the activities in Steps 1–5.

7.4.6 Examples of Application

An example application of a CCF analysis was developed to examine the likelihood of having an uncontrolled descent of a waste-package transporter train during travel to the subsurface. An FT analysis was performed to examine the reliability of the brake system(s) of the WP transporter train. The most recent analysis is reported in *Subsurface Transporter Safety Systems Analysis* (CRWMS M&O 2000) based on FT models developed in *Application of Logic Diagrams and Common-Cause Failures to Design Basis Events* (CRWMS M&O 1997). The logic model made extensive use of CCF modeling.

The train was theoretically comprised of two locomotives and a shielded waste-package transporter car. Each vehicle had air-actuated tread brakes and hydraulic actuated disk brakes. Each of the vehicles had elements of redundancy within each of the respective brake systems. The actuation of the transporter brakes was controlled by the counterpart brake system on the primary locomotive. Thus, one mode of failure of transporter brakes was dependent on failure of the locomotive brake actuation system. This dependency was modeled explicitly in the FT analysis. Actuation of the brakes, however, could be initiated from either locomotive or from a central control room.

The beta factor method in this analysis was used at three levels: intra-vehicle (i.e., among redundant components on either of two locomotives or the transporter), inter-locomotive (i.e., among redundant and like components on both locomotives), and inter-vehicle (among redundant and like components on both locomotives and the transporter car).

The standard generic beta factor of 0.1 was used for the intra-vehicle level. This beta factor was applied to mechanical and electronic components in redundant configurations. Thus, the two channels of brake actuation signals were modeled as two paths of independent failures in series with one path of CCF. Redundant air-brake system components were modeled similarly.

Table 7-5. Generic Beta Factors

Component	Generic Beta Factor ^a
Reactor Trip Breakers	0.19
Diesel Generators	0.05
Motor Operated Valves	0.08
Safety or Relief Valves	
Pressurized Water Reactor	0.07
Boiling Water Reactor	0.22
Check Valves	0.06
Pumps	
Safety Injection	0.17
Residual Heat Removal	0.11
Containment Spray	0.05
Auxiliary Feedwater	0.03
Service Water	0.03
Chillers	0.11
Fans	0.13
All ^b	0.10 ^b

Source: Modified from NUREG/CR-4780 (Mosleh et al. 1988)

NOTES: ^a Based on classification of 3000 events from experience data. Dependent failure types were classified. Generic common cause events included potential as well as actual events. See Table 3-7 and the explanation in NUREG/CR-4780 (Mosleh et al. 1988, Section 3).

^b Average of all component beta factors.

A second level of CCF was introduced using a beta factor of 0.01 (using the argument that the probability is less likely than the intra-vehicle situation) to allow for the possibility that there may be mechanisms for CCF among components on the two locomotives (e.g., root causes of common erroneous maintenance, calibration, and installation). Similarly, a third level beta factor of 0.001 was used to allow for CCFs among components on all three vehicles. By using three beta factors that differ by orders of magnitude, the issue of double counting of some of the failure modes is less important.

The analysis indicated, as expected, that use of diverse and redundant brake systems on multiple vehicles reduce the probability of failure by independent failures or intra-vehicle CCFs. The assumed inter-vehicle CCFs are seen to be potentially significant contributors (even when a beta factor of 0.001 was used). The insights gained from such analyses indicate that programmatic controls should be put into place to eliminate or reduce the likelihood of such CCFs. The

numerical results must not be taken too literally or used to infer that brake systems cannot be made sufficiently reliable.

INTENTIONALLY LEFT BLANK

7.5 TECHNICAL INFORMATION

7.5.1 Introduction

This section defines the bases and methods for gathering and quantifying technical information that is used in the quantification of FTs and ETs. The technical information needs for ET and FT quantification consist generally of IE frequencies, failure rates and probabilities, CCF parameters, HEP, mission times, repair times, inspection intervals, and demand rates. This section also describes the methods for quantifying the uncertainty factors in the parameters based on concepts described in Section 9. Because of the precise use of the term "data" on the Yucca Mountain Project, this section uses the term "technical information" for the sources of information described.

This section will concentrate on the bases and methods for gathering and quantifying failure rates and probabilities for hardware and software along with associated mission times, repair times, inspection intervals, and demand rates. Information for common-cause and dependent failures, and for HEP, are presented in Sections 7.3 and 7.4, respectively.

This section also includes methods for combining various sources of generic databases and for combining generic databases with repository-specific information. The bases for estimating uncertainty factors in parameters are described, as well as reference to the concepts presented in Section 9.

7.5.2 Overview of Approach

Other sections of this guide present methods for modeling and analyzing ETs, FTs, CCFs, and human errors. All of those models require numerical quantities of various types of inputs. Most of these parameters will be used to quantify the probabilities of basic events in FT models or the probabilities of event headings in ETs. Another application of the information is for use in quantifying the frequency of IEs (i.e., the frequency is expressed as probability per unit time). The fundamental parameters, however, are in the form of failure rates (i.e., number of failures per unit time) and failure probability on demand (e.g., number of failures per number of trials). Other parameters include T&M intervals. This section describes the techniques for producing the parameters and sources of information upon which to base the parameters.

This section will follow the presentation in Section 5 of the *PRA Procedures Guide* (NRC 1983) for the following elements:

- Selection and Use of Event Models
- Information (Data) Gathering
- Estimation of Model Parameters
- Uncertainties in Information and Event Probabilities
- Documentation

The *PRA Procedures Guide* (NRC 1983, Section 5.6.2) also provides a brief discussion of the evaluation of dependent failures and the estimation of parameters for a shock model for the treatment of dependent failures. This material is not applied as a recommended model in this

PSA guide. The methods for identifying and modeling dependent failures are described in Section 7.4. For example, the principal approach for CCF analysis in the PSA is the beta-factor method described in Section 7. For initial scoping analyses, a beta factor of 0.1 is often used. For more refined analyses, however, the beta factor should reflect generic information on similar components in operating conditions similar to a repository. The evaluation of the parameters and the uncertainty for modeling dependent failures is essentially the same as that described in this section for treating failure-on-demand and constant failure rate information.

The Selection and Use of Event Models refers to the mathematical expression used to quantify a specific failure probability, the unavailability of SSC, or the frequency of an initiator. In many cases, the mathematical expression will be time-based to express the probability that a given failure will occur within some mission time or the probability that a particular SSC will be unavailable because it is out of service for T&M or inspection. Each of these time-based situations has a rigorous mathematical formula for calculating the desired probability. Furthermore, each of the rigorous expressions is often approximated by simpler mathematical expressions.

For example, the exponential formula is used to calculate the probability that a component will not be available for a mission time, T , when the failure rate, λ , is constant in time. The probability is expressed as $q = 1 - \exp(-\lambda * T)$. When λ , T , or both are small, the expression is approximated as $q \approx \lambda * T$. The exponential and other models are described in Section 7.5.3.

Information (Data) Gathering involves the selection and acquisition of generic databases, generic event data, and repository-specific event data, when available. Because a repository is a first-of-kind and will not have any operational experience prior to licensing, repository-specific data will not be available. Therefore, the PSA must rely heavily on generic information, principally information from generic databases developed for PRAs, but also from experience data for equipment and systems similar to those that will be used in a repository. However, for some parameters, site-related information such as the frequency of natural phenomena, nearby hazardous activities, and historical information is available for components used in the Exploratory Studies Facility (ESF) (e.g., ground support).

Estimation of Model Parameters is the process of assigning a value to each of the parameters. If generic databases are used, the parameters of interest are already in the proper form (e.g., a failure rate and its uncertainty). Therefore, the estimation may involve adjustment factors to alter the generic failure rate to account for repository-specific conditions (such as operational environments or quality assurance program). In some cases, there may be several pieces of generic information (and their uncertainty ranges) that are combined in specified ways to arrive at the best values for repository application.

Otherwise, the parameters have to be derived from event data. The number of observed failures must be divided by the number of trials or the length of exposure time. The associated uncertainty factors are also derived.

The Bayesian approach is the generally accepted method for parameter estimation in PRAs. It is based on subjective probabilities applied with empirical information. In many reliability analyses, however, the classical or Frequentist approach is used. When enough information is

available, the two approaches give essentially the same numerical results. The Bayesian approach has some advantages, however, when less information is available (e.g., when the number of observed failure events is zero).

Uncertainties in Information and Parameters are the sources of uncertainty that are accounted for, and propagated in, the event sequence quantification (as described in Section 9). The uncertainty derives from issues such as the amount of information (e.g., number of trials), variability between sources (e.g., the failure rate for similar components vary significantly between two or more compilations), and the potential inaccuracies in the reported values. The uncertainty distributions (i.e., probability density functions PDFs) ascribed to basic parameters such as failure rates and repair times are propagated throughout the event models, resulting in PDFs for the event probabilities that are input to the ET and FT analyses.

The following sections provide the details of each of the five elements.

7.5.3 Details of Approach

This section provides the essential methods and sources that are expected to be applied in the PSA. It is not intended to be exhaustive. In some cases, the analyst may find a need for alternative approaches that can be found in PRA and reliability literature.

7.5.3.1 Selection and Use of Event Models

Section 7.2, FTA, describes the event models most likely to be used in a PSA, but the mathematical formulas are repeated here for clarity. The analyst must determine the appropriate model to apply to a particular basic event. These models are summarized in Table 7-6. PRA or FTA programs, such as SAPHIRE (Russel et al. 1994), include these event models as options for quantifying basic event probabilities.

Except for quantifying IE frequencies, the purpose of an event model is to quantify a probability (that ranges from 0 to 1.0). The probability evaluation may be time-based or demand-based. Component or system faults are characterized as one of the following probabilities:

- Failure on demand – probability of failure per demand
- Standby failure – probability of failure on demand after a given non-operational period, usually given as time-between-inspections
- Operational failure – probability of failing to run or operate (provide required function) during a specified time period (i.e., the mission time)

In addition to the failures of equipment or software due to random causes, failures may be caused by:

- Human errors in T&M that leave the equipment or software in a disabled state
- Human errors during operation that cause a loss of the safety function

Such events are treated probabilistically by methods described in Section 7.3

Table 7-6. Sources of Facility-Specific and Operations-Specific Experience Information

Parameter	Information Requirements	Potential Sources ^a
Probability of failure on demand	Number of failures Number of demands	Repository and ESF inspection and T&M reports Surrogate and generic reports
Standby failure rate	Number of failures Time in standby	Same as above
Operating failure rate	Number of failures Time in operation	Same as above
Repair-time distribution parameters	List of kinds of repairs (principally on-line) of interest to PSA Repair times	Preliminary hazards and event sequence analyses Sources as above
Unavailability due to T&M	List of kinds of T&M of interest to PSA Frequencies and length of T&M	Preliminary hazards and event sequence analyses Sources as above
Recovery	List of kinds of recovery actions of interest to PSA Recovery times	Preliminary hazards and event sequence analyses Sources as above
Human errors	Lists of HAs of interest to PSA Number and categories of errors Number of opportunities Recovery	Preliminary hazards and event sequence analyses Detailed HRA for PSA Sources as above

NOTE: ^a When available, parameters should be estimated from repository, ESF, or other Yucca Mountain specific sources. Otherwise, the best available and applicable surrogate sources should be used. Surrogate sources represent operations, equipment, and environments similar to a repository.

Finally, there may be cases where a system or subsystem is taken out of service for scheduled maintenance. The unavailability may be modeled in the system FTA. The unavailability for this case is a function of a scheduled maintenance interval and the expected time duration for the maintenance.

The symbol used for the probability in discussions, tables, or qualitative FTA is very often a “p.” However, in many cases the symbol “q” is used to connote the probability of failure (per demand), or the probability of unavailability (i.e., the probability of being unavailable when needed or unavailable for the time required).

The value of “q” may be derived directly from demand-based experience data or indirectly from time-based (or rate/frequency) experience data, as described in the following sections.

7.5.3.1.1 Time-Based Event Models

Unless special cases dictate the use of a different model, it will be assumed that all time-based failures are governed by a failure rate that is constant in time. This produces the well-known exponential failure model, which is expressed as

$$q(t) = 1 - \exp(-\lambda t) \quad (\text{Eq. 7-51})$$

where

$q(t)$ is the probability that the component or system will fail within a time, t ; and
 λ is the constant failure rate.

A graph of $q(t)$ is illustrated in Figure 7-23.

The PDF for $q(t)$ is given as

$$f(t)dt = \lambda \exp(-\lambda t) dt \quad (\text{Eq. 7-52})$$

where

$f(t)dt$ is the probability of a component or system failing within a time interval dt about t .

Using the PDF, the mean-time-to-failure is evaluated as

$$\bar{t} = \int_0^{\infty} \lambda t \exp(-\lambda t) dt = 1/\lambda \quad (\text{Eq. 7-53})$$

This is an important relationship that is used in parameter estimation. The mean-time-to-failure is the inverse of the constant failure rate λ in an exponential model.

There is an uncertainty distribution (i.e., a PDF) associated with the parameter λ that will result in an uncertainty distribution for $q(t)$. If the 5th percent lower bound and the 95th percent upper bound are expressed as λ_{LB} and λ_{UB} , the corresponding expressions for the event probability are:

$$q_{LB}(t) = 1 - \exp(-\lambda_{LB} t) \quad (\text{Eq. 7-54})$$

$$q_{UB}(t) = 1 - \exp(-\lambda_{UB} t) \quad (\text{Eq. 7-55})$$

These probabilities are illustrated in Figure 7-23. The methods for quantifying λ_{LB} and λ_{UB} are described in Section 7.5.3.3. Several time-based event models are derived from the exponential failure model (Equation 7-51), as defined in the following section.

Operational Unavailability (No-repair Model)—The unavailability of a component or system in the exponential reliability model without repair is:

$$q(t_M) = 1 - \exp(-\lambda t_M) \quad (\text{Eq. 7-56})$$

where t_M is the mission time. The term $q(t_M)$ is the probability that that the component or system will not perform its safety function for at least a time t_M when it is needed. The longer the mission time, the higher the probability of the failure event modeled in the ET or FT.

Because the failure rate for highly reliable components is usually small, (i.e., such that $\lambda t_M < 0.1$) the expression for $q(t_M)$ can usually be approximated as:

$$q(t_M) \approx \lambda t_M \quad (\text{Eq. 7-57})$$

This event model is applied to the failure-upon-demand of standby components that are not inspected or repaired. It is often applied to failure-to-run of a normally operating system or to a standby system after successful starts-upon-demand.

Standby Unavailability (With-Repair or Renewal, Unannunciated)—This unavailability applies to a system or component that is on standby, but whose condition is not known between periodic inspections or tests (i.e., failures are unannunciated). If a system is found to be failed or not performing to specification, the system or component is repaired. It is assumed that after repair, the component or system becomes good-as-new with a failure rate of λ_s , and the failure probability between inspections/tests follows the exponential function. This function is presented in Equation 7-51 (in Equation 7-51, λ is replaced by the standby failure rate of λ_s).

The average unavailability of a system that is on standby but is periodically inspected, tested, and repaired, is given by:

$$q(\tau) \approx \lambda_s \tau/2 \tag{Eq. 7-58}$$

Here τ is the inspection or test interval.

Figure 7-24 illustrates the time behavior of the exponential function between inspection intervals of varying length (calculated with Equation 7-56) and the corresponding average unavailability (calculated with Equation 7-58). The figure illustrates how the average unavailability increases with the inspection or test interval. In addition, the maximum failure probability can be significantly higher than the average unavailability and occurs just before the inspection or test.

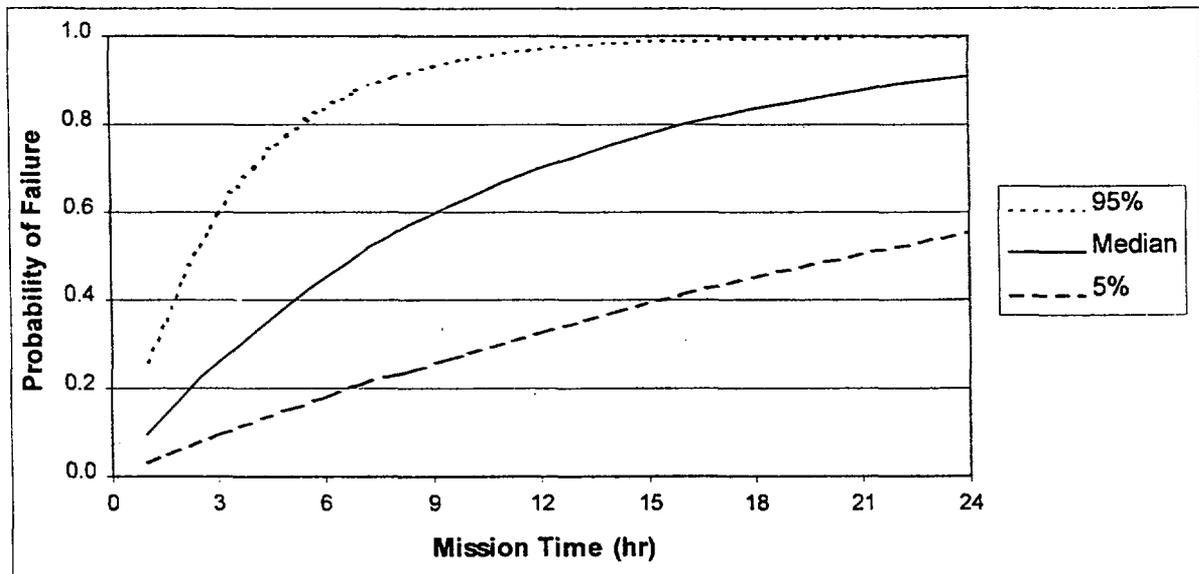


Figure 7-23. Exponential Probability of Failure

Standby Unavailability (With-Repair or Renewal, Annuciated)—This unavailability applies to a system or component that is on standby, but whose condition is known continuously due to instrumentation or some performance characteristic that indicates when the item is unavailable. The event model becomes that of the operational unavailability. Here it is assumed that repair or restoration begins immediately and that normal operations continue without having the item available.

The average unavailability of a system that is on standby but is periodically inspected, tested, and repaired, is given by:

$$q(\tau) \approx \lambda T / (1 + \lambda T) \tag{Eq. 7-59}$$

Here T is the average total time to respond to the failure indication, repair, and return the item to service.

As above, if λT is small compared to unity, the expression is approximated as:

$$q(\tau) \approx \lambda T \tag{Eq. 7-60}$$

Recovery within Required Time—This case represents an event that is represented in a logic model as an intersection (AND logic) with a primary failure (unavailability) event. It may be applied to failures during mission time, to failures to start-and-run on demand, and to IEs such as loss-of-primary power source.

In many instances, the exponential function (Equation 7-51) is applied as an exponential repair model, given as:

$$p_R(t_C) = 1 - \exp(-t_C/\tau_R) \tag{Eq. 7-61}$$

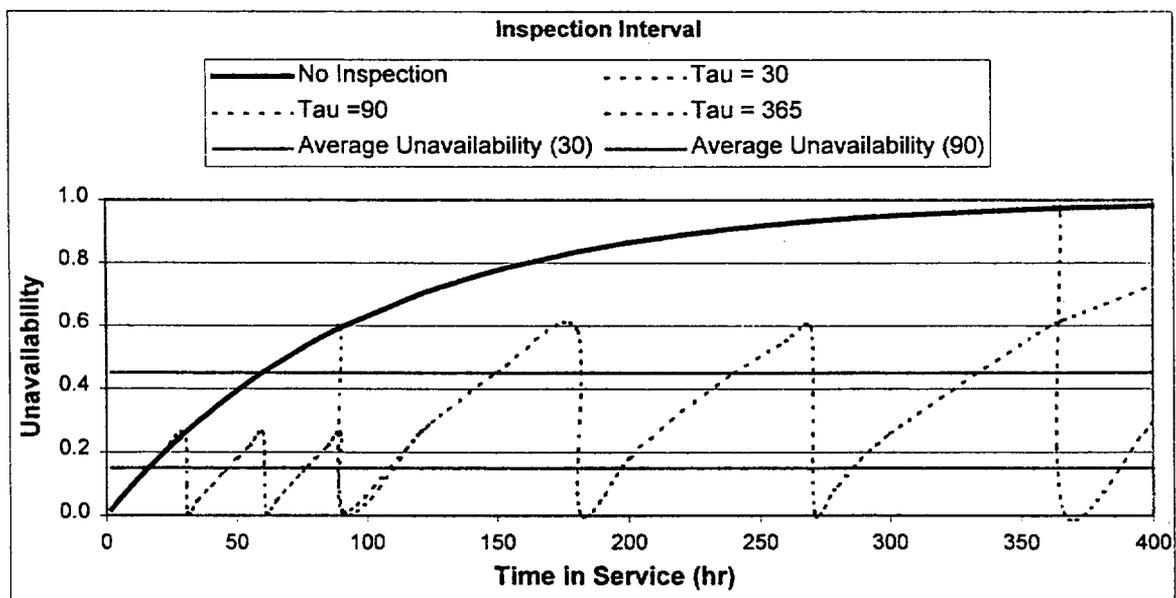


Figure 7-24. Unavailability with Inspection and Test

where

τ_R is the mean-time-to-restore

$p_R(t)$ is the probability that the unavailable item is recovered (returned to functionality) within a required time t_C .

Figure 7-25 illustrates the behavior of this function for a range of τ_R . It is observed that the probability of successful restoration for a given required time, t_C , is closer to 1.0 for small values of τ_R . In quantifying an event for an ET or FT application, a value of t_C is specified, based on safety functional requirements. If t_C were 1.0 hours, the probability of success would be 0.982 for a mean-time-to-restore τ_R of 0.25 hours, but only 0.632 for τ_R of 1.0 hours.

This failure probability is applied in the event sequence modeling. For the examples cited previously, where t_C is 1.0 hours, the probability of failure is small (0.018 [1-0.982]) for a mean-time-to-restore τ_R of 0.25 hours, but 0.3680 for τ_R of 1.0 hours.

The joint probability of having the item unavailable to provide its safety function is the product of the primary failure probability and the probability of non-recovery in the required time. If the primary failure probability is $q_P = 0.01$ and τ_R is 0.25 hours, then the joint probability is calculated as:

$$q = q_P * p_R(t_C) = 0.01 * 0.018 = 0.00018$$

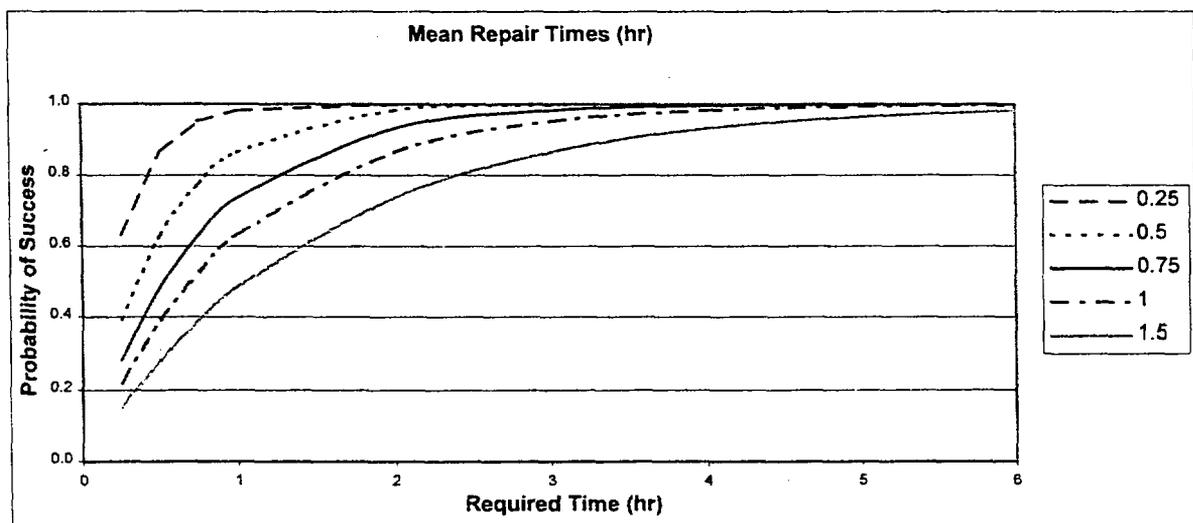


Figure 7-25. Probability of Restoration – Exponential Repair Model

Estimates of the mean-time-to-restore, τ_R , are developed for each situation, where required. This parameter is also subject to uncertainty analysis. The LN distribution has been shown to be a good representation of the repair and restoration times.

7.5.3.1.1.1 Specifying Mission Times and Allowable Recovery Time

The analyst must specify a mission time when the non-repairable time-based model is used. The specification must be defensible to the NRC as being adequate for a specific safety function. The specified mission time may be based on an engineering analysis or dictated by a regulatory requirement or precedent. However, the mission time may be somewhat arbitrary as long as the performance is shown to meet 10 CFR Part 63 requirements. For example, requiring that the Waste-Handling Building HVAC/HEPA filter system (for the inner-most zone) must function for at least 24 hours following a release of radioactivity from a breached waste form may be based, initially, on the qualitative argument that most of the important filtration will have occurred. Should offsite doses indicate that a longer operational period is required, however, the mission time would have to be extended.

The analyst must provide similar justification for allowable recovery times for repairable systems. The logic is similar to the specification of a mission time, but asks the complementary question of "how long can we be without this safety function before the 10 CFR Part 63 performance criteria cannot be met?" Using the example of the HVAC/HEPA filter system, it may be allowable for components of the secondary or tertiary zones to be out of service for many hours without compromising the negative pressure that ensures that airflow is inward toward the primary zone. The allowable time would set the limit on the recovery time in the repairable event model.

7.5.3.1.1.2 Specifying Time between Tests or Inspections

The probability of a failure-on-demand of standby SSCs is assumed to increase between inspections or tests, at which time they are restored to good-as-new. The probability of failure on demand must be low enough to ensure that a repository can meet the risk-informed performance requirements. It may be required to specify a shorter inspection interval or developing a more reliable standby system having a lower standby failure rate. This activity may be iterative.

The analyst may initially specify a reasonable typical interval such as one year, three months, one month, or a week, depending on how important it is to ensure the availability of a given system or component. If the risk-informed performance is demonstrated to meet the requirements of 10 CFR Part 63, then the specified interval may become part of the licensing specifications. If the performance is unacceptable, then shorter testing and inspection intervals may be explored or alternative designs (e.g., having more redundancy or diversity) may be considered.

7.5.3.1.2 Demand-Based Event Models

The failure-on-demand event model, as described in the *PRA Procedures Guide* (NRC 1983), is also termed the constant-failure-rate-per cycle model in the *Fault Tree Handbook* (Vesely et al. 1981).

The failure-on-demand model applies to a component or system that is in a dormant state until the instant there is a demand for it. This concept applies to standby components, as described previously. The failure-on-demand model also applies to structural and passive components that may never be challenged during their operational lifetime or are not amenable to testing, inspection, or refurbishing after the initial installation or construction. The weld on a WP is an example of such a component.

However, the constant-failure-rate-per cycle model may be applicable for operating or standby equipment that may be required to perform several, repeated operations (demands) for which there is a fixed probability of failure per demand.

For point estimates of event probabilities in an ET or FT analysis, the failure on demand is simply the value of the constant probability for a given situation, calculated as:

$$q_D = p_D = r/n \quad (\text{Eq. 7-62})$$

where p_D is derived from tests or event reports for r failures in n trials. The expression for q_D is a limiting case (for $r \geq 1$ failure) of the binomial probability distribution.

The demand-based event model should be applied to events that are modeled as a one-time demand in the PSA ET and FT analyses. This quantity is subject to considerations of uncertainty.

When the event involves a cycling of a system or component during some operational time span (or mission time), the expected number of cycles (demands) during the time interval is important. If N cycles are expected during a mission time T and the probability of failure per demand is p_D , then the probability of failure during T is estimated as:

$$q_T = N * p_D \quad (\text{Eq. 7-63})$$

This expression may be evaluated as a probability (pure number) or as a frequency (probability per unit time), depending on the application.

If the system or component is used during the response (mitigation) as part of an event sequence, or as a basic event in an FT, the probability form is used. The event modeling will specify the number of demands that will be expected. For example, a pressure relief damper may be required to cycle N times during a hot cell purging operation following a drop and breach of an SNF assembly. The value of N may be derived from considerations of the pressure equalization between the Waste Handling Building zones or be based on a performance-time requirement. The probability of failure, then, is $q_T = N * p_D$.

The frequency form is used if the system or component failure could be an IE of an event sequence. Event modeling will specify an operational frequency for demands (e.g., N is the number of lifts per year of SNF assemblies). If p_D represents the probability per lift of dropping a SNF assembly, then the frequency of dropping SNF assemblies becomes $f_T = N * p_D$ drops per year (here, f_T is used in place of q_T).

7.5.3.1.2.1 Binomial Distribution

The binomial distribution is a discrete form of a PDF:

$$b(x;n,p) = \binom{n}{x} p^x (1-p)^{n-x} \quad (\text{Eq. 7-64})$$

This expression gives the probability that exactly x number of failures will be observed in n independent trials, given a constant probability per trial, p . The parameter needed in this model is p . The expression for $b(n;n,p)$ is a built-in function in the Microsoft Excel spreadsheet program.

The binomial form of the cumulative probability function is often used in ET and FT analysis. It is expressed as:

$$B(r;n,p) = \sum \binom{n}{s} p^s (1-p)^{n-s}; \text{ sum from } s = 0 \text{ to } s = r \quad (\text{Eq. 7-65})$$

This expression gives the probability that x , the number of failures observed in n independent trials, will be less than or equal to r , given a constant probability per trial, p . The statistical average of the binomial distribution is np and the variance is $np(1-p)$. The expression for $B(r;n,p)$ is a built-in function in the Microsoft Excel spreadsheet program.

If the binomial PDF is taken to the limit as n goes to infinity for the product, $m = np$ is constant and finite, given the Poisson distribution that is expressed as:

$$p(x) = [m^x/x!] \exp(-m) \quad (\text{Eq. 7-66})$$

This expression represents the rare event approximation for a small number of failures in a large number of trials. It gives the probability that exactly x number of failures will be observed in a large number (effectively infinite) of independent trials having a small probability per trial, p . The parameter needed in this model is $m = np$. The expected number (mean) is m , and the variance is also m . The probability that $x \leq r$ is the summation of Equation 7-66 over x , from 0 to r . The Poisson distribution of Equation 7-66 is the basis for the exponential failure models, described below.

The Poisson distribution is a good approximation for the binomial, even for rather large values of p and small values of n . As an example, the *Fault Tree Handbook* asks "what is the probability of finding exactly one defective unit in a random lot of 10, given $p = 0.1$?" The exact value using the binomial distribution is 0.3874; the Poisson formula gives 0.3679. This estimation may be adequate for many probability estimates in light of other uncertainties. When the lot size is increased to 20, the respective values are 0.2702 and 0.2707; thus, an excellent agreement.

It is further noted that for most event tree and fault tree analyses, the probability of interest is that for exactly 0 failures. Setting $x = 0$ in Equation 7-66 gives:

$$p(0) = \exp(-m) = \exp(-np) \quad (\text{Eq. 7-67})$$

The available failure event data are given as time-based data, (i.e., a failure is observed to occur with an average interval of τ hours). Expressed another way, if the mean arrival interval of failures is τ a number R failures would be expected in some time interval T , where $R = T/\tau$. Since m , (Equation 7-66) is the number of failures, replacing M with $R = T/\tau$, gives:

$$p(0) = \exp(-R) = \exp(-T/\tau) = \exp(-\lambda T) \quad (\text{Eq. 7-68})$$

Here $\lambda = 1/\tau$ is a constant failure rate. This expression is observed to be the exponential event model, thus demonstrating the similarities between the demand-based and time-based event models. Equation 7-68 gives the probability of having exactly zero failures in the time T . The probability of having at least one failure in a time period, T , is given by $P_F = 1 - p(0) = \exp(-\lambda T)$.

7.5.3.1.3 Dependent and Common Cause Failures

A more complete discussion of dependent failures and CCFs is presented in Section 7.4.

In developing FT models that include redundant components or subsystems, it is generally recognized that the joint probability of the concurrent failure of two or more redundant components may not be the product of independent failure probabilities. That is, the failures of the individual components or subsystems may be dependent (i.e., coupled). This possibility is modeled in the FT when the construction rules are applied. Similarly, events in a sequence may not be independent (i.e., the success or failure of one system may influence the probability of failure of a system [component, or human] that occurs later in the sequence).

The probabilities of the dependent or CCFs are quantified using demand-based or rate-based parameters, as appropriate for the event being quantified. Dependencies are explicitly modeled in ETAs and quantified by sequence-dependent probabilities (see Section 7). Potential CCFs are identified and quantified in FTAs. It is expected that most CCF quantification will apply the beta factor method (see Section 7.4).

7.5.3.1.4 Initiating Event Frequency

When the purpose of information analysis in an FTA is to quantify the frequency of an event sequence (or accident scenario), the frequency of the IE has to be scaled to match the operational load of the system. For example, the IE definition may be “crane drops SNF canister” and the quantification may require “ F_D drops per year.” The operational throughput of the system may be Z canisters per year. Demand-based and rate-based data can be used to calculate the frequency of the IE, as follows:

Demand-Based Data—Experience data indicate that the probability of dropping any given canister during a lift is Q_D drops per lift (i.e., more precisely defined as the probability of a canister drop per lifting operation). If the frequency of lifting canisters is Z per year, then the frequency of the postulated IE is calculated as:

$$F_D = Z * Q_D \text{ (drops per year)} \quad (\text{Eq. 7-69})$$

Rate Based Data—Experience data show that the rate of dropping any given canister during operational time is λ_D drops per hour (e.g., this rate might be derived from related information like a crane failure rate). In this situation, the exposure time (or mission time) must be defined for each lift operation to derive the probability of a drop per lift. The estimated time that each canister is suspended in a vulnerable condition during each operation is T_L minutes. The probability of canister drop per lift is derived as:

$$Q_D = \lambda_D * T_L \text{ (drops per lift)} \quad (\text{Eq. 7-70})$$

The time units must be converted, as appropriate, from hours to years.

Proceeding in the same manner as in the demand-based case, the frequency of the postulated IE is calculated as:

$$F_D = Z * Q_D \text{ (drops per year)} \quad (\text{Eq. 7-71})$$

7.5.3.1.5 Human Error Probabilities or Rates

Many basic events in ET or FT models represent human errors in operations or maintenance. Special techniques have been developed for estimating the probabilities of various kinds of human errors. The events are sometimes called HAs to include positive effects (recoveries or interventions) as well as to recognize that the basic causes of an undesired event involving a human may be situational and not a true human error. HRA is the process of analyzing situations where human errors (or human recovery actions) may occur and quantifying the probability of those actions. Section 7.3 describes an approach for support of the PSA.

7.5.3.2 Information (Data) Gathering

A repository is a first-of-a-kind facility. Therefore, there is no facility-specific operational experience to draw from to support the PSA for the LA submittal for CA. Therefore, the estimates of event probabilities or failure rates will be based on surrogate experience or generic information. Since the operational portions of the facility will employ many systems and components that are common in general industry, mining, and the nuclear industry, there are many potential sources of information that can be applied in the PSA. This section identifies some of the known sources and describes the kind of information that is available in each. Guidance is provided on how to employ such information in the PSA development.

This section does not proffer a single, definitive database as a mandatory input to the PSA, however. The establishment, maintenance, and configuration control of such a database should be established outside of this Guide.

The two primary categories of information are operational experience and tabulated generic data.

7.5.3.2.1 Operational Experience

Operational experience provides raw data on the number, modes, and causes of failures of systems, components, and software and a baseline that quantifies the time-in-service or number of demands represented in the reporting. A failure rate (or failure probability) of a given failure mode is derived from the ratio of the number of failures during the operational time (or number of demands). While it is relatively easy to find reports on the number and modes of failures in reports from many industries (i.e., to quantify the numerator), it is usually difficult to determine the baseline (i.e., to quantify the denominator). The analyst must often make assumptions on the baseline, estimating the time-in-service or number of demands based on throughput rates of the surrogate facility, preferably with input from operating personnel at that facility.

In many instances, the analyst will have to adjust the raw information to make it applicable to a particular repository operation. For example, if information is available on commercial railway locomotive derailments per mile traveled, and the causal breakdown shows that 25 percent are due to bad weather, the analyst might reduce the raw number by 25 percent as an estimate for subsurface transporter locomotives to account for the fact that there is no weather underground.

In applications of surrogate data, the analyst must provide a rationale to support selection of the source and how the information is applied.

Representative sources of operational information sources are described in the following paragraphs.

- **Exploratory Studies Facility**—The ESF experience can be applied where appropriate. For example, records on ground support system installation, maintenance, and inspections may provide bases for estimating the reliability of the repository ground support system.
- **U.S. Department of Transportation, Federal Railway Association**—Statistics and analysis of causal factors of accidents on commercial railways may provide bases for estimating derailment, brake failure, and human error rates.
- **British Mining Locomotive Data (U.K. Health and Safety Executive)**—Statistics and analysis of causal factors of accidents on commercial mining locomotives may provide bases for estimating derailment, brake failure, and human error rates.
- **U.S. Nuclear Regulatory Commission**—The NRC maintains databases of licensee event reports for cranes, fuel handling equipment, instrumentation and controls, electrical distribution, emergency diesel generators, HVAC systems, and other systems that will be used in a repository.
- **Waste Isolation Pilot Project**—Experience information accumulated on this project should be examined and incorporated into event probability estimates.
- **Institute of Nuclear Power Operations**—Performance information has been collected for many years, but for confidentiality, the Institute and the participating utilities closely

hold the information. Some summary information has been published, but access to compiled reliability databases has been restricted. Available information should be examined for applicability to the PSA for a repository.

List of other specific sources. [Information for this section is under development and will be provided later.]

7.5.3.2.2 Tabulated Generic Data

There are many tabulations of generic information that can be used for PSA. A bibliography of generic data sources is provided in Appendix 7A. The following paragraphs describe some of the principal databases.

- **Savannah River Site Generic Data Base** (Blanton and Eide 1993)—This document describes a project for improving the component failure rate database at the Savannah River Site. It provides a representative list of components and failure modes, approximately 75 percent of which are based on actual events. Many sources of generic data are noted, but a major generic source was NUCLARR (see below), but also incorporated data from the INEEL chemical processing plant. A Bayesian approach was used for estimation. The information was aggregated to obtain generic failure rate distributions (given as mean and EF of LN) for each component failure mode. EF is the ratio of 95 percent upper bound to median (50 percentile).
- **Savannah River Site Human Error Rate Database** (Benhardt et al. 1994)—A counterpart of the Savannah River Site component database. This report tabulates HEP for 35 representative HAs in Savannah River Site safety analyses: 16 are based on generic information, and 19 are based on site-specific information.
- **IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems** (IEEE 1998)—This document provides a limited summary of equipment reliability data (see also IEEE 1984).
- **NUCLARR, NUREG/CR-4639** (INEEL 1989)—This database, sponsored by the NRC, is a compilation of event data extracted from many PRA and individual plant examinations. Not all of the information is independent, especially some of the generic information that is replicated in several studies. The entries are categorized as 1, 2, and 3 to indicate the degree of independence and quality so the user may reject some entries, or use them with caution or weighting. Access to the NUCLARR database requires a subscription.
- **Eide and Calley (1993)**—This paper presents a comprehensive tabulation of generic component failure rates developed for light-water reactor PRAs. NUCLARR was used, so that most of the failure rates are based on actual plant experience. Failure rates and their EFs are given for several failure modes of each component. The EFs are the ratio of the 95th percentile to the 50th percentile. NUCLARR has automatic aggregation routines to pool information from different sources. Table 7-7 illustrates the format of the information in that paper.

- **Eide et al. (1993)**—This paper presents failure rates for fluid system components to support internal flooding PRAs for NPPs. The basic information was gathered from licensee event reports reported in Nuclear Power Experience. Rupture probabilities and leakage frequencies were estimated using Bayesian update with a noninformative prior. Component exposure times were estimated if they were not explicitly given in the information base.
- **IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Station (IEEE 1984)**—This document contains failure rate point values and intervals for electronic, electrical, and sensing components. The values reported were elicited from about 200 experts and pooled using geometric averaging. Some of the information is based on operational and test information, but the user cannot tell which information has this basis versus that based purely on expert opinion.
- **Rome Air Force Base, NPRD-2, Nonelectronic Parts Reliability Data (Arno 1981)**—This document is intended to complement MIL-HNBK-217F (DOD 1991) by providing information on mechanical, fluid, and air-handling system components. For example, the table includes failure modes and rates for vehicle brakes in various applications. The tables provide rates (mean and confidence interval) for various failure modes, and where available, it provides raw data (number of failures and number of trials or operational time).
- **AIChE Guidelines for Process Equipment Reliability Data with Data Tables (AIChE 1989)**—This source contains information on components used in non-nuclear facilities. Tables include failure rates for different modes of failure and the lower bound, mean, and upper bound.
- **MIL-HDBK-217F, Military Handbook Reliability Prediction of Electronic Equipment (DOD 1991)**—This document is a compilation of baseline failure rates for a wide variety of electronic components, and it includes adjustment factors to account for the environment, duty or load, quality factor, and similar items. This document should be considered a prime source of information for the PSA because it is applied widely in government-supported activities.
- **Waste Isolation Pilot Project Safety Analysis**—Research database for potential use. [Information for this section is under development and will be provided later.]
- **Reactor Safety Study (WASH 1400) (NRC 1975)**—This work was compiled in the mid-1970s. It has tabulations of component and system failure rates and probabilities applicable to NPPs. The tabulations include data on pumps, valves, and reactor protection systems, which are not relevant to PSA; however, information on electrical components and instrumentation may be applicable. Parts of this report are still quoted and are embedded in some of the other generic databases (e.g., NUCLARR [INEEL 1989]). For PSA, preference should be given to more recent sources, provided they are applicable and reliable.

Component/Failure Mode	Recommended Failure Rate, Mean	Error Factor, 95/50	NUCLARR Component Failure Information				NUCLARR Source
			Sources	Failures	Demand	Hours	
<u>Mechanical Components</u>							
Valve - Motor Operated							
Fail to open/close	3.0E-03 /d	5	13	480	141474		Category 1
Spurious operation	5.0E-08 /h	10	4	1		2.00E+07	Category 1
Plug	5.0E-09 /h	10		0		1.24E+08	Category 2
Internal leakage							None
Internal rupture	1.0E-07 /h						Other
.
.
Pump - Motor Driven							
Fail to start	3.0E-03 /d	5	17	137	48459		Category 1
Fail to run	3.0E-05 /h	10	16	216		7.46E+06	Category 1
.
.
<u>Electrical Components</u>							
Battery							
Failure	1.0E-05 /h	5	6	8		9.44E+05	Category 1
Battery charger							
Failure	1.0E-05 /h	5	7	29		1.62E+06	Category 1
Switch-General							
Failure to open/close	1.0E-05 /d	5					Other
Spurious operation	1.0E-06 /h	10					Other
Switch-Limit							
Failure to open/close	3.0E-05 /d	5	1	0	12550		Category 1
Spurious operation	1.0E-06 /h	10	1	7		8.10E+06	Category 1
.
.

Table 7-7. Example of Generic Component Failure Rates Database

- **Government Industry Data Exchange Database (GIDEP)**—Primarily oriented toward aerospace and defense industries. Generic failure rate information is similar to that presented in the Rome Air Force Base (Arno 1981) and MIL-HDBK-217F (DOD 1991) documents. Subscribers pay no fees, but must contribute data.
- **Plant-Specific PRAs and Individual Plant Examinations**—Every PRA and individual plant examination submitted to the NRC contains a tabulation of basic event data. These will be a mixture of generic and plant-specific information. If other generic sources do not support a particular facet of the PSA, the analyst may have to use this source.
- **Foreign Databases**—Component failure rate data have been compiled by foreign nuclear programs such as those in France and Sweden.

7.5.3.3 Estimation of Model Parameters

This section describes the methods for quantifying parameters needed to quantify the event probabilities and frequencies using the models described in Section 7.5.3.1. Two general classes

of methods are described that are known, respectively, as classical (or Frequentist) estimation and Bayesian (or subjectivist) estimation.

The classical approach relies on statistical theories that equate probability to the frequency of observed outcomes, usually invoking hypothetical runs of many trials. The classical approach has been applied in traditional reliability engineering. The classical approach has limitations in trying to estimate the probability of events that have never been observed, but which are believed to be possible.

The Bayesian approach is probability based, not statistical based. In this concept, probability is related to the state of knowledge or degree of belief of the analysts, hence the notion of subjectivity. The method is not entirely subjective in applications, however, since there is a robust theoretic foundation for incorporating empirical evidence into the estimation of event probabilities. Notably, there is a technique for Bayesian updates of facility-specific reliability databases. Further, Bayesian concepts are applied in the pooling, or aggregating, of information from several sources. Although the approach was fostered in the development of PRA methods, it has been adapted in modern reliability engineering.

Both the classical and Bayesian methods provide for estimating the uncertainties or in the model parameters. These are termed confidence intervals in classical estimation, and probability intervals or error factors in Bayesian estimation. In all cases, the intervals represent the range about the point estimate of a given parameter where the integral of the PDF is the fraction α of possible values reported from a large number of observations (i.e., the interval is expected to include the true value of the parameter with probability of 100α percent. The respective limits on the confidence interval are calculated as the area in the upper and lower tails of the particular PDF. The intervals are expressed as the value of the parameter that represents the upper $100(1-\frac{\alpha}{2})$ percent and lower $100(1-\frac{\alpha}{2})$ percent values of the parameter.

The following sections are based, in large measure, on the *PRA Procedures Guide* (NRC 1983).

7.5.3.3.1 Classical Parameter Estimation

The classical approach is presented for point estimates and confidence intervals for the binomial, Poisson and LN distributions. The information requirements for quantifying each distribution are also presented.

7.5.3.3.1.1 Binomial Distribution

The fundamental parameter is p , the probability of failure on demand (unitless) (see Section 7.5.3.1). It is derived from test or experience information as follows:

Point Estimate: $p^* = f/n$ (Eq. 7-72)

where information needs are:

f = number of observed or recorded failures in n demands or trials

n = number of recorded demands or trials in reporting period.

Confidence Interval: The exact method for interval estimation for the binomial distribution is to use the expression $B(f;n,p)$ for the cumulative distribution solving for p_U and p_L , respectively, that give the upper and lower $100(1 - \alpha)$ percent confidence limits:

$$\alpha = B(f;n,p_U) = \sum_{s=0}^f \binom{n}{s} p_U^s (1 - p_U)^{n-s}; \text{ sum from } s = 0 \text{ to } s = f \quad (\text{Eq. 7-73})$$

$$\alpha = B(f;n,p_L) = \sum_{s=f}^n \binom{n}{s} p_L^s (1 - p_L)^{n-s}; \text{ sum from } s = f \text{ to } s = n \quad (\text{Eq. 7-74})$$

These expressions may be solved using standard tables or by using built-in formulas in a spreadsheet (e.g., the Microsoft Excel spreadsheet program).

For small f and large n , the interval may be approximated using:

$$P_U(1 - \alpha) = [\chi^2(2f + 2, \alpha)]/2n \quad (\text{Eq. 7-75})$$

$$P_L(1 - \alpha) = [\chi^2(2f, 1 - \alpha)]/2n \quad (\text{Eq. 7-76})$$

where $\chi^2(m, \gamma)$ is the value of the Chi-Squared distribution for the 100γ -percentile for m degrees of freedom. The interval between $P_L(1-\alpha)$ and $P_U(1-\alpha)$ constitutes a confidence interval. For example, $2\alpha = 0.1$, the range constitutes a 90% confidence interval and $\alpha = 0.05$ in Equations 7-75 and 7-76,

These expressions may also be solved using standard tables or by using built-in formulas in a spreadsheet (e.g., the Microsoft Excel spreadsheet program).

7.5.3.3.1.2 Poisson Distribution

The fundamental parameter is λ , the probability of failure per unit time (see Section 7.5.3.1). It is derived from test or experience information as follows:

Point Estimate: $\lambda^* = f/T \quad (\text{Eq. 7-77})$

where the information needs are

f = number of observed or recorded failures (or an IE) in a time interval T .

T = time duration in reporting period.

Confidence Interval: The interval estimation for the Poisson distribution is to solve for λ_U and λ_L using the following expressions:

$$\lambda_L(1 - \alpha) = [\chi^2(2f + 2, 1 - \alpha)]/2T \quad (\text{Eq. 7-78})$$

$$\lambda_U(1 - \alpha) = [\chi^2(2f, \alpha)]/2T \quad (\text{Eq. 7-79})$$

where

$\chi^2(m, \gamma)$ is the value of the Chi-Squared distribution for the 100 γ -percentile for m degrees of freedom

These expressions may also be solved using standard tables or by using built-in formulas in a spreadsheet (e.g., the Microsoft Excel spreadsheet program). Note that these expressions are similar to the above approximate interval estimate for p in the binomial case, except that T replaces n .

7.5.3.3.1.3 Lognormal Distribution

Parameter estimation for the LN distribution is different than the prior two in two respects: 1) it describes a transformed variable rather than the fundamental parameter of interest, and 2) it requires two-parameters, the sample mean, μ^* , and the sample variance and σ^{2*} . Further discussions of the properties of the very important LN distribution are provided in Section 9, Uncertainty Analysis.

The fundamental parameter might be an observable quantity like a repair time for some component or system, τ , which is to be estimated from experience records.

In this example, the Information Needs are N independent observations such as of repairs time, say t_1, t_2, \dots, t_N . The transformed variable is $x_i = \ln(t_i)$; $i = 1, 2, \dots, N$.

The parameters of the PDF of the transformed variable x_i are calculated as follow:

$$\mu^* = \sum x_i/N \quad \text{sum for } i = 1 \text{ to } n, \text{ for the sample mean} \quad (\text{Eq. 7-80})$$

$$\sigma^{2*} = \sum (x_i - \mu^*)^2 / (N-1), \text{ sum for } i = 1 \text{ to } n, \text{ for the sample variance} \quad (\text{Eq. 7-81})$$

Confidence Intervals: Because the distribution requires two parameters, confidence intervals are calculated for μ and σ^2 .

For μ , the upper and lower 100 $(1 - \alpha)$ percent confidence limits are:

$$\mu_L = \mu^* - t(n-1, 1-\alpha)[\sigma^*/n^{0.5}] \quad (\text{Eq. 7-82})$$

$$\mu_U = \mu^* + t(n-1, 1-\alpha)[\sigma^*/n^{0.5}] \quad (\text{Eq. 7-83})$$

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

For σ^2 , the upper and lower 100 (1 - α) percent confidence limits are:

$$\sigma^2_L = [(n-1) \sigma^{2*}] / \chi^2 (n-1, 1-\alpha) \quad (\text{Eq. 7-84})$$

$$\sigma^2_U = [(n-1) \sigma^{2*}] / \chi^2 (n-1, \alpha) \quad (\text{Eq. 7-85})$$

where $\chi^2 (m, \gamma)$ is the value of the Chi-Squared distribution for the 100 γ -percentile for m degrees of freedom.

These expressions involving χ^2 and Students t distributions may also be solved using standard tables or by using built-in formulas in a spreadsheet (e.g., the Microsoft Excel spreadsheet program).

7.5.3.3.2 Bayesian Parameter Estimation

The Bayesian approach also yields point estimates and interval estimates to represent the range where the analyst is confident that the true parameter lies. Its basis is different than the classical estimation, however, in that it permits incorporation of analysts' belief and information not contained in observed data. Such belief and information are incorporated by assigning a probability distribution, termed the prior distribution that describes the analyst's belief about the parameter. The prior describes the best estimate point value, uncertainty range, and an assumed shape (e.g., normal, LN, or binomial). In cases where the analyst has no information or weak belief in the value of a parameter, the Bayesian approach permits use of a noninformative prior (see discussion below). By applying evidence that exists (e.g., test results, experience data from surrogate systems, or facility-specific experience data), a posterior probability distribution is generated using the Bayes theorem (NRC 1983). The posterior distribution yields a revised (updated) estimate of the best estimate (median or mean) and the uncertainty ranges.

As will be shown, the Bayesian approach uses an integration over the joint distribution of the prior distribution and a likelihood function. It has been shown that the integration can be performed in closed form if the priors are represented by conjugate distributions, and each primary distribution has a natural conjugate (see *PRA Procedures Guide* [NRC 1983, Section 5] for more information). When the prior distribution is not described by a standard probability distribution, it is usually approximated with a discrete (rather than continuous) distribution, where a summation over the joint distribution of prior and likelihood function is used.

After a summation of concepts that are common to all Bayesian estimates, this section provides the methods for applying the approach to point estimates and confidence intervals for the binomial, Poisson (including exponential), and LN distributions. The information requirements for quantifying each distribution are also presented.

7.5.3.3.2.1 Basic Elements of Bayesian Estimation

Bayesian Point and Interval Estimation—The prior distribution summarizes the uncertainty in a parameter based on judgement or generic information sources. Similarly, the posterior distribution summarizes the uncertainty in the facility-specific or surrogate information.

Two commonly used values of point estimates are used, the mean and the median, which are based on the properties of PDFs. For example, if a failure rate λ is the parameter of interest, and its uncertainty is described by a PDF $f(\lambda)$, the respective point estimates are calculated as follows:

$$\mu_\lambda = \int_0^{\infty} \lambda f(\lambda) d\lambda, \text{ is the mean} \quad (\text{Eq. 7-86})$$

while the median is the solution to the integral equation:

$$F(\lambda) = \int_0^{\lambda} f(t) dt = 0.5 \quad (\text{Eq. 7-87})$$

where $F(\lambda)$ is the CDF.

The point estimate definitions are applied to both the prior and the posterior distribution, as needed.

The Bayesian interval estimate also uses the probability distribution for the parameter. The range of integration is set so that the range includes the desired probability that the range contains the true value. If the desired probability is given as $(1 - \gamma)$, the respective upper (λ_U) and lower (λ_L) interval limits are calculated as follow:

$$\int_0^{\lambda_U} f(\lambda) d\lambda = \gamma/2 \quad (\text{Eq. 7-88})$$

$$\int_{\lambda_L}^{\infty} f(\lambda) d\lambda = \gamma/2 \quad (\text{Eq. 7-89})$$

The interval definitions are applied to both the prior and the posterior distribution, as needed.

If the desired probability of success $(1 - \gamma)$ is 0.90, then $\gamma = 0.10$, so $\gamma/2 = 0.05$.

The application of the point and interval calculations is demonstrated below for the parameter of the binomial, Poisson, and LN distributions.

7.5.3.3.2 Steps in Bayesian Estimation Approach

The *PRA Procedures Guide* (NRC 1983) identifies the following steps for applying the Bayesian approach to information processing. These steps are listed here in abbreviated form as applicable to the PSA.

- Identify sources and forms of generic information to be used in generating an appropriate prior distribution
- Select a prior distribution family if none has been specified in the generic information

- Define a particular prior distribution from parameters derived from generic information by reducing or combining, as appropriate
- Plot the prior distribution and characterize it: mean, median, variance, and summary percentiles (e.g., upper and lower 95 percent limits)
- If generic estimates are to be used, generate from the prior
- If facility, or application-specific estimates are required, additional sub-steps are used:
 - Obtain specific information
 - Identify appropriate form for the likelihood function
 - Apply the Bayes theorem to generate the posterior distribution
 - Plot posterior on same graph as prior to observe effect of specific information (e.g., shift in central measure, change in distribution shape)
 - Characterize posterior distribution: mean, median, variance, and summary percentiles (e.g., upper and lower 95 percent limits)

7.5.3.3.2.3 Defining Prior Distributions

Unless a noninformative prior is selected, a prior distribution is developed from generic information. When estimating a parameter such as the failure rate of a given component, the analyst usually has available generic information consisting of engineering knowledge about the design, construction, expected performance, and expected operating environment associated with the component, and the past performance and reliability of similar components. Section 7.5.3.2 describes some of the sources of generic information. When little or no generic prior information is available, a noninformative prior may be used.

In many instances, a natural conjugate distribution is used in Bayesian estimation to permit closed form integration. For a given likelihood function, such as the exponential, a natural conjugate function has the property that the posterior and prior distributions are member of the same family of distributions (i.e., a LN prior distribution on λ yields LN posterior distribution on λ).

Sometimes in practice, a particular distribution may be mapped into its conjugate by moments matching, and after the Bayesian integration over the conjugate and likelihood function, the posterior distribution is mapped back to its conjugate (Blanton and Eide 1993).

Generic information may be obtained from single or multiple sources. Sufficient information to generate the distribution parameters of the priors. For example, at least two independent pieces of information are required to generate the parameters needed to define a LN prior distribution for λ . Thus, pairs of information like a) upper and lower limits, b) mean and variance, or 3)

median and EF must be defined by the analyst. The information may be derived from tabulated failure rates, reported experience, or expert judgement.

For much of the PSA analysis, tabulated data that have been applied in various PRA studies or in MIL-HDBK-217P (DOD 1991) will suffice, particularly when there is a clear match between a repository component or system and a component or system represented in the tabulation. In other cases, the analyst may not be able to clearly establish the direct applicability of one or more tabulated items and must resort to multiple information sources. Such sources are combined using one of the methods described in the following section.

7.5.3.3.3 Pooling and Combining Information from Multiple Sources

Since the PSA will be based in large measure on surrogate information, there may be instances where two or more sources provide event data or failure rates for systems or components that are judged to be representative of those in a repository. For purposes of event probability estimation, a single prior distribution is needed. Numerous methods are available, but the *PRA Procedures Guide* (NRC 1983) describes three processes for pooling multiple information sources to arrive at a single distribution. One process, termed the mixture method is judged to be too cumbersome for PSA application, so two of the methods are presented here.

The first, based on a geometric mean, is simple to apply and is believed to be sufficient for the PSA for the LA for construction authorization. This method is noted to underestimate the uncertainties. The second method, a two-stage Bayesian, has been applied in numerous PRA studies. It is based on developing a prior distribution that is grounded in generic information before updating the distribution with facility-specific information. Since a repository will have little specific information to apply, this method is not developed in detail in this edition of the PSA Guide.

Martz and Waller (1978) examined several methods of pooling information sources. They concluded that simple averaging techniques are satisfactory when a small number of sources are to be pooled, but more sophisticated methods are required when 15 or more sources are to be combined.

7.5.3.3.3.1 Geometric Mean Method

If there are M sources of information for a failure rate λ_i and each source provides a point estimate and interval estimate, the composite values for the prior distribution are calculated as geometric means, as

$$\langle \lambda_0 \rangle = \left(\prod_{i=1, m} \lambda_{0,i} \right)^{1/M}; \text{ where } i = 1 \dots m \text{ for the composite point value} \quad (\text{Eq. 7-90})$$

$$\langle \lambda_{LB} \rangle = \left(\prod_{i=1, m} \lambda_{LB,i} \right)^{1/M}; \text{ where } i = 1 \dots m \text{ for the composite lower bound} \quad (\text{Eq. 7-91})$$

$$\langle \lambda_{UB} \rangle = \left(\prod_{i=1, m} \lambda_{UB,i} \right)^{1/M}; \text{ where } i = 1 \dots m \text{ for the composite lower bound} \quad (\text{Eq. 7-92})$$

where $\lambda_{0,i}$ is the point value from the i^{th} information source

$\lambda_{LB,i}$ and $\lambda_{UB,i}$, respectively, are lower and upper bounds of the i^{th} information source

With the composite point estimate treated as a mean or median, as deemed appropriate for the assumed family of the prior distribution, the available experience data (evidence) can be applied to derive the posterior distribution, as described in Section 7.5.3.3.4.1

7.5.3.3.3.2 Two-Stage Bayesian Method

[Information for this section is under development and will be provided later.]

7.5.3.3.4 Applications of Bayesian Estimation to Event Quantification

For PSA purposes, important techniques for parameter estimation have been extracted from reference material. The first application is for estimating failure-on-demand probabilities, and the second is for estimating constant failure rates. The presentations give the mathematical formulas for distribution parameters when noninformative and conjugate distributions are used.

7.5.3.3.4.1 Bayesian Estimation of Failure-on-Demand Probabilities

The binomial distribution, given in Equation 7-64 in Section 7.5.3.1.2, gives the probability of observing exactly r failures in n trials, given a probability of failure per trial of p . That equation is used as the likelihood function. The purpose of the Bayesian estimation is to determine the best estimate for p and its uncertainty distribution.

The first case is application of a noninformative prior. The form of noninformative prior given in Section 5.5.2.3.2 of the *PRA Procedures Guide* (NRC 1983) is

$$[q(1-q)]^{-0.5}/\pi; \text{ for } (0 \leq q \leq 1) \quad (\text{Eq. 7-93})$$

where it may be shown that

$$\begin{aligned} \text{Prior mean:} \quad q_0 &= 0.5 \\ \text{Prior median:} \quad q_{0,0.5} &= 0.5 \\ \text{Prior variance:} \quad \sigma_0^2 &= 0.125 \end{aligned}$$

and the $100(1 - \gamma)$ percent (e.g., 95 percent) symmetric probability is a function of the F-distribution with a and b degrees of freedom, $F_{1-\gamma/2}(a,b)$, as follows:

$$\text{Prior lower bound:} \quad q_{0,L} = 0.5/[0.5 + 0.5 F_{1-\gamma/2}(1,1)] \quad (\text{Eq. 7-94})$$

$$\text{Prior upper bound:} \quad q_{0,U} = 0.5 F_{1-\gamma/2}(1,1)/[0.5 + 0.5 F_{1-\gamma/2}(1,1)] \quad (\text{Eq. 7-95})$$

The posterior distribution is shown to have the form of a beta distribution as follows:

$$[\Gamma(n+1)/\Gamma(r+0.5)\Gamma(n-r+0.5)] [q^{r-0.5}(1-q)]^{n-r-0.5}; \text{ for } (0 \leq q \leq 1) \quad (\text{Eq. 7-96})$$

where $\Gamma(x)$ is the gamma function.

The parameters of the posterior distribution are the following:

Posterior mean:
$$\underline{q} = (r + 0.5)/(n + 1) \quad (\text{Eq. 7-97})$$

Posterior median:
$$q_{0.5} = (r + 0.5)/[(r + 0.5) + (n - r + 0.5)F_{0.5}(2n - 2r + 1, 2r + 1)] \quad (\text{Eq. 7-98})$$

Posterior variance:
$$\sigma^2 = (r + 0.5)(n - r + 0.5)/[(n + 1)^2 (n + 2)] \quad (\text{Eq. 7-99})$$

and the 100(1 - γ) percent symmetric probability is a function of the F-distribution with a and b degrees of freedom, $F_{1-\gamma/2}(a,b)$, as follows:

Posterior lower bound:

$$q_L = (r + 0.5)/[(r + 0.5) + (n - r + 0.5)F_{1-\gamma/2}(2n - 2r + 1, 2r + 1)] \quad (\text{Eq. 7-100})$$

Posterior upper bound:

$$q_U = [(r + 0.5)F_{1-\gamma/2}(2r + 1, 2n - 2r + 1)]/[(n - r + 0.5) + (r + 0.5)F_{1-\gamma/2}(2r + 1, 2n - 2r + 1)] \quad (\text{Eq. 7-101})$$

The noninformative prior is very useful when the available performance records show zero failures for a finite number of trials. In this instance, the classical estimation must assert at least one failure has occurred, or the estimation interval on p becomes indeterminate (see Section 7.5.3.4.1).

The second application assumes a beta prior that is derived from information available prior to the analysis. Such prior information may be derived from generic sources. The beta prior has the form:

$$[\Gamma(n_0)/\Gamma(r_0)\Gamma(n_0 - r_0)] [q^{r_0-1} (1 - q)^{n_0-r_0-1}; \text{ for } (0 \leq q \leq 1) \quad (\text{Eq. 7-102})$$

where the values of n_0 and r_0 are the parameters of the assumed beta prior distribution, but may also be interpreted as information derived from the prior information, where n_0 represents the number of trials, and r_0 the number of failures. $\Gamma(x)$ is the gamma function.

The parameters of this distribution are:

Prior mean:
$$q_0 = r_0/n_0 \quad (\text{Eq. 7-103})$$

Prior median:
$$q_{0.5} = r_0/[r_0 + (n_0 - r_0)F_{0.5}(2n_0 - 2r_0, 2r_0)] \quad (\text{Eq. 7-104})$$

Prior variance:
$$\sigma_0^2 = r_0(n_0 - r_0)/n_0^2(n_0 + 1) \quad (\text{Eq. 7-105})$$

and the 100(1 - γ) percent symmetric probability is a function of the F-distribution with a and b degrees of freedom, $F_{1-\gamma/2}(a,b)$, as follows:

Prior lower bound:
$$q_{0,L} = r_0/[r_0 + (n_0 - r_0)F_{1-\gamma/2}(2n_0 - 2r_0, 2r_0)] \quad (\text{Eq. 7-106})$$

Prior upper bound:
$$q_{0,U} = r_0 F_{1-\gamma/2}(2r_0, 2n_0 - 2r_0)/[(n_0 - r_0) + r_0 F_{1-\gamma/2}(2r_0, 2n_0 - 2r_0)] \quad (\text{Eq. 7-107})$$

Posterior mean: $q = (r + r_0)/(n + n_0)$

Posterior median:

$$q_{0.5} = (r + r_0)/[(r + r_0) + (n - r + n_0 - r_0) F_{0.5}(2n - 2r + 2n_0 - 2r_0, 2r + 2r_0)]$$

Posterior variance:

$$\sigma^2 = (r + r_0)(n - r + n_0 - r_0)/[(n + n_0)^2(n + n_0 + 1)]$$

and the $100(1 - \gamma)\%$ symmetric probability is a function of the F-distribution with a and b degrees of freedom, $F_{1-\gamma/2}(a,b)$, as follows:

Posterior lower bound:

$$q_L = (r + r_0)/[(r + r_0) + (n - r + n_0 - r_0) F_{1-\gamma/2}(2n - 2r + 2n_0 - 2r_0, 2r + 2r_0)]$$

Posterior upper bound:

$$q_U = [(r + r_0) F_{1-\gamma/2}(2r + 2r_0, 2n - 2r + 2n_0 - 2r_0)]/[(n - r + n_0 - r_0) + (r + r_0) F_{1-\gamma/2}(2r + 2r_0, 2n - 2r + 2n_0 - 2r_0)].$$

The third application assumes a LN prior distribution on q . This distribution is often used for failure rates, especially for low rates like 10⁻⁶ per demand or unit time. The LN is so named because the random variable represented by the distribution, x , is the logarithmic transform of a random variable of interest (i.e., the failure rate per demand, q). Thus, $x = \ln(q)$ is the random variable, and x is assumed to follow a normal (or Gaussian) distribution. All the well-known statistical properties and tabulations of the normal distribution can then be applied. The transformation between moments of the transformed variable and the failure rate are shown below.

The LN distribution requires two parameters, μ and σ , the mean and standard deviation of a normal distribution on x . These distribution parameters are derived from the assumed LN distribution on q , as follows.

The analyst estimates or specifies two symmetric percentiles for the interval containing q with a given probability, $1 - \gamma$, where $0 < \gamma < 0.5$ (usually, γ is 0.1 or 0.05). The respective percentiles are labeled q_γ (or q_L , lower bound) and $q_{1-\gamma}$ (or q_U , upper bound), and are symmetrical, giving:

$$p(q < q_\gamma) = p(q > q_{1-\gamma}) = \gamma \quad (\text{Eq. 7-108})$$

The median value of q is the geometric mean of the interval limits, that is:

$$q_{0.5} = (q_\gamma q_{1-\gamma})^{1/2} \quad (\text{Eq. 7-109})$$

and the EF is defined as:

$$EF = (q_{1-\gamma} / q_\gamma)^{1/2} \quad (\text{Eq. 7-110})$$

and a useful property of the EF is its relationship to the median, as follows:

$$EF = (q_{0.5} / q_{\gamma}) = (q_{1-\gamma} / q_{0.5}) \quad (\text{Eq. 7-111})$$

The parameters of the associated LN distribution, μ and σ , become:

$$\mu = \ln(q_{0.5}) \quad (\text{Eq. 7-112})$$

$$\sigma = \ln(EF) / z_{1-\gamma} \quad (\text{Eq. 7-113})$$

where $z_{1-\gamma}$ is the $100(1-\gamma)^{\text{th}}$ percentile of a normal (Gaussian) distribution. Values of $z_{1-\gamma}$ are tabulated in virtually all statistics books and can be obtained from the normal distribution function that is built into the Microsoft Excel spreadsheet program.

The moments of the fitted LN are derived from the parameters as follow:

$$\text{Mean:} \quad q = \exp(\mu + \sigma^2/2) \quad (\text{Eq. 7-114})$$

$$\text{Mode:} \quad q_{Md} = \exp(\mu - \sigma^2) \quad (\text{Eq. 7-115})$$

$$\text{Median:} \quad q_{0.5} = \exp(\mu) \quad (\text{Eq. 7-116})$$

$$\text{Variance:} \quad \sigma_q^2 = [\exp(2\mu + \sigma^2)][\exp(\sigma^2) - 1] \quad (\text{Eq. 7-117})$$

The variance σ_q^2 is for the distribution of the failure rate q , while σ^2 is the variance of the transformed random variable $x = \ln(q)$.

The evidence in the form of r failures in n trials is incorporated into the Bayesian analysis. Since the LN does not allow a closed-form integral solution, numerical integration is used (see Section 5.5.2.3.4 of the *PRA Procedures Guide* [NRC 1983]).

An alternative method, applied at the Savannah River Site (described in Blanton and Eide [1993]), converts the prior LN into a beta distribution, applies the specific evidence (number of failures, r , and number of trials, n) in the Bayesian integration, which in turn produces a beta posterior distribution. The beta posterior distribution is then converted to a LN.

7.5.3.3.4.2 Bayesian Estimation of Constant Failure Rates

The methods for estimating constant failure rates are very similar to those for failure-on-demand with two primary differences. First, the likelihood function is the Poisson distribution, rather than the binomial. Second, the natural conjugate for the Poisson distribution is the gamma distribution, rather than the beta distribution. A third difference, demonstrated below, is the form of the noninformative prior that is recommended.

The method is aimed at deriving a best estimate and probability interval for a constant failure rate, λ , given information on the number of failures, r , in a given test-time duration, T . The failure on demand uses r and the number of trials, n , rather than the time.

The likelihood function for constant failure rates is the Poisson distribution, expressed as:

$$L(E|\lambda) = (\lambda T)^r \exp(-\lambda T)/r! \quad (r = 0, 1, 2, \dots) \quad (\text{Eq. 7-118})$$

The estimation methods are presented for three cases using different prior distributions: noninformative, gamma, and LN.

The first case is the application of a noninformative prior. The form of noninformative prior given in Section 5.5.2.4.2 of the *PRA Procedures Guide* (NRC 1983) is:

Prior density: $f_0(\lambda) = \lambda^{-0.5}$ (an improper distribution) ($\lambda > 0$) (Eq. 7-119)

Posterior density: $f(\lambda) = [T^{r+0.5}/\Gamma(r+0.5)] \lambda^{r-0.5} \exp(-\lambda T)$ ($\lambda > 0$) (Eq. 7-120)

Posterior mean: $\underline{\lambda} = (2r+1)/2T$ (Eq. 7-121)

Posterior median: $\lambda_{0.5} = \chi^2_{0.5}(r+0.5)/(2T)$ (Eq. 7-122)

where $\chi^2_{1-\gamma}(x)$ is the 100(1 - γ) percent (e.g., 95 percent) percentile of a chi-square distribution.

The symmetric probability interval is given by

Posterior lower bound: $\lambda_L = \chi^2_{\gamma/2}(2r+1)/(2T)$ (Eq. 7-123)

Posterior upper bound: $\lambda_U = \chi^2_{1-\gamma/2}(2r+1)/(2T)$ (Eq. 7-124)

The noninformative prior is very useful when the available performance records show zero failures for a finite time at test. In this instance, the classical estimation must assert at least one failure has occurred, or the estimation interval on λ becomes indeterminant. In the noninformative prior, the analyst asserts that the probability of failure per demand is somewhere in the range of (0,1) with equal likelihood, giving the prior mean of 0.5 as the best estimate (i.e., the analyst asserts that the item is equally likely to succeed or fail in any given trial.) The effect of 0 failures in n trials is to adjust the denominator so that the posterior gives the probability of 0.5 that the device will fail in n + 1 trials.

The second application assumes a gamma distribution prior that is derived from information available prior to the analysis. Such prior information may be derived from generic sources. The gamma prior has the form:

$$f_0(\lambda) = [\beta_0 \alpha_0 / \Gamma(\alpha_0)] \lambda^{\alpha_0-1} \exp(-\beta_0 \lambda); \quad (\text{for } \lambda > 0) \quad (\text{Eq. 7-125})$$

where the parameter α_0 (shape factor) can be interpreted as the prior number of failures in β_0 prior total operating time (β_0 is the scale factor).

The parameters of the gamma distribution are:

Prior mean: $\lambda_0 = \alpha_0 / \beta_0$ (Eq. 7-126)

Prior median: $\lambda_{0,0.5} = \chi^2_{0.5} (2\alpha_0) / (2\beta_0)$ (Eq. 7-127)

Prior variance: $\sigma_0^2 = \alpha_0 / \beta_0^2$ (Eq. 7-128)

where $\chi^2_{1-\gamma}(x)$ is the 100(1 - γ) percent percentile of a chi-square distribution. The prior 100(1 - γ) percent (e.g., 95 percent) symmetric probability interval is given by:

Prior lower bound: $\lambda_{0,L} = \chi^2_{\gamma/2} (2\alpha_0) / (2\beta_0)$ (Eq. 7-129)

Prior upper bound: $\lambda_{0,U} = \chi^2_{1-\gamma/2} (2\alpha_0) / (2\beta_0)$ (Eq. 7-130)

The posterior distribution is also a gamma distribution given as:

$$f(\lambda) = [(\beta_0 + T)^{\alpha_0+r} / \Gamma(\alpha_0 + r)] \lambda^{\alpha_0+r-1} \exp[-(\beta_0 + T) \lambda]; \text{ (for } \lambda > 0 \text{)} \quad \text{(Eq. 7-131)}$$

The parameters of the posterior distribution are:

Posterior mean: $\lambda = (\alpha_0 + r) / (\beta_0 + T)$ (Eq. 7-132)

Posterior median: $\lambda_{0.5} = \chi^2_{0.5} (2\alpha_0 + 2r) / (2\beta_0 + 2T)$ (Eq. 7-133)

Posterior variance: $\sigma^2 = (\alpha_0 + r) / (\beta_0 + T)^2$ (Eq. 7-134)

and the prior 100(1 - γ) percent symmetric probability interval is given by:

Posterior lower bound: $\lambda_L = \chi^2_{\gamma/2} (2\alpha_0 + 2r) / (2\beta_0 + 2T)$ (Eq. 7-135)

Posterior upper bound: $\lambda_U = \chi^2_{1-\gamma/2} (2\alpha_0 + 2r) / (2\beta_0 + 2T)$ (Eq. 7-136)

The third application assumes a LN prior distribution on λ . The presentation in Section 7.5.4.3.4.1 applies by replacing q with λ in all of the expressions. As noted above, there are two difficulties in using this prior, and the Bayesian integration cannot produce a closed form posterior distribution. Numerical solutions are required.

An alternative method, applied at the Savannah River Site (described in Blanton and Eide [1993]), converts the prior LN on λ into a gamma distribution, applies the specific evidence (number of failures, r , and time on test, T) in the Bayesian integration, which in turn produces a gamma posterior distribution. The gamma posterior distribution is then converted to a LN.

7.5.3.3.4 Uncertainties in Information and Event Probabilities

Section 9 provides a full discussion of treatment of uncertainties in event sequence quantification, including the propagation of uncertainties through the sequence frequencies. Part of the uncertainty stem from uncertainties in the probabilities and frequencies of events. This

section (Section 7.5) discusses the sources of uncertainties contained in the information sources and its application in estimation of parameters and event probabilities.

The *PRA Procedures Guide* (NRC 1983) identifies two categories of uncertainties in event probabilities: modeling uncertainty and information (data) uncertainty. These sources are evaluated differently, as described below.

- **Modeling Uncertainty**—No physical occurrence exactly fits a mathematical model such as having a constant failure rate, adherence to a Poisson time to failure, or failure on demand fitting a binomial with constant probability per demand. In Bayesian estimation, the selection of the prior distribution is another source of modeling uncertainty. So, the selection of the event model by the analyst introduces uncertainty. Different values for the point estimate, the PDF family, and different 90 percent confidence interval can result with different event models. Such uncertainty is evaluated with a sensitivity analysis. The event probability is re-evaluated with alternative models.
- **Information Uncertainty**—Uncertainty in estimated event probabilities and their associated distribution parameter arise from several sources: 1) amount of information (number of trials, duration, number of failure events), 2) diversity of information sources when pooling (i.e., various kinds of equipment, vendors, applications and environments) 3) accuracy of information sources (i.e., quality of tests or record keeping), and 4) applicability to repository facilities.

The uncertainty due to the amount of data is treated explicitly in the event estimation techniques described in Section 7.5.3.3. The amount of data affects the variance, the mean, and the confidence (classical) or probability (Bayesian) interval. The greater the number of trials (or duration), the tighter the distribution of the estimated parameters and event probabilities.

The uncertainties in the diversity or accuracy of information (which may be forced on the analyst if sufficient and relevant information is not available) can be alleviated by the application of the pooling procedures described in Section 7.5.3.3.3, but this requires analyst's judgement. If all sources are judged equally representative of the system or component of interest, all information is weighted equally and the uncertainties in the respective source are propagated through the pooling formulas to give composite mean, medium, variance, and intervals that reflect the overall uncertainty. Otherwise, the analyst may want to assign weights to the various sources in proportion to their respective applicability or accuracy.

Likewise, if multiple sources are judged equally accurate, the equal-weight pooling can be used.

The uncertainty in the applicability of a particular information source to an event in the PSA for a repository is also treated by analyst judgement. In some instances, this may require increasing an estimated event probability derived from a given source to account for repository operating environment or duty. In other instances, the probability may be

decreased for the same reasons, or to take credit for quality assurance, expected tests, and inspections. For example, crane failure rates derived from general industrial sources may be judged to be too high for repository cranes that are designed to nuclear industry standards. The analyst must decide on whether to increase (decrease) the point estimate, the upper or lower uncertainty bounds, or both, to account for the application. Section 9 provides guidance to the analyst on such treatment of uncertainties.

7.5.3.3.5 Documentation of Parameters and Event Probabilities

To support the PSA for LA, the analyst must provide a clear, auditable record. For each event identified in the PSA event sequence analyses, an event probability (or frequency) will be tabulated.

The tabulation will be annotated to point to, for each event probability, the following:

- Event Model Used
- Information Source(s) Used
- Calculation File for Estimation of Model Parameters and Event Probability
- Treatment and Bases for Uncertainties.

Such documentation will be prepared and checked in accordance with the applicable procedure.

7.5.3.4 Examples of Parameter Estimation – Contrast of Classical and Bayesian Methods

This section presents several simple applications of the estimation methods described in Sections 7.5.4.3.1 and 7.5.4.3.2. Examples are presented for both a failure-on-demand and constant failure rate models using both classical and Bayesian approaches. For the latter, applications of noninformative and other prior distributions are illustrated.

The basic information assumed is either repository-specific (or ESF-specific) performance records or representative surrogates (e.g., records of events related to failures of spent fuel handling equipment at NPPs). Two basic information sets are used in the examples below:

Failure on Demand—Crane drop of load - 0 failures in 47,400 lifts (surrogate information; Lloyd 2001).

This information will be augmented with alternative information in the demonstration of pooling information.

Constant Failure Rate—Failure of steel sets in ESF ground support system; experience gives 0 failures in 9200 steel-set years (BSC 2001).

7.5.3.4.1 Estimation of Parameters - Failure on Demand

Classical Estimation—(see Section 7.5.3.3.1).

Point Estimate:

$$p^* = f/n$$

(Eq. 7-137)

where

f = number of observed or recorded failures in n demands or trials,
 n = number of recorded demands or trials in reporting period.

For small f and large n , the 5th to 95th percentile interval ($\alpha = 0.05$) may be approximated using the following:

$$p_U(1 - \alpha) = [\chi^2(2f + 2, 1 - \alpha)]/2n = [\chi^2(2f + 2, 0.95)]/2n \quad (\text{Eq. 7-138})$$

$$p_L(1 - \alpha) = [\chi^2(2f, \alpha)]/2n = [\chi^2(2f, 0.05)]/2n \quad (\text{Eq. 7-139})$$

Basis: Crane drop of load (0 failures in 47,400 lifts) or:

$$f = 0$$

$$n = 47,400$$

Initial Trial: Insert information into formulas:

$$p_i^* = f/n = 0/47,400 = 0, \text{ which is not credible, while}$$

$$p_U = 6.3 \times 10^{-5}, \text{ and}$$

$$p_L \text{ is indeterminate, that is, } \chi^2(0, 0.05) \text{ cannot be determined.}$$

Second Trial: Assume that there will be a failure on the next demand, so adjust input to:

$$f' = f + 1, \text{ and } n' = 47,400 + 1$$

using Equations 7-75 and 7-76 the estimation gives:

$$p^* = f'/n' = 1/47,401 = 2.1 \times 10^{-5} \text{ (point estimate)}$$

and the 90% confidence interval is given by

$$p_U = [\chi^2(2f' + 2, 0.05)]/2n' = [\chi^2(4, 0.05)]/94802 = 9.49/94802 = 1.0 \times 10^{-4}$$

$$p_L = [\chi^2(2f', 0.95)]/2n' = [\chi^2(2, 0.95)]/94802 = 0.71/94802 = 1.08 \times 10^{-6}$$

Now, the point estimate p^* is more useful (i.e., not equal to 0) and appears more credible (i.e., no equipment is perfect), and the point estimate falls within and interval that has a very low lower bound and a conservative upper bound.

Bayesian Estimation—(see Section 7.5.3.3.4.1).

The first case is application of a noninformative prior:

$$[q(1 - q)]^{-0.5}/\pi; \text{ for } (0 \leq q \leq 1) \quad (\text{Eq. 7-140})$$

The evidence gives:

$f = 0$, number of observed or recorded failures in n demands or trials, and
 $n = 47,400$, number of recorded demands or trials in reporting period. Using
 Equation 7-97 to 7-101 the Bayesian estimation gives:

$$\text{Posterior mean: } q = (f + 0.5)/(n + 1) = (0.5)/47,401 = 1.05 \times 10^{-5} \quad (\text{Eq. 7-141})$$

$$\begin{aligned} \text{Posterior median: } q_{0.5} &= (f + 0.5)/[(f + 0.5) + (n - f + 0.5)F_{0.5}(2n - 2f + 1, 2f + 1)] \quad (\text{Eq. 7-142}) \\ &= (0.5)/[(0.5) + (47,400 + 0.5)F_{0.5}(94801, 1)] \\ &= 2.32 \times 10^{-5} \end{aligned}$$

and the 90 percent symmetric probability is a function of the F-distribution with a and b degrees of freedom, $F_{1-\gamma/2}(a, b)$, as follows:

Posterior lower bound:

$$\begin{aligned} q_L &= (0.5)/[(0.5) + (47400.5)F_{0.05}(94801, 1)] \quad (\text{Eq. 7-143}) \\ &= 4.15 \times 10^{-8} \end{aligned}$$

Posterior upper bound:

$$\begin{aligned} q_U &= [(f + 0.5)F_{0.05}(1, 94801)]/[(47400.5) + (0.5)F_{0.05}(1, 94801)] \quad (\text{Eq. 7-144}) \\ &= 4.05 \times 10^{-5} \end{aligned}$$

The noninformative prior is very useful when the available performance records show zero.

The Bayesian approach shifts the estimation toward lower points values and intervals. This result may be viewed as a better result given that no failures were observed. By selecting the noninformative prior, the analyst says "The probability of failure, q , is between 0 and 1. I am confident that q can not be 0, because nothing is perfect, and I am confident that it can not be approaching 1.0, because then there would be many observed failures." Using the evidence of zero failures for the large number of trials gives a point estimate that is approximately half of the classical estimate with one assumed failure (the Bayesian approach does not require this arbitrary assumption). Moreover, the upper 95th percent limit is 4.05×10^{-5} versus 1.0×10^{-4} from the classical estimation. The lower 5th percent limit is 4.15×10^{-8} , which can be regarded as approaching 0 versus the larger value of 1.08×10^{-6} from the classical approach.

7.5.3.4.2 Estimation of Parameters – Constant Failure Rate

[Information for this section is under development and will be provided later]

7.5.3.4.3 Estimation of Parameters – Pooling Information

Table 7-8 presents crane failure on demand rates as derived from three different sources. The Bayesian approach with noninformative prior was applied, independently, to each set of the raw information to get the posterior parameters shown in the table. These three set of parameters were processed this way to simulate how the analyst might find different sets of processed data

(e.g., in the generic databases described in Section 7.5.3.2.2). The purpose here is to demonstrate the result of combining tabulated information sources. When the source provides the raw information, it may be more appropriate to apply a successive Bayesian update, as shown below.

For demonstration information is pooled using the geometric mean (see Section 7.5.3.3.1)

$$\langle q_0 \rangle = (\prod q_{0,i})^{1/M}; \text{ for the composite point value} \quad (\text{Eq. 7-145})$$

$$\langle q_{LB} \rangle = (\prod q_{LB,i})^{1/M}; \text{ for the composite lower bound} \quad (\text{Eq. 7-146})$$

$$\langle q_{UB} \rangle = (\prod q_{UB,i})^{1/M}; \text{ for the composite upper bound} \quad (\text{Eq. 7-147})$$

Where $q_{0,i}$, $q_{LB,i}$, and $q_{UB,i}$ are the point value, lower bound, and upper bound, respectively from the i^{th} information source.

In this example, $M = 3$.

Using the mean values in Table 7-8 gives the following composite parameter estimates:

$$\begin{aligned} \langle q_0 \rangle &= [(1.44 \times 10^{-5}) (4.97 \times 10^{-5}) (1.05 \times 10^{-5})]^{1/3} &&= 1.96 \times 10^{-5} \\ \langle q_{LB} \rangle &= [(8.6 \times 10^{-6}) (3.80 \times 10^{-5}) (4.15 \times 10^{-5})]^{1/3} &&= 2.38 \times 10^{-6} \\ \langle q_{UB} \rangle &= [(2.14 \times 10^{-5}) (6.27 \times 10^{-5}) (4.05 \times 10^{-5})]^{1/3} &&= 3.79 \times 10^{-5} \end{aligned}$$

Table 7-8. Crane Failure Demand Rates

Source	Failures	Trials	Posterior		
			Using Noninformative Prior		
Event: Drop of Load by Crane			Mean	Lower 5%	Upper 95%
Newport News (CRWMS M&O 1998, Attachment X)	13	939,000	1.44E-5	8.60E-6	2.14E-5
NUREG-0612 (NRC 1980)	43	8.75E+5	4.97E-5	3.80E-5	6.27E-5
Lloyd (2001)	0	47,400	1.05E-5	4.15E-8	4.05E-5

INTENTIONALLY LEFT BLANK

7.6 EVENT SEQUENCE FREQUENCY BINNING

7.6.1 Purpose

This guide defines the bases and methods for applying the results of ET sequence quantification to categorize (or bin) credible event sequences as Category 1 or Category 2 according to the definitions of 10 CFR 63.2. Potential radiological consequences of the event sequences are then subject to the performance criteria of 10 CFR 63.111. Event sequences that are not Category 1 or Category 2 are categorized as BC2 and are not subjected to performance criteria. Since there are various degrees of uncertainty associated with the quantification of event sequence frequencies, this guide recommends means for dealing with uncertainty factors in categorizing sequences.

7.6.2 Scope

This section provides guidance on interpreting and using the results of ET analyses performed in accordance with Section 7.1, and considerations of uncertainties per Section 9. This section does not describe ET construction or analysis.

7.6.3 Overview of Approach

The results of ET analyses, in addition to the graphical display of the alternative sequences (or scenarios) that can result following a particular IE, include calculations of the frequency (or annual probability of occurrence) of all sequences that are modeled. The sum of the frequencies of all sequences equals that of the IE frequency.

The endpoint of each pathway through the ET represents a particular state of the system being analyzed. Each endpoint state has a measure of radiological consequence (or performance) associated with it; in most instances, the radiological consequences are nil (all consequences prevented or mitigated) or very small (mitigation features are effective). The 10 CFR Part 63 is a risk-informed, performance-based rule that imposes performance objections according the FC of each event sequence that results in radiological exposure or releases. The Category 1 and Category 2 event sequences form the bases for defining the 10 CFR 63.2 design basis for a repository, and in classifying the SSCs important to safety that are associated with prevention and mitigation of events that make up the various event sequences.

For event sequences that are below the threshold FC-2 event sequences (i.e., BC2 event sequences), there are no radiological performance requirements in 10 CFR Part 63. However, the SSCs that are credited in the frequency analyses of BC2 event sequences may be subject to classification as important to safety.

Since there are various degrees of uncertainty associated with the quantification of event sequence frequencies, it is necessary to deal with uncertainty factors in categorizing sequences. That is, a point estimate (or best estimate) of an event frequency may result in a value that is slightly below the threshold of Category 2. Should this sequence be declared to be a BC2 or Category 2 event sequence in view of the degree of uncertainty in the frequency analysis? Or, another sequence may be slightly below the breakpoint between Categories 1 and 2. Should this sequence be categorized as Category 1 or Category 2 in view of the degree of uncertainty in the

frequency analysis? This guide provides a basis for answering such questions. The treatment of uncertainties differs for analyses performed in support of LA submittal for CA versus the analyses for the support of a LA to receive and possess nuclear materials.

7.6.4 Details of Approach

7.6.4.1 Fundamental Screening Criteria

Event sequence Category 1 and Category 2 are defined by 10 CFR 63.2 (see Sections 2 and 3). If a 100-year period before permanent closure is used as a basis, then frequency bounds can be defined for the respective event sequence categories as

$$\text{Category 1: } f(\text{event sequence}) \geq 1 \times 10^{-2} \text{ per year} \quad (\text{Eq. 7-148})$$

$$\text{Category 2: } 1 \times 10^{-2} > f(\text{event sequence}) \geq 1 \times 10^{-6} \text{ per year}$$

This guide will use these definitions as Fundamental Screening Criteria in the context of event sequence frequency binning.

It is noted, however, that other preclosure time periods may be defined for all or portions of operations, but the principles described herein are to be applied to those time bases, nevertheless. See Section 3.4 for a discussion of preclosure time periods.

This guide is based on quantitative evaluations of event sequence frequencies. Alternative approaches using qualitative arguments could be considered, if they satisfy all the requirements of 10 CFR Part 63 for performing a PSA. Such alternative approaches are not addressed.

7.6.4.2 Screening Criteria with Consideration of Uncertainties

Section 9 describes methods for identifying sources of uncertainty in event sequence modeling and Section 7.5 discusses uncertainty in probabilities of basic events that are input to FTA (Section 7.2) and HRA (Section 7.3).

In formal analysis of uncertainties, results of event sequence quantification are expressed in the form of a probability distribution. The complementary cumulative probability distribution represents the probability (between 0 and 1) that the frequency (of a given sequence of events) is less than or equal to a particular value. The point estimates derived in preliminary sequence quantification will fall near the middle of the distribution, often being the true median (i.e., the frequency corresponding to a probability of 0.5).

The PSA that supports the LA for construction authorization will categorize event sequences based on the mean value of the sequence frequencies. The mean is a probability-weighted measure of an event-sequence frequency over the range and distribution of uncertainties. Section 9 describes the general treatment of uncertainties and illustrates the significance of the mean as a measure of the true value of an event-sequence frequency. If the mean is less than the threshold frequency for Category 1 event sequences, the sequence is designated Category 2. If the mean is less than the threshold frequency for Category 2 event sequences, the sequence is designated Beyond Category 2.

7.6.4.3 Beyond Category 2 Event Sequences: Quantitative Screening

7.6.4.3.1 Application of Fundamental Screening Criteria

This category (bin) of event sequences is addressed first because the quantitative approach supplements the hazards analyses for event sequence screening. The fundamental criterion for screening out a potential event sequence is the following:

A BC2 event sequence consists of an IE and one or more additional events whose joint frequency is less than 1×10^{-6} per year.

This is expressed mathematically as:

If $f(\text{sequence})$ is less than 1×10^{-6} per year,
then the sequence is considered to be BC2.

where

$f(\text{sequence})$ = frequency of the event sequence.

If, however, $f(\text{sequence}) = 1 \times 10^{-6}$ per year, the test fails and the sequence must be included as a Category 2 event sequence. The test is applied to the frequencies of every sequence modeled in an ET.

7.6.4.3.2 Consideration of Uncertainties in Beyond Category 2 Event Sequences: Screening and Stopping Rules

Stopping Rule—10 CFR 63.112(d) requires that the PSA include the technical basis for either inclusion or exclusion of specific, naturally occurring and human-induced hazards in the safety analysis.

This has been interpreted to mean that the NRC expects the PSA to tabulate those sequences that have been declared BC2 and to provide the bases. To avoid having an infinitely long list of sequences to pedigree that includes sequences of extremely small frequencies, it is necessary to define a lower limit on sequence frequency to be documented. This is termed a stopping rule. The definition and application of the stopping rule must be compatible with considerations of uncertainties. The following is the stopping rule recommended for use in use in preliminary documentation of the PSA:

No event sequence having a mean frequency less than 1×10^{-8} per year will be included in the list of BC2 event sequences.

No uncertainty analysis will be applied in executing the stopping rule. This stopping rule provides two orders of magnitude below the Category 2 lower threshold, which is a wide margin.

Note that the stopping rule can be applied during ET construction and preliminary quantification as a means of simplifying the ETs. Tree branches that are readily seen to be on the order of 10^{-8} per year can be pruned from the tree.

As design evolves and uncertainties are reduced, or formal uncertainty analyses are applied, the cutoff frequency for the mean sequence frequency may be raised to 1×10^{-7} per year.

7.6.4.3.3 Identifying Controls Credited for Prevention or Mitigation of Beyond Category 2 Event Sequences

Except for event sequences that are below 1×10^{-8} per yr (i.e, per the stopping rule), the events comprising each of the documented BC2 event sequences must be examined to identify items important to safety.

The primary evaluation assesses the effect on sequence frequency for each event in the sequence, other than the IE, when the event probability is set equal to 1.0. If the recalculated mean sequence frequency is greater than the Category 2 threshold (10^{-6} per year) for any one item (e.g., an SSC, or a specific HA), then a coarse estimate of potential consequences is made. If the consequences appear to exceed the regulatory limits, then the item represented by that event may be subject to classification as an potential item important to safety and appropriate controls (e.g., quality assurance controls). If the consequences appear to be within regulatory limits for Category 2, then no such classification is necessary (see Section 12 for the discussion of the classification process).

When the event probability within an event sequence is set equal to 1.0 for a given item and the recalculated mean sequence frequency remains below the Category 2 threshold (10^{-6} per year) with sufficient margin, then no further action is required.

7.6.5 Examples of Application

[Information for this section is under development and will be provided later.]

7.7 REFERENCES

7.7.1 Documents Cited

AIChE (American Institute of Chemical Engineers) 1989. "Partial List of External Events." Table 3.13 of *Guidelines for Chemical Process Quantitative Risk Analysis*. New York, New York: American Institute of Chemical Engineers. TIC: 241701.

Arno, R.G. 1981. *Nonelectronic Parts Reliability Data*. NPRD-2. 24, 25. Griffiss Air Force Base, New York: Reliability Analysis Center. TIC: 245435.

Benhardt, H.C.; Eide, S.A.; Held, J.E.; Olsen, L.M.; and Vail, R.E. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)*. WSRC-TR-93-581. Aiken, South Carolina: Westinghouse Savannah River Company.

Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U)*. WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.

BSC (Bechtel SAIC Company) 2001. *Analysis of Preclosure Design Basis Rock Fall onto Waste Package*. ANL-EBS-MD-000061 REV 00. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20011127.0110.

CRWMS M&O (Civilian Radioactive Waste Management Systems Management and Operating Contractor) 1997. *Application of Logic Diagrams and Common-Cause Failures to Design Basis Events*. BCA000000-01717-0200-00018 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980206.0272.

CRWMS M&O 1998. *Preliminary Preclosure Design Basis Event Calculations for the Monitored Geologic Repository*. BC0000000-01717-0210-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19981002.0001.

CRWMS M&O 2000. *Subsurface Transporter Safety Systems Analysis*. ANL-WER-ME-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000225.0052.

DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment and Production*. MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.

Eide, S.A. and Calley, M.B. 1993. "Generic Component Failure Data Base." *PSA '93, Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, Clearwater Beach, Florida, January 26-29, 1993*. 2, 1175-1182. La Grange Park, Illinois: American Nuclear Society. TIC: 247455.

Eide, S.A., S.T. Khericha, M.B. Calley, and D. A. Johnson 1993. *Component External Leakage and Rupture Frequency Estimates*. Proceedings Probabilistic Safety Assessment and Management, PSA'93. American Nuclear Society, Clearwater Beach, Florida, January, 1993.

Hannaman, G.W. and Spurgin, A.J. 1984. *Systematic Human Action Reliability Procedure (SHARP)*. EPRI-NP-3583. Palo Alto, California: Electric Power Research Institute.

IEEE Std 500-1984. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 240502.

IEEE Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205.

INEEL (Idaho National Engineering and Environmental Laboratory) 1989. *Nuclear Computerized Library for Assessing Reactor Reliability*. NUREG/CR-4639. Washington, D.C.: U.S. Nuclear Regulatory Commission.

Joksimovich, V.; Orvis, D.; and Moieni, P. 1993. *Safety Culture Assurance via Integrated Risk Management Programs*. Proceedings of the International Topical Meeting on Probabilistic Safety Management. Clearwater Beach, Florida: American Nuclear Society.

Lloyd, R.L. 2001. *Technical Assessment Generic Issue 186 Potential Risk and Consequences of Heavy Load Drops in Nuclear Power Plants*. Pre-Draft NUREG-xxxx (ML012620352). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Martz, H.F. and Waller, R.A. 1978. *An Exploratory Comparison of Methods for Combining Failure-Rate Data from Different Data Sources*. LA-7556-MS. Los Alamos, New Mexico: Los Alamos Scientific Laboratory.

Moieni, P., Spurgin, A.J., and Singh, A. 1994. "Advances in Human Reliability Analysis Methodology." *Reliability Engineering and System Safety*, 44, (1994), 27-55, 57-66. Dublin, Northern Ireland: Elsevier Science Limited.

Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Procedural Framework and Examples*. Volume 1 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

NRC (U.S. Nuclear Regulatory Commission) 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH-1400. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 236923.

NRC 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624. Washington, D.C.: U.S. Nuclear Regulatory Commission.

Russell, K.D.; Kvarfordt, K.J.; Skinner, N.L.; Wood, S.T.; and Rasmuson, D.M. 1994. *Integrated Reliability and Risk Analysis System (IRRAS) Reference Manual*. Volume 2 of *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE), Version 5.0*. NUREG/CR-6116. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249497.

Swain, A.D. and Guttman, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*. NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.

Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook*. NUREG - 0492. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 208328.

Wakefield, D.J.; Parry, G.W.; Spurgin, A.J.; and Moieni, P. 1992. *Systematic Human Action Reliability Procedure (SHARP) Enhancement Project: SHARPI Methodology Report*. EPRI-RP-3206-01. Palo Alto, California: Electric Power Research Institute.

Watson, I.A. 1987. "Analysis of Dependent Events and Multiple Unavailabilities with Particular Reference to Common Cause Failures." *The SRS Quarterly Digest, 1987*, (February), . Warrington, United Kingdom: Systems Reliability Service, National Centre of Systems Reliability.

7.7.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada.

INTENTIONALLY LEFT BLANK

APPENDIX 7A

BIBLIOGRAPHY OF INFORMATION SOURCES

- AIChE. *Guidelines for Process Equipment Reliability Data with Data Tables*. Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York, NY. 1989.
- Arno, R.G. 1981. *Nonelectronic Parts Reliability Data*. NPRD-2. 24, 25. Griffiss Air Force Base, New York: Reliability Analysis Center. TIC: 245435.
- Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U)*. WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.
- Dexter, A. H. and W. C. Perkins. *Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant*. E.I. du Pont de Nemours, Savannah River Laboratory. July 1982.
- DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment and Production*. MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.
- Eide, S.A. and Calley, M.B. 1993. "Generic Component Failure Data Base." *PSA '93, Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, Clearwater Beach, Florida, January 26-29, 1993*. 2, 1175-1182. La Grange Park, Illinois: American Nuclear Society. TIC: 247455.
- Eide, S.A. , S.T. Khericha, M.B. Calley, and D. A. Johnson (1993). *Component External Leakage and Rupture Frequency Estimates*. Proceedings Probabilistic Safety Assessment and Management, PSA'93. American Nuclear Society, Clearwater Beach, Florida, January, 1993.
- IEEE Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205.
- IEEE 1983. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Station*. IEEE Std 500-1984. The Institute of Electrical and Electronic Engineers, Inc.
- INEEL (Idaho National Engineering and Environmental Laboratory) 1989. *Nuclear Computerized Library for Assessing Reactor Reliability*. NUREG/CR-4639. Washington, D.C.: U.S. Nuclear Regulatory Commission.
- NRC 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH 1400/NUREG75/014. U.S. Nuclear Regulatory Commission.
- WIPP Safety Analysis.

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMNS	iii
8. CONSEQUENCE ANALYSIS	8-1
8.1 INTRODUCTION	8-1
8.2 EXAMPLES OF SOURCE TERMS	8-2
8.2.1 Source Terms for Commercial Spent Nuclear Fuel and Crud	8-2
8.2.2 Source Terms for U.S. Department of Energy Spent Nuclear Fuel	8-6
8.2.3 Source Terms for Vitrified High-Level Radioactive Waste	8-7
8.2.4 Source Terms for Plutonium Disposition Waste Form	8-7
8.3 CATEGORY 1 OFFSITE DOSES	8-7
8.3.1 GENII-S Dose Calculation Methodology	8-7
8.3.2 Dose Conversion Factors	8-9
8.3.3 Atmospheric Dispersion Factors	8-10
8.3.4 Breathing Rate	8-10
8.3.5 Category 1 Event Sequences	8-11
8.3.6 Uncertainty in Consequence Analysis	8-11
8.3.7 Category 1 Dose Calculation Examples	8-11
8.4 CATEGORY 2 OFFSITE DOSES	8-16
8.4.1 Category 2 Event Dose Calculation Methodology	8-17
8.4.2 Dose Conversion Factors	8-19
8.4.3 Atmospheric Dispersion Factors	8-19
8.4.4 Breathing Rate	8-20
8.4.5 Category 2 Event Sequences	8-20
8.4.6 Uncertainty in Consequence Analysis	8-20
8.4.7 Category 2 Dose Calculation Example	8-21
8.5 CATEGORY 1 WORKER DOSES AND EXPOSURES	8-24
8.6 RELEASE FRACTIONS	8-25
8.6.1 Commercial Spent Nuclear Fuel Release Fractions	8-25
8.6.2 U.S. Department of Energy Spent Nuclear Fuel Release Fractions	8-26
8.7 MITIGATION FACTOR	8-26
8.8 REFERENCES	8-27
8.8.1 Documents Cited	8-27
8.8.2 Codes, Standards, Regulations, and Procedures	8-29
8.8.3 Source Data	8-29

TABLES

	Page
8-1 Dose Criteria for Category 1 and Category 2 Event Sequences	8-2
8-2 Example of Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) Spent Nuclear Fuel (SNF) Radionuclide Inventories.....	8-3
8-3 Example of Category 1 Crud Source Term Calculations.....	8-6
8-4 Example of High-Level Radioactive Waste Activity (Curies Per Canister).....	8-8
8-5 Example of Annual Releases from the Subsurface Due to Normal Operations	8-12
8-6 Example of Calculating Annualized Cesium-137 Release for Category 1 Event Sequences.....	8-13
8-7 Example of Source Terms for GENII-S Computer Runs	8-14
8-8 Inhalation Dose Calculation Example	8-22
8-9 Submersion Dose Calculation Example.....	8-23
8-10 Example of Dose Summary Table	8-23
8-11 Example of CSNF Release Fractions in Air for Category 2 Event Sequences.....	8-26

ACRONYMS

ARF	airborne release fraction
BWR	boiling water reactor
CDE	committed dose equivalent
CEDE	committed effective dose equivalent
CI/FA	curies per fuel assembly
CR	cladding release fraction
CSNF	commercial spent nuclear fuel
DCF	dose conversion factor
DDE	deep-dose equivalent
DEP	deposition factor
DF	damage fraction
DOE	U.S. Department of Energy
DSNF	DOE spent nuclear fuel
EDE	effective dose equivalent
HEPA	high efficiency particulate air
LDE	lens dose equivalent
NRC	U.S. Nuclear Regulatory Commission
PWR	pressurized water reactor
RF	respirable fraction
SDE	skin dose equivalent
SNF	spent nuclear fuel
TEDE	total effective dose equivalent
WHB	Waste Handling Building
YMP	Yucca Mountain Site Characterization Project

INTENTIONALLY LEFT BLANK

8. CONSEQUENCE ANALYSIS

8.1 INTRODUCTION

The consequence analysis demonstrates that the preclosure performance objectives for the repository operations area, specified in 10 CFR 63.111, have been met. Dose criteria specified in 10 CFR Part 63 and 10 CFR Part 20 (Table 8-1) specify the offsite and worker dose limits during normal operations and for Category 1 event sequences, and the offsite dose limits for Category 2 event sequences.

In this section, the methodology for calculating offsite doses for Category 1 and Category 2 event sequences and for calculating worker doses for Category 1 event sequences is presented. Because the regulatory limit for Category 2 event sequences is a total effective dose equivalent (TEDE) of 5 rem per event (10 CFR 63.111), the doses due to Category 2 event sequences are calculated on a per event basis. The regulatory limit for Category 1 event sequences is an annual TEDE of 15 mrem per year (10 CFR 63.111). Therefore, all Category 1 event sequence doses are calculated on a per year basis. It should be noted that the data presented in Section 8 is preliminary in nature and should not be interpreted as the final data to be used in the final design.

Four dose measures applicable to Category 1 and Category 2 event sequences include:

- **The TEDE**—For purposes of assessing doses to workers, the TEDE is equal to the sum of the deep-dose equivalent (DDE) (for external exposures) and the committed effective dose equivalent (CEDE) (for internal exposures) (10 CFR 63.2). For purposes of assessing doses to members of the public, the TEDE is equal to the sum of the effective dose equivalent (EDE) (for external exposures) and the CEDE (10 CFR 63.2). The CEDE is calculated using the effective inhalation dose conversion factor (DCF). The EDE is calculated using the effective air submersion DCF. For normal operations and Category 1 event sequences, the TEDE also includes ingestion and groundshine doses in addition to inhalation and submersion doses. In assessing compliance with the individual radiation protection standard, the DDE is replaced by the EDE per the U.S. Nuclear Regulatory Commission (NRC) guidance on the use of the DDE and EDE for external exposure (66 FR 55732).
- **The Highest of the Committed Dose Equivalents (CDEs) plus the DDE**—The organs evaluated to determine the highest CDEs are the lungs, breasts, gonads, red marrow, bone surface, thyroid, and remainder. The remainder is not an organ, but rather a weighted combination of the five remaining organs or tissues (e.g., liver, kidneys, spleen, and brain, but excluding skin, lens of the eye, and the extremities) receiving the highest doses (Eckerman et al. 1988). The DDE, which is added to the highest CDE, is equal to that used to calculate the TEDE. In assessing compliance with the individual radiation protection standard, the DDE is replaced by the EDE per the NRC guidance on the use of the DDE and EDE for external exposure (66 FR 55732).
- **Lens of the Eye**—In Federal Guidance Report 11 (Eckerman et al. 1988), only one lens of the eye DCF (i.e., Kr-83m) can be found. The lens dose equivalents (LDEs) are not calculated using the lens of the eye DCFs, as the lens of the eye DCFs given in Federal

Guidance Report 11 (Eckerman et al. 1988) are incomplete. However, in NUREG-1567 (NRC 2000), it is stated that compliance with the lens of the eye dose limit is achieved if the sum of the skin dose equivalent (SDE) and the TEDE does not exceed 15 rem.

- **Skin and Extremities**—The dose to the skin and extremities is only due to the air submersion pathway. SDEs are calculated using the DCFs for air submersion in Federal Guidance Report 12 (Eckerman and Ryman 1993).

Table 8-1. Dose Criteria for Category 1 and Category 2 Event Sequences

Event Sequence Type	Dose Type	Dose Criteria	
		Worker ^a	Offsite ^b
Category 1	1. Annual TEDE during normal operations and for Category 1 event sequences; 2. Aggregate TEDE for Category 1 event sequences	—	15 mrem/yr
Category 1	TEDE	5 rem/yr	100 mrem/yr
Category 1	CDE + DDE	50 rem/yr	—
Category 1	Lens of the Eye	15 rem/yr	—
Category 1	Skin & Extremities	50 rem/yr	—
Category 1	External Dose: Highest of DDE, Skin Dose, or Dose to Lens of the Eye	—	2 mrem/hr
Category 2	TEDE	—	5 rem/event
Category 2	CDE + DDE	—	50 rem/event
Category 2	Lens of the Eye	—	15 rem/event
Category 2	Skin & Extremities	—	50 rem/event

^a 10 CFR 20.1201

^b 10 CFR 20.1301, 10 CFR 63.111, and 10 CFR 63.204

8.2 EXAMPLES OF SOURCE TERMS

8.2.1 Source Terms for Commercial Spent Nuclear Fuel and Crud

Commercial Spent Nuclear Fuel (CSNF)—Examples of average and maximum source terms for pressurized water reactor (PWR) and boiling water reactor (BWR) CSNF can be found in *PWR Source Term Generation and Evaluation* (CRWMS M&O 1999a) and *BWR Source Term Generation and Evaluation* (CRWMS M&O 1999b). Future revisions to these documents should be referenced as needed.

The SAS2H sequence in SCALE V4.3 (CRWMS M&O 1997) was used to calculate the PWR and BWR source terms (CRWMS M&O 1999a and 1999b) for selected fuel assemblies as a function of assembly average burnup and cooling time. The prime functional module of the SAS2H code sequence utilized is the ORIGEN-S code. This code performs a point depletion and decay calculation of a selected fuel type with user-specified irradiation conditions and decay times. The resulting source terms are then extracted from the SAS2H output and used as input to consequence analysis.

For preclosure consequence analysis, source terms for PWR and BWR spent fuel assemblies with four different combinations of initial enrichment, burnup, and decay time should be considered:

Assembly	Percent	GWd/MTU	Years
Average PWR	4.0	48	25
Maximum PWR	5.0	75	5
Average BWR	3.5	40	25
Maximum BWR	5.0	75	5

Example of Source Term Usage—Average PWR fuel was selected for consequence analysis of all Category 1 event sequences because it was found to result in a higher offsite dose consequence as compared to average BWR fuel (BSC 2001). This result is generally attributed to a higher enrichment, burnup, and concentration of long-lived radionuclides in PWR fuel.

For Category 2 event sequences, either the maximum PWR fuel or the maximum BWR fuel was used to calculate maximum doses, depending on which source term results in the highest dose. For events occurring in spent fuel pools, maximum PWR fuel results in the largest offsite dose due to the larger inventory of radioactive gases compared to maximum BWR fuel (BSC 2001). For events involving particulate releases in a dry environment (e.g., hot cell), however, maximum BWR fuel results in a larger offsite dose than maximum PWR fuel because of the increased crud inventory (BSC 2001). For Category 2 event sequences, mean doses should also be calculated using the average PWR or average BWR fuel. These mean doses will be compared with the regulatory dose limits given in Table 8-1.

Radionuclide inventories in curies per fuel assembly (Ci/FA) for each nuclide and fuel type evaluated are presented in Table 8-2. These radionuclide inventories were used in site recommendation public and worker dose calculations, and they may be revised later for license application.

Table 8-2. Example of Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) Spent Nuclear Fuel (SNF) Radionuclide Inventories

Nuclide	Average PWR (Ci/FA)	Maximum PWR (Ci/FA)	Average BWR (Ci/FA)	Maximum BWR (Ci/FA)
Ac-227	1.61E-05	0.00E+00	0.00E+00	0.00E+00
Am-241	1.98E+03	8.71E+02	5.58E+02	2.66E+02
Am-242m	6.39E+00	1.02E+01	2.17E+00	3.40E+00
Am-243	2.20E+01	5.22E+01	5.35E+00	1.93E+01
C-14	3.32E-01	4.89E-01	1.75E-01	3.16E-01
Cd-113m	7.66E+00	3.82E+01	2.26E+00	1.39E+01
Cl-36	6.80E-03	9.69E-03	2.93E-03	4.99E-03
Cm-242	5.27E+00	3.43E+01	1.79E+00	1.13E+01
Cm-243	1.03E+01	3.83E+01	2.48E+00	1.12E+01
Cm-244	1.36E+03	1.12E+04	2.56E+02	3.95E+03
Cm-245	3.07E-01	1.41E+00	4.04E-02	3.54E-01
Cm-246	1.04E-01	8.38E-01	1.45E-02	2.97E-01
Co-60	3.13E+02	5.66E+03	4.40E+01	8.56E+02

Table 8-2. Example of Pressurized Water Reactor and Boiling Water Reactor Spent Nuclear Fuel Radionuclide Inventories (Continued)

Nuclide	Average PWR (Ci/FA)	Maximum PWR (Ci/FA)	Average BWR (Ci/FA)	Maximum BWR (Ci/FA)
Cs-134	2.52E+01	3.72E+04	6.32E+00	1.16E+04
Cs-135	3.50E-01	5.99E-01	1.39E-01	2.82E-01
Eu-155	5.16E+01	1.68E+03	1.64E+01	6.37E+02
Fe-55	3.47E+00	6.84E+02	1.09E+00	2.35E+02
H-3	1.14E+02	4.72E+02	3.95E+01	1.76E+02
I-129	2.20E-02	3.38E-02	7.43E-03	1.36E-02
Kr-85	1.13E+03	5.63E+03	3.81E+02	2.03E+03
Nb-93m	1.30E+01	4.54E+01	4.74E-01	1.22E+00
Nb-94	8.39E-01	1.27E+00	1.87E-02	3.39E-02
Ni-59	2.09E+00	2.78E+00	5.03E-01	7.80E-01
Ni-63	2.52E+02	4.16E+02	5.87E+01	1.16E+02
Np-237	2.47E-01	3.85E-01	6.89E-02	1.33E-01
Pa-231	2.97E-05	4.25E-05	1.39E-05	2.94E-05
Pb-210	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Pd-107	8.41E-02	1.45E-01	2.65E-02	5.70E-02
Pm-147	1.19E+02	2.34E+04	3.98E+01	7.46E+03
Pu-238	2.29E+03	6.16E+03	5.85E+02	2.11E+03
Pu-239	1.77E+02	1.85E+02	5.35E+01	5.36E+01
Pu-240	3.18E+02	3.90E+02	1.14E+02	1.48E+02
Pu-241	2.47E+04	7.91E+04	6.78E+03	2.25E+04
Pu-242	1.64E+00	3.01E+00	5.09E-01	1.26E+00
Ra-226	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Ra-228	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Ru-106	1.23E-02	1.27E+04	3.00E-03	3.29E+03
Sb-125	9.71E+00	2.05E+03	2.89E+00	6.21E+02
Se-79	4.57E-02	6.95E-02	1.59E-02	2.89E-02
Sm-147	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Sm-151	2.11E+02	3.13E+02	5.39E+01	8.22E+01
Sn-126	3.85E-01	6.28E-01	1.27E-01	2.52E-01
Sr-90	2.72E+04	6.30E+04	9.54E+03	2.52E+04
Tc-99	8.99E+00	1.28E+01	3.20E+00	5.35E+00
Th-229	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Th-230	1.48E-04	3.56E-05	6.09E-05	2.05E-05
Th-232	0.00E+00	0.00E+00	0.00E+00	0.00E+00
U-232	2.05E-02	5.31E-02	4.64E-03	2.00E-02
U-233	4.07E-05	2.42E-05	1.14E-05	0.00E+00
U-234	6.77E-01	5.46E-01	2.49E-01	2.26E-01
U-235	7.36E-03	4.15E-03	2.62E-03	9.40E-04
U-236	1.72E-01	2.24E-01	6.26E-02	9.55E-02
U-238	1.48E-01	1.43E-01	6.32E-02	6.07E-02
Zr-93	8.94E-01	1.33E+00	3.38E-01	6.03E-01

Source: CRWMS M&O 1999a; CRWMS M&O 1999b.

Crud—Crud is a corrosion product that has been found on the exterior surface of spent nuclear fuel (SNF) assemblies due to irradiation and imperfect water chemistry control in the reactor coolant system. Crud can be released to the environment during an accident involving CSNF at the potential repository.

After decaying for five years, the nuclide species that have significant activity in the crud are Fe-55 and Co-60. Crud activities used for the average and maximum PWR and BWR assemblies can be based on values recommended in *Commercial SNF Accident Release Fractions* (CRWMS M&O 1999c). Future revisions to this document should be referenced as appropriate.

CSNF fuel assemblies have the following initial crud activities at the time of discharge from the reactor:

Radionuclide	PWR ($\mu\text{Ci}/\text{cm}^2$)	BWR ($\mu\text{Ci}/\text{cm}^2$)
Co-60	140	1254
Fe-55	5902	7415

These crud activities are bounding estimates based on analysis in *Commercial SNF Accident Release Fractions* (CRWMS M&O 1999c).

The crud surface activity for a given assembly is a function of time after discharge from the reactor. The time-dependent crud surface activity is based on the radioactive decay equation given in CRWMS M&O 1999a, Section 5.6. The radioactive decay equation is: $N(t) = N(0) \exp(-t \times \ln 2 / t_{1/2})$, where $N(t)$ is the crud activity at time t , $N(0)$ is the crud activity at time 0, $t_{1/2}$ is the radionuclide half-life in years, and t is the decay time in years.

The crud source term (Ci/FA) released to the environment, on a per assembly basis, is calculated as follows:

$$ST_{crud} = SA_{crud} \times A_{SFA} \times conv \quad (\text{Eq. 8-1})$$

where

ST_{crud} = Crud source term (Ci/FA)

SA_{crud} = Crud surface activity ($\mu\text{Ci}/\text{cm}^2$)

A_{SFA} = Surface area per assembly (cm^2/FA)

$conv$ = Conversion factor (10^{-6} Ci/ μCi)

CSNF fuel assemblies have the following surface areas, A_{SFA} :

PWR = 449,003 $\text{cm}^2/\text{assembly}$

BWR = 168,148 $\text{cm}^2/\text{assembly}$

These surface areas are bounding estimates based on the assemblies with the highest known surface areas, a South Texas PWR assembly (CRWMS M&O 1999a) and an ANF 9x9 JP-4 BWR assembly (CRWMS M&O 1999b).

Crud source terms for Category 1 event sequences were based on average PWR fuel with a 25-year decay time (BSC 2001). An example of crud source term calculations is given in Table 8-3.

Table 8-3. Example of Category 1 Crud Source Term Calculations

Fe-55 Included In Crud Calculation. (Y/N):	Y
Crud Decay Time (years):	25
Fe-55 PWR Surface Activity (uCi/cm ²) =	10.3 ^a
Fe-55 BWR Surface Activity (uCi/cm ²) =	13.0 ^a
Co-60 PWR Surface Activity (uCi/cm ²) =	2.6 ^a
Co-60 BWR Surface Activity (uCi/cm ²) =	23.4 ^a
Bounding PWR Surface Area (cm ²) =	449,003
Bounding BWR Surface Area (cm ²) =	168,148
Co-60 Half Life	5.271 yrs
Conversion factor (Bq per uCi) =	3.70E+04
Conversion factor (rem per Sv) =	100
Crud Source	(Ci/FA)
Fe-55 PWR	4.60E+00
Fe-55 BWR	2.20E+00
Co-60 PWR	1.20E+00
Co-60 BWR	3.90E+00

^a Values are corrected for half-life and average surface activity if there is more than one FA.

8.2.2 Source Terms for U.S. Department of Energy Spent Nuclear Fuel

The U.S. Department of Energy (DOE) SNF isotopic compositions, (DTN: MO0001SPADBE00.001) currently provided by the National Spent Nuclear Fuel Program for over 250 fuel types, are given in terms of the entire fuel inventories scheduled to be disposed of at the proposed repository. For example, if a fuel inventory were made up of 400 canisters, the isotopic data provided would be for all 400 canisters. Since the entire inventory of a given fuel type would not be involved in a potential canister breach event, a scaling factor should be used to adjust the total isotopic inventory to the amount involved in the event. The use of a scaling factor results in an average source term.

The National Spent Nuclear Fuel Program is developing average and bounding source terms for over 250 DOE fuel types using a template methodology (INEEL 2000). The bases for the template methodology are templates consisting of radionuclide inventories that have been precalculated using validated calculational methodologies for specific reactor types, fuel types, burnups, and decay times. The templates are first segregated by reactor and fuel type, which includes reactor moderator type, fuel cladding, fuel enrichment, and the fuel's beginning-of-life

heavy metal constituents. For each reactor and fuel type, a family of templates may be developed by parametrically varying burnup and decay times. Each template will be based on a depletion calculation with a given set of input conditions and assumptions that can be conservatively mapped to a fuel's reactor moderator type, fuel type, burnup value, and decay time. After choosing an appropriate template based on reactor and fuel type, one selects the specific template that bounds the burnup and decay time. The template radionuclides are then scaled to account for the fuel's mass and, if necessary, its burnup, in order to conservatively estimate the radionuclide inventories for the fuel.

8.2.3 Source Terms for Vitrified High-Level Radioactive Waste

Post-irradiated isotopic concentrations for high-level radioactive waste forms from the Savannah River Site, Hanford, West Valley, and Idaho National Engineering and Environmental Laboratory are presented in Table 8-4. The isotopic concentrations in Table 8-4 were provided by the waste generators and documented in several topical reports. These data were used in site recommendation public and worker dose calculations, and they may be revised later for license application if the designs change. The methodology for calculating the HLW isotopic concentrations will not be discussed in this section.

8.2.4 Source Terms for Plutonium Disposition Waste Form

The DOE plutonium disposition waste form program is currently on-hold and there is no decision regarding the final disposition of a small amount of plutonium that cannot be made into mixed oxide reactor fuel. Therefore, no source terms or dose calculations will be discussed in this section.

8.3 CATEGORY 1 OFFSITE DOSES

8.3.1 GENII-S Dose Calculation Methodology

The annual doses to a hypothetical subsistence farmer at the site boundary due to Category 1 event sequences and normal operational releases are calculated using the GENII-S (Leigh et al. 1993) dose calculation methodology described in BSC (2001, Attachment IV). Offsite public dose calculations for Category 1 event sequences consider all of the potential exposure pathways, including inhalation, ingestion, submersion, and groundshine.

Table 8-4. Example of High-Level Radioactive Waste Activity (Curies Per Canister)

Isotope	SRS	Hanford	West Valley	INEEL
Ac-227	0.00E+00	0.00E+00	9.07E-03	0.00E+00
Am-241	2.28E+01	5.72E+02	2.10E+02	2.61E+00
Am-242m	0.00E+00	0.00E+00	1.23E+00	0.00E+00
Am-243	0.00E+00	0.00E+00	1.36E+00	0.00E+00
Cd-113m	0.00E+00	1.18E+01	6.75E+00	0.00E+00
Ce-144	1.16E+02	3.50E+02	0.00E+00	1.23E+02
Cm-243	0.00E+00	0.00E+00	4.67E-01	0.00E+00
Cm-244	8.89E+01	1.03E+01	2.48E+01	5.48E-01
Co-60	8.80E+01	0.00E+00	1.57E+00	0.00E+00
Eu-154	4.14E+02	2.24E+02	2.51E+02	1.54E+02
Eu-155	2.40E+02	0.00E+00	0.00E+00	0.00E+00
Np-237	0.00E+00	2.00E-01	9.22E-02	0.00E+00
Pa-231	0.00E+00	0.00E+00	5.97E-02	0.00E+00
Pm-147	6.46E+03	1.06E+04	0.00E+00	4.09E+03
Pu-238	1.43E+03	7.40E-01	3.14E+01	8.60E+01
Pu-239	1.29E+01	1.41E+00	6.38E+00	8.92E-01
Pu-240	8.70E+00	5.46E-01	4.67E+00	8.27E-01
Pu-241	1.32E+03	2.03E+01	2.50E+02	1.61E+02
Th-228	0.00E+00	0.00E+00	3.43E-02	0.00E+00
U-232	0.00E+00	0.00E+00	2.68E-02	0.00E+00
I-129	0.00E+00	1.63E-05	0.00E+00	0.00E+00
Cs-134	6.28E+01	2.23E+02	3.78E+00	7.85E+02
Cs-137	3.87E+04	4.54E+04	2.52E+04	1.48E+04
Ru-106	7.40E+01	1.64E+02	1.82E-03	4.07E+01
Sr-90	4.28E+04	3.82E+04	2.41E+04	1.52E+04
Y-90	4.28E+04	3.82E+04	2.41E+04	1.52E+04

Source: CRWMS M&O 1999d, Attachment VI. The most recent revision to this calculation should be referenced.

NOTE: SRS = Savannah River Site; INEEL = Idaho National Engineering and Environmental Laboratory.

The total Category 1 annual dose is based on contributions from three sources: Category 1 event sequences, normal operational (routine) releases from the Waste Handling Building (WHB), and normal operational releases from the subsurface repository. The total Category 1 annual dose (mrem/yr) is generally described by the following equation:

$$D_{Cat.1}^{TOT} = D_{Cat.1}^{DBEs} + D_{NO}^{WHB} + D_{NO}^{Sub} \quad (\text{Eq. 8-2})$$

where

$D_{Cat.1}^{DBEs}$ = Annual dose due to all Category 1 event releases (mrem/yr)

D_{NO}^{WHB} = Annual dose due to normal operational releases from the WHB (mrem/yr)

D_{NO}^{Sub} = Annual dose due to normal operational releases from the subsurface repository (mrem/yr)

$D_{Cat.1}^{DBEs}$, D_{NO}^{WHB} , and D_{NO}^{Sub} are calculated using GENII-S. The radiological release (Ci/yr) estimates for each of these three components are used as input to GENII-S dose calculations. The annual releases due to normal operations in the WHB and normal operations in the subsurface repository have been obtained from CRWMS M&O (2000a and 2000b). Current references for annual releases should be used as appropriate. The annual release due to all Category 1 event sequences is calculated using the following equation:

$$R_{DBEs}^{TOT} = \sum_{i=1}^n R_i^{DBE} \cdot f_i \quad (\text{Eq. 8-3})$$

where

- i = Index for a given Category 1 event sequence ($i= 1, 2, \dots, n$)
- n = Total number of Category 1 event sequences
- R_i^{DBE} = Radiological release due to event sequence i (Ci/event)
- f_i = Frequency of event sequence i (events/yr)

To show compliance with 10 CFR 63.111, the calculated annualized (aggregate) dose, $D_{Cat.1}^{TOT}$, is compared with the regulatory dose limit of 15 mrem per year. In addition, the calculated TEDE due to each Category 1 event sequence and a combination of Category 1 event sequences that can occur in one single year are also compared with the regulatory dose limit of 15 mrem per year.

The external doses calculated using the GENII-S semi-infinite or finite plume model will be used to estimate the dose rates due to external exposures. The calculated dose rates will be compared with the 2 mrem per hour dose rate limit given in Table 8-1.

8.3.2 Dose Conversion Factors

For Category 1 dose assessment, inhalation DCFs are derived by the GENII-S code based on the dosimetric methodology from International Commission on Radiological Protection Publication 30 (ICRP 1979).

External DCFs for air submersion, water surface, soil surface, deep soil, and buried waste, used by GENII-S to calculate doses for Category 1 event sequences, are taken from input file GRDF.15 (BSC 2001, Attachment IV, Figure 3). This file is a modification to the original GENII-S input file GRDF.DAT, and incorporates the latest data from Federal Guidance Report No. 12 (Eckerman and Ryman 1993) and DTN: MO9912RIB00066.000.

Internal and external DCFs used in GENII-S were evaluated in *Dose Conversion Factor Analysis: Evaluation of GENII-S Dose Assessment Methods* (CRWMS M&O 1999e). This analysis found that, as compared to Federal Guidance Report No. 11 (Eckerman et al. 1988), GENII-S overestimates internal doses from some radionuclides and underestimates internal

doses from others, but concluded that the differences are acceptable considering the level of uncertainties inherent in the dose assessment process.

8.3.3 Atmospheric Dispersion Factors

Atmospheric dispersion factors are taken from *Calculations of Acute and Chronic "Chi/Q" Dispersion Estimates for a Surface Release* (CRWMS M&O 1999f). Normal operational releases are modeled as chronic releases while Category 1 event releases are modeled as acute releases. The acute exposure χ/Q is based on a 2-hr exposure at the Exclusion Area Boundary (Regulatory Guide 1.145), which corresponds to the site boundary for the purpose of consequence analysis. The chronic exposure is based on the annual average, best-estimate exposure at the site boundary, in accordance with Regulatory Guide 1.111. Stack releases are not assumed in either the acute or chronic exposures.

The 50 percent acute χ/Q and chronic χ/Q are evaluated at either 8 km for subsurface releases or 11 km for surface releases. These distances should be reviewed and modified as necessary for the design used in license application.

A site boundary distance of 11-km should be used to calculate doses due to radiological releases from the WHB. This distance corresponds to the distance from the WHB ventilation exhaust shaft to the nearest point on the proposed Yucca Mountain Site Characterization Project (YMP) Withdrawal Area boundary (to the West) (DTN: MO0001YMP00001.000), which is the closest point that any member of the public could be standing or living at the time of a postulated radiological release. It is assumed that no persons will be allowed to live within the YMP Withdrawal Area and that administrative controls will be in place to evacuate any members of the public that could potentially be located within the YMP Withdrawal Area but outside of the Preclosure Controlled Area Boundary following an event sequence.

A site boundary distance of 8-km should be used to calculate potential doses due to radiological releases from the subsurface repository. This distance corresponds to the approximate distance between the potential repository and the nearest point of public access on the proposed YMP Withdrawal Area boundary (to the West) (DTN: MO0001YMP00001.000).

Atmospheric dispersion factors of $2.98 \times 10^{-7} \text{ sec/m}^3$ and $1.99 \times 10^{-7} \text{ sec/m}^3$ have been used to calculate offsite doses at 8 km and 11 km, respectively, due to chronic (normal operational) releases.

Atmospheric dispersion factors may be revised later for license application if the decision to use more recent meteorological data (up to 2001) is made. Most recent atmospheric dispersion data should be used in dose calculations for license application.

8.3.4 Breathing Rate

A breathing rate of $2.662 \times 10^{-4} \text{ m}^3/\text{s}$ ($266.2 \text{ cm}^3/\text{s}$) is used by GENII-S to calculate Category 1 doses. This breathing rate is the GENII-S input parameter for reasonable representation cases (BSC 2001, Attachment IV, Figure 2).

8.3.5 Category 1 Event Sequences

The Category 1 dose assessment includes contributions from three sources:

- Routine radiological releases from the surface facilities
- Routine radiological releases from the subsurface facility
- Category 1 event sequences – event sequences expected to occur one or more times before permanent closure (i.e., frequency $\geq 10^{-2}$ per year).

The total annual release from annual surface and subsurface routine releases (Ci/yr) and annualized releases from Category 1 event sequences should be calculated. The total annual release is then input to the offsite dose calculation performed using the GENII-S code (BSC 2001, Attachment IV).

8.3.6 Uncertainty in Consequence Analysis

Consequence analysis performed for normal operational releases and Category 1 event sequences will use either average or best-estimate input parameter values. The reasons for using average or best-estimate values are normal operations and Category 1 event sequences are expected to occur several times a year and aggregate doses are calculated for a combination of Category 1 event sequences that could occur in one single year. Therefore, each consequence analysis input parameter should be an average value that represents a waste form with different burnup values, a range of waste form damage conditions, or a range of weather conditions over one year period. For example, average source terms, annual average, best-estimate atmospheric dispersion factors, best-estimate release fractions, and best-estimate annual food consumption rates for a real member of the public will be used for Category 1 event sequences. Uncertainty analysis will not be performed for normal operational releases and Category 1 event sequences.

8.3.7 Category 1 Dose Calculation Examples

The offsite dose consequences for Category 1 event sequences are based on the methodology described in Section 8.2.1.

Example of Calculating Annualized Releases—The total estimated release from the surface facilities (4,010 Curies per year) is due entirely to Kr-85 releases from the WHB. This release was estimated based on the postulated failure of PWR and BWR spent fuel assemblies during normal handling operations (CRWMS M&O 2000a). The Waste Treatment Building is not expected to generate significant radiological emissions, based on current, best-available information (CRWMS M&O 2000a).

The total estimated releases from the subsurface facility, due to normal operations, are shown in Table 8-5 below:

Table 8-5. Example of Annual Releases from the Subsurface Due to Normal Operations

Routine Release - Subsurface (Ci/yr)		Half Life ($T_{1/2}$)
Activated Air		
N-16	2.909E-3	7.13 sec
Ar-41	5.728E+1	1.82 hr
Activated Dust		
N-16	1.189E-8	7.13 sec
Na-24	6.471E-3	14.96 hr
Al-28	3.963E-3	2.25 min
Si-31	7.170E-4	2.62 hr
K-42	8.041E-4	12.36 hr
Fe-55	1.492E-4	2.73 yr

This release was estimated based on the postulated activation of air and dust in the subsurface facilities during normal operations (CRWMS M&O 2000b). Subsurface releases are due to radionuclides generated by activation of air (Ar-41 and N-16) and dust (N-16, Na-24, Al-28, Si-31, K-42 and Fe-55). Nitrogen-16, Aluminum-28 and Potassium-42 are not considered in the GENII-S dose assessment because they are not included in the default GENII-S radionuclide libraries. However, their releases and half-lives are so small that their annual offsite dose contributions are insignificant. Iron-55 (Fe-55) is the only subsurface radionuclide released that has a half life measured in years (2.73), but its total Curie release (1.492×10^{-4}) is insignificant compared to Curie releases from Category 1 event sequences (BSC 2001, Attachment IX).

Fourteen Category 1 event sequences for CSNF have been identified (BSC 2001, p. IX-2). The Category 1 event frequency calculations were performed in BSC (2001, p. VII-5). Category 1 event releases are calculated based on the event frequencies (events per year) and event source terms (Ci/event) as described in BSC (2001, Attachments VII and VIII, respectively). Radiological releases due to Category 1 event sequences are annualized by multiplying the expected release from each event by the event frequency, as indicated in Equation (8-3). An example of annualized release calculations is shown in Table 8-6 for Cs-137.

Table 8-6. Example of Calculating Annualized Cesium-137 Release for Category 1 Event Sequences

Event No. (1)	Frequency (events/yr) (2)	Source Term (Ci/event) (3)	Annualized Release (Ci/yr) =(2) × (3)
1-01	2.34E-01	0	0
1-02	3.90E-02	0	0
1-03	4.22E-02	0	0
1-04	1.92E-01	0	0
1-05	4.10E-02	0	0
1-06	4.10E-02	0	0
1-07	4.10E-02	0	0
1-08	4.10E-02	0	0
1-09	4.10E-02	0	0
1-10	4.10E-02	3.29E-01	1.35E-02
1-11	4.10E-02	6.59E-01	2.70E-02
1-12	2.34E-01	1.65E-01	3.85E-02
1-13	2.34E-01	8.25E-02	1.93E-02
1-14	2.34E-01	1.65E-01	3.85E-02
Total			1.37E-01

The calculations shown in Table 8-6 should be repeated for all radionuclides in spent fuel or waste form of interest.

Example of GENII-S Dose Calculation—Using the aforementioned annual releases as input to GENII-S, the annual offsite TEDE dose is calculated for a receptor at the offsite boundary using the methodology described in BSC (2001, Attachment IV). An example for GENII-S dose calculation for normal operational releases or Category 1 event sequences from the surface or subsurface facility can be found in BSC (2001, Attachment IV). For these event sequences, the GENII-S input parameters are documented in BSC (2001, Attachment IV).

Because no more than 25 radionuclides can be input to GENII-S, the source term inputs must be divided into four computer runs. The source terms for four computer runs PRCHGS, PRCHP1, PRCHP2, and PRCHP3 are given in Table 8-7.

The GENII-S input data are taken as a reasonable representation case from biosphere analysis model reports. The GENII-S default parameters for the reasonable representation case can be found in BSC (2001, Attachment IV).

This calculation example used subsistence farmer's food consumption rates (BSC 2001, Attachment IV). A subsistence farmer is defined as the maximally exposed individual of the critical group who grows all of their own food using irrigation water from a well. An individual lives in the vicinity of Yucca Mountain and draws untreated ground water for drinking water supply. This individual also uses the ground water to irrigate crops and lawns and raise livestock. It was assumed that the groundwater is not contaminated during the preclosure period. Consequently, this individual will not be exposed to radiation resulting from ingestion of ground water. However, this individual will consume locally produced food; inhalation of resuspended

Table 8-7. Example of Source Terms for GENII-S Computer Runs

GENII-S Run	Radionuclide	Air Release (Ci/yr)
PRCHSF	Kr-85	4.01E+03
PRCHSB	Na-24	6.471E-03
	Si-31	7.17E-04
	Ar-41	5.728E+01
	Fe-55	1.492E-04
PRCHGS	H-3	1.46E+02
	Kr-85	1.45E+03
	I-129	2.82E-02
PRCHP1	Cl-36	3.39E-09
	Fe-55	7.72E-02
	Co-60	1.9656E-02
	Se-79	2.28E-08
	Zr-93	4.46E-07
	Nb-93m	6.49E-06
	Nb-94	4.19E-07
	Ru-106	6.14E-09
	Pd-107	4.20E-08
	Cd-113m	3.82E-06
	Sb-125	4.85E-06
	Sn-126	1.92E-07
	Pm-147	5.94E-05
	Sm-147	0
	Sm-151	1.05E-04
	Eu-154	3.35E-04
	Eu-155	2.57E-05
	Ra-226	0
	Pb-210	0
	Ra-228	0
	Cm-242	2.63E-06
	Cm-244	6.79E-04
	Cm-245	1.53E-07
Cm-246	5.19E-08	
Cm-243	5.14E-06	
PRCHP2	C-14	1.66E-07
	Ni-63	1.26E-04
	Sr-90	1.36E-02
	Tc-99	4.49E-06
	Cs-137	1.37E-01
	U-232	1.02E-08
	U-234	3.38E-07
	U-236	8.58E-08

Table 8-7. Example of Source Terms for GENII-S Computer Runs (Continued)

GENII-S Run	Radionuclide	Air Release (Ci/yr)
PRCHP2	Pa-231	1.48E-11
	Ac-227	8.03E-12
	Np-237	1.23E-07
	U-233	2.03E-11
	Th-229	0
	U-238	7.39E-08
	Pu-238	1.14E-03
	Pu-240	1.59E-04
	Am-241	9.88E-04
	Am-243	1.1E-05
	Pu-239	8.83E-05
	Ni-59	1.04E-06
	Cs-134	8.38E-05
	Cs-135	1.16E-06
	Th-230	7.39E-11
	Th-232	0
	U-235	3.67E-09
	Am-242m	3.19E-06
	Pu-242	8.18E-07
	PRCHP3	Pu-241
Cs-134		8.38E-05

dust; and direct external exposure to contaminated soil. Domestic water was assumed to come from a well.

Data can be entered into GENII-S software through a series of interactive data input screens and by modifying input data files located in GENII-S directory. The GENII-S input parameters for this calculation were based on output data from the TSPA-VA (CRWMS M&O 1998), five Data Tracking Numbers (DTNs), and other source documents shown below:

- MO0003RIB00061.001. *Input Parameter Values for External and Inhalation Radiation Exposure Analysis.*
- MO9911RIB00064.000. *Environmental Transport Parameter Values for Dose Assessment.*

- MO9912RIB00066.000. *Parameter Values for Internal and External Dose Conversion Factors.*
- MO9912SPAING06.033. *Ingestion Exposure Pathway Parameters.*
- SN0002T0512299.003. *Revised Leaching Coefficients for GENII-S Code.*
- CRWMS M&O 1998. "Biosphere." Chapter 9 of *Total System Performance Assessment-Viability Assessment (TSPA-VA) Analyses Technical Basis Document.* B00000000-01717-4301-00009 REV 01.
- CRWMS M&O 1999f. *Calculations of Acute and Chronic "Chi/Q" Dispersion Estimates for a Surface Release.* TDR-MGR-MM-000001 REV 00.
- CRWMS M&O 2000a. *Estimated Annual MGR Normal Radiological Release.* Input Transmittal RSO-SUF-99389.T.a.
- CRWMS M&O 2000c. *Non-Disruptive Event Biosphere Dose Conversion Factors.* ANL-MGR-MD-000009 REV 00.

Three data files in GENII-S were modified to accommodate the results of site-specific studies on the GENII-S input parameters. The original names of these three files are FTRANS.DAT, DEFAULT.IN, and GRDF.DAT.

FTRANS.DAT is the default GENII-S food transfer and soil leaching factor library. The soil leaching factors are important parameters for determining radionuclide buildup in soil. The food transfer factors relate concentrations of elements in soil to concentrations in farm products grown in that soil and concentrations in animal feed to concentrations in animal products. FTRANS.DAT was used in computer runs PRCHSF, PRCHGS, and PRCHP1. An updated FTRANS.DAT, renamed as FTRANRR.TXT, was developed and used in computer runs PRCHP2 and PRCHP3.

Examples of the GENII-S input parameters, the FTRANRR.TXT file, the food transfer and soil leaching factor library, the DEF_RR.TXT file, and the GRAF.15 file can be obtained from BSC (2001, Attachment IV). These files were used in GENII-S dose calculations.

8.4 CATEGORY 2 OFFSITE DOSES

Only inhalation and air submersion doses are considered in calculating offsite doses from Category 2 event sequences. The ingestion pathway, if it occurs, is a slow-to-develop pathway and is not considered an immediate threat to an exposed population in the same sense as airborne plume exposures. Therefore, the ingestion pathway is not included in the calculation of the radiological doses resulting from Category 2 event sequences for comparison against the dose criteria given in Table 8-1.

Exposure through the ingestion pathway occurs when radioactive materials that have been deposited offsite are ingested, either by eating crops grown in contaminated soil, or through inadvertent ingestion of trace amounts of contaminated soil, or through ingestion of

contaminated drinking water. Potential doses from the ingestion pathway are not included in the comparison to the regulatory dose limits because during the preclosure operations period there would be interdiction programs in place (to be established in a DOE emergency response program) to prevent the ingestion of contaminated food and water in the event of a Category 2 event sequence. The U.S. Environmental Protection Agency provides protective action guides for radiological protection guidance for federal, state, and local government in the *Manual of Protective Actions for Nuclear Incidents* (EPA 1980) that may be used for responding to a nuclear incident or radiological emergency. Protective action guides are defined as the projected dose to a standard man from an unplanned release of radioactive material at which a specific protective action to reduce or avoid that dose is warranted. The protective actions recommended to avoid or reduce the radiation dose are based on exposure pathway (i.e., inhalation, plume, ground deposition) and incident phase (i.e., early, intermediate, late). The *Criteria for the Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants* (Podolak et al. 1988) provides a basis for NRC licensees and state and local governments to develop radiological response plans and improve emergency preparedness. In this report it is stated that the basis for the choice of protective actions will be established. Further, the protective measures to be used will be established for the ingestion pathway, including the methods of protecting the public from consumption of contaminated foodstuffs. It is also stated that the plan shall identify procedures for detecting contamination, for estimating the dose commitment consequences of uncontrolled ingestion, and for imposing protection procedures such as impoundment, decontamination, processing, decay, product diversion, and preservation. Category 2 event sequences result in acute releases over a period of a few hours and the doses from these pathways (i.e., ingestion via crops, soil, or water) may be controlled by interdiction as needed, thus precluding ingestion, water immersion and contaminated soil (groundshine) source term pathways.

Two methods can be used to calculate offsite doses for Category 2 event sequences. The first method uses GENII-S to calculate the offsite doses for Category 2 event sequences. However, the code does not calculate the SDE or the LDE. Therefore, separate spreadsheet calculations for the SDE and LDE are needed. The methodology for calculating the SDE and LDE is discussed in Section 8.4.1. The Category 2 event sequence dose calculations using GENII-S are similar to the Category 1 event dose calculations discussed in Section 8.3.7, except for the ingestion pathway input data. As discussed above, the ingestion dose is not calculated for Category 2 event sequences.

The second method uses the spreadsheet calculations entirely to calculate TEDE, CDE+DDE, SDE, and LDE. The methodology for calculating these doses is presented in the following sections.

8.4.1 Category 2 Event Dose Calculation Methodology

In Category 2 event sequences, radioactive materials are assumed to be released as a ground-level radioactive plume, which is dispersed en route to the site boundary and results in a 2-hr acute individual exposure. All potential radiation doses from inhalation and air submersion pathways are considered for Category 2 event sequences.

The TEDE dose measure is expressed as:

$$TEDE = CEDE + EDE = \sum_j D_{j,effective}^{inh} + \sum_j D_{j,effective}^{sub} \quad (\text{Eq. 8-4})$$

where

$$\begin{aligned} TEDE &= \text{TEDE (rem)} \\ CEDE &= \text{CEDE (rem)} \\ EDE &= \text{EDE (rem)} \\ D_{j,effective}^{inh} &= \text{Whole body effective inhalation dose from the } j^{\text{th}} \text{ isotope (rem)} \\ D_{j,effective}^{sub} &= \text{Whole body effective submersion dose from the } j^{\text{th}} \text{ isotope (rem)} \end{aligned}$$

The CDE+DDE dose measure is expressed as:

$$CDE_k + EDE_k = \sum_j D_{j,k}^{inh} + \sum_j D_{j,k}^{sub} \quad \text{where } k \neq \text{effective or skin} \quad (\text{Eq. 8-5})$$

where

$$\begin{aligned} CDE_k &= \text{CDE to the } k^{\text{th}} \text{ organ (rem)} \\ D_{j,k}^{inh} &= \text{Radiation dose from the } j^{\text{th}} \text{ isotope to the } k^{\text{th}} \text{ organ due to inhalation (rem)} \\ D_{j,k}^{sub} &= \text{Radiation dose from the } j^{\text{th}} \text{ isotope to the } k^{\text{th}} \text{ organ due to air submersion (rem)} \\ k &= \text{Organ index, where organs are gonads, breast, lungs, red marrow, bone surface, thyroid, and remainder} \end{aligned}$$

The inhalation and air submersion doses shown above can be further expressed as:

$$D_{j,k}^{inh} = ST_j \times FA \times \frac{\chi}{Q} \times BR \times conv \times DCF_{j,k}^{inh} \quad (\text{Eq. 8-6})$$

$$D_{j,k}^{sub} = ST_j \times FA \times \frac{\chi}{Q} \times conv \times DCF_{j,k}^{sub} \quad (\text{Eq. 8-7})$$

where

$$\begin{aligned} ST_j &= \text{Inventory source term release per FA or per canister for the } j^{\text{th}} \text{ isotope} \\ &\quad (\text{Ci/FA or Ci/canister}) \\ FA &= \text{Number of fuel assemblies or canisters involved in the release (\# FAs or} \\ &\quad \text{\# canisters)} \\ \frac{\chi}{Q} &= \text{Atmospheric dispersion factor (s/m}^3\text{)} \\ BR &= \text{Breathing rate (m}^3\text{/s)} \end{aligned}$$

- $DCF_{j,k}^{inh}$ = Inhalation DCF of the j^{th} isotope for the k^{th} organ (Sv/Bq) (Eckerman et al. 1988)
 $DCF_{j,k}^{sub}$ = Air submersion DCF of the j^{th} isotope for the k^{th} organ [(Sv-m³)/(Bq-s)] (Eckerman and Ryman 1993)
 $conv$ = DCF unit conversion factor: 3.7×10^{-12} (rem-Bq)/(Ci-Sv) (Eckerman et al. 1988)

The SDE is equal to

$$SDE = \sum_j D_{j,skin}^{sub} \quad (\text{Eq. 8-8})$$

where

- SDE = SDE (rem)
 $D_{j,skin}^{sub}$ = Radiation dose from the j^{th} isotope to the skin due to air submersion (rem)

In NRC 2000, it is stated that compliance with the LDE limit is achieved if the sum of the SDE and the TEDE does not exceed 15 rem. Therefore, the LDE may be expressed as

$$LDE = TEDE + SDE \quad (\text{Eq. 8-9})$$

where

- LDE = LDE (rem)

8.4.2 Dose Conversion Factors

DCFs for inhalation are dependent on the chemical form of the radionuclide, which is represented by the lung clearance class (D = daily, W = weekly, Y = yearly) and the fractional uptake from the small intestine to blood (f_l). Some isotopes have only one lung clearance class (e.g., H-3), whereas others have multiple lung clearance classes (e.g., Pu-239). For Category 2 inhalation dose assessment of radionuclides with multiple lung clearance classes, the lung clearance class corresponding to the oxide form of the radionuclide (Eckerman et al. 1988) is assumed. The inhalation DCFs utilized for Category 2 dose assessment are from Table 2.1 of Federal Guidance Report No.11 (Eckerman et al. 1988). The air submersion DCFs for gonads, breast, lungs, red marrow, bone surface, thyroid, remainder, effective (i.e., whole body), and skin for Category 2 dose assessment are from Table III.1 of Federal Guidance Report No. 12 (Eckerman and Ryman 1993). The inhalation and submersion DCFs used for Category 2 dose assessment are listed in BSC (2001, Attachment VIII).

8.4.3 Atmospheric Dispersion Factors

Atmospheric dispersion factors are taken from *Calculations of Acute and Chronic "Chi/Q" Dispersion Estimates for a Surface Release* (CRWMS M&O 1999f). Category 2 event releases are modeled as acute releases. The maximum sector 99.5 percentile acute (0.5 percent exceedance) χ/Q values are used to calculate the maximum doses and the

50 percentile acute χ/Q values are used to calculate the mean doses. The selection of the maximum sector 99.5 percent χ/Q value is based on it being larger than the 95 percent overall site χ/Q value, per Regulatory Guide 1.145.

Atmospheric dispersion factors of 2.94×10^{-5} sec/m³ and 2.17×10^{-5} sec/m³ were used to calculate the maximum offsite doses (BSC 2001) at 8 km and 11 km, respectively, due to acute (Category 2 event) releases. These χ/Q values are based on the 99.5 percentile values at each distance, which corresponds with Wind Sector 14 (West-Northwest to East-Southeast). The maximum doses can be used to account for the uncertainty/variability of the input parameters (see Section 8.4.6). The mean doses based on 50 percentile acute χ/Q values should also be calculated.

Atmospheric dispersion factors may be revised later for license application if the decision to use more recent meteorological data (up to 2001) is made. Most recent atmospheric dispersion data should be used in dose calculations for license application.

8.4.4 Breathing Rate

For calculating offsite doses due to acute releases (Category 2 event sequences), a reference man breathing rate of 3.3×10^{-4} m³/s should be used (ICRP 1975).

8.4.5 Category 2 Event Sequences

Thirteen Category 2 event sequences for the surface facilities and one Category 2 event for the subsurface facility have been identified (BSC 2001, p. X-2). The Category 2 event frequency calculations were performed in BSC (2001, p. VII-5).

The Category 2 TEDE dose (Equation 8-4) to an individual receptor at the offsite boundary is calculated based on the methodology in Section 8.4.1. Category 2 doses are calculated on a per event basis for each of the Category 2 event sequences. Details of the Category 2 dose calculations are provided in BSC (2001, Attachment X).

8.4.6 Uncertainty in Consequence Analysis

Uncertainty analysis should be performed to account for uncertainty and variability in input parameter values. Three methods are used in the determination of uncertainty in consequence analysis.

Method of Stacking of Conservatism - The first method uses conservative or bounding values for all input parameters, which stacks conservatism on top of conservatism. This ensures that the calculated public and workers doses are conservative. For example, bounding event sequences, bounding source terms, and 99.5 percent maximum sector acute χ/Q values can be used to calculate offsite doses for Category 2 event sequences.

Using GENII-S - The second method is the GENII-S Monte Carlo method. The "S" in the name of this consequence analysis code stands for SUNS (Sensitivity and Uncertainty Analysis Shell). For each of the variable input to GENII-S, a range of parameter values and distribution types are specified. The available distribution types in GENII-S include fixed, normal, lognormal,

triangular, uniform, and empirical. Sampling from the ranges and distributions assigned to the variable input is performed within a GENII-S routine using the Monte Carlo sampling technique. GENII-S variable input parameter ranges and distribution types are documented in CRWMS M&O (1998, Table 9-3). A GENII-S statistical run generates mean, minimum, and maximum values, as well as standard deviation for each output variable. The graphical output includes cumulative distribution functions, complementary cumulative distribution functions, and histogram. These features of GENII-S provide insights into the significance of uncertainties in consequence analyses. The GENII-S output variables include organ doses, total inhalation EDE, total ingestion EDE, internal EDE, external dose, and annual EDE. The mean doses calculated by GENII-S will be compared with the regulatory dose limits in Table 8-1.

Running GENII-S includes the following input information provided by the analyst:

- Scenario options – near-field or far-field; population or individual dose; acute or chronic
- Transport options – air; surface water; biotic; waste form degradation
- Exposure pathways and options – external (immersion in finite or infinite plume, ground exposure); inhalation; ingestion
- Select radionuclides - select up to 25 from a built-in radionuclide library
- Run options – select deterministic or statistical output
- Correlations between variables.

GENII-S input variables and values are discussed in Section 8.7.3.

Using Excel with @RISK – A spreadsheet model is created to multiply the factors such as source term, airborne release fraction (ARF), respirable fraction (RF), breathing rate, DCFs, and atmospheric dispersion factors. An uncertainty distribution is assigned to each factor in the consequence model. The @RISK program is used to perform a Monte Carlo or Latin Hypercube simulation to propagate all of the uncertain variables to the output. The results are tabular giving the mean, median, standard deviation, and percentiles. The results may be plotted as probability distribution functions, cumulative distribution functions or histograms using Excel graphics.

8.4.7 Category 2 Dose Calculation Example

An example of Category 2 dose calculation is Event No. 12, Shipping Cask Drop into Cask Unloading Pool (BSC 2001, Attachments X). An example of inhalation dose calculation for this event sequence is shown in Table 8-8.

Table 8-8. Inhalation Dose Calculation Example

Group	Source Term (rem/FA)	# of FA's	Release Fraction	Mitigation Factor	Breathing Rate (m ³ /sec)	χ/Q (sec/m ³)	Offsite Dose (rem)	% of Total
Particulates	1.90E+12	68	1.50E-07	1.0E-02	3.3E-04	2.17E-05	1.38E-03	5.96
Noble Gas	1.36E+04	68	3.00E-01	1.0E+00	3.3E-04	2.17E-05	1.99E-03	8.57
Cesium	1.77E+09	68	2.00E-04	1.0E-02	3.3E-04	2.17E-05	1.73E-03	7.43
Strontium	6.03E+09	68	1.50E-07	1.0E-02	3.3E-04	2.17E-05	4.41E-06	0.02
Crud	1.24E+07	68	3.00E-01	1.0E-02	3.3E-04	2.17E-05	1.81E-02	78.02
Total							2.32E-02	100.00

NOTE: Inhalation dose to the whole body. Event: 2-12, Shipping cask drop into cask unloading pool. Fuel type: maximum BWR

In Table 8-8, source term (rem/FA) to each organ, for each nuclide group, are calculated by multiplying the crud inventory (Ci/FA) or the inventory in Table 8-2 by its respective inhalation DCF for the organ taken from Federal Guidance Report 11 (Eckerman et al. 1988). For example, in Table 8-8, the crud group includes Co-60 and Fe-55. Therefore, the crud source term (rem/FA) is equal to:

$$\text{Crud source term (rem/FA)} = \text{Co-60 inventory (Ci/FA)} \times \text{inhalation DCF}_{\text{Co-60}} (\text{Sv/Bq}) \times \text{conv} \\ + \text{Fe-55 inventory (Ci/FA)} \times \text{inhalation DCF}_{\text{Fe-55}} (\text{Sv/Bq}) \times \text{conv}$$

where conv is the DCF unit conversion factor: 3.7×10^{-12} (rem-Bq)/(Ci-Sv) (Eckerman et al. 1988). The 56 radionuclides listed in Table 8-2 are divided into four groups: particulates, noble gas, cesium, and strontium. The noble gas group includes H-3, I-129, and Kr-85. The cesium group includes Cs-134, Cs-135, and Cs-137. The strontium group includes Sr-90. The rest of radionuclides in Table 8-2 are included in the particulates group. The release fraction for each group is taken from CRWMS M&O (1999c). The mitigation factor is discussed in Section 8.7.

An example of an air submersion dose calculation including only H-3 and Kr-85 is shown in Table 8-9.

In Table 8-9, air submersion dose rates (rem-m³/FA-s) to each organ, for H-3 and Kr-85, are calculated by multiplying the inventories (Ci/FA) of H-3 and Kr-85 in Table 8-2 by its respective air submersion DCF for the organ taken from Federal Guidance Report 12 (Eckerman and Ryman 1993).

An example of a dose summary table is given in Table 8-10.

Table 8-9. Submersion Dose Calculation Example

Submersion Dose (Due to Noble Gases H-3 and Kr-85 Only)						
Event:	2-12	Shipping Cask Drop Into Cask Unloading Pool				
Fuel Type:	Maximum BWR					
	Maximum BWR Submersion Dose Rate (rem-m ³ /FA-s)	# of FA's	Release Fraction	Mitigation Factor	χ/Q (sec/m ³)	Offsite Dose (rem)
(Column No.)	(1)	(2)	(3)	(4)	(5)	(6)=(1)*(2)*(3)*(4)*(5)
Gonad	8.79E-01	68	3.00E-01	1.00E+00	2.17E-05	3.89E-04
Breast	1.01E+00	68	3.00E-01	1.00E+00	2.17E-05	4.45E-04
Lung	8.58E-01	68	3.00E-01	1.00E+00	2.17E-05	3.80E-04
R Marrow	8.19E-01	68	3.00E-01	1.00E+00	2.17E-05	3.62E-04
B Surface	1.65E+00	68	3.00E-01	1.00E+00	2.17E-05	7.31E-04
Thyroid	8.86E-01	68	3.00E-01	1.00E+00	2.17E-05	3.92E-04
Remainder	8.19E-01	68	3.00E-01	1.00E+00	2.17E-05	3.62E-04
Whole Body	8.94E-01	68	3.00E-01	1.00E+00	2.17E-05	3.96E-04
Skin	9.91E+01	68	3.00E-01	1.00E+00	2.17E-05	4.39E-02
Eye Lens	0.00E+00	68	3.00E-01	1.00E+00	2.17E-05	0.00E+00

Table 8-10. Example of Dose Summary Table

Summary of Inhalation and Submersion Dose Calculations						
Event:	2-12	Shipping Cask Drop Into Cask Unloading Pool				
Fuel Type:	Maximum BWR					
Organ	Inhalation Dose (rem)	Dose Term for Regulation	Submersion Dose (rem)	Dose Term for Regulation	Sum of Inhalation and Submersion (rem)	Dose Term for Regulation
Gonad	5.43E-03		3.89E-04		5.82E-03	
Breast	8.95E-03		4.45E-04		9.40E-03	
Lung	1.10E-01	<MAX CDE	3.80E-04		1.10E-01	<MAX CDE
R Marrow	1.03E-02		3.62E-04		1.04E-02	
B Surface	2.75E-02		7.31E-04		2.82E-02	
Thyroid	1.98E-02		3.92E-04		2.02E-02	
Remainder	1.57E-02		3.62E-04		1.61E-02	
Whole Body	2.32E-02	<CEDE	3.96E-04	<DDE	2.36E-02	<TEDE=CEDE +DDE
Eye Lens	N/A		0.00E+00	<EYE		
Skin	N/A		4.39E-02	<SKIN		
					1.10E-01	<MAX CDE + DDE

NOTE: The maximum organ inhalation dose (CDE) is to the Thyroid.
 Bolded results are added together to calculate TEDE (CEDE + DDE).

RESULTS:

Dose Term	Offsite Dose (rem)
TEDE =	2.36E-02
Max. CDE + DDE =	1.10E-01
Eye =	0.00E+00
Skin =	4.39E-02

8.5 CATEGORY 1 WORKER DOSES AND EXPOSURES

The expected annual dose to a non-involved worker located 100 meters from the release point is calculated for all Category 1 event releases, including normal operational releases from the surface and subsurface facilities. The dose calculation for the non-involved worker assumes that a single worker receives a chronic exposure, at a distance of 100 m from the release point, from potential Category 1 event sequences and normal operational releases in a single year. No credit is taken for worker training, administrative controls, or emergency response procedures to minimize worker exposures to Category 1 event sequences. In general, the annualized worker doses are based on following assumptions:

- Chronic exposure over a period of one year.
- Frequency weighted dose contributions from Category 1 event sequences.
- Only inhalation and submersion pathways are considered. Ingestion and ground contamination pathways are not included because there will be no crops produced onsite and the radiation protection program will prevent worker exposures to contaminated soil.
- Mitigated (high efficiency particulate air [HEPA]-filtered) particulate releases from the surface facilities.
- Chronic χ/Q evaluated at a distance of 100 m from the WHB (surface release) or the subsurface facility (subsurface release) to the nearest non-involved worker.

An example of Category 1 non-involved worker dose calculations can be found in BSC (2001, Attachment V).

The occupational dose limits for adults are specified in 10 CFR 20.1201, which include:

- An annual limit of either (whichever is more limiting): TEDE of 5 rem, or the sum of the DDE and the CDE to any individual organ or tissue, other than the lens of the eye, of 50 rem.
- Annual limits to the lens of the eye and to the skin: an LDE of 15 rem, and a SDE of 50 rem.

The calculated worker doses should be compared with the above regulatory dose limits.

8.6 RELEASE FRACTIONS

8.6.1 Commercial Spent Nuclear Fuel Release Fractions

The total release fraction is defined as the fraction of total inventory of a given radionuclide that is released to the environment from a waste form following an event sequence (e.g., drop of a fuel element). The release fraction for CSNF is primarily a measure of the inventory of fuel particulates, gases and volatile species present in the plenum region (a.k.a. gap release) of a breached fuel element.

The total release fraction for calculating the source term released from Category 1 event sequences is a function of the cladding damage fraction (DF), cladding release fraction (CR), ARF, RF, and the local deposition factor (DEP):

$$\text{Total Release Fraction} = DF \times CR \times ARF \times RF \times DEP \quad (\text{Eq. 8-10})$$

The DF is the fraction of fuel rods that are assumed to fail by cladding breach during a event sequence. The CR is the fraction of the total radionuclide inventory in the gap between fuel elements and cladding. The ARF is the fraction of the total radionuclide inventory in damaged fuel rods that is released from breached cladding and is suspended in air as an aerosol following an event. The RF is the fraction of airborne radionuclide particles having an aerodynamic equivalent diameter of 10- μm and less, which can be transported through air, inhaled into the human respiratory system, and contribute to the inhalation dose. The DEP is the fraction of the ARF that reaches the ventilation system after local deposition (i.e., plate-out and gravitational settling) within the WHB. The mitigation factor is the fraction of radionuclides that is released to the environment after escaping from the HEPA filters in the WHB ventilation system.

The ARF and RF parameters for Category 1 event sequences involving CSNF releases in air were based on *Commercial SNF Accident Release Fractions* (CRWMS M&O 1999c). The only exception for releases in air is the RF for Category 1 releases. In this case, a RF of 1.0 is assumed, which means all particle sizes are included in the dose calculation for the ingestion pathway. Particle sizes larger than respirable sizes could deposit on the ground and contribute to radiation doses through the ingestion pathway (i.e., human consumption of crops, fruits, and vegetables grown on the contaminated soil).

For events occurring in a spent fuel pool, an ARF equal to zero ($ARF = 0$) is assumed for all particulate and volatile species. In these events, only the noble gases are released from the pool. The release fractions for CSNF releases in air and water for Category 1 and Category 2 dose assessments are shown in BSC (2001, Attachments IX and X, respectively).

The CSNF release fractions in air, for Category 2 dose assessment, are shown in Table 8-11.

It should be noted that the release fractions given in Table 8-11 are very conservative (e.g., crud release fraction of 0.3) and they are being revised to reduce conservatism.

Table 8-11. Example of CSNF Release Fractions in Air for Category 2 Event Sequences

Nuclide	Airborne Release Fraction	RF	Effective Release Fraction
H-3	0.3	1.0	0.3
Kr-85	0.3	1.0	0.3
I-129	0.3	1.0	0.3
Cs	2.0E-04	1.0	2.0E-04
Sr	3.0E-05	5.0E-03	1.5E-07
Ru	3.0E-05	5.0E-03	1.5E-07
Crud	1.0E+00	3.0E-01	3.0E-01
Fuel Fines	3.0E-05	5.0E-03	1.5E-07

NOTE: These release fractions are conservative estimates based analysis in *Commercial SNF Accident Release Fractions* (CRWMS M&O 1999c).

8.6.2 U.S. Department of Energy Spent Nuclear Fuel Release Fractions

There are a large number of DOE spent nuclear fuels (DSNFs) with different characteristics. These fuel types are placed in six event groups: stable metal, intact; stable metal, not intact; non-metal, intact; non-metal, not intact; other, intact; other, not intact (CRWMS M&O 1999g). Since each event group has different physical and chemical characteristics, the release fractions are assigned to each event group. For each of these groups, a bounding fuel that bounds the offsite dose consequences of all fuels in that group was selected (CRWMS M&O 1999g). Screening analysis, to identify bounding event sequences from a list of Category 2 event sequences, has been performed in CRWMS M&O (1999h). To make the consequence analysis tractable, only event sequences involving bounding fuels in canisters were analyzed.

ARFs and RFs for DSNF can be found in CRWMS M&O (1999c and 1999g). Credit for a reduction in DSNF source terms due to retention of radionuclides in canisters can be taken by use of the canister leakpath factor. Canister leakpath factors for DOE SNF can be found in CRWMS M&O (2000d).

8.7 MITIGATION FACTOR

The mitigation factor refers to the mitigation of particulates provided by HEPA filters that are present in the WHB ventilation system. A mitigation factor of 0.01 should be applied to all particulate releases to calculate offsite doses. The mitigation factor of 0.01 corresponds to a particulate removal efficiency of 99 percent, which is consistent with the NRC-recommended credit for accident dose evaluations in Regulatory Guides 1.140 and 1.52.

Due to the high reliability of the WHB Heating, HVAC system, all event sequences that involved a failure of the HVAC system have been found to be beyond Category 2 event sequences (BSC 2001).

8.8 REFERENCES

8.8.1 Documents Cited

BSC (Bechtel SAIC Company) 2001. *Design Basis Event Frequency and Dose Calculation for Site Recommendation*. CAL-WHS-SE-000001 REV 01 ICN 02. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20011211.0094.

CRWMS M&O (Civilian Radioactive Waste Management System Management and Operating Contractor)1997. *Software Qualification Report for THE SCALE Modular Code System Version 4.3*. CSCI: 30011 V4.3. DI: 30011-2002, Rev. 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19970731.0884.

CRWMS M&O 1998. "Biosphere." Chapter 9 of *Total System Performance Assessment-Viability Assessment (TSPA-VA) Analyses Technical Basis Document*. B00000000-01717-4301-00009 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19981008.0009.

CRWMS M&O 1999a. *PWR Source Term Generation and Evaluation*. BBAC00000-01717-0210-00010 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000113.0333.

CRWMS M&O 1999b. *BWR Source Term Generation and Evaluation*. BBAC00000-01717-0210-00006 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000113.0334.

CRWMS M&O 1999c. *Commercial SNF Accident Release Fractions*. ANL-WHS-SE-000002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000310.0356.

CRWMS M&O 1999d. *Source Terms from DHLW Canisters for Waste Package Design*. BBA000000-01717-0210-00044 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990222.0176.

CRWMS M&O 1999e. *Dose Conversion Factor Analysis: Evaluation of GENII-S Dose Assessment Methods*. ANL-MGR-MD-000002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19991207.0215.

CRWMS M&O 1999f. *Calculations of Acute and Chronic "Chi/Q" Dispersion Estimates for a Surface Release*. TDR-MGR-MM-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000106.0439.

CRWMS M&O 1999g. *DOE SNF DBE Offsite Dose Calculations*. CAL-WPS-SE-000004 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990720.0402.

CRWMS M&O 1999h. *Preliminary Design Basis Event Analysis of DOE SNF*. ANL-WPS-SE-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990720.0405.

CRWMS M&O 2000a. *Estimated Annual MGR Normal Radiological Release*. Input Transmittal RSO-SUF-99389.T.a. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000125.0174.

CRWMS M&O 2000b. *Estimated Annual Monitored Geologic Repository (MGR) Subsurface Normal Radiological Releases*. Input Transmittal RSO-SSR-99412.T. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000105.0146.

CRWMS M&O 2000c. *Non-Disruptive Event Biosphere Dose Conversion Factors*. ANL-MGR-MD-000009 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000307.0383.

CRWMS M&O 2000d. *Leakpath Factors for Radionuclide Releases from Breached Confinement Barriers*. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000901.0021.

Eckerman, K.F. and Ryman, J.C. 1993. *External Exposure to Radionuclides in Air, Water, and Soil, Exposure-to-Dose Coefficients for General Application, Based on the 1987 Federal Radiation Protection Guidance*. EPA 402-R-93-081. Federal Guidance Report No. 12. Washington, D.C.: U.S. Environmental Protection Agency, Office of Radiation and Indoor Air. TIC: 225472.

Eckerman, K.F.; Wolbarst, A.B.; and Richardson, A.C.B. 1988. *Limiting Values of Radionuclide Intake and Air Concentration and Dose Conversion Factors for Inhalation, Submersion, and Ingestion*. EPA 520/1-88-020. Federal Guidance Report No. 11. Washington, D.C.: U.S. Environmental Protection Agency. ACC: MOL.20010726.0072.

EPA (Environmental Protection Agency) 1980. *Manual of Protective Actions for Nuclear Incidents*. EPA-520/1-75-0001. Washington, D.C.: U.S. Environmental Protection Agency. ACC: NNA.19871027.0007.

ICRP (International Commission on Radiological Protection) 1975. *Report of the Task Group on Reference Man: A Report Prepared by a Task Group of Committee 2 of the International Commission on Radiological Protection*. ICRP Number 23. Tarrytown, New York: Elsevier Science. ACC: MOL.20000516.0124.

ICRP 1979. *Limits for Intakes of Radionuclides by Workers*. Volume 2, No. 3/4 of *Annals of the ICRP*. Sowby, F.D., ed. ICRP Publication 30 Part 1. New York, New York: Pergamon Press. TIC: 4939.

INEEL (Idaho National Engineering and Environmental Laboratory) 2000. *Guide for Estimating DOE Spent Nuclear Fuel Source Terms*. DOE/SNF/REP-059 Rev. 0. Washington, D.C.: U.S. Department of Energy, National Spent Nuclear Fuel Program. TIC: 248604.

Leigh, C.D.; Thompson, B.M.; Campbell, J.E.; Longsine, D.E.; Kennedy, R.A.; and Napier, B.A. 1993. *User's Guide for GENII-S: A Code for Statistical and Deterministic Simulations of Radiation Doses to Humans from Radionuclides in the Environment*. SAND91-0561. Albuquerque, New Mexico: Sandia National Laboratories. ACC: MOL.20010721.0031.

NRC (U.S. Nuclear Regulatory Commission) 2000. *Standard Review Plan for Spent Fuel Dry Storage Facilities*. NUREG-1567. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 247929.

Podolak, E.M., Jr.; Sanders, M.E.; Wingert, V.L.; and Donovan, R.W. 1988. Criteria for the Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Criteria for Utility Offsite Planning and Preparedness, Final Report. NUREG-0654, Rev. 1, Supp. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 234538.

8.8.2 Codes, Standards, Regulations, and Procedures

10 CFR 20. Energy: Standards for Protection Against Radiation. Readily available.

10 CFR 63. Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

66 FR 55732. Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, NV. Final Rule 10 CFR Part 63. Readily available.

Regulatory Guide 1.111, Rev. 1. 1977. *Methods for Estimating Atmospheric Transport and Dispersion of Gaseous Effluents in Routine Releases from Light-Water-Cooled Reactors*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.140, Rev. 1. 1979. *Design, Testing, and Maintenance Criteria for Normal Ventilation Exhaust System Air Filtration and Adsorption Units of Light-Water-Cooled Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.145, Rev. 1. 1982. *Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.52, Rev. 2. 1978. *Design, Testing, and Maintenance Criteria for Postaccident Engineered-Safety-Feature Atmosphere Cleanup System Air Filtration and Adsorption Units of Light-Water-Cooled Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

8.8.3 Source Data

MO0001SPADBE00.001. DOE Spent Nuclear Fuel Data Contained in DBEFEB99.XLS Workbook. Submittal date: 01/04/2000.

MO0001YMP00001.000. Minimum Distances from Selected Yucca Mountain Project Sites to Public Lands. Submittal date: 01/26/2000.

MO0003RIB00061.001. Input Parameter Values for External and Inhalation Radiation Exposure. Submittal date: 03/14/2000.

MO9911RIB00064.000. Environmental Transport Parameter Values for Dose Assessment. Submittal date: 11/10/1999.

MO9912RIB00066.000. Parameter Values for Internal and External Dose Conversion Factors.
Submittal date: 12/03/99.

MO9912SPAING06.033. Ingestion Exposure Pathway Parameters. Submittal date: 12/22/1999.

SN0002T0512299.003. Revised Leaching Coefficients for GENII-S Code.
Submittal date: 02/09/2000.

CONTENTS

	Page
ACRONYMS	ii
9. UNCERTAINTY AND SENSITIVITY ANALYSIS, GENERAL CONCEPTS, AND METHODS	9-1
9.1 INTRODUCTION	9-1
9.2 OVERVIEW OF APPROACH.....	9-1
9.3 DETAILS OF APPROACH	9-2
9.3.1 Background.....	9-2
9.3.2 Identifying Sources of Uncertainty in Models and Input Information	9-4
9.3.3 Representing Uncertainties in Input and Output Variables	9-6
9.3.4 Propagating Uncertainties in Frequency and Consequence Analyses	9-10
9.3.5 Uncertainty Analysis versus Sensitivity Analysis	9-12
9.3.6 Importance Measures Analysis.....	9-13
9.3.7 Examples of Uncertainty Analyses.....	9-14
9.4 REFERENCES	9-14
9.4.1 Documents Cited.....	9-14
9.4.2 Codes, Standards, Regulations, and Procedures	9-15

TABLES

	Page
9-1 Properties of the Mean of a Lognormal Distribution.....	9-10

ACRONYMS

BI	Birmbaum Importance
EF	error factor
FV	Fussell-Vesely importance
IM	importance measure
LA	license application
LB	lower bound
LN	lognormal
NRC	U.S. Nuclear Regulatory Commission
PDF	probability density function
PLC	programmable logic controller
PRA	probabilistic risk analysis
PSA	preclosure safety analysis
RAW	risk-achievement worth
RRW	risk-reduction worth
SSC	structures, systems, and components
UB	upper bound

9. UNCERTAINTY AND SENSITIVITY ANALYSIS, GENERAL CONCEPTS, AND METHODS

9.1 INTRODUCTION

This section provides guidance on methods for identifying, quantifying, propagating, and interpreting uncertainties in event sequence frequency and consequence analyses. The material provides general concepts and methods for qualitatively and quantitatively assessing uncertainties associated with event sequence frequency analysis, or radiological consequence analysis.

9.2 OVERVIEW OF APPROACH

Two primary sources were used to develop this section: the *PRA Procedures Guide* (NRC 1983, Chapter 12) and the CPQRA guidelines (AIChE 1989). Additional information has been incorporated from several sources including Regulatory Guide 1.174, NUREG-0800 (NRC 1987, Chapter 19), and NUREG/BR-0184 (NRC 2001).

Calculations of probabilities, frequencies, source terms, and doses used in preclosure safety are often expressed as single numbers (i.e., point values) for simplicity and convenience of presentation. It is generally understood, however, that virtually every input parameter and every output value has uncertainty associated with it. When the point value represents the mean or expectation value of the quantity, it is often a sufficient parameter for decision making or compliance evaluation because the mean value represents a probability-weighted integration over the uncertainty range. When the mean of an output quantity like event sequence frequency is far (e.g., an order of magnitude or more) from a decision point like the frequency boundary between Category 1 and Category 2, then the analyst and U.S. Nuclear Regulatory Commission (NRC) has confidence that the sequence is properly categorized. But when the mean is only a factor of two or so from the boundary, the shape and range of the uncertainty distribution come into question. The probability that the true value of the frequency is in the other category may be unacceptable. In either case, an expression of uncertainty distribution is needed to support the decision-making. This section describes the process.

The geologic repository is a first-of-a-kind facility. There is no prototype or repository-specific test facility from to derive equipment performance information. The PSA must rely on generic or surrogate information. The application of such information to the repository introduces uncertainty because the exact equipment represented in information bases may not be used, and the physical and operational environments at the repository may not be represented in the surrogate information. Further, portions of the facility design may not be mature or finely detailed at the time of license application (LA). Such issues are sources of uncertainty.

Section 7.5 describes the processes for defining the uncertainty distributions for parameters that are inputs to the PSA fault-tree and event-tree modeling. Therefore, these sources of uncertainty are briefly mentioned in this section. This section concentrates on how uncertainties are identified, propagated through the analyses, and examined through sensitivity analyses.

Mathematically, the uncertainty in an input parameter is expressed by a probability distribution that represents the probability that a given value of, for example, an event sequence frequency, is

the true frequency. Each input parameter is expressed in terms of a probability density function (PDF) that represent the uncertainty in that parameter, and the calculation of an event sequence frequency requires the multiplication and addition of scores of input parameters. The output of the frequency quantification is also represented as a PDF that reflects not only the product or sum of all of the input median (or mean) values, but also the uncertainty distributions of all of the input PDFs. This effect is termed propagation of uncertainties.

The propagation of uncertainties can be performed by hand under certain conditions. Generally, the solution is too complex, however, so computer solutions are used. For the PSA, therefore, the Monte Carlo or Latin Hypercube methods will be used for most of the uncertainty analyses of event sequence frequencies. These techniques are embedded in the SAPHIRE workstation, but can also be performed in a Microsoft Excel spreadsheet using the @RISK add-in. In this regard, much of the real effort in uncertainty analysis is that of identifying and quantifying the sources of uncertainty and representing it as an appropriate, quantitative PDF.

In some instances, the source of uncertainty may not be amenable to being expressed as a PDF. For example, there may be uncertainty regarding the presence of a certain operational or environmental condition, or a design feature (e.g., does the power supply system have redundant trains?). In such cases, a sensitivity analysis may be performed to explore the significance of assuming one condition over another (e.g., calculate the event frequency with single-train and with two-train redundancy to evaluate the significance of the alternative design on the results).

Many of the concepts and methods of uncertainty analysis have been developed around the statistical properties of the Normal distribution. Section 7.5 describes other distributions that serve significant roles in the ability to quantify and propagate uncertainty. In particular, the lognormal (LN) distribution has become the workhorse for uncertainty analysis in probabilistic risk analysis (PRA) and, likewise, will have substantial application in the PSA.

Subsection 9.4 presents the details of the approach.

9.3 DETAILS OF APPROACH

This section describes the basic approaches for applying and interpreting measures of uncertainty in the PSA. The discussion will include identification of sources of uncertainty and means to evaluate and interpret uncertainty, both qualitatively and quantitatively. The discussion includes guidance on when to use sensitivity analysis and importance analysis as means to evaluate the significance of sources of uncertainty.

9.3.1 Background

The well known bell curve of the Normal Distribution is a typical example of an expression of the uncertainty, or variability, that is known to be present in a measured parameter. The bell curve is a PDF. Such variability is known as random or chance errors. There is a true, or most representative, value of some parameter (e.g., the tensile strength) of a certain kind of steel. Results of repeated tensile tests on several specimens are expected to give slightly different values, some above and some below some central value. The statistical analysis produces an expected value (the mean) and a measure of the dispersion, characterized by the variance (or the standard deviation). More recently, such chance variability is termed aleatory uncertainty.

Most analysts are familiar with basic statistical concepts that express random variability in measured parameters in terms of the number standard deviations from the mean, or the 95% confidence level. In risk analysis, the ratio of the 95th percentile to the median (which is also the mean for the normal distribution) is termed the error factor (EF). For the LN distribution, the mean is not equal to the median but is readily calculated from the median and the EF.

Similarly, most analysts are familiar with the concept of propagating uncertainties through any calculations that use two or more uncertain parameters (e.g., in adding two quantities, the standard deviation of the sum is calculated value as the root-of-sum-of-squares as the standard deviation of each input parameter, while the mean of the sum is the sum of the means of the input parameters). The greater the number of uncertain variables that are combined, the wider becomes the dispersion (uncertainty) in the output.

In fault tree and event sequence quantification, however, the end result may involve sums and products of many quantities having different kinds of probability distributions, other than the normal. These facts make the propagation of uncertainty more difficult and usually not amenable to an analytic (i.e., closed form) solution. Therefore, alternative methods must be applied, including approximations and computer simulation (e.g., Monte Carlo analysis).

The concept of epistemic uncertainty and means of dealing with it are not as well known to most analysts. The term encompasses many forms of knowledge uncertainty that can be considered in assessing the frequency and consequences. Epistemic uncertainties include, for example, model uncertainties, applicability of generic information and parameters, and effects of environmental factors, and human error rates.

For the PSA, analysts will have to make judgements on how to apply information (e.g., failure rates for equipment, human error rates, and radionuclide release fractions) that are adapted from various sources. The analysts must decided on whether or not to adjust the best-estimate value (mean or median) to suit repository conditions, alter the EF, or pool information from multiple sources.

Many of the parameters used in the PSA modeling are not amenable to direct physical measurement as in a laboratory, but are derived from operational (field) data in many instances. The parameters needed include equipment failure rates, human error rates, and equipment repair times. For example, to estimate a failure rate for a component or system like a gantry crane, the kind of information used is 1) a count of the number of failures and 2) the time in which the failures occurred. For most industrial components or systems, the information gathered is imprecise and subject to considerable uncertainties (i.e., the information is not collected during controlled experiments). The raw information may involve scouring operating logbooks, maintenance records, and estimates of operational time. Generally, there are only a few components of a given type at a given plant in the sample. Results of several different failure modes may be intermixed in the information. The preclosure safety analyst must establish some expression of uncertainty for the derived failure rate and its applicability to repository operations. The uncertainty in this instance will include aleatory and epistemic uncertainty (see Section 7.6).

In a few cases, component failure rate may be developed from reliability tests conducted by manufacturers or the military. For example, a large lot of solid-state devices are subjected to

operational tests. The number of failures is precisely known and the time-on-test is precisely known. Further, post-test examinations can reveal the precise mode or cause of each failure. In such instances, the variability in derived failure rate is aleatory uncertainty.

When the source of uncertainty cannot be described as a PDF, such as uncertainty in a design configuration, then sensitivity analyses may be used to examine the effect of alternative configurations.

With such PDFs defined for all parameters in the event probabilities in fault tree or fault tree models, the uncertainty can be propagated quantitatively by one of the various methods. In this guide, the Monte Carlo-Latin Hypercube computer-based approach is the primary method. Other methods are described.

9.3.2 Identifying Sources of Uncertainty in Models and Input Information

Until the mid-1990s, uncertainty in risk analysis was considered to arise from three sources: parameter uncertainty, model uncertainty, and completeness uncertainty. In more recent risk analysis literature, the terms aleatory (chance) uncertainty, and epistemic (knowledge) uncertainty have been introduced. However, these terms are essentially a re-packaging of the prior concepts. These newer terms are not used in this section unless the distinction is important.

The parameter uncertainty is further divided into 1) randomness inherent in any measured quantity, and 2) applicability uncertainty (e.g., using generic failure rate data to a specific facility). Both of these sources of uncertainty can be quantified and propagated through frequency and consequence analyses. Further, the significance of such uncertainties can be evaluated through sensitivity analyses (e.g., by letting a given parameter go to an extreme value) and importance analyses.

Model uncertainty is treated more philosophically, wherein the analyst recognizes that models are abstractions of reality, and therefore quantification was limited. Model uncertainty for systems safety include the use of event trees and fault trees that may not realistically model dependent failures (e.g., by using a simple beta-factor model) or human interactions. Event free and fault free modeling are generally accepted methods and will not be subjected to any uncertainty analysis with respect to alternative models. The logic models will be checked for accuracy. Uncertainties in specific modeling elements, such as mapping the physical configuration of equipment or systems into the logic models and treatment of dependent failures, can be subjected to sensitivity analysis, as needed. Further, use of exponential failure model (constant failure rate) in estimating event probabilities and various human reliability models are abstractions that introduce uncertainty. These methods are generally accepted and are not subjected to uncertainty analysts. Modeling uncertainties in consequences include the source term, damage mechanisms, release fractions, and leak-path mechanisms, as well as environmental transport. These factors can be evaluated by sensitivity analyses.

Completeness uncertainty is also treated philosophically. It is the residual, or unknown, that may remain after performing an exhaustive, structured PSA. After examining the preclosure operations using the risk triplet questions (see Section 4) by a cognizant team of safety analysts and designers, such uncertainty should be low. The LA will represent to a high level of

confidence that credible Category 1 and Category 2 event sequences have been identified and treated. Further, the LA can discuss event sequences identified as Beyond Category 2 with respect to modeling assumptions and parameters used. This will provide more transparency to reviewers (e.g., the NRC) who can perform their own sensitivity analysis, if desired, to assure themselves that the list of credible sequences is complete.

Finally, it is possible that differences between analysts introduce another source of uncertainty. The application of this Guide, however, and associated Yucca Mountain Project procedures should essentially eliminate this source of uncertainty from the PSA.

9.3.2.1 Uncertainties in Input Parameters

Section 7.5 discusses three sources of uncertainty that are associated with the input information used to quantify event probabilities and frequencies: random variability, uncertainty associated with information source, and uncertainty associated with applicability to repository facilities.

Similar types of parameter uncertainty are associated with consequence analyses.

Other sources of uncertainty in input parameters include the waste stream year-to-year loadings.

Such sources of uncertainty are amenable to quantification and propagation through the event sequence frequency and consequence analyses.

9.3.2.2 Uncertainties in Model Inputs and Modeling

Uncertainty in model inputs relates to the level of detail on design and operations that is available. For the LA for construction authorization, it is anticipated that the level of detail will be limited. Principal operations and associated equipment will be defined, along with the degree of redundancy, dependence on power supplies, spatial relationships, and anticipated human interactions. Therefore, the PSA will require some imagination on the part of analysts, with concurrence of design personnel, to define potential hazards and event sequences, and to synthesize system fault trees and event sequences. This lack of certainty in design and operations becomes a source of modeling uncertainty, described below. The PSA to support the LA to Receive and Process will not have this source of uncertainty.

Uncertainties in modeling stem from generic and specific causes. The generic uncertainties stem from use of standard event probability models, such as constant failure rate, repair models, common-cause failure models, and human reliability models. In general, such sources of uncertainty will not be addressed in the PSA unless such modeling effects appear to affect the PSA results. If deemed necessary, sensitivity analyses must be performed to examine the results with alternative models.

Repository-specific modeling uncertainties stem from the representation of reality in the event sequence and fault tree logic models. For example, event sequence (event tree) analysis (Sections 7.1 and 10.1) may include dependencies between events whose conditional probabilities are estimated. The presence and nature of the dependency may be uncertain, and the associated conditional probability may be an assumption. Similarly, a fault tree models of a control systems might include a redundant train and might include components like PLCs that

are expected to be used, but which have not been completely specified in design documents. Such models may include a common-cause failure model for redundant components. Such modeling is potentially a source of significant uncertainty and stems, in part, from the uncertainty in the model inputs and level of design detail. For these kinds of modeling uncertainties, sensitivity analysis should be performed to demonstrate how significantly they affect the PSA results.

All bases for modeling will be documented so that design-dependent issues and assumption-dependent uncertainties can be identified and appropriate sensitivity analyses performed as necessary.

9.3.3 Representing Uncertainties in Input and Output Variables

For the PSA, particularly for the LA for construction authorization, it is recommended that all event probabilities and frequencies be treated as LN distributions, except in cases where a normal distribution is more appropriate. The LN is a good fit to the distribution that result when several distributions are multiplied, as in an event sequence quantification. As described and illustrated in Section 7.5, the LN in inputs can be converted back and forth to other distributions that are better to work with analytically in event probability estimation (e.g., in an empirical Bayesian analyses). Further, the parameters of the LN are readily associated with the properties and tabulations of the normal distribution. The principal properties of the LN and normal distributions used in the PSA are described in the following subsections.

9.3.3.1 Uncertainty Interval and Bounds

The uncertainty in a variable x is described by a PDF that gives the probability $p(x)dx$ that the true value of the variable is within the dx about x . The cumulative probability function is given as $P(x_p)$, defined as the probability that the true value of the variable is less than or equal to x_p . $P(x_p)$ is the integral of $p(x)dx$ between the lower limit of the distribution and the value x_p . The cumulative probability function, $P(x_p)$, is used to define the confidence interval, or range, for the input variable or calculated value.

Unless otherwise specified or required, uncertainty on input variables and calculated outputs of event sequence frequencies and consequences will always imply a 90 percent confidence interval (range). This means that 10 percent of the values of inputs or of results can fall outside of the interval. Generally, the PSA will use confidence intervals that span the range from the 5th percentile to the 95th percentile.

The bounding, or limiting, values that define the 90 percent confidence interval of a variable x are the values of $x_{0.05}$ and $x_{0.95}$, where $P(x_p) = 0.05$ and 0.95 , respectively. The median value of distribution occurs at the value $x_{0.5}$ where $P(x_p) = 0.5$. The EF is defined as the ratio $x_{0.95} / x_{0.5}$.

These definitions apply irrespective of the particular form of PDF that is used. The following subsections describe how these definitions are applied to normal and LN distributions.

9.3.3.2 Properties of the Normal and Lognormal Distributions

Normal Distribution—For a variable y , the properties of the normal distribution apply. The normal distribution is a symmetric ranging from $-\infty$ to $+\infty$. The measures of central tendency are numerical equal: mean (y) = median (y) = mode (y). Dispersion about the mean (μ) is described by the variance (σ^2) or the standard deviation (σ).

The normal distribution is often expressed in normalized form in terms of a variable:

$$z = [y - \mu]/\sigma$$

The PDF for z has a mean value of 0.0 and a standard deviation of 1.0. The cumulative probability of the normal distribution from $-\infty$ to a value $z = Z$, sometimes termed the normal curve of error function for Z , is amenable to direct integration and has been extensively tabulated and built into spreadsheet programs like Microsoft Excel. In the normalized form, the percentiles of the cumulative distribution are given as:

$Z_{0.5}$	=	0	median (and mean)
$Z_{0.05}$	=	-1.64	5th percentile
$Z_{0.84}$	=	1.00	84th percentile
$Z_{0.95}$	=	1.64	95th percentile
$Z_{0.99}$	=	2.33	99th percentile.

Note: For brevity, the Z values are shown only to two decimal places. For hand calculations, at least three to four places should be used. When using Microsoft Excel or SAPHIRE, the functions are built in and will display as many places as selected.

From the definition of z , the corresponding values of the variable y are given as:

$y_{0.50}$	=	μ	median (and mean)
$y_{0.05}$	=	$\mu - 1.64\sigma$	5th percentile
$y_{0.84}$	=	$\mu + 1.00\sigma$	84th percentile
$y_{0.95}$	=	$\mu + 1.64\sigma$	95th percentile
$y_{0.99}$	=	$\mu + 2.33\sigma$	99th percentile.

The parameters μ and σ characterize the normal distribution. μ may be considered a location parameter (defines the central value) and σ may be considered a shape parameter that describes the degree of spreading or peaking in the distribution of the variable x . The larger the value of σ , the wider the distribution and the greater the uncertainty.

For the normal distribution, the EF, as defined above becomes:

$$EF_{\text{normal}} = 1 + 1.64\sigma/\mu.$$

The EF is not often directly used with the normal distribution. The application of the EF comes when estimating uncertainty ranges and assuming distributions.

For example, if the analyst (supported by design or vendors) believes that 90 percent of a failure rate for some component lie between a lower bound (LB) of 1×10^{-3} and an upper bound (UB) of 5×10^{-3} , and are normally distributed. Using the relationships above, the statement of belief gives the following:

$$\begin{aligned} \text{LB} &= y_{0.05} = 1 \times 10^{-3} = \mu - 1.64\sigma \\ \text{UB} &= y_{0.95} = 5 \times 10^{-3} = \mu + 1.64\sigma \end{aligned}$$

which yield

$$\begin{aligned} \mu &= 3 \times 10^{-3} \\ \sigma &= 1.2 \times 10^{-3} \end{aligned}$$

The EF becomes $1.67 (5 \times 10^{-3} / 3 \times 10^{-3})$, but is a derived quantity in this example. The EF has a more fundamental role for the LN distribution, however.

The properties of the normal can be applied to a lognormally distributed variable as described below.

Lognormal Distribution—The properties of a LN distribution for a random variable x is developed from the properties of the normal distribution for the transformed variable $y = \ln(x)$, where $\ln(\cdot)$ is the natural logarithm. The LN distribution on x , the non-transformed variable is not symmetric. It ranges from $x = 0$ to $x = +\infty$. The mean value of x is not equal to the median or mode.

Mathematical expressions for the parameters of the LN are somewhat complex, but they are derived from the properties of the normal distribution for the transformed variable y .

To describe a LN distribution, the analyst needs only two values such as the median value of x and a value for EF, or the median and UB, or the UB and LB. The latter is the 90 percent confidence range on x . The following relationships apply:

$$\begin{aligned} M(x) &= x_{0.50} = \text{UB}/\text{EF} = \text{LB} \times \text{EF} = (\text{UB} \times \text{LB})^{1/2} \\ \text{EF} &= \text{UB}/M = M/\text{LB} = (\text{UB}/\text{LB})^{1/2} \end{aligned}$$

These expressions relate to parameters for the distribution of the non-transformed variable, x . When the variable is transformed to $y = \ln(x)$, the parameters for the normal distribution on y , are derived as follow:

$$\begin{aligned} \mu_{\text{LN}} &= \ln(M), \text{ the location parameter (mean of the } y \text{ distribution)} \\ \sigma_{\text{LN}}^2 &= \ln(\text{EF})/Z_{0.95} = \ln(\text{EF})/1.64 \end{aligned}$$

With these parameters so defined, the mean of the LN distribution of the non-transformed variable, x , becomes:

$$\text{mean}(x) = \underline{x} = \exp[\mu_{LN} + \frac{1}{2} \sigma_{LN}^2],$$

which can be expressed alternatively as:

$$\text{mean}(x) = \underline{x} = M \times [EF]^a, \text{ where } a = 1/(2 Z_{0.95}) = 1/(3.29).$$

For example, the analyst (supported by design or vendors) believes that 90 percent of a failure rate for some component lies between a LB of 1×10^{-4} and a UB of 1×10^{-2} , and it is lognormally distributed (this range covers two orders of magnitude). Using the relationships above for the LN, the statement of belief gives:

$$LB = x_{0.05} = 1 \times 10^{-4}$$

$$UB = x_{0.95} = 1 \times 10^{-2}$$

which yield

$$M(x) = x_{0.50} = (UB \times LB)^{1/2} = (1 \times 10^{-2})(1 \times 10^{-4})^{1/2} = 1 \times 10^{-3}$$

$$EF = UB/M = 1 \times 10^{-2}/1 \times 10^{-3} = 10$$

$$\mu_{LN} = \ln(M) = \ln(1 \times 10^{-3}) = -6.907$$

$$\sigma_{LN}^2 = \ln(EF)/1.64 = \ln(10)/1.64 = 1.40$$

$$\underline{x} = \exp[\mu_{LN} + \frac{1}{2} \sigma_{LN}^2] = \exp[-6.907 + (1.40)^{1/2}] = 3.3 \times 10^{-3}.$$

In this case, with an EF of 10, the mean \underline{x} is a factor of 3.3 greater than the median. The UB is a factor of 3 above the mean.

The LN distribution is asymmetrical and, because the variable may range over several decades, the distribution presents interesting properties with respect to the relationship of mean to median, and mean to the upper 95 percent confidence limit. Table 9-1 illustrates how the parameter σ_{LN} varies with the EF (note that an EF of 30 indicates a factor of 900 for the ratio of UB/LB). The table also shows how the ratio of mean/median, mean/UB, and UB/mean vary with EF. It is noted that the ratio of mean/median ranges from about 1.1 to 8.5 for the range of EF shown. This indicates that the mean is within a factor of three or less of the median for EF less than 10. The ratio of UB/mean indicates that the mean is within a factor of about 2 to 4 of the upper bound over the range of EF shown.

The last column in Table 9-1, CDF(Mean), is the value of the CDF of the LN evaluated at the mean. This column indicates, somewhat paradoxically, that as the uncertainty increases, characterized by the EF ranging from 2 to 30, the probability that the true value exceeds the mean actually decreases. For example, for an EF of 2, the CDF is 0.54, meaning that there is 0.54 probability that the true value is less than or equal to the mean, and a probability of 0.45 that

the true value exceeds the mean. By contrast, for an EF of 10, the CDF is 0.84 and the complement probability is 0.16.

Because of the characteristics of the LN, the mean value is a suitable measure for binning event sequence frequencies or for evaluating consequences against regulatory limits.

9.3.3.3 Comparison of Output Values with Limits

The PSA will calculate two kinds of output quantities that must be used in the risk-informed performance-based compliance with 10 CFR Part 63. These variables represent frequency and consequence, respectively. Limits on frequency relate to the boundaries between Category 1 and Category 2, and between Category 2 and Beyond Category 2. Limits on consequences relate to the respective dose limits for the public and workers defined in 10 CFR 63.111.

The PSA will use mean values of frequency and doses. Thus, if the mean value of a dose is 4 rem total effective dose equivalent and therefore less than the limit of 5 rem, the result is compliant with the regulations.

Similarly, if the mean value of the frequency of an event sequence is less than 1×10^{-2} per yr, the sequence is considered to be Category 2. If the mean value of the frequency of an event sequence is less than 1×10^{-6} per yr, the sequence is considered beyond Category 2.

The uncertainty factors associated with frequency and consequence analyses should be quantified, however. If the PDF for the frequency or consequences of a given event sequence is shown to be lognormally distributed. Table 9-1 illustrates that the mean value is within a factor of 2 to 4 of the 95th percentile upper confidence bound. Therefore, there is confidence that event sequences will be appropriately categorized with respect to frequency.

As noted in Section 3, the LA for CA will use one-half the regulatory limit as guidance for estimating dose consequences. Therefore, if the mean value of an estimated dose is less than or equal to one-half of the regulatory limit, and the uncertainty in dose is shown to be lognormally distributed, there will be low probability of exceeding the regulatory limits.

Table 9-1 Properties of the Mean of a Lognormal Distribution

EF	Mean/Median	Mean/UB	UB/Mean	CDF(Mean)
2	1.09	0.55	1.83	0.54
3	1.25	0.42	2.40	0.59
5	1.61	0.32	3.10	0.68
10	2.66	0.27	3.75	0.84
30	8.48	0.28	3.54	0.98

9.3.4 Propagating Uncertainties in Frequency and Consequence Analyses

This subsection describes the principal means for propagating uncertainties. The discussion is based on frequency analyses. Consequence analyses are treated similarly.

The *PRA Procedures Guide* (NRC 1983) and CPQRA Guidelines (AIChE 2000) describe several methods that could be used for propagating uncertainties. It is noted that direct (analytical) integration of the multivariable probability distribution is generally not possible. Therefore, the favored techniques are numerical integration, which includes the discrete probability method and Monte Carlo simulation, and moments methods. For complex analyses, the moments methods also appear to be untractable unless the output moments are approximated by using a Taylor series expansion where only second-order terms are retained.

Since current desktop software like SAPHIRE, GENII-S, and Microsoft Excel with an @RISK add-in can perform Monte Carlo simulation, or the similar Latin Hypercube Analysis. Numerical analysis will be the primary technique to be used in frequency and consequence analysis for the PSA. The SAPHIRE workstation permits eleven forms of distribution functions for uncertainty.

The analyst must specify the mean and one other parameter, depending on the distribution selected. However, for some purposes, including checking of results, a Taylor-series approximation could be used. The following describes the basic steps for sequence uncertainty analysis. The users' manual for the particular program (e.g., SAPHIRE) should be consulted.

9.3.4.1 Sequence Uncertainty Analysis

The following are the principal steps for developing an event sequence analysis that includes propagation of uncertainty:

1. Construct the logic models (event tree, fault tree, and human reliability) for the initiating events and systems (see Sections 7.1, 7.2, and 7.3)
2. Obtain and quantify input information for each basic event and initiating event used in the logic models, including quantification of uncertainty distribution (see Section 7.5)
3. Perform sequence quantification analysis to generate minimal cutsets and point estimates (see Section 7.1)
4. Select method for uncertainty analysis. For simple sequences, it may be appropriate to use Microsoft Excel with the @RISK add-in.

If the event sequence quantification is performed in a program like SAPHIRE (Smith et al. 2000), however, it will be more efficient to use the uncertainty propagation that is built in. The analysis may be performed on individual sequences, group, or family. For example, it may be necessary to add the frequencies of two or more Category 1 sequences for the same or different initiating events for a given repository operations area. For either @RISK or SAPHIRE, the analyst must select either Monte Carlo or Latin hypercube, number of trials, and random number seed.

1. Obtain tabular and graphical outputs of uncertainty analysis. The output of sequence uncertainty analysis typically includes: mean, median, standard deviation, 5th and 95th percentiles, maximum and minimum (for the run of N samples), seed number, and sample size.

2. Interpret results. Examine acceptability of results and identify dominant contributors to sequence frequency and uncertainty in results

The sequence uncertainty analysis will be used primarily to generate the mean and EFs to evaluate sequence categorization and to demonstrate compliance with 10 CFR Part 63. Where appropriate, sequence sensitivity analysis will be performed.

9.3.4.2 System (Fault Tree Top Event) Uncertainty Analysis

The steps for evaluating system uncertainty are essentially the same as for the event sequence uncertainty analysis, and are not repeated here.

The system uncertainty analysis will be used primarily to generate insights into the dominant contributors to system reliability and safety performance. Where appropriate, system sensitivity analysis or IM will be obtained.

9.3.4.3 Uncertainties in Consequences

Section 8 describes the approach to consequence analyses for the PSA. Analyses for Category 1, Category 2, and Beyond Category 2 event sequences are described. The bases for identifying and treating uncertainties are discussed, including the use of conservative or bounding values, where appropriate.

9.3.5 Uncertainty Analysis versus Sensitivity Analysis

Some sources of uncertainty cannot be analyzed by assigning a PDF, but insights on their significance may be investigated quantitatively through sensitivity analysis.

A sensitivity analysis for event sequence frequency analysis is performed by changing features of logic models, human reliability models, input parameter values, or the features of the physical facility or operations. In general, a sensitivity analysis examines rather large-scale changes such as:

- Changing the redundancy of a system (i.e., adding a train or deleting a train)
- Changing the probability of a basic event (hardware, software, or human failure) from a best-estimate probability to a bounding value (i.e., to 1.0 or to 0.0)
- Changing the failure logic by adding or deleting elements, such as adding or deleting an alarm that alert the human operator to take action (e.g., using AND logic).

Such changes are made one at a time in fault tree and event sequence quantification so the output can be compared to the baseline result.

In addition, a sensitivity analysis can be used the effect of changing the assumed probability distribution for an input parameter. If it is uncertain, for example, whether to use a LN or a normal distribution for a particular input, the alternative distributions are used and results compared.

A sensitivity analysis of consequences is performed by changing source term parameters (i.e., age and burnup, and fraction of inventory that is released) and the presence of mitigating features (i.e., high-efficiency particulate air filters and deposition). The process is essentially the same as for frequency analysis.

9.3.6 Importance Measures Analysis

Importance analysis may be regarded as a special form of sensitivity analysis. There are several standard definitions of IMs that have been applied in PRAs and regulatory evaluations. An IM analysis can be performed on fault trees or event sequence frequency quantification. Analysis of the standard IMs are performed automatically by programs such as SAPHIRE. Therefore, the discussion here is brief.

In fault tree analysis for a system, the top event represents the probability that the defined event will occur (e.g., HVAC fails to run and filter particulates for at least 24 hours). Suppose the fault tree analysis shows the mean probability is 1×10^{-4} , and lists all of the cutsets (products of basic event probabilities) above a cutoff probability of 1×10^{-7} . The value for all of the cutset and top event probabilities are subject to the values input for basic event probabilities.

The IM can be used to analyze the sensitivity of the result to the inputs in the following way:

1. The risk-achievement worth (RAW) of every basic event, with respect to output, is calculated by setting the probability of each basic event to 1.0 one-at-a-time while holding the baseline values of probabilities of all of the other basic events. The analysis program then produces a table, which ranks every basic event according to its RAW value. The RAW for a given structure, system, or component (SSC) represents the increase in system failure probability if the SSC is removed from the system model. The RAW, like the Birnbaum Importance (BI), may be interpreted as a measure of the margin of safety contributed by proper operation of the model element (i.e., the SSCs). The RAW process is similar to the take-away process described in Section 12.
2. The risk-reduction worth (RRW) of every basic event, with respect to output, is calculated by setting the probability of each basic event to 0.0 one-at-a-time while holding the baseline values of probabilities of all of the other basic events. The analysis program then produces a table, which ranks every basic event according to its RRW value. The RRW for a given SSC represents the decrease in system failure probability if the SSC is perfectly reliable.
3. The BI is calculated, in essence, by taking the difference between the RAW and RRW for each basic event. The analysis program produces a table, which ranks every basic event according to its BI value. The BI is interpreted as a measure of the margin of safety contributed by proper operation of the model elements (i.e., the SSCs). The BI is sometimes interpreted as the maintenance importance for a given SSC (i.e., the importance of keeping it operational). Because the RRW is usually small compared to the RAW, the BI is usually quite close to the RAW numerically.

4. Fussell-Vesely Importance (FV) is calculated, in essence, by taking the product of each basic event probability time its BI (there are other, more fundamental definitions of FV). The analysis program produces a table, which ranks every basic event according to its FV value. The FV illustrates the fraction of current risk (or top event probability) involving the failure of the model element (i.e., a particular SSC). The BI portion of the product gives the relative magnitude of the risk achievement by the presence of the model element and the event probability in the product gives a weight of the relative likelihood of having the SSC fail to achieve the risk reduction.

Such IMs provide insight to the dominant contributors to system failure and can be used to develop risk-informed maintenance, Quality Assurance, and training programs. Further, IM can be used to scope an uncertainty analysis where more attention is given to identifying and quantifying uncertainties in the basic events that have the dominant IMs.

When sequence quantification is performed by the fault-tree linking method (see Sections 7.1 and 7.2), the top event becomes the frequency that the sequence occurs. All of the sequence cutsets include the initiating event frequency times one or more basic event probabilities. Since the initiating event frequency is common to all, it can be set equal to 1.0 and the IMs of the remaining cutsets are evaluated as described above.

The application of IMs has been described in Regulatory Guide 1.174. In those applications, the baseline risk is a measure of integral risk like core-damage frequency of a reactor core damage that stems from multiple event sequences. The change in core-damage frequency is calculated using the RAW, RRW, BI, and FV. At the present, the PSA for the repository will not employ an integral risk measure. Therefore, the application of IMs will be limited to developing insights on SSC risk significance from fault-tree analysis and event sequence analysis.

9.3.7 Examples of Uncertainty Analyses

Information for this section is under development and will be provided later.

9.4 REFERENCES

9.4.1 Documents Cited

AIChE (American Institute of Chemical Engineers) 1989. "Partial List of External Events." Table 3.13 of *Guidelines for Chemical Process Quantitative Risk Analysis*. New York, New York: American Institute of Chemical Engineers. TIC: 241701.

AIChE 2000. *Guidelines for Chemical Process Quantitative Risk Analysis*. 2nd Edition. Center for Chemical Process Safety Series. New York, New York: American Institute of Chemical Engineers.

NRC (U.S. Nuclear Regulatory Commission) 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

NRC 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

NRC 2001. *Regulatory Analysis Technical Evaluation Handbook*. Washington, D.C.: U.S. Nuclear Regulatory Commission. NUREG/BR-0184.

Smith, C.L.; Wood, S.T.; Kvarfordt, K.L.; McCabe, P.H.; Fowler, R.D.; Hoffman, C.L.; Russell, K.D.; and Lois, E. 2000. *Testing, Verifying, and Validating SAPHIRE Versions 6.0 and 7.0*. NUREG/CR-6688. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249459.

9.4.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

Regulatory Guide 1.174, Rev. 01 Draft. 2001. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

INTENTIONALLY LEFT BLANK

CONTENTS

	Page
ACRONYMS	iii
10. EXTERNAL EVENTS	10-1
10.1 SEISMIC ANALYSIS	10-1
10.1.1 Introduction	10-1
10.1.2 Overview of Approach	10-1
10.1.3 Details of Approach	10-4
10.1.4 Examples of Application of Seismic Analyses	10-6
10.1.5 Development and Application of Seismic Event Trees	10-8
10.1.6 Frequency Quantification of Seismic Sequences Using Deterministic, Step-Function Fragility Functions or Seismic Margins Analysis	10-19
10.1.7 Frequency Quantification of Seismic Sequences Using Fragility Functions or Seismic Margins Analysis	10-20
10.2 FLOODING	10-28
10.2.1 Purpose	10-28
10.2.2 Scope	10-28
10.2.3 Overview of Approach	10-28
10.2.4 Details of Approach	10-28
10.2.5 Flooding Protection Requirements	10-31
10.2.6 Consequence Analysis	10-31
10.3 WINDS and TORNADOS	10-32
10.3.1 Purpose	10-32
10.3.2 Scope	10-32
10.3.3 Overview of Approach	10-32
10.3.4 Details of Approach	10-32
10.3.5 Wind and Tornado Protection Requirements	10-36
10.3.6 Consequence Analysis	10-36
10.4 LIGHTNING AND EXTREME WEATHER	10-37
10.5 WILDLAND FIRES	10-37
10.6 OTHER EXTERNAL EVENTS	10-38
10.6.1 Loss-of-Offsite Power	10-38
10.6.2 Aircraft	10-38
10.6.3 Military and Industrial Hazards	10-43
10.7 REFERENCES	10-49
10.7.1 Documents Cited	10-49
10.7.2 Codes, Standards, Regulations, and Procedures	10-51
10.7.3 Source Data	10-52

FIGURES

	Page
10-1 Event Sequence Diagram for Internal Initiated Drop Event.....	10-12
10-2 Event Sequence Diagram for Seismic Initiated Drop Event.....	10-13
10-3 Event Sequence Diagram for Fire Initiated Drop Event.....	10-14
10-4 Event Sequence Diagram for Seismic & Fire Initiated Drop Event.....	10-14
10-5 Baseline Seismic Event Tree for Load Drop	10-15
10-6 Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake.....	10-21
10-7 Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake, but Earthquake greater than Frequency Category 1	10-22
10-8 Example Fragility Curves	10-24

TABLES

	Page
10-1 Examples of Seismic Consequences of Roof Collapse onto Waste Forms (Hypothetical System)	10-9
10-2 Example Seismic Calculations for Seismic Failure in Hypothetical Assembly Transfer System	10-10
10-3 Example Seismic Classification of Structures, Systems, and Components for Hypothetical Assembly Transfer System.....	10-11
10-4 Example Maximum Estimated and Observed Wind Speeds near Yucca Mountain, Nevada.....	10-33
10-5 Design Basis Tornado Characteristics	10-34
10-6 Tornado Wind Speed (miles per hour) by Region.....	10-34
10-7 Example Tornado Wind Speed for 5-Degree Latitude and Longitude Box Containing Yucca Mountain, Nevada.....	10-35
10-8 Spectrum II Missiles	10-36

ACRONYMS

AFB	Air Force Base
ALARA	as low as is reasonably achievable
ATS	assembly transfer system
BLM	U.S. Bureau of Land Management
DOE	U.S. Department of Energy
ESD	event sequence diagram
FC	frequency category
GF	guaranteed failure
HCLPF	high confidence of low probability of failure
HEPA	high-efficiency particulate air
HVAC	heating, ventilation, and air-conditioning
LOSP	loss of offsite power
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
NTS	Nevada Test Site
PDF	probability density functions
PGA	peak ground acceleration
PMF	probable maximum flood
PRA	probabilistic risk assessment
PSA	preclosure safety analysis
PSHA	probabilistic seismic hazards analysis
QA	quality assurance
QL	quality level
RF	random failure
SET	seismic event tree
SMA	seismic margins analysis
SNF	spent nuclear fuel
SNFA	spent nuclear fuel assembly
SSCs	structures, systems, and components
SSE	safe shutdown earthquake
TNT	2,4,6-Trinitrotoluene (explosive)
UBC	Uniform Building Code

ACRONYMS (Continued)

VGM	Vibratory ground motion
WHB	Waste Handling Building

10. EXTERNAL EVENTS

This section provides a bridge between the external events hazards analysis and the design basis such that no credible event sequences which do not meet 10 CFR Part 63 performance objectives can occur. Each section may have a different scope, approach, and length depending on the topic.

The sections will provide means to (a) identify those structures, systems, or components (SSCs) that need to withstand credible external events and thereby prevent a radiological release; and (b) describe methods to develop controls that prevent a credible release scenarios given the occurrence of the initiating event.

10.1 SEISMIC ANALYSIS

10.1.1 Introduction

This section describes the bases and methods for analyzing the design of surface and subsurface repository facilities and waste package design for potential vulnerability to seismically-induced event sequences that could potentially lead to a criticality or radiological release. The safety strategy includes the prevention of any credible scenarios that could potentially lead to consequences that exceed the performance requirements of 10 CFR Part 63. This guide defines the steps in the analyses that, in many cases, link to other portions of the Preclosure Safety Analysis (PSA) and to the seismic design strategy that has been presented to the U.S. Nuclear Regulatory Commission (NRC) in a series of seismic topical reports.

Examples presented are based on hypothetical situations. None of the values of event sequence frequencies on doses should be taken as results applicable to a repository.

10.1.2 Overview of Approach

10.1.2.1 Background

Precedents from Nuclear Power Plants—The licensing basis for the repository, with respect to seismic design, adapts the principal tenets of regulatory precedence that the NRC has applied to nuclear power plants (NPPs) (which are regulated per 10 CFR Part 50). The fundamental licensing concept for NPPs includes the definition of a design basis earthquake (termed a safe shutdown earthquake [SSE]) and requirements stipulating that important to safety SSCs must be designed to withstand the vibratory motions associated with that earthquake. These important to safety SSCs are classified as a single category termed Seismic Category 1 SSCs.

The SSE is specified by the peak ground acceleration (PGA) and other characteristics of the vibratory ground motion, such as spectral acceleration and time-history, that become input parameters to the design of SSCs important to safety. Approved regulatory guides and industry codes and standards are applied in the design. It is deterministically argued that, for the NPPs, as long as an earthquake of intensity greater than the SSE does not occur at the site, there will be no seismically-induced accident sequences that cannot be prevented or mitigated such that the plant cannot be brought to a safe condition. Design principles and approaches for seismic hardening are provided in sections of the NPP standard review plan (NRC 1987).

The PGA and other parameters have previously been defined based on the largest historical earthquake for the site. Although the return period of the SSE for power plants can be defined, it was not used in the initial licensing basis for most NPPs. In more recent regulatory practices for NPPs, however, probabilistic seismic hazard analysis have been used to define the return period for the design basis earthquake and its vibratory motion characteristics. Seismic probabilistic risk assessments (PRAs), for example, use the return period or the frequency of exceedence of a spectrum of earthquakes as input to the risk analysis. The characteristics of the SSE are included in the spectrum of earthquakes. Instead, the risk analysis determines the annual probability (or frequency) of a seismically initiated sequence of events that cannot be brought to a safe condition (i.e., for NPPs, the core damage frequency that is attributed to seismic events is calculated).

Monitored Geologic Repository Preclosure Seismic Strategy—The precedent seismic design principles for NPPs have been adapted for the repository by requiring that all SSCs important to safety must withstand a design basis earthquake. The adaptation of this deterministic principle to the repository licensing basis is more complicated because it is applied in a two-tiered, risk-informed, performance criteria.

Seismic Topical Report No. 2 (YMP 1997), submitted by the DOE and tentatively approved by the NRC pending their receipt and approval of Topical Report No. 3, describes the rationale for this approach as well as design principles to be applied to surface facility SSCs, waste package SSCs, subsurface openings and ground support SSCs, and other SSCs in the subsurface facility. With certain exceptions as noted in Topical Report No. 2, the design of surface and subsurface SSCs will apply the principles of the *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants* (NRC 1987).

The two-tiered design basis earthquake approach, however, leads to several departures from a strict carryover of analyses from the power plant precedent and becomes somewhat more complex when applied to items important to safety that have been classified into three categories of quality level QL-1, QL-2, and QL-3 (see Section 12). Because of the two-tiered, risk-informed, approach, two design basis earthquakes are defined. For the repository, the PGA and ground motion characteristics are to be defined (via the forthcoming Topical Report No. 3) based on the probabilistic seismic hazards analysis (PSHA) for site-specific earthquakes having return periods that correspond to Frequency Category (FC)-1 and Frequency Category 2 (FC)-2 as defined in Topical Report No. 2 (YMP 1997). The design basis earthquake to be applied to the design of a given SSC depends on the magnitude of potential radiological exposures to the public or workers with respect to compliance with 10 CFR 63.111.

The safety case for the repository will be based on deterministic design basis applied to the repository SSCs. In this licensing basis, a specific SSC designed to withstand one of the respective design basis earthquakes is assumed able to perform its safety function during earthquakes of magnitudes up to, and including, that magnitude specified as the design basis earthquake for that SSC. However, the SSC is assumed to fail with a probability of 1.0 in the event of an earthquake that exceeds the magnitude of the design basis earthquake for that SSC. This approach may be characterized as assigning a step-function fragility factor to each SSC (i.e., the conditional probability of the SSC failing, given the occurrence of an earthquake, is 0.0 up to, and including, the vibratory ground motion (VBM) associated with the design basis

earthquake; however, the probability becomes 1.0 for higher VBMs). As described in Topical Report No. 2 (YMP 1997), however, it is implicit that there will be margins in the design of the SSC such that the actual probability of failure, given a design basis earthquake, will be a factor of 0.1 or less. This margin provides assurance, for example, that in the event of a FC-2 design basis earthquake at 1×10^{-4} per year, the annual probability of an offsite dose that exceeds the limits of 10 CFR 63.111(b) will be less than 1×10^{-5} per year. Although this probability is not demonstrated to be below the 1×10^{-6} per year probability threshold for screening out events, it is in accordance with regulatory precedence.

It is expected that additional analyses will be required, such as SSC fragility analyses or SMAs, as well as associated uncertainty analyses to demonstrate that high-consequence seismically-induced sequences are beyond design basis. It is further expected that this demonstration can be provided for a limited number of sequences and a limited number of SSCs; therefore, it will not be necessary to perform a comprehensive seismic PRA.

10.1.2.2 Summary of Approach

The PSA will address potential seismically-induced radiological release events through a comprehensive hazards analysis and limited event sequence analysis as a means to identify the SSCs important to safety that are required to withstand the vibratory ground motions associated with the respective FC-1 or FC-2 design basis earthquake for those SSCs.

The following analysis steps will be applied:

- Review available design descriptions and drawings.
- Review available hazards, event sequences, criticality scenarios, and consequence analyses for events initiated by internal events, internal fires, and internal floods.
- For each of the repository operational areas, define the scenarios by which radionuclides could be released, or a critical condition could result, due to events initiated by an earthquake as a result of the direct or indirect effects of seismically-induced failure of the SSCs.
- Use mean values for source terms to calculate the offsite and worker dose that could result from each hypothetical seismic scenario and the postulated failure of a given SSC. Calculate the dose with and without mitigation features, if mitigation is currently used in the design, or could be applied.
- Determine the design basis earthquake frequency category to apply to each SSC based on the approach described in Topical Report No.2 (YMP 1997). Event sequence evaluations should include the considerations of potential criticality events, the importance of ensuring waste isolation, the importance of ensuring the ability to retrieve waste packages, and ALARA (i.e., as low as is reasonably achievable) principles and practices.

Several issues regarding this approach have not been resolved at this time. The detailed discussion of the approach identifies some of these issues.

10.1.3 Details of Approach

10.1.3.1 Design Requirement per Seismic Topical Report 2

The DOE and NRC have established the principles for the seismic design of items important to safety in the repository in a topical report, *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain* (YMP 1997) (otherwise known as Topical Report No. 2). The report provides design principles for the following categories of SSCs: surface facilities, underground openings, other underground SSCs, and waste package. Seismic design principles are provided for both vibratory ground motion and ground fault displacement.

A project position paper, *Monitored Geologic Repository Seismic Design Requirements Strategy* (CRWMS M&O 1998), provided a method for applying the principles of Topical Report No. 2 to the design of the repository for SSCs that were previously classified as important to radiological safety. Although Topical Report No. 2 was written by the DOE and reviewed by the NRC according to the regulations of 10 CFR Part 60, the fundamental approach can be adapted to address 10 CFR Part 63, since the two-tiered Category 1 and Category 2 event sequence structure has been retained in 10 CFR Part 63.

The principle difference between 10 CFR Part 60 and 10 CFR Part 63 is the change from prescriptive requirements to performance-based requirements. Section 10.1.4.2 summarizes the impact of moving from 10 CFR Part 60 to 10 CFR Part 63. It has been concluded that the change has little substantive effect on the requirements for seismic design for preclosure safety.

Previously SSCs classified as important to safety (i.e., preclosure radiological safety) were designated by a single quality assurance classification level (QA-1). The application of Topical Report No. 2 required that each of the QA-1 SSCs be able to withstand a FC-1 or FC-2 design basis earthquake, depending on the potential magnitude of the resultant radiological doses. The process for the quality assurance classification of items important to safety has been revised to include three levels of QL-1, QL-2, and QL-3 (as described in Section 12). The application of Topical Report No. 2 becomes somewhat more complex because each SSC will carry a QL designation as well as a seismic classification (i.e., FC-1 or FC-2).

The seismic design requirements are expressed in terms of two design basis earthquakes that are characterized by their mean frequency (or return period) labeled as FC-1 and FC-2, respectively. For the vibratory ground motion design basis earthquakes, FC-1 is defined as having a mean annual probability of 1×10^{-3} per year, and FC-2 is defined as having a mean annual probability of 1×10^{-4} per year. The determination of the parameters associated with the intensity of the respective design basis earthquakes will be the subject of the forthcoming Topical Report No. 3. Topical Report No. 3 will provide the information associated with the intensity and characteristics such as peak acceleration and the resulting ground motion response spectra. This information is required to ensure that the structural design of SSCs can withstand the dynamic loads resulting from an earthquake.

In addition, for fault displacement design basis earthquakes, FC-1 is defined as having a mean annual probability of 1×10^{-4} per year, and FC-2 is defined as 1×10^{-5} per year. The principal design defense against fault displacement is fault avoidance as described in Topical Report No. 2 (YMP 1997).

Guidance from prior regulatory positions, such as the *Standard Review Plan for Spent Fuel Dry Storage Facility* (NRC 2000a), requires that subcriticality be maintained for all normal event, abnormal events and postulated accidents. These events include the effects of natural phenomena. Therefore, SSCs that might lead to criticality events were assigned the FC-2 design basis earthquake. Furthermore, the FC-2 design basis earthquake was assigned to SSCs that could significantly impair the ability of the repository to retrieve waste packages or degrade waste if the SSCs were damaged.

The principles of ALARA and defense-in-depth are addressed in the consideration of seismic classification. The final step in the seismic classification process provides a catch all where prudence or engineering judgement may dictate a more stringent seismic design, commensurate with cost-benefit considerations or throughput/availability considerations that may be more limiting than the radiological safety considerations.

10.1.3.2 Impact of 10 CFR Part 63

The principal difference between 10 CFR Part 60 and 10 CFR Part 63 is the change from prescriptive requirements to risk-informed, performance-based requirements. However, 10 CFR Part 63 retains the requirement stipulating that credible natural phenomena must be considered in the design of the repository. After comparing the respective requirements of the two regulations, it is concluded that there is no substantive difference in regulations that affect the requirements for seismic design for preclosure safety. Topical Report No. 2 remains applicable but regulatory references in Topical Report No. 2 will have to be updated to refer to the appropriate sections of 10 CFR Part 63 instead of 10 CFR Part 60. For example, the radiological performance requirements are now provided in 10 CFR 63.111 and references to 10 CFR Part 60 definitions for important to safety and the design basis event frequency categories (with their corresponding dose limits) must be replaced by counterpart references to 10 CFR Part 63.

A change in these regulations that may affect the application of Topical Report No. 2 involves the requirement that states that doses from Category 1 event sequences must be less than, or equal to, the final Environmental Protection Agency criteria for Yucca Mountain (15 mrem total effective dose equivalent (TEDE)-per year). It was previously assumed in the preclosure Seismic Strategy that the 10 CFR Part 20 dose limit of 100 mrem would be applied to determine which SSCs are required to withstand a FC-1 design basis earthquake.

10.1.3.3 Process for Assigning Design Basis Earthquake

The following steps are applied to assign the appropriate design basis earthquake to SSCs:

1. Define the scenarios by which radionuclides could potentially be released by event sequences initiated by an earthquake. The postulated scenarios include the failures of SSCs directly associated with the handling, storing, or containment of radioactivity of high-level radioactive waste forms, SSCs that could interact with those SSCs

associated with the handling or storage of waste forms; the failure of fire protection systems, and radiation waste treatment systems.

2. The analysis may build on prior hazards analyses or event sequence analyses that have been developed for internal events, internal fires, internal floods, and criticality scenarios. As appropriate, to aid in identifying potential seismic scenarios, seismic event trees (SETs) may be constructed as described in Section 10.1.6.
3. Calculate the offsite dose that could result from each postulated failure of a given SSC and the resulting radiological release. Calculate doses with, and without, mitigation features, if mitigation is currently used in the design or could be applied.
4. Subject each SSC to the following dose comparisons:
 - a. If the individual offsite dose is greater than or equal to the 10 CFR 63.111(b)(2), then the SSC must be designed to withstand the vibratory ground motion of a FC-2 design basis earthquake. One guideline from 10 CFR 63.111(b)(2) is a dose less than 5 rem TEDE for the public.
 - b. If, however, the offsite dose is less than 10 CFR 63.111(b)(2) limits but greater than or equal to 10 CFR 63.111(b)(1) [which in turn references 10 CFR 63.111(a)] then the SSC must be designed to withstand the vibratory ground motion of a FC-1 design basis earthquake. The guidelines of 10 CFR 63.111(a) for Category 1 event sequences include paragraph (1), which requires meeting 10 CFR Part 20 limits. These limits include worker dose limits (per 10 CFR 20.1201) and annual doses of less than 100 mrem to the public, and paragraph (2) which presents a limit of an annual TEDE of less than 15 mrem to the public.
 - c. If both the offsite doses and worker doses are less than the 10 CFR 63.111(a) requirements for both workers and the public, then the SSC may be designated as non-seismic and designed accordingly (e.g., to the Universal Building Code).
5. For SSCs designated as non-seismic or as FC-1, examine the SSCs and determine if there are any radiological exposure, waste retrieval, or waste isolation issues that suggest designing to a more stringent category earthquake. If, after a cost analysis, it is shown that with only a small increase in costs that it is reasonable to design an SSC to a more stringent category earthquake and the redesign results in a reduction in dose, then this approach should be taken to promote ALARA.

The QA requirements associated with the seismic design will be considered at a later date as the graded QA program is developed.

10.1.4 Examples of Application of Seismic Analyses

The seismic methodology is demonstrated by application to a conceptual repository surface facility design. The first example is a scoping calculation applied to the structure of the Waste

Handling Building (WHB). The other examples represent conceptual handling and operations in the WHB.

The examples presented here (Section 10.1.5) are based on a evaluation of an earlier conceptual design. The examples are intended to illustrate how seismic classifications are assigned to SSCs. To support the LA submittal, however, the evaluations must be performed in a structured and thorough manner to ensure that potentially significant seismic vulnerabilities are identified. The SET described is one approach that will aid in the structured analysis. As noted, the seismic classification analysis should draw from prior analyses, including existing event trees non-seismic initiating events that can be modified to include seismic effects.

10.1.4.1 Consequences of Hypothetical Waste Handling Building Collapse

The structures of a waste handling building (WHB), including the outer shell and the structures of individual operations areas, have to be examined for two vulnerabilities to seismic radiological releases. First, the massive structural elements that could fall onto waste forms have to be examined as potential initiators of release scenarios. Second, these same structures may be required to provide confinement of releases initiated within the WHB by an earthquake. This section addresses the first issue by determining the appropriate design basis earthquake to assign to various structural elements such as the roof, walls, and foundation.

For this analysis, the WHB operational and staging areas are assumed to be full to maximum capacity in order to present the potentially largest radiological source term in the event of an earthquake. Further, the spent nuclear fuel assembly (SNFA) operations and staging areas are assumed to be full of pressurized water reactor or boiling water reactor spent-fuel assemblies, whichever is shown to produce the maximum source term. Where possible, falling structural elements having mass too small to breach a given waste form or to damage staging racks are eliminated from consideration. Otherwise, it is postulated that fragments of the roof or wall fall onto and damage the struck waste form or storage rack. The source term for the maximum inventory of the area is used, along with the release fractions and atmospheric transport parameters, to calculate the offsite and worker doses.

Table 10-1 presents several examples of offsite doses using conservative release fractions and atmospheric transport factors to a site boundary (assumed conservatively to be a distance of 5 km). All of the doses (which are unmitigated) exceed 5 rem. Therefore, it would be concluded from this hypothetical exercise that the roofs, walls, and foundation must be designed to withstand an FC-2 design basis earthquake. The application of this methodology, with current release fractions and a larger site boundary, is expected to change the evaluation.

10.1.4.2 Seismically Induced Releases in Operations Area

Within the WHB, a hypothetical Assembly Transfer System (ATS) receives and unloads SNFAs from transport casks. Several potential release scenarios have been identified for the ATS (as well as other operations) from hazards analysis and internal event sequence analysis. Event trees may be available for some of the initiating events. Each of the release scenarios is examined for potential initiation directly, or indirectly, in an earthquake. In addition, each operation (e.g., each lift, movement, or staging) is examined independently for potential direct or indirect

vulnerability to faults induced by the occurrence of an earthquake. The ATS may have several parallel operations that could each contain a maximum inventory when an earthquake occurs, so it can be assumed that parallel operations will fail concurrently during the earthquake. The source term is the sum from parallel operations that could have concurrent seismically induced releases.

The hypothetical offsite doses are shown in Table 10-2 for the seismic-induced failures of SSCs in several operations areas of the ATS. The doses are calculated using the same assumptions of conservative release fractions and atmospheric transport factors to the site boundary described in Section 10.1.5.1. For the example, that the hypothetical unmitigated doses are made to exceed 5 rem; therefore, in this example some of the SSCs will have to be classified for seismic design.

Table 10-3 presents the seismic classification for the alternative design strategies. In the confinement-mitigation strategy, it is assumed that the WHB (ATS) structure and the heating, ventilation, and air-conditioning (HVAC) and high-efficiency particulate air (HEPA) filter system(s) will be designed to withstand the FC-2 design basis earthquake. In this case, the seismic classification of waste-handling SSCs, such as transfer carts or cranes, for example, can be designated as FC-1 or Uniform Building Code. In the prevention strategy, it is assumed that the handling and staging equipment within the ATS will be designed to withstand the FC-2 design basis earthquake. In this case, no credit is taken for the mitigation effects of the HVAC/HEPA filter system and it is classified as Uniform Building Code. The structure of the WHB (ATS) would remain FC-2 because of the results of the analysis described in Section 10.1.5.1.

The examples presented here are based on a somewhat superficial evaluation of a previous conceptual design and are intended to illustrate how seismic classifications are ultimately assigned to each SSC. To support the LA submittal, however, the evaluations will be performed in a structured and thorough manner to ensure that potentially significant seismic vulnerabilities are identified. The seismic event tree described in the following section is one approach that will aid in the structured analysis. As noted previously, the seismic classification analysis should draw from prior analyses, including existing event tree analyses that can be modified to include seismic effects.

10.1.5 Development and Application of Seismic Event Trees

Section 7.1 describes the techniques used in event tree construction and analyses for any event sequence initiated by any kind of internal or external event. The discussion in Section 7.1 includes the treatment of dependent failures between event tree headings and initiating events. The event tree modeling of such dependent failures represents failures that are induced, or made more probable, by the occurrence of a precursor event. Earthquakes, fires, floods, winds and tornadoes, and loss of offsite power are potentially significant because they can act as common-cause initiators that not only initiate an event sequence but can concurrently induce failure of mitigative SSCs that are in the design. The event tree format helps to define the potential event sequences and potential common-cause vulnerabilities. Such vulnerabilities, if resulting in an unacceptable dose, are identified and the associated SSCs are required to be hardened to withstand the common-cause initiator. In the case of earthquakes, each SSC important to safety is identified as having to withstand one of the two design basis earthquakes.

Table 10-1. Examples of Seismic Consequences of Roof Collapse onto Waste Forms (Hypothetical System)

Building Cell	Worst Case Waste Form	Max. Inventory (PWR/BWR)	VA Roof Material	Roof Height (m)	Roof Area, A (m ²)	Note 1	Note 2	Note 3		Note 4			
						Min. Roof Mass, M (MT)	Max. Roof Thickness [t=M/(d*A)] (m)	Conservative Offsite Dose - No Mitigation (rem)		Conservative Offsite Dose - with Mitigation (rem)			
								Canister	PWR	BWR	Canister	PWR	BWR
Waste Treatment			Steel	9.14	4,831								
Carrier Bay	Cask	52/122	Steel	3.35	1,691	33	3.20	>>5	>>5		1.8E-02	2.5E-02	
ATS Cask Prep/Air Lock	Cask	78/183	Steel	21.64	260	5	3.22	>>5	>>5		6.4E-02	8.9E-02	
Pool Area (Note 5)	SFA	792/1584	Steel	21.64	334	0.04	0.02	>>5	>>5		7.3E-01	8.3E-01	
DC Hot Cell (dryer)	SFA	126/264	Concrete	15.24	130	0.06	0.24	>>5	>>5		8.6E-02	1.0E-01	
DC Load/Decon (ATS)	DC	63/132	Concrete	8.23	146	20	74.51	25	31		7.5E-03	9.3E-03	
CTS Corridor	Canister	10	Steel	18.29	752	1	0.18	>5			7.50E-03		
CTS Cask Prep/Decon	Canister	10	Steel	12.19	260	1	0.79	>5			5.10E-03		
CTS Lag Storage	Canister	40	Concrete	19.51	37	1	11.48	>>5			3.20E-02		
DC Load Area (CTS)	Canister	10	Concrete	19.51	272	1	1.57	>5			8.10E-03		
DC Handling Cell	DC	105/220	Concrete	18.29	1,208	9	4.06	>>5	>>5		8.3E-02	1.0E-01	
DC Staging Area	DC	420/880	Concrete	18.29	637	9	7.70	>>5	>>5		2.9E-01	3.6E-01	
DC Transfer/Load	DC	21/44	Concrete	9.14	242	18	40.64	>5	>5		7.5E-03	9.3E-03	
WP Remediation	DC	21/44	Concrete	4.88	195	34	94.25	>5	>5		7.5E-03	9.3E-03	

Notes:

- 1 Minimum roof mass equivalent to a waste form drop from above the design height
- 2 Assumes roof is homogeneous with a density equal to steel or concrete
- 3 Deterministic TEDE dose with PWR/BWR/DHLW DBF source term, and no HEPA filtration
- 4 Deterministic TEDE dose with PWR/BWR/DHLW DBF source term, and single-stage HEPA filtration
- 5 Max inventory source term assumes no water is present in the pools

Calculation method: Using the design basis drop height for each waste form, equated the potential energy of the waste form mass dropping from its design basis height to the potential energy of the roof mass dropping from the roof height.

$MxgxH = mxgxh$

M = Roof mass

H = roof height

m = waste form mass

h = design basis drop height

Table 10-2. Example Seismic Calculations for Seismic Failure in Hypothetical Assembly Transfer System

ATS Location/Activity	Equipment	Potential DBE	SSC Failure	Equivalent Drop Height (in)	Source Term Number PWR/BWR SFAs Seismic Event	Consequences, Rem	
						With HEPA's	Without HEPA's
Receive Trans. Cask from CBS							
A. Transfer from CHB	Cask transfer cart	Slapdown from transfer cart Collision with ATS Airlock Door	Cask Tr. Cart	210	78/183	1.33E-2/1.53E-2	>5 / >5
Cask Prep and Decon Room							
A. Remote cask cavity gas sampling	Cask transfer cart	Slapdown from transfer cart	Yoke				
B. Cask venting	Cask unloading area bridge crane	Cask drop from bridge crane into pit	Bridge Crane	129	78/183	1.13E-2/1.26E-2	>5 / >5
C. Cask gas and water cool-down	Cask prep manipulator	Handling equipment drops on cask	Lifting Fixtures				
D. Outer lid removal	Cask lid lifting fixture						
E. Inner shield plug lifting fixture attachment	Dry cask lifting yoke						
F. DPCs remotely sampled, vented, cooled	Large, small DPC lifting fixtures						
G. DPC lifting fixture remotely attached	Wet cask lifting yoke						
Cask Unloading Pool							
A. Cask placed in pool, inner shield plug out	Large, small DPC overpacks	Handling equipment drops on cask	Lifting grapples				
B. Cask inner shield plug removed	Large, small DPC lid severing tools	Handling equipment drops on DPC					
C. Cask containing DPC put into pool	Wet assembly lifting grapple	Cask drop from bridge crane into pool	Bridge Crane	N/A	78/183	7.53E-3/7.40E-3	7.53E-3/7.40E-3
D. DPC removed from cask, put in overpack	Wet assembly transfer machine	Assembly drop onto pool floor, cask	Wet assembly transfer machine				
E. DPC lid severed and removed	Pool, downstream valves and drains						
F. Assemblies taken from DPC/cask to baskets							

Table 10-3. Example Seismic Classification of Structures, Systems, and Components for Hypothetical Assembly Transfer System

Location/Equipment	Equipment Identifier	SSC Seismic Failure	Seismic Frequency Category VA Design	Basis
Airlock Roof, walls	N/A	Concrete mass falls onto cask	FC-2	Heavy mass impacts cask > design basis & concurrent loss of confinement
Cask transfer cart	PU-CR-110	Slapdown from transfer cart; impact with cell walls	FC-1	Drop or impact on hard surface > cask design basis; credit for confinement
Cask transfer cart - control & motive systems	PU-CR-110	Collision with Airlock Door, breach cask; or breach building confinement	FC-1	Prevent uncontrolled motion of transfer cart to avoid collision with structures, other objects; avoid damage to airlock doors; credit for confinement
Airlock doors	N/A	Fail to maintain building confinement	FC-1	Loss of confinement for cell and waste handling building
Cask Preparation and Decontamination Room; Roof, walls	N/A	Concrete mass falls onto cask	FC-2	Heavy mass impacts cask > design basis & concurrent loss of confinement

Event trees for seismically induced sequences may be built on event trees developed previously for internal or external event initiators. The cause of the prior initiating event (e.g., drop, loss of offsite power [LOSP], and fire) in the SET is assumed to be an earthquake, however, rather than a random failure (RF). Alternatively, a SET may be developed from scratch.

In some cases, construction of an event sequence diagram (ESD) will aid in creation of a SET. The potential for common-cause failures among SSCs induced by the earthquake can be diagrammed on the ESD. These dependencies are accounted for in the structure of the SET. The ESDs are briefly described in a following paragraph.

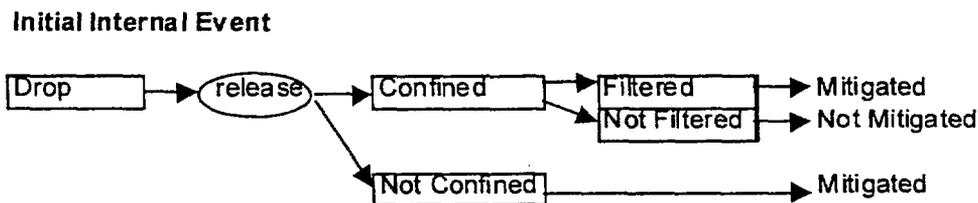
Initially, the SET is applied qualitatively without the consideration of event frequencies with assumed dependencies between the initiating earthquake and mitigative events to define the vulnerabilities and the need for seismic hardening of SSCs. Consequences associated with each sequence of events are quantified; however, to designate the design basis earthquake associated with each SSC. After a given SSC is designed to withstand a given design basis earthquake, the failure dependency with the earthquake initiator is removed from the SET. In more advanced analyses, it may be necessary to evaluate seismic margins or to quantify the frequencies of seismic sequences using fragilities of the SSCs. This section describes both applications of SETs.

10.1.5.1 Seismic Event Sequence Diagrams

An ESD is a less rigid structure than an event tree. It allows the systems analyst to respond to the question "what can happen?" in a brainstorming mode. Several examples of ESDs are described here to illustrate how they are constructed and modified to include earthquakes and intermediate events.

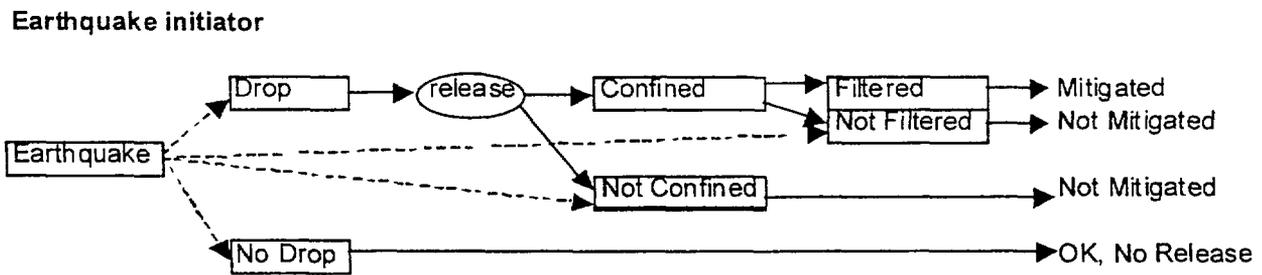
Figure 10-1 illustrates a simple ESD for a drop of a waste form (e.g., a spent nuclear fuel [SNF] assembly) in the WHB. The initiating event is the Drop. The immediate “what can happen?” is assumed (or known) to be a release of radioactivity from breached fuel rod cladding. With the knowledge that the purpose of the hot cell structure of the WHB and its HVAC/HEPA filters is to confine and filter any releases, respectively, it is recognized that the confinement function may be functioning or not functioning. If it not functioning (another “what can happen?”), the release may be assumed to go directly to the environment, bypassing the HVAC/HEPA filters. The consequence of this sequence of events (drop-release-not confined) is not mitigated and may not meet the regulatory dose limits. If the confinement is functioning, another “what can happen?” is the failure of the HVAC/HEPA filters to filter the release. The consequences of this sequence (drop-release-confined-not filtered) is also not mitigated and may exceed the regulatory dose limits. As discussed in Section 10.1.6.2, an event tree is developed from the ESD of Figure 10-1 as shown in Figure 10-5. Except for the event heading “Release” that is assumed to be guaranteed for a drop of an SNF assembly, all of the event headings are assumed to be independent, so the potential failure modes are random mechanical, software, or human failures.

Figure 10-2 illustrates how the example ESD is modified for an earthquake initiator. The top portion of the diagram from “Drop” to the right includes the same events as the base case. An event “No drop” has been added to illustrate that the earthquake may not induce a drop for the particular lifting device (e.g., especially if it has been designed to withstand an earthquake of a given magnitude). This diagram also indicates by dashed lines the possibility that the earthquake may directly and concurrently induce failure of the safety functions of the confinement structure and the HVAC/HEPA filter system. The consequences for the various sequences are assumed to be the same as for the internally-initiated drop, although each situation has to be evaluated for potential exacerbating factors brought about by the earthquake (e.g., previously trapped particulates in the HEPA filter might be released if the HEPA filter is failed by the earthquake, thus giving a higher consequence than the base case). The event tree for this case, now a SET, is described in Section 10.1.6.2.



NOTE: All failures events are random.

Figure 10-1. Event Sequence Diagram for Internal Initiated Drop Event



NOTE: Failures events may be random or seismic. Potential seismic interactions/failures indicated by dashed lines.

Figure 10-2. Event Sequence Diagram for Seismic Initiated Drop Event

More complex seismic scenarios can be modeled in ESDs before developing SETs. Figure 10-3, for example, illustrates an ESD for internal fire-induced sequences. This ESD is seen to have the same structure as the earthquake-only case presented in Figure 10-1. However, it is unlikely that a single fire, confined to a given locale in the WHB, will be able to concurrently cause a drop and induce failure of the other safety functions. The internal-fire ESD is modified in Figure 10-4 to include an earthquake as an initiating event. Now the fire (or several fires) may be caused by the earthquake and the fire(s), in turn, may induce the drop and other failures of safety systems. However, the earthquake may concurrently cause the drop and/or other failures as well as initiate the fire. Potential consequences include radiological as well as non-radiological releases. The latter are not considered in the seismic classification of SSCs. A SET for the earthquake-fire cases is not developed in this guide, as it would be too general and speculative. As necessary, the PSA team will develop SETs specific to the WHB and other operational areas.

Similar ESDs and SETs could be developed for loss of off-site power LOSEP-induced sequences. This ESD would have a similar structure as the earthquake-only case in Figure 10-2, except that there are not LOSEP-induced failures of the confinement. Depending on the design of the lifting device, HVAC/HEPA filters, and the electrical supply system, however, it may be possible for a LOSEP event to concurrently cause a drop and induce failure of the HVAC/HEPA filters. The earthquake-LOSEP cases is not developed in this guide, as it would be too general and speculative. As necessary, the PSA team will develop SETs specific to the WHB and other operational areas.

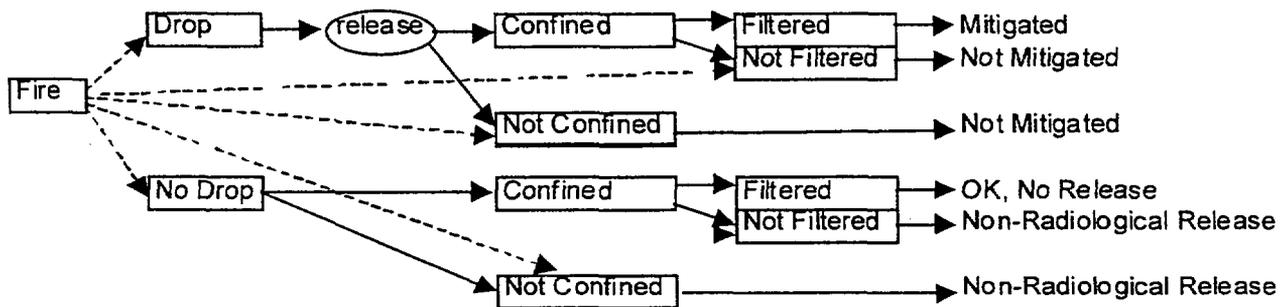
Further, an ESD on each SET could be developed to analyze indirect effects of seismic induced failures of SSC that are not important to safety by themselves. Such SSCs, however, may be located in such a way, or function in such a way, that a seismic event could cause the SSC to interact with one or more other SSC that are important to safety and, thereby, cause a loss of its safety function. (Such seismic interactions are known as two-over-one situations in NPP regulations, meaning that a Seismic Category 1 SSC (safety-related) is vulnerable to a seismic-induced fall or impact by a Non-Seismic-Category 1 component.) Logically, the seismic ESD is similar to that of the seismic fire-induced case since there is potential spatial interaction between items directly affected by the earthquake and one or more SSCs important to safety.

10.1.5.2 Generic, Initial Seismic Event Tree

Figure 10-5 presents an example of a simple event tree structure for a hypothetical sequence of events associated with a facility that handles a radioactive waste form. The hypothetical

operation includes a crane that lifts and transports a particular waste form. Should the crane drop the waste form from a height exceeding its design basis, the waste form shell (i.e., its containment barrier) may breach and its contents (e.g., spent fuel assemblies) may breach, releasing radioactivity to the interior of a hot cell. If the hot cell structure remains intact, and if the HVAC ducting and HEPA filter remain intact, any releases are vented in a controlled manner. An accidental release scenario can be generated by a sequence of independent events (e.g., random failures or human errors) by seismically induced events, or by a combination of independent and seismically induced failures.

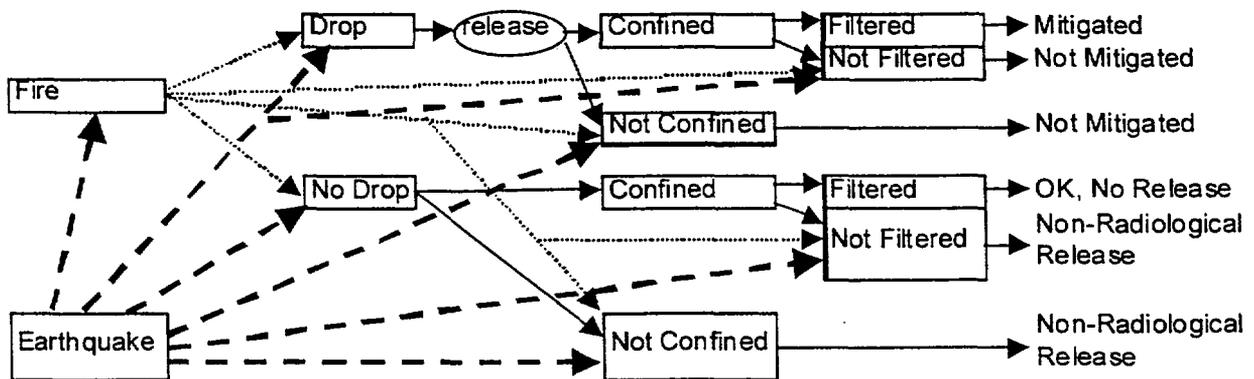
Fire initiator



NOTE: Failures events may be random or fire induced. Potential fire induced interactions/failures indicated by dashed lines.

Figure 10-3. Event Sequence Diagram for Fire Initiated Drop Event

Seismic Initiated Fire



NOTE: Failures events may be random, seismic, or fire induced. Potential fire induced failures indicated by light-dotted lines. Potential seismic induced interactions/failures indicated by heavy-dashed lines.

Figure 10-4. Event Sequence Diagram for Seismic & Fire Initiated Drop Event

Initiating Event: Earthquake	Crane Maintains Functional (1)	No Drop or Breach of WP (3)	Spent Fuel Remains Intact (4)	Confinement Maintained in Hot Cell (5)	HVAC Remains Intact and Functional (2)	Seq. No.	Source Term	Offsite Consequence (rem)
	yes	NA	NA	NA	NA	1	none	0
	GF or RF	GF	yes	yes	yes	2	C/SC, mitigated	2.00E-03
					GF or RF	3	C/SC, not mitigated	2
				GF or RF	GF - bypass	4	C/SC, not mitigated	2
		no	yes	yes		5	SNF inventory, mitigated	6.00E-03
					GF or RF	6	SNF inventory, not mitigated	6
				GF or RF	GF - bypass	7	SNF inventory, not mitigated	6

NOTES:

Potential seismic failures in hypothetical facility include:

- (1) the failure of a crane lifting a spent fuel waste package inside a waste handling building,
- (2) damage to the building ventilation (filtration) system,
- (3) the drop and breach of the waste package,
- (4) damage to the spent fuel,
- (5) partitioning of a fraction of the radionuclide inventory to the building atmosphere,
- (6) release of some radioactive material through the damaged ventilation (filtration) system, and
- (7) exposure of an individual (either a worker or a member of the public) to the released radioactive material.

Bypass = failure of hotcell structure allows airborne radiation to bypass the HVAC ducting and HEPA filters; C/SC = crud, surface contamination, or both; GF = guaranteed failure, dependent on precursor event or on initiating event; N/A = Not asked, precursor event preclude; RF = random failure; SNF Inventory = radionuclides from inside fuel rods, surface crud, and any contamination from waste package.

Figure 10-5. Baseline Seismic Event Tree for Load Drop

Although not illustrated in Figure 10-5, an earthquake may be able to initiate a fire inside the WHB and at the same time cause failure of the fire-protection system and other systems. This scenario could evolve into a sequence of events that leads to a release of radioactivity. Similarly, an earthquake may cause a flood or a spurious actuation of the fire protection system that, in conjunction with seismic failure of geometry controls, could lead to a criticality condition. The seismic analysis for preclosure safety must be exhaustive in identifying such possibilities.

Figure 10-5 is developed for a hypothetical facility as a baseline event tree that will be modified to illustrate how seismic classifications are developed. Initially, an earthquake of unspecified intensity or frequency is represented as the initiating event. The event tree in Figure 10-5 includes five events shown across the top of the figure. These event labels are known as the event headings. The logic diagram shows a single line for the initiating event (earthquake), but allows for two branches for each challenge to each of the event headings. The two branches represent, respectively, upward (yes) when the heading event is successful (or TRUE) and downward (no) when the heading event is FALSE (e.g., the function fails or is unavailable).

The failure criteria for the function have been precisely defined so that the meaning of the “no” branch is unambiguous.

In Figure 10-5, the causes of the various “no” branches are indicated as RF (random failure), independent of the occurrence of the earthquake, or GF (guaranteed failure) due to the occurrence of a preceding event (either a random event or the initiating earthquake). A special case of GF is indicated by GF-bypass to indicate that failure to maintain hot-cell structural integrity guarantees failure of the HVAC/HEPA filter function because the radioactive air is vented via other pathway(s). When an event succeeds, such as Crane Maintains Functions, some potential succeeding events cannot occur or are irrelevant. Such branches are indicated by “NA” to indicate that the branch-point question is not asked, or is not applicable for that event heading in that sequence of events.

The cause of the crane failure may be GF (dependent on the earthquake) or RF (an independent event). The GF cases are discussed in Section 7.1). In this example, it is assumed that any drop of the waste form results in its breach, so the breach is labeled as GF. Depending on the assumptions, all or a portion of the SNF assemblies could remain intact. This event could be correlated to the height of the drop, but for this illustration it is assumed to be an independent, random event with “yes” and “no” branches. The probability of the “no” branch can be varied in sensitivity analyses.

Tracing through a particular path in Figure 10-5 arrives at an End State that represents the severity of, or absence of, a release of radioactivity to the environment. Event sequences 1 through 7 are described as follows

- **Sequence 1**—An earthquake occurs but the crane maintains its functions and does not drop the waste form. Therefore, all other event headings are irrelevant and are labeled “NA.” Since there is no release in this sequence, there is no source term nor consequences.
- **Sequence 2**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence all of the SNF assemblies remain intact and all other event headings function normally (all yes). The only potential source term in this scenario might be contaminants from inside the breached waste form and/or crud that has been freed from the surfaces of the SNF assemblies. Since the HVAC/HEPA filter is functioning normally, the resulting release would be limited to whatever gaseous contaminant that might have been contained in the initial waste form. As discussed in Sections 10.1.4 and 10.1.5, the magnitude of dose from this source term determines important to safety classification and the seismic classification of the crane function.
- **Sequence 3**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence all of the SNF assemblies remain intact and all other event headings function normally (all yes) except the HVAC/HEPA filters. The HVAC/HEPA filters may fail dependently because of the earthquake (GF) or independently (RF). The only potential source term in this scenario might be

contaminants from inside the breached waste form and/or crud that has been freed from the surfaces of the SNF assemblies. Since the HVAC/HEPA filters are not functioning normally, however, the resulting release would include volatile and particulate matter, as well as gaseous contaminants and/or crud released from surfaces of the SNF assemblies or interior of the waste form. The unmitigated dose would be expected to be higher than that of Sequence 2.

- **Sequence 4**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence all of the SNF assemblies remain intact. The confinement of the hot cell fails to be maintained due to a dependent failure because of the earthquake (GF) or independently (RF). In this case the failure of the HVAC/HEPA filters is labeled as GF-bypass, representing the dependency on maintaining the hot cell confinement and controlled pathway through the HVAC. The only potential source term in this scenario might be contaminants from inside the breached waste form and/or crud that has been freed from the surfaces of the SNF assemblies. Because the HVAC/HEPA filters are not providing filtration, the resulting release would include volatile and particulate matter, as well as gaseous contaminants and/or crud released from surfaces of the SNF assemblies or interior of the waste form. The unmitigated dose would be similar to that of Sequence 3.
- **Sequence 5**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence, the SNF assemblies do not remain intact. The remaining part of the sequence is similar to Sequence 2. The potential source term in this scenario might be the radionuclide contents of the breached fuel rods, in addition to contaminants from inside the breached waste form and/or crud that has been freed from the surfaces of the SNF assemblies. Since the HVAC/HEPA filters are functioning normally, the resulting release would be gases. The mitigated dose would be similar to, but larger than, expected to be that of Sequence 2.
- **Sequence 6**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence, the SNF assemblies do not remain intact. The remaining part of the sequence is similar to Sequence 3. The HVAC/HEPA filters may fail dependently because of the earthquake (GF) or independently (RF). The potential source term in this scenario might be the radionuclide contents of the breached fuel rods in addition to contaminants from inside the breached waste form and/or crud that has been freed from the surfaces of the SNF assemblies. Since the HVAC/HEPA filters are not functioning normally, however, the resulting release would include volatile and particulate matter, as well as gases, contaminants, and/or crud released from surfaces of the SNF assemblies or interior of the waste form. The unmitigated dose would be expected to be higher than that of Sequence 5.
- **Sequence 7**—An earthquake occurs and the crane fails to maintain its functions and drops the waste form. The cause of the crane failure may be GF, dependent on the earthquake, or RF, an independent event. In this sequence, the SNF assemblies do not remain intact.

The remaining part of the sequence is similar to Sequence 4. The confinement of the hot cell fails to be maintained due to a dependent failure because of the earthquake (GF) or independently (RF). In this case the failure of the HVAC/HEPA filters is labeled as GF-bypass representing the dependency on maintaining the hot cell confinement and controlled pathway through the HVAC. Since the HVAC/HEPA filters are not functioning normally, the resulting release would include volatile and particulate, as well as gases, contaminants, and/or crud released from surfaces of the SNF assemblies or interior of the waste form. The unmitigated dose would be similar to that of Sequence 6.

10.1.5.3 Applying Seismic Event Tree in Seismic Classification

The SET defines potentially seismic-initiated or exacerbated event sequences. The source term and resulting consequences for each event sequence determines its importance to safety and its seismic classification. The sequences are examined one at a time to identify which, if any, of the SSCs associated with the event headings have to be hardened to withstand a design basis earthquake per the design approach of Seismic Topical Report No. 2 (YMP 1997). For illustration purposes, the following hypothetical offsite dose consequences are assumed for the sequences defined in Figure 10-5:

Sequence Number	Offsite Consequences (rem)
1	0
2	0.002
3	2
4	2
5	0.006
6	6
7	6

- **Sequence 1**—SSCs require no seismic classification because the initiating earthquake is not strong enough to cause SSC failure or radiological release.
- **Sequence 2**—The dose is less than the 15 mrem limit for Category 1 event sequences so the crane function and the no-breach function of waste form are not important to safety and, therefore, these SSCs do not require seismic classification.
- **Sequence 3**—The dose is greater than 15 mrem, but less than 5 rem, so the HVAC/HEPA filter function is important to safety and must withstand an FC-1 design basis earthquake. With the HVAC/HEPA filter designed as FC-1, the crane function remains not important to safety and does not require seismic classification.
- **Sequence 4**—The dose is greater than 15 mrem, but less than 5 rem, so the hot cell confinement function is important to safety and must withstand an FC-1 design basis earthquake. With the hot cell designed as FC-1, the crane function remains not important to safety and does not require seismic classification.
- **Sequence 5**—The dose is less than 15 mrem, so the crane function is not important to safety and, therefore, does not require seismic classification.

- **Sequence 6**—The dose is greater than 5 rem, so the HVAC/HEPA filter function is important to safety and must withstand an FC-2 design basis earthquake. With the HVAC designed as FC-2, the crane function remains not important to safety and does not require seismic classification.
- **Sequence 7**—The earthquake causes a failure of the confinement and a bypass of the HVAC/HEPA filter system. The unmitigated dose is greater than 5 rem, so the hot cell confinement function is important to safety and must withstand an FC-2 design basis earthquake.

This example illustrates the application of the deterministic approach to the selection of design basis earthquakes for SSCs important to safety. The application of ESDs and/or SETs ensures a more structured analysis to identify the SSCs that need to withstand the design basis earthquakes. These tools help in carrying out the approach described in Sections 10.1.4 and 10.1.5.

This safety case will assume that SSCs designed to a given design basis earthquake will not fail under earthquake conditions up to, and including, the design basis earthquake as a direct result of the earthquake. The deterministic approach is also termed the Step Function Fragility approach to indicate that the conditional probability of failure of an SSC is zero for earthquakes of intensity less than or equal to its design basis and one for any earthquake that exceeds the design basis earthquake. The following section describes how seismic sequence frequencies could be quantified using this approach. Section 10.1.8 describes how seismic sequence frequencies would be quantified using other fragility functions.

10.1.6 Frequency Quantification of Seismic Sequences Using Deterministic, Step-Function Fragility Functions or Seismic Margins Analysis

The safety case will assume that SSCs designed to a given design basis earthquake will not fail under earthquake conditions up to, and including, the design basis earthquake as a direct result of the earthquake. If the SSCs do fail as result of the earthquake, the consequences will be within the consequence regulatory limits. It is possible, however, that independent failures of one or more SSCs could occur during an earthquake and lead to doses beyond the regulatory limits; the frequencies of such sequences, however, will have to be less than $1 \times 10^{-6}/\text{yr}$ (i.e., beyond category 2 event sequences). This should not be too difficult since it is essentially the intersection of two independent events: an earthquake having a frequency of 1×10^{-3} per year for FC-1 (or 1×10^{-4} per year for FC-2) and an internal event sequence involving the independent failure of one or more SSCs that prevent or mitigate a release within a short time (e.g., 24 hours) after the earthquake.

Case 1—Figure 10-6 presents an event tree that illustrates the case where all SSCs are hardened to withstand an FC-1 design basis earthquake. The probability that the crane drops the waste form within 24 hours after the earthquake due to random failures is conservatively shown to be 1×10^{-3} (or 1×10^{-5} per lift for the lift that is in progress). Similarly, the probability that the confinement function of the hot cell and the HVAC/HEPA filters are unavailable in the release scenarios is 1×10^{-6} and 1×10^{-5} , respectively. It is seen that the frequency of all of the release scenarios resulting in doses of 2 rem or 6 rem is less than approximately 1×10^{-11} per year. This

frequency is too low to be considered credible. This conclusion is not surprising since the design was hardened.

Case 2—Figure 10-7 presents an event tree that illustrates the case where all SSCs are hardened to withstand an FC-1 design basis earthquake. However, an earthquake of a magnitude slightly larger than the FC-1 earthquake (and having a slightly lower frequency; assumed to be 9×10^{-4} per year) is assumed to occur. All of the SSCs (crane and lifting devices, confinement structure, and HVAC/HEPA filters fail dependently) (GF with a probability of 1.0). This results in sequences 1, 2, 3, 5, and 6 of Figure 10-6 being removed from the SET shown in Figure 10-7. The frequency of one release scenario in Figure 10-7 (Sequence 4) exceeds the Category 1 dose limits is 9×10^{-6} per year, (i.e., it is a credible event). However, its frequency makes it a Category 2 event sequence and its dose is less than the Category 2 limits, therefore, no seismic classification is required. The frequency of Sequence 7 is 9×10^{-4} which is also a Category 2 event sequence but the dose exceeds the Category 2 dose limits. Since this result is unacceptable, it indicates that some of the SSCs contributing to Sequence 7 must be hardened to withstand the FC-2 design basis earthquake.

Similarly, the SET can be modified to examine the effects of hardening some components (like the crane and HVAC/HEPA filter) to FC-1 and the hot cell confinement to FC-2. The consequences and event sequence frequencies are examples of how design bases conform with Seismic Topical Report No. 2 (YMP 1997).

While the NRC has tentatively concurred with Topical Report No. 2, they may request a demonstration of the seismic design margins that contribute to the risk-reduction factors. This demonstration will require confirmatory design analyses in the form of fragility factors or SMAs. These design analyses are beyond the scope of this PSA guide but are briefly described in Section 10.1.6. The application of such analyses in seismic sequence analyses is discussed in the following section.

10.1.7 Frequency Quantification of Seismic Sequences Using Fragility Functions or Seismic Margins Analysis

The purpose of this type of analysis is to provide a confirmatory demonstration that the Category 2 dose limits will not be exceeded in credible seismic sequences. Two approaches can be used: a seismic PRA or an SMA. Section 10.1.8.2 describes this method and the application of SETs. A seismic PRA may be performed later as part of a general PRA for the repository, if desired. The steps in a seismic PRA are briefly summarized in Section 10.1.8.1.

10.1.7.1 Seismic Probabilistic Risk Assessment Analysis

In a seismic PRA approach, three separate analyses are combined through probabilistic analyses (a convolution process) to estimate the frequencies of individual event sequences:

- **Preclosure Safety Seismic Systems Analysis**—This analysis, described in this chapter of the PSA guide, applies the methodology of event tree analysis to identify the seismically-induced sequences of events and the SSCs that come into play, and fault tree analysis to model the specific failure modes of the SSCs that come into play. The

combinations of earthquake initiator and concurrent failures of one or more SSCs are modeled in a top-event fault tree that provides

Initiating Event Earthquake	Crane Maintains Functional (1)	No Drop or Breach of WP (3)	Spent Fuel Remains Intact (4)	Confinement Maintained in Hot Cell (5)	HVAC Remains Intact and Functional (2)	Seq. No.	Source Term	Offsite Consequence (rem)	Frequency
1.00E-03	yes	NA	NA	NA	NA	1	none	0	9.99E-04
9.99E-01	RF	GF	yes	yes	yes	2	C/SC, mitigated	2.00E-03	1.00E-08
1.00E-03	1	0.01	1.00E+00	1.00E+00	RF	3	C/SC, not mitigated	2	1.00E-13
					RF	4	C/SC, not mitigated	2	1.00E-14
					GF-bypass	4	C/SC, not mitigated	2	1.00E-14
		no	yes	yes		5	SNF inventory; mitigated	6.00E-03	9.90E-07
		0.99	1.00E+00	1.00E+00	RF	6	SNF inventory; not mitigated	6	9.90E-12
					RF	7	SNF inventory; not mitigated	6	9.90E-13
					GF-bypass	7	SNF inventory; not mitigated	6	9.90E-13

NOTES:

Assume crane and lifting devices, hotcell structure, and HVAC designed to withstand FC-1 earthquake.

Numbered potential seismic failures identified in Figure 10-8.

Bypass = failure of hotcell structure allows airborne radiation to bypass the HVAC ducting and HEPA filters; C/SC = crud, surface contamination, or both; GF = guaranteed failure, dependent on precursor event or on initiating event; N/A = Not asked, precursor event preclude; RF = random failure; SNF Inventory = radionuclides from inside fuel rods, surface crud, and any contamination from waste package.

Figure 10-6. Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake

the appropriate logic model for the combinations of specific subsystems or components that have to fail during the earthquake to obtain the undesired release scenario. A PRA workstation program such as SAPHIRE (Smith et al. 2000) provides features to model the dependent, common-cause failures associated with earthquakes among multiple components in a system. The outputs of such analyses are seismic cutsets that include the various combinations of seismically induced failures and RFs.

The analysis includes the potential interactions with other SSCs (i.e., potential failure modes of a given SSC due to the impact of other SSCs in close proximity or overhead). In addition, the analyses will identify any potential seismically-initiated fire (or flooding) scenarios that can propagate into a release sequence or a criticality.

These analyses are performed by PSA personnel with the assistance of system/component design personnel.

Initiating Event: Earthquake	Crane Maintains Functional (1)	No Drop or Breach of WP (3)	Spent Fuel Remains Intact (4)	Confinement Maintained in Hot Cell (5)	HVAC Remains Intact and Functional (2)	Seq. No.	Source Term	Offsite Consequence (rem)	Frequency
9.00E-04						1	(removed from tree)	0	9.00E-10
	GF	GF	yes			2	(removed from tree)	2.00E-03	9.00E-18
	1.00E+00	1	0.01			3	(removed from tree)	2	9.00E-12
				GF	GF-bypass	4	C/SC, not mitigated	2	9.00E-06
				1.00E+00	1	5	(removed from tree)	6.00E-03	8.91E-16
		no				6	(removed from tree)	6	8.91E-10
		0.99				7	SNF inventory; not mitigated	6	8.91E-04
				GF	GF-bypass				
				1.00E+00	1				

NOTES:

Assume crane and lifting devices, hotcell structure, and HVAC designed to withstand FC-1 earthquake.

Numbered potential seismic failures identified in Figure 10-8.

Earthquake exceeding VBM of FC-1 earthquake occurs at 9×10^{-4} ; assume step function fragility for SSCs hardened to FC-1.

Bypass = failure of hotcell structure allows airborne radiation to bypass the HVAC ducting and HEPA filters; C/SC = crud, surface contamination, or both; GF = guaranteed failure, dependent on precursor event or on initiating event; N/A = Not asked, precursor event preclude; RF = random failure; SNF Inventory = radionuclides from inside fuel rods, surface crud, and any contamination from waste package.

Figure 10-7. Seismic Event Tree – Structures, Systems, and Components Hardened to Frequency Category 1 Earthquake, but Earthquake greater than Frequency Category 1

- SSC Fragility Analysis**—This analysis is applied to SSCs that appear in the seismic event sequences to determine the conditional probability of failure (or loss of safety function) given the occurrence of a peak vibratory ground motion of a given magnitude. Figure 10-8 is an example of the format of a fragility curve. It was generated as a family of lognormal distributions represented by a median value of acceleration at which a particular SSC fails to perform its safety function and through the use of uncertainty factors representing the random (aleatory) and knowledge (epistemic) uncertainty in the seismic response of the SSC.

The fragility function for each SSC is displayed as a set of three S-curves that are plots of probability (ranging from 0 to 1) versus the PGA associated with an earthquake (the acceleration ranges from fraction of g to tens of g's). The three curves represent, from top to bottom, the upper 95th percent, median, and lower 5th percent confidence levels. The abscissa of the fragility function of a given SSC is dependent upon its elevation and location within the structure (e.g., WHB) because the amplifications of motion due to

the lever-arm above the ground and the damping associated with the structure and mountings are factored in. This analysis is performed by structural analysts and/or fragility specialists. Figure 10-8 displays the format of fragility curves (this figure does not represent a real SSC). The three principal curves represent, from top to bottom, the upper 95th percent, median, and lower 5th percent confidence levels.

- **Probabilistic Seismic Hazards Analysis**—This analysis is the subject of Seismic Topical Reports Nos. 1 and 3. Topical Report No. 1 describes the method; Topical Report No. 3 provides the results. The PSHA results are in the form of a family of curves representing the annual probability (or frequency) of exceedence versus PGA at the repository site. The SMA is represented by a family of curves that include the median, mean, 5th percent Confidence Level, and 95th percent Confidence Level. This analysis is performed by a team of PSHA experts.
- **Seismic Event Sequence Frequency Analysis**—The three analyses are brought together in a probabilistic analyses, such as a Monte Carlo analysis or a Latin Hypercube analysis. Each sequence from the seismic sequence analysis is represented by one or more cutsets consisting of the product of the initiating event and the conditional failure of all of the contributing SSC.

Since the frequency of the initiating event and the fragility are both represented as probability density functions (PDFs), the product function will result in a PDF. The product PDF is obtained by a convolution analysis that is most easily performed numerically using a Monte Carlo-Latin Hypercube analysis. The output PDF provides the median, mean, 5th percent, and 95th percent bounds for each seismic sequence. The PDFs of several seismic release event sequences, having similar consequence levels, can be combined probabilistically to obtain a PDF for group of scenarios, which could all occur given an earthquake.

These analyses are performed by PSA personnel.

The seismic PRA approach is seen to be rather complex. Such analysis is not warranted for the LA submittal for construction authorization.

10.1.7.2 Seismic Margins Analysis

SMA has some similarity to seismic PRA. SMA makes use of the fragility factors and event sequence analysis, but the overall analyses are simpler than seismic PRA. The seismic hazards PDF is not directly used in the analysis, nor is an event sequence seismic PDF produced.

The goal of a SMA, as developed for NPPs, is to demonstrate that there is a high confidence of low probability of failure (HCLPF) to achieve a safe condition after the occurrence of a seismic margins earthquake (SME). The SME is stronger than a design basis earthquake. For NPPs, the safe condition is a safe shutdown and the design basis earthquake is the SSE. The SME is generally specified to be twice the SSE (i.e., for a 1-g SSE, the SME would be a 2-g PGA) for NPPs. The annual probability of exceedence of the SME is not used directly in the SMA, but it is usually assumed or shown to be at least an order of magnitude less probable than the SSE.

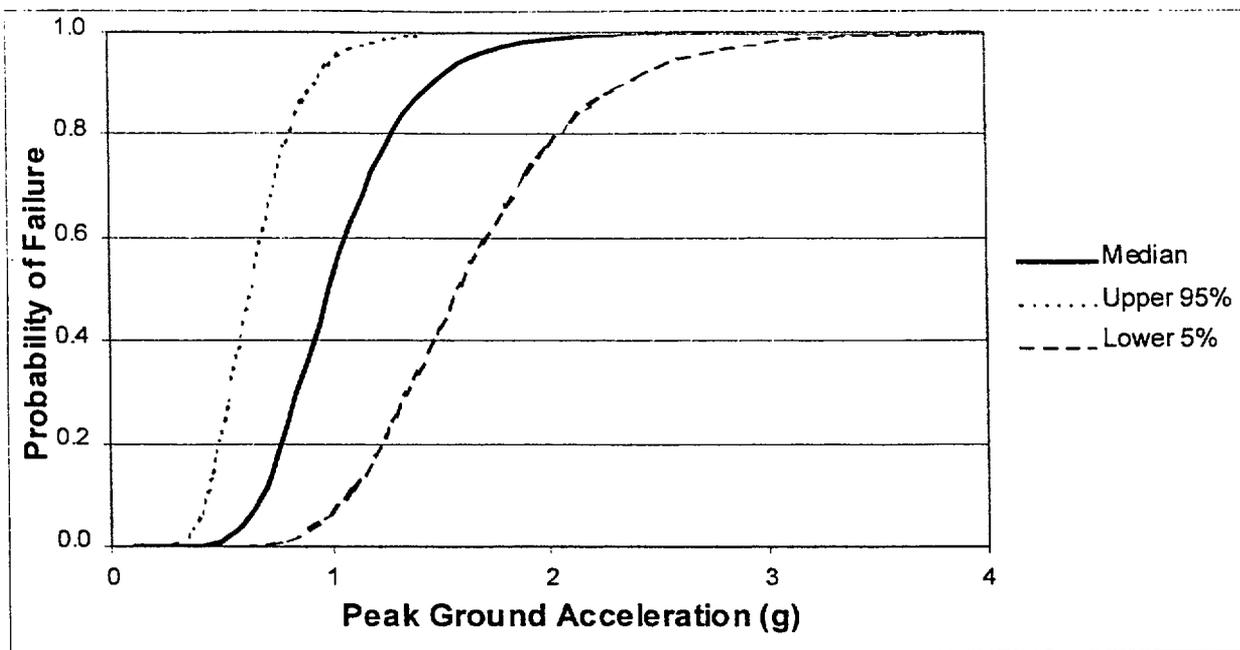


Figure 10-8. Example Fragility Curves

The SMA employs two of the three types of analyses used in seismic PRA, with some differences, as described in the following paragraphs:

- **Preclosure Safety Seismic Systems Analysis**—The approach described in Sections 10.1.4 and 10.1.5 are applied to identify the SSCs that must be designed to withstand, respectively, the FC-1 or FC-2 design basis earthquake. Designers of the affected SSCs apply appropriate methods, codes, and standards to ensure that the SSCs will perform the respective safety function while withstanding a design basis earthquake.
- **Seismic Margin Earthquake Definition**—Following the precedence of NPPs, the SME is defined to have a PGA that is twice that of the FC-2 design basis earthquake. The goal of the SMA is to demonstrate that there is a High Confidence of Low Probability of Failure (HCLPF). This HCLPF is a probabilistic measure that a seismically induced event sequence will not result in an offsite dose that exceed 10 CFR 63.111(b)(2) i.e., not exceed the dose limits for Category 2 event sequences. It is expected that no SMA will be performed for those SSCs designed to withstand an FC-1 design basis earthquake because such SSCs are already backed up by SSCs that withstand the FC-2 design basis earthquake and such an analysis is not in keeping with the philosophy of the SMA developed for NPPs.
- **SSC Fragility and HCLPF Analysis**—
 1. **Fragility analyses**—These analyses are performed for the SSCs that appear in the seismic event sequences to determine the conditional probability of failure (or loss of safety function) given the occurrence of a peak vibratory ground motion of a given magnitude. The fragility function for each SSC is displayed as a set of three

S-curves that are plots of probability (ranging from 0 to 1) versus the PGA associated with an earthquake. See Figure 10-8 and the discussion in Section 10.1.8.1.

2. **HCLPF analysis**—This analysis uses the upper 95th percent fragility curve for each SSC. The PGA of the SME is used as input on the abscissa of the 95th percent fragility curve to determine the conditional probability of failure. Using NRC precedence for SMA, if the probability of failure is less than or equal to 0.05 at the 95th percent confidence, it is considered to have HCLPF. The HCLPF value for a given SSC is expressed as the PGA, in units of “g,” at which the SSC would fail to perform its safety function with a probability of 0.05 at the 95th percent confidence level. Such analyses are performed by structural analysts and/or fragility specialists.

The step in performing a seismic margins analysis systems analysis as described in NUREG/CR-5632 (NRC 1990). As in a PRA approach, the systems analysis must define accident sequences for a range of feasible initiating events. Event sequences and consequence analyses may have been performed previously for internal-event or seismically induced initiator. Although the baseline safety analysis may have treated each of these initiating events as an independent event (i.e., drops of waste forms, loss of offsite power, fires inside the WHB, or runaway transporter), each initiating event is examined to determine if it could also be initiated by an earthquake. In addition, each event heading in the event tree for each initiator is examined for potential vulnerability to an earthquake. The vulnerability includes not only the failure of the front-line prevention or mitigation SSCs, but also the support systems (e.g., electrical power supplies, instrumentation, and control systems) and human actions that may be influenced by the occurrence of an earthquake.

The overall probability of an event sequence following an earthquake will account for dependent and independent failures. However, basic events are screened to delete the low probability independent events and dependent events that do not contribute significantly to the seismic sequences. The bases for the screening are described later.

Modification of System Fault Trees—The fault tree logic models for SSCs that appear in event tree headings are modified to include the potential seismically-induced failures. Each basic event (see Section 7.2) is assumed initially to be a candidate for both seismically-induced and independent (random) failures. If not already treated, the fault trees are modified to include potential common-cause failures and human induced failures. Preliminary, a non-quantitative evaluation of the cutsets is performed to check the fault-tree logic. For reactor SMA systems analyses, such fault trees are generally too complex, so screening and/or pruning is performed. Such extensive screening (or the criteria for screening) may not be necessary for the event sequences and simpler repository systems.

Screening of SMA System Fault Trees—The first seismic screening for a commercial nuclear power plant applies SMA guidelines (NRC 1986) that include generic HCLPF values (given in terms of PGA) for various categories of equipment. The applicability of the generic HCLPF values has to be verified by the systems and fragility analysts based on guidance and notes attached to the table of generic HCLPF values. The SSE for a typical commercial nuclear

reactor plant in the Eastern U.S. is 0.15 g and, therefore, the SME is 0.3 g (NRC 1990). Many commercial NPP SSCs have HCLPF values greater than 0.3 g and would be screened out of system fault trees. The generic databases indicate that for a SME in the range of 0.3 g to 0.5 g, most equipment has to be evaluated on a plant-specific basis. In many cases, verification of adequate equipment anchorages is sufficient to eliminate concern about the failure of a given piece of equipment during a SME.

For an SME greater than 0.5 g, however, virtually no SSCs can be screened out for the generic commercial nuclear reactor plants. Since the SME for the repository site may exceed 0.5 g, the generic HCLPF values may not provide the bases for screening. Instead, site-specific HCLPF values will have to be derived for repository SSCs.

In addition to direct seismic failure, some safety-significant SSCs in the system fault tree could be vulnerable to failure by secondary system interaction effects. These interaction effects could include failure of structural walls, falling equipment, relay chatter in the controls, or failure of electrical supply systems. Unless the specific interaction can be ruled out from design criteria or drawings, they may have to be kept in the fault trees until they are eliminated by as-built considerations such as a facility walkdown.

The next screening process aims to eliminate low-probability, non-seismic events. Since the event sequences of interest are all conditional on the unlikely occurrence of an SME, there is no point in being concerned about unlikely random events or combinations of events. Since the FC-2 design basis earthquake for the repository has an annual probability of 1×10^{-4} , any random event having a probability of less than approximately 1×10^{-3} would result in a sequence below the Category 2 threshold. Therefore, events with probability less than approximately 1×10^{-3} should be screened out (i.e., deleted from the fault tree model) unless there is some other reasons for retaining them, as discussed in the following paragraph.

Generally, only those equipment failure modes or human interactions with a probability greater than 1×10^{-3} that could exacerbate an event sequence are kept in the logic model. However, a failure with a probability less than 1×10^{-3} may be retained in the model if the failure could result in failures of one train each in multiple (different) systems or if the failure could result in failures of multiple trains in the same system. This screening rule was developed for reactor plant SMAs and may not be applicable to a repository.

The simplified system fault trees are then quantified using the appropriate repository database and mission times for the non-seismic events using a fault-tree program (e.g., the SAPHIRE program [Smith et al. 2000]). Cutsets to order 3 and 4 with probabilities to 1×10^{-6} are generated. The higher order and low probability cutsets are examined to see if any events were overlooked in the screening process. Such leftovers, if any, are subjected to the screening rules to further simplify the system fault trees.

Fault Tree Construction for Seismic Margins Event Sequences—A sequence fault tree is constructed for each seismic sequence that has been identified as having consequences that would exceed the 10 CFR Part 63 performance requirements if not mitigated by one or more SSCs that can withstand the design basis earthquake. The top event is the occurrence of a sequence that exceeds the performance requirements. The initiating event (earthquake) and other

events are input to the top event through an AND gate. The sequence fault tree is then analyzed to identify the minimal cutsets for the sequence. Each cutset will include, in addition to the initiating earthquake, one or more seismically-induced failures or random events. The random events include equipment failures, human errors, and common-cause failures.

The list of minimal cutsets for each sequence reveals the seismically-induced failures that can result in the top event. Seismic failures may appear in the cutsets as singles or doubles.

Seismic Margins Evaluation—Since 10 CFR Part 63 does not include an integral risk measure, the seismic margins evaluation can be applied to each sequence whose consequences exceed 10 CFR 63.111(2).

The probability of the initiating event is assumed to 1.0. The objective of the analysis is to demonstrate that a suitably low conditional probability of an unacceptable release exists, given an earthquake of the magnitude of the SME (specified here as vibratory ground motion having peak ground acceleration of g_{SME}). Because the components having a HCLPF greater than g_{SME} were already screened out of the model, the remaining potential seismically-induced events could potentially cause the unwanted release. However, it is desired that none of the events will appear in cutsets as singles, but only in doubles or higher-order cutsets.

In SMA for NPPs that have complex sequence analyses involving fault trees from several preventive and mitigation systems, it is typical to apply additional screening rules to the sequence cutsets to keep only cutsets that meet the following criteria:

1. Single events, either seismic or random
2. Double cutsets that contain at least one seismic failure
3. Triple cutsets that contain at least one seismic failure
4. Quadruple cutsets containing at least one seismic failure and a conditional event that effectively reduces the cutset to a triple.

After applying these screening rules, a reduced cutset list is obtained. The laws of Boolean algebra (mainly the absorption law) are applied so that many cutsets containing the same seismic failure, or RF, are absorbed into the lowest order cutset containing that failure event. The result is the final Boolean expression for a given sequence or the top event probability that is being considered (e.g., the sum of several sequences that give the unwanted consequence).

The final Boolean expression is examined for the final conditional probability. As long as there is no single-event seismic term (having an HCLPF less than g_{SME}) in the final Boolean expression and such seismic failures appear only in double or triples whose non-seismic probability is less than 1×10^{-3} , it can be concluded that the sequence probability meets the seismic margins criteria. If the seismic margin is adequate, it is generally concluded that the only path for the unwanted sequence(s) will result from RFs (often from human action or common-cause failure). The likelihood for a human error, for example, may be assumed to be quite high following a SME.

10.2 FLOODING

10.2.1 Purpose

This section defines the methods to determine the potential for flooding and the extent of any flood protection required for SSCs important to radiation safety or waste isolation.

10.2.2 Scope

This section provides guidance for the interpretation and use of NRC guidance and industry standards to determine the applicability of flooding for the repository. Areas to be considered include historical flooding, intense precipitation, upper level of possible flood conditions, facility design to determine whether flood effects need to be considered in plant design or emergency procedures, and the extent of any flood protection required for SSCs necessary for preclosure safety and waste isolation.

10.2.3 Overview of Approach

Compliance with 10 CFR 63.21(c)(1)(iii), NRC guidance provided by NUREG-0800 (NRC 1987, Chapter 2), and industry standards are used for guidance for acceptable criteria for license application.

10.2.4 Details of Approach

10.2.4.1 Potential for Flooding

The flood history and the potential for flooding are to be reviewed for applicability. This section should provide a summary and identification of the flood-producing phenomena applicable to the site or region considered in establishing the flood design bases for SSCs. Phenomena to be examined include the following:

- Stream flooding (probable maximum flood [PMF])
- Surges
- Seiches
- Tsunami
- Seismically induced dam failures
- Flooding caused by landslides
- Ice loadings from water bodies.

Regulatory Guide 1.59, *Design Basis Floods for Nuclear Power Plants*, provides previous NRC guidance for estimating the design basis for flooding considering the worst single phenomena and combinations of less severe phenomena. Regulatory Guide 1.29 identifies the SSCs and Regulatory Guide 1.102 describes acceptable flood protection to prevent the SSCs from being adversely affected.

10.2.4.2 Determination of Maximum Water Level

ANSI/ANS-2.8-1992, *American National Standard for Determining Design Basis Flooding at Power Reactor Sites* (ANSI/ANS 1992), defines the PMF as:

The hypothetical flood (peak discharge, volume, and hydrograph shape) that is considered to be the most severe reasonably possible, based on comprehensive hydrometeorological application of probable maximum precipitation and other hydrologic factors favorable for maximum flood runoff such as sequential storms and snowmelt.

The same ANSI/ANS standard also defines the probable maximum precipitation as follows:

The estimated depth of precipitation for a given duration, drainage area, and time of year for which there is virtually no risk of exceedance. The probable maximum precipitation for a given duration and drainage area approximates the maximum that is physically possible within the limits of contemporary hydrometeorological knowledge and techniques.

These definitions describe events that are the most severe or the greatest physically possible for a specific site. The probability of occurrence of these events should be extremely low. By conservatively assuming the occurrence frequency is greater than 1×10^{-6} , rainfall-related flooding events will be evaluated as Category 2 event sequences. The following steps should be followed to perform a flood analysis:

- Review and comply with the Yucca Mountain Standard Review Plan (when issued).
- Identify flooding events that are applicable to the site or operating facilities. Candidate events are documented in the *MGR External Events Hazards Analysis* (CRWMS M&O 2000a) and *Monitored Geologic Repository Internal Hazards Analysis* (CRWMS M&O 2000b). The list of applicable internal and external events was screened at a high level for gross credibility, applicability to preclosure, radiological safety, and applicability to the Yucca Mountain location. Stream flooding, surges, seiches, tsunami, seismically induced dam failures, flooding caused by landslides, and ice loadings from water bodies are to be considered as required by NUREG-0800 (NRC 1987, Section 2.4.2).
- Identify historical flooding at the site and the region of the site. Identify the types of flood-producing phenomena that are considered in establishing the flood design bases for important to safety design features (e.g., stream flooding, surges, seiches, tsunami, dam failure, flooding caused by landslides, and ice loadings from water bodies).
- Consider 10 CFR Part 50, Appendix A, *General Design Criterion 2, Design Bases for Protection Against Natural Phenomena*, as it relates to important to safety SSCs being designed to withstand the effects of applicable external flooding initiating events.

- Consider 10 CFR Part 100, *Reactor Site Criteria*, as it relates to identifying and evaluating specific criteria for flood history, flood design considerations, effects of local intense precipitation.
- Consider Regulatory Guide 1.29, *Seismic Design Classification*, for estimating design basis flooding considering the worst single phenomena and combinations of less severe phenomena. This guide identifies important to safety SSCs and Regulatory Guide 1.102, *Flood Protection for Nuclear Power Plants*, describes acceptable flood protection to prevent important to safety facilities from being adversely affected.
- Consider publications of the U.S. Geological Survey, National Oceanic and Atmospheric Administration, Soil Conservation Service, Corps of Engineers, applicable State and river basin authorities, and other similar agencies relating to hydrological characteristics and extreme events in the region.
- A sample statement of an NRC evaluation of water level findings is provided in NUREG-0800 (NRC 1987, Section 2.4.2.IV). This sample statement will provide a sample of the results the NRC must be able to confirm.

10.2.4.3 Probable Maximum Flood on Streams and Rivers

The PMF as defined in Regulatory Guide 1.59, *Design Basis Floods for Nuclear Power Plants*, should be evaluated to establish the stream and river flooding design basis referred to in 10 CFR Part 50, Appendix A, *General Design Criterion 2*. The probable maximum precipitation should also be evaluated for the roofs of important to safety structures. One of the following three conditions must be met:

1. The elevation attained by the PMF establishes a required protection level to be used in the design of the facility.
2. The elevation attained by the PMF is not controlling; the design basis flood protection level is established by another flood phenomenon (e.g., the probable maximum hurricane).
3. The site is dry (i.e., the site is well above the elevation attained by a PMF).

For condition 3, the site grade must be well above the NRC-determined PMF water levels. The evaluation of the adequacy of the margin (difference in flood and site elevations) is generally a matter of engineering judgement. This judgement is based on the confidence in the flood level estimate and the degree of conservatism in each parameter used in the estimate.

The following documents may be used as appropriate to determine the PMF data acceptability:

- Regulatory Guide 1.59 provides guidance for estimating the PMF design basis.
- Regulatory Guide 1.29 identifies the important to safety SSCs.

- Regulatory Guide 1.102 describes acceptable flood protection to prevent important to safety facilities from being adversely affected.

10.2.4.4 Potential Dam Failures, Surge, Seiche, and Tsunami Flooding

Justify the conclusion (as found in the *MGR External Events Hazards Analysis* [CRWMS M&O 2000a]) that there are no water control failure, surge, seiche, or tsunami flooding to evaluate for the Site.

10.2.5 Flooding Protection Requirements

Review and consider, as appropriate, SSCs relied upon for plant flood protection whose failure could result in uncontrolled release of significant radioactivity to assure conformance with 10 CFR Part 63.

If flood protection is required for any important to safety SSCs, consider, as appropriate, 10 CFR 50.55a requirements for SSCs to be designed and constructed to quality standards commensurate with the importance of the safety function to be performed.

NUREG-0800 (NRC 1987) requires a determination as to which SSCs are important to safety and should be protected against floods or flooded conditions. A failure modes and effects analysis may be performed to determine that the flooding consequences resulting from failures of such liquid-containing systems close to essential equipment will not preclude required functions of safety systems.

10.2.6 Consequence Analysis

For each applicable credible event, either individually or in combination with other events in an accident sequence, perform: (1) a frequency analysis that demonstrates the event is not credible (2) a nuclear safety analysis that demonstrates a radiological release does not occur as a result of the event (3) a consequence analysis that demonstrates that the radiological consequences of the event are within regulatory requirements or that identifies required preventative or mitigative SSCs that ensure the radiological consequences are within regulatory requirements.

For each of the credible events identified, dose assessments will be performed to show compliance to 10 CFR Part 63 requirements as applicable.

The frequency analysis of an event determines if the event is credible. If not credible, no quantitative dose limits are promulgated by 10 CFR Part 63, no further analysis is required, and there is no impact to other repository design or licensing organizations. Event sequences that are beyond Category 2 will be tracked to show safety design margin. If the event is determined to be credible, it is categorized based on the 10 CFR Part 63 definition, and an analysis is performed to determine if the dose limits associated with the applicable event category can be met.

Category 1 event sequences (i.e., frequency greater than 1×10^{-2} events per year) require that the sum of annual doses, exposures, and releases do not exceed limits specified in 10 CFR Part 63 for the public and 10 CFR Part 20 for occupational workers. Category 2 event sequences (i.e., frequency less than 1×10^{-2} and greater than 1×10^{-6} events per year) require that the

consequences of a specific Category 2 event sequence not exceed dose limits as specified in 10 CFR Part 63 for the public beyond the preclosure controlled area.

The consequence analysis determines if the calculated doses are within the applicable regulatory limits. If the calculated dose exceeds applicable limits, SSCs important to radiological safety are designated, new requirements are allocated to the system, assumptions are revised, the design configuration is revised (if necessary), and the dose is recalculated and again compared to applicable regulatory dose limits.

10.3 WINDS AND TORNADOS

10.3.1 Purpose

This analysis defines the methods to determine the design basis wind speed and design basis tornado (including tornado-generated missile) and the protection required for SSCs important to preclosure safety and waste isolation. These parameters will serve as the basis for the requirements that are developed to mitigate the effect of design basis winds and a design basis tornado on the structural stability of the repository surface facilities. The primary systems that will contain requirements developed from this section include the WHB, Waste Treatment Building, and Carrier Preparation Building.

10.3.2 Scope

This section provides guidance on the interpretation and use of NRC guidance and industry standards to determine the applicability of external storm events for the repository. A preliminary hazard analysis performed in 1996 for the repository screened out the majority of the postulated external storm events (CRWMS M&O 1996). The analysis was unable to screen out extreme winds and tornado-related events.

10.3.3 Overview of Approach

Compliance with 10 CFR 63.21(c)(1)(iii), NRC guidance provided by NUREG-0800 (NRC 1987, Chapter 3) and industry standards are used for guidance for acceptable design basis/requirements for the LA submittal.

10.3.4 Details of Approach

10.3.4.1 Methodology

Currently, no regulations for design basis tornadoes or extreme winds have been promulgated for high-level radioactive waste sites. Therefore, the criteria used to develop the repository design basis for those phenomena have been adopted from the guidance provided in NUREG-0800 (NRC 1987).

10.3.4.2 Extreme Winds

The typical method for demonstrating compliance of the design of structures that have to withstand the effects of extreme winds is provided in NUREG-0800 (NRC 1987, Sections 2.3.1

and 3.3.1). This NUREG states that the 100-year return period “fastest mile of wind,” including the vertical velocity distribution and gust factor, should be used as the design and operating bases (NRC 1987, Section 2.3.1) and be based on applicable ANSI building code requirements, with suitable corrections for local conditions. The current standard published by the American National Standards Institute is ASCE 7-98, *Minimum Design Loads for Buildings and Other Structures* (ASCE 2000). The basic wind speed defined in this document is a 3-second gust with an annual probability of 0.02 of being equaled or exceeded (50-year mean recurrence interval). Regional data can be used to determine the basic wind speed.

The most recent site-specific wind speed data must be used in preclosure safety analyses. Wind speed data is being collected near the repository site, and includes observed maximum daily one-second gust and one-minute wind speed at nine locations for the period from 1993 to 1996 (CRWMS M&O 1997). The magnitude of the 50-year and 100-year return wind speeds were also estimated from this site-specific data. The example data shown in Table 10-4 corresponds to the location with the highest value in the meteorological monitoring network.

Table 10-4. Example Maximum Estimated and Observed Wind Speeds near Yucca Mountain, Nevada

	Wind Speed (m/sec)[mph]	
	50-year (3 second gust)	100-year (1 minute)
Observed	40.22 [90]	33.16 [74]
Estimated	54.11 [121]	48.47 [109]

Source: CRWMS M&O 1997

10.3.4.3 Tornado

Regulatory Guide 1.76 provides guidance for the selection of a design basis tornado for the three regions applicable to the continental United States. The design basis tornado characteristics for the applicable region can be used in the design of important to safety SSCs. A design basis tornado with less conservative parameter values than the regional values given in Regulatory Guide 1.76 can be selected. If the less conservative design basis tornado is selected for use the MGR, a comprehensive analysis must be performed to justify the selection. The subjects in the following paragraphs should be considered when determining the design basis tornado for the Yucca Mountain site.

The method for demonstrating compliance of the design of structures that have to withstand the effects of design basis tornadoes is provided in NUREG-0800 (NRC 1987). This guide states that facilities must be designed so that facilities remain in a safe condition in the event of the most severe tornado that can reasonably be predicted to occur at a site as a result of severe meteorological conditions.

The design basis tornado characteristics provided by Regulatory Guide 1.76 are shown in Table 10-5. Using these properties, it is possible to develop a definition for a design basis tornado in terms of the six tornado parameters and use analytical techniques for estimating values of these parameters for purposes of design with an adequate level of conservatism.

Table 10-5. Design Basis Tornado Characteristics

Region**	Maximum Speed* (mph)	Rotational Speed* (mph)	Translational Speed (mph)		Radius of Maximum Rotational Speed (feet)	Pressure Drop (psi)	Rate of Pressure Drop (psi/sec)
			Max	Min			
I	360	290	70	5	150	3.0	2.0
II	300	240	60	5	150	2.25	1.2
III	240	190	50	5	150	1.5	0.6

Source: Regulatory Guide 1.76

* The maximum wind speed is the sum of the rotational speed component and the maximum translational speed component.

** Region refers to the three tornado intensity regions within the contiguous United States as listed in Figure 1 of Regulatory Guide 1.76. Region III applies to the area surrounding Yucca Mountain.

The design basis tornado characteristics in Table 10-5 are based on a tornado that has a probability of occurrence of 10^{-7} per year (Ramsdell and Andrews 1986).

Subsequent to the issuance of Regulatory Guide 1.76, the American Nuclear Society, through the American Nuclear Standards Institute, published ANSI/ANS-2.3-1983, *Standard for Estimating Tornado and Extreme Wind Characteristics at Nuclear Power Sites* (ANSI 1983). This publication established guidelines to estimate the frequency of occurrence and the magnitude of parameters associated with tornadoes, hurricanes, and other extreme winds. Figures were presented that illustrated the regionalized tornado wind speed corresponding to a given probability. The information is summarized in Table 10-6. Although this publication expired in 1993, it represented the current state of knowledge on tornado and extreme wind characteristics at the time of publication (ANSI 1983).

Table 10-6. Tornado Wind Speed (miles per hour) by Region

Region *	Probability of Occurrence per Year		
	10^{-5}	10^{-6}	10^{-7}
I	200	260	320
II	150	200	250
III	100	140	180

Source: *Standard for Estimating Tornado and Extreme Wind Characteristics at Nuclear Power Sites* (ANSI 1983)

* Region III applies to the area surrounding Yucca Mountain.

In 1986, the NRC issued new guidance on tornado strike and intensity probabilities in NUREG/CR-4461, *Tornado Climatology of the Contiguous United States* (Ramsdell and Andrews 1986). The new guidance was based on 30 years of data contained in the National Severe Storms Forecast Center tornado database from the period of January 1, 1954 through December 31, 1983. The report contains tornado characteristics including the number of occurrences, frequencies of occurrence, and average dimensions. Values are provided for 5-degree latitude and longitude boxes for the contiguous United States.

Table 10-7 lists example wind speeds provided for 10^{-5} , 10^{-6} , and 10^{-7} per year probabilities of occurrence for the 5-degree latitude and longitude box containing the repository site. Both the nominal (expected) value and the value associated with the upper end of the 90 percent confidence interval for strike probabilities are shown. Statistically, this latter value is interpreted as the maximum value in a range that has a 90 percent chance of containing the true strike probability. The wind speed value (10^{-6} per year) selected for the repository is 189 miles per hour.

Table 10-7. Example Tornado Wind Speed for 5-Degree Latitude and Longitude Box Containing Yucca Mountain, Nevada

	Strike Probability of Occurrence per Year		
	10^{-5}	10^{-6}	10^{-7}
Nominal Wind Speed* (mph)	-	131	Not provided
Upper 90% Wind Speed* (mph)	151	189	189

Source: Ramsdell and Andrews (1986)

* Wind speed is the sum of the translational and rotational components.

The pressure drop and the rate of pressure drop associated with a maximum tornado vortex (funnel) impacting a structure are two additional design basis tornado requirements needed for repository structural analyses. These values were not provided with the example estimated speed shown in Table 10-7.

Table 10-5 shows Regulatory Guide 1.76 pressure terms corresponding to the wind speeds given for the three regions of the United States. The table lists maximum tornado wind speeds, rotational speeds, maximum and minimum translation speeds, an assumed vortex radius of 150 feet, and the corresponding pressure drop and rate of pressure drop. The maximum pressure drop (pounds-force per square-inch) values can be calculated from the total and translation speeds using the methodology presented in ANSI/ANS-2.3-1983 (ANSI 1983):

10.3.4.4 Tornado-Generated Missiles

The typical method for demonstrating compliance with the design of structures that have to withstand the effects of tornado-generated missiles is provided in Sections 3.5.1.4 (*Missiles Generated By Natural Phenomena*) and 3.5.3 (*Barrier Design Procedures*) of NUREG-0800 (NRC 1987). Important-to-safety equipment must be protected, as required, against damage from missiles that might be generated by the design basis tornado.

NUREG-0800 (NRC 1987, Section 3.5.1.4) requires that at least three objects (missiles) must be postulated: a massive high kinetic energy missile that deforms on impact, a rigid missile to test penetration resistance, and a small rigid missile of a size sufficient to just pass through any openings in protective barriers. The NUREG identifies two missile spectrums that will satisfy these criteria. Spectrum I missiles include: an 1,800 Kg automobile, a 125 Kg 8-inch armor-piercing artillery shell, and a 1-inch solid steel sphere. The impact speed required is 35 percent of the maximum horizontal wind speed of the design basis tornado. The first two missiles are to impact at normal incidence, the last to impinge upon barrier openings in the most

damaging directions. Spectrum II missiles may be used as an alternative to Spectrum I missiles. Spectrum II missiles and associated horizontal speed are shown in Table 10-8.

Table 10-8. Spectrum II Missiles

Missile	Mass (Kg)	Dimensions (m)	Velocity (m/sec)*
A. Wood Plank	52	0.092 x 0.289 x 3.66	58
B. 6-inch Sch 40 pipe	130	0.168D x 4.58	10
C. 1-inch Steel Rod	4	0.0254D x 0.915	8
D. Utility Pole	510	0.343D x 10.68	26
E. 12-inch Sch 40 pipe	340	0.32D x 4.58	7
F. Automobile	1,810	5 x 2 x 1.3	41

Source: NRC (1987).

NUREG-0800 (NRC 1987).

* Associated with Region III, Regulatory Guide 1.76.

Vertical velocities of 70 percent of the postulated horizontal velocities are used in both spectra except for the small missile in Spectrum I or missile C in Spectrum II. These missiles should have the same velocity in all directions. Missiles A, B, C and E are to be considered at all elevations and missiles D and F at elevations up to 30 feet above all grade levels within ½ mile of the facility structures.

10.3.5 Wind and Tornado Protection Requirements

The typical method showing compliance with the protection of SSCs important to radiological safety and waste isolation that have to withstand the effects of extreme winds and tornadoes is provided in NUREG-0800 (NRC 1987, Sections 3.5.2) and Regulatory Guide 1.117. SSCs to be protected from externally generated missiles include all SSCs that have been provided to ensure radiological safety and waste isolation. Based on their relation to safety, SSCs are identified as requiring protection from externally generated missiles if a missile could prevent the intended safety function, or if as a result of a missile impact on a non-important to safety SSC, its failure could degrade the intended safety function of a important to safety SSC.

The primary repository surface facilities to be considered for protection should include the Carrier Preparation Building, the Waste Treatment Building, the WHB, and any other facility structure that contains radioactive material. The QL-1 systems within identified affected structures must be protected against extreme winds, tornadic winds, and tornado-generated missiles because of the potential to cause a radiological release. It is necessary to demonstrate that failure of any structure or component will not affect the capability of other structures or components to perform their required safety function(s).

10.3.6 Consequence Analysis

Identify those SSCs that must withstand the effects of extreme winds, tornadoes, and tornado generated-missiles. An analysis must determine the design basis tornado frequency for repository design. This will ensure that a tornado-initiated sequence resulting in a radioactive

release that exceeds 10 CFR Part 63 performance objectives is categorized as non-credible event (having a frequency less than the Category 2 event sequence frequency cutoff).

The information provided in NUREG/CR-4461 (Ramsdell and Andrews 1986) represents the latest guidance on design basis tornadoes published by the NRC. This guidance will be used to determine the maximum wind speed of the design basis tornado. This value represents the upper end of the 90th percent confidence interval and reduces the uncertainty due to limited data sets associated with tornadic phenomena in western regions.

Either the Spectrum I or Spectrum II missile spectrum may be used to design the repository surface facilities for tornado generated missiles. Example design basis requirements for tornado generated missiles are shown in Table 10-9. Future analyses may determine whether the wind speed of the design basis tornado is sufficient to generate missiles with the entire generic missile spectrum. Portions of the missiles spectrum may be removed from the design basis missile spectrum if it is determined that they are not applicable to the location of the repository surface facilities.

10.4 LIGHTNING AND EXTREME WEATHER

Lightning and extreme weather are natural phenomena that will be assumed to occur at least yearly. Lightning is a large-scale high-tension natural electric discharge in the atmosphere. When lightning strikes a building, a transporter, or an electrical component, the consequences may be a localized temperature increase, a loss-of-offsite power, or a short circuit. In addition, a lightning strike may initiate a fire.

Lightning and/or extreme weather are (at a minimum) to be analyzed as potential initiators for a loss-of-offsite power event and an internal fire. Analysis of lightning- and extreme weather-initiated event sequences is expected to demonstrate that there are no credible release scenarios that result from a lightning strike.

10.5 WILDLAND FIRES

The objective of this section is to outline an approach for analysis of an external-initiated fire and related hazards identification for repository facilities sufficient to minimize the potential for: (1) damage from a wildland fire or related event; (2) an external-initiated fire that causes an unacceptable onsite or offsite release of hazardous or radiological material that will threaten the health and safety of employees, the public or the environment; and (3) critical process controls and safety class systems being damaged as a result of an external-initiated fire and related events.

The *MGR External Events Hazards Analysis* (CRWMS M&O 2000a) has previously identified wildland fire as a potential hazard to the repository. An analysis of the wildland fire hazard should consider the potential event sequences that could result in fire or fire-related damage to the repository facilities. The area surrounding the repository site is mostly barren with no trees and small, low-growing vegetation. The *Standard for the Protection of Life and Property from Wildfire*, NFPA 299 (NFPA 1997), should be used as guidance for site protection from wildfire. This standard presents minimum planning criteria for the protection of life and property from wildfire. Practices such as defensible spaces around buildings NFPA 299 (NFPA 1997) and use of noncombustible building materials may reduce the probability of damage from wildfire.

The section of the PSA that provides the analysis of fires should provide a comprehensive list of wildland fire hazards such that mitigation and response plans can adequately address the hazard, including adequate water supplies, reliable means of taking water to the fire, access route for emergency response vehicles, and personnel trained in wildland fire-fighting.

The hazards from a wildland fire can be reduced by the use of a fire protection program and design requirements for facilities that are designed and constructed to meet the applicable building code and National Fire Protection Association codes and standards, or exceeding them (when necessary to meet safety objectives).

The fire hazards analyses for the repository facilities will consider the hazards of wildland fires. The conclusions of the fire hazards analyses will be integrated into design basis and beyond design basis accident conditions.

10.6 OTHER EXTERNAL EVENTS

10.6.1 Loss-of-Offsite Power

The likelihood of loss-of-offsite power should be estimated for the Yucca Mountain site based on historical information for the region.

Loss-of-offsite power events at the repository may be likely to occur one or more times during the preclosure operations. Therefore, loss-of-offsite power will be a Category 1 initiating event sequence. The strategy for this event is to prevent credible release scenarios by design. Repository SSCs important to safety may be designed to fail safe during a loss-of-offsite power event. Important-to-safety cranes may also be designed in accordance with NUREG-0554 (NRC 1979) to preclude single point failures.

Emergency backup power sources and redundant offsite power lines/sources may be used to ensure continuous power is supplied to SSCs important to safety. The repository design may also include features such as external lightning rods to protect against a lightning-initiated loss-of-offsite power event.

Using the frequency of loss-of-offsite power event trees (see Section 7.1) and fault trees (see Section 7.2) should be developed. Event sequences determined from this study can be used to identify possible credible event sequences that result in offsite releases.

10.6.2 Aircraft

10.6.2.1 Purpose

This guide recommends methods to determine aircraft hazard potential and the extent of any protection required for SSCs important to radiation safety or waste isolation.

Aircraft crashes were determined to be potentially applicable to the potential repository at Yucca Mountain in the *MGR External Hazards Analysis* (CRWMS M&O 2000a). This determination was conservatively based on limited knowledge of the flight data in the area of concern and the crash data on aircraft of the type flying near the repository. An aircraft frequency analysis will

meet the requirements of NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants* (NRC 1987). The aircraft frequency analysis will establish the frequency of aircraft crashes into radioactive material control facilities at the repository. The results of that analysis will determine if an aircraft crash event is credible and warrants performing consequence analyses needed to quantify the risk of public exposure to radioactive materials.

10.6.2.2 Scope

The recommended approach to be used in performing aircraft crash analysis for the repository surface facilities is presented in this section. The NRC requires a determination of the probability of an aircraft crash and a consequence analysis if the probability exceeds allowable dose limits. Meeting this requirement could involve up to three phases: development of a vicinity map, crash frequency analyses, and, if necessary, a consequence analysis. This section focuses on the approach to be used for the first two phases. Example calculations are described to illustrate how these methods could be applied. All information used in these examples is subject to change.

10.6.2.3 Overview of Approach

Nuclear waste repository licensing requirements are defined in 10 CFR Part 63 wherein events with probabilities greater than 1 in 10,000 (based on an expected surface facility lifetime of 100 years) are considered credible event sequences. This probability limit equates to an event sequence frequency of 1.0×10^{-6} per year, which is used to determine if an aircraft crash event is credible and, if so, the consequences of the event must be evaluated. If the event is not credible and the NRC accepts this conclusion, no further analysis is required.

The Nellis Air Force Base (AFB) is located near Las Vegas. The potential repository site is located in the northwestern section of the NTS. The Nevada Test and Training Range includes the Nellis Air Force Range and surrounding military operations areas. The Nevada Test and Training Range surrounds the NTS on the east, north, and west sides. As such, it must be shown that aircraft flying from the base to the range and other aircraft related activities in the range and other surrounding areas would not result in a safety issue that cannot be prevented or mitigated. In addition, civilian air traffic to and from the Las Vegas McCarran International Airport and other smaller airports must be considered.

The airspace in Southern Nevada includes military operations areas, restricted areas, and general aviation areas. The responsibility for managing the airspace within these areas is delegated to the United States Air Force, DOE, and the Federal Aviation Administration as appropriate. Air traffic outside of restricted areas is routed on commercial airways and military training routes. Air traffic within restricted areas does not follow specific flight corridors, but fly mission-specific routes resulting in a random distribution of aircraft within these areas. The Air Force has agreements with DOE for use of the NTS airspace for ingress and egress of the Nevada Test and Training Range.

Military air traffic is mainly composed of fighter and attack aircraft such as F-15s, F-16s, and A-10s. During large training exercises, other types of aircraft including bombers, tankers,

helicopters, and other U.S. and non-U.S. fighter aircraft are added to the air traffic. Military aircraft generally fly in normal cruise mode during ingress and egress of the test and training ranges but can perform some preliminary tactical maneuvers such as g-awareness exercises during this phase.

The typical military training missions within the military operations areas and restricted areas include basic flight maneuvers, air combat maneuvers, day/night weapons delivery, and large multi-aircraft exercises. Several types of ordnance are carried on these aircraft. Military Training Routes are used for low-altitude and navigational training.

10.6.2.4 Details of Approach

NUREG-0800 (NRC 1987) includes three acceptance criteria, and meeting all three would eliminate the need for crash frequency analyses. Because of the extensive military traffic in the vicinity of the potential repository, each of the three criteria may not be met and frequency analysis is performed as part of phase 2. Various analytical models used to determine the crash frequencies of different aircraft-related activities involve a determination of effective target areas, crash rates, number of flights, flight corridor widths and potential crash areas.

Because use of the NUREG-0800 (NRC 1987) airway model may be conservative for application to a repository at Yucca Mountain, another model should be evaluated to provide a comparative analysis. Suggested models are provided in the following sections.

10.6.2.4.1 Use of NUREG-0800

The analytical model in NUREG-800 (NRC 1987, Section 3.5.1.6.III.2) is best suited for calculating crash frequency of aircraft that fly well-defined routes such as Federal Aviation Administration commercial airways and jet routes. This NUREG addresses aircraft hazards to NPPs; however, this same methodology can be applied to other nuclear facilities. The NUREG includes proximity criteria, which, if met, would dismiss the event by inspection. If the proximity criteria are not met, a detailed review of the aircraft hazards must be performed.

The NUREG defines a process to be used by the NRC staff in reviewing the applicant's assessment of aircraft hazards. This process includes models for determining the probability of an aircraft crash at the repository site from airways, airports, and designated airspaces. The total aircraft hazard probability at the repository equals the sum of the individual probabilities obtained from these models. An example aircraft crash hazard defined in the *MGR External Events Hazards Analysis* (CRWMS M&O 2000a) involves military aircraft flying through the R4808N restricted airspace (DMA 1995) over the NTS which includes the site of the repository surface facilities. These aircraft are at high altitudes in an enroute/inflight phase while inside the R4808N airspace. Although they are not flying in standard Federal Aviation Administration airways, they fly within specifically defined areas. The model provided in NUREG-0800 (NRC 1987) for airways can be used to approximate the crash frequency and determine if the event is credible.

10.6.2.4.2 Uniform Overflight Density Model

The Uniform Overflight Density Model (Kimura et al. 1998) is better suited for calculating crash frequencies when aircraft overfly a defined area along various routes as in the case of aircraft in transit the NTS between Nellis AFB and the Nevada Test and Training Range. The route taken by pilots when traversing the NTS depends on the particular training mission and location on the Nevada Test and Training Range where this training will be executed. A crash hit frequency analysis (Kimura et al. 1998) for the NTS was completed as part of a DOE facility safety analysis. A model was developed in that analysis to address U.S. Air Force overflights of the DOE R-4808N restricted area. The Uniform Overflight Density Model can be applied to the repository surface facilities to provide a comparative analysis to the NUREG Airways Model.

In this model, the aircraft crash frequency equals the product of the number of aircraft, which overfly a particular area, the probability that the aircraft crashes in that particular area, and the probability that the aircraft hits a facility in this particular area. The Uniform Overflight Density Model is developed in detail in *Crash Hit Frequency Analysis of Aircraft Overflights of the Nevada Test Site (NTS) and the Device Assembly Facility (DAF)* (Kimura et al. 1998), and the resultant equation for the special case of the NTS is shown in Equation 15 of Kimura et al. (1998).

10.6.2.4.3 NUREG Airport Model

NUREG-0800 (NRC 1987) provides a model for determining the crash frequency associated with aircraft takeoff and landings from civilian and military airports. However, the NRC has determined that the crash frequency is negligible beyond 10 miles from the end of a runway (NRC 2000b). There are no airports or airstrips within 10 miles of the potential repository surface facility. If this situation were to change, an analysis using the NUREG Airport Model would be performed.

10.6.2.4.4 Designated Airspace Model

A variation of the Uniform Overflight Density Model can be used to determine the crash frequency of events involving military aircraft while flying in the Nevada Test and Training Range that have not been screened out during the vicinity map development phase. This variation was developed by the Private Fuel Storage Limited Liability Company for their aircraft crash analysis of a nuclear fuel storage facility in Utah, also located near a U.S. Air Force test and training range (Private Fuel Storage 2000). The crash impact hazard for each altitude band for each range sector is shown in Private Fuel Storage (2000).

The variation from the Uniform Overflight Density Model involves developing the crash rate per year. The Private Fuel Storage model develops an annual crash rate per square mile and multiplies it to the site specific cutout area. The cutout area is bounded by the edge of a specific range and an arc, centered on the nuclear facility, with a radius equal to the maximum distance wherein loss of pilot control is possible.

10.6.2.5 Regulatory Requirements

NUREG-0800 (NRC 1987) defines the requirements for reviewing the adequacy of an applicant's aircraft hazard evaluation. Additionally, nuclear waste repository licensing requirements are defined in 10 CFR Part 63 wherein events with probabilities greater than 1 in 10,000 (based on an expected surface facility lifetime of 100 years) are considered credible events. This probability limit equates to an event frequency of 1.0×10^{-6} per year, which is used to determine if an aircraft crash event is credible and, if so, the consequences of the event must be evaluated. If the event is not credible and the NRC accepts this conclusion, no further analysis is required.

The results of the repository aircraft crash frequency analysis will be compared with an evaluation criterion that determines if a crash hit event is credible. A crash hit event is defined as an aircraft impacting a potential repository surface radiological control facility that has sufficient radionuclide inventory to exceed the proposed rule 10 CFR Part 63 dose limits if released. The event is not credible and needs no further analysis if it meets the following criteria:

The Crash Hit Frequency of an aircraft into a radiological control facility from aircraft shall be less than 1×10^{-6} per year. Category 2 event sequences are defined in 10 CFR Part 63 as other natural and human-induced events that have at least one chance in 10,000 of occurring before permanent closure of the repository. The performance requirement for retrieval is assumed to require 100 years from the time of initial SNF/high-level radioactive waste receipts until permanent closure of the repository.

10.6.2.5.1 Example of Application of NUREG-0800 Proximity Criteria

NUREG-0800 (NRC 1987, Section 3.5.1.6.II) defines proximity criteria, which are applied to the various types of aircraft flying in the regional airspace surrounding the repository surface facility. These criteria, identified as requirements in the NUREG, are listed below. According to the NUREG, the probability is considered below the threshold for further evaluation if the distances from the plant (repository surface facilities) meet all of these requirements:

1. The plant-to-airport distance, D , is between 5 and 10 statute miles, and the projected annual number of operations is less than $500 D^2$ or the plant-to-airport distance D is greater than 10 statute miles, and the projected annual number of operations is less than $1,000 D^2$.
2. The plant is at least 5 statute miles from the edge of military training routes, including low-level training routes, except for those associated with a usage greater than 1,000 flights per year, or where activities (such as practice bombing) may create an unusual stress situation.
3. The plant is at least 2 statute miles beyond the nearest edge of a federal airway, holding pattern, or approach pattern.

For an example of an aircraft analysis that was performed for the Yucca Mountain site (see *MGR Aircraft Crash Frequency Analysis*; CRWMS M&O 1999a).

10.6.2.5.2 Defining the Vicinity for Crash Frequency Analysis

A preliminary crash frequency analysis completed in late 1998 focused on military aircraft traversing the NTS en-route from the Nellis AFB to the Nevada Test and Training Range. After review of this analysis by the NRC, it was agreed that extended evaluations over a wider area were needed to determine if other aircraft-related activities could impact the frequency of a crash into the potential repository surface facilities. Military operations areas are located on the east and north sides of the Nellis Air Force Range.

The area extending south below Las Vegas, Nevada, north to Tonopah, Nevada, and east beyond Highway 93 and west to Death Valley, California should define the vicinity for detailed frequency analysis.

The approach to be used to establish this vicinity involves screening of non-credible events using both qualitative and quantitative methods. Prepare a description of the various areas and airfields within the area, the aircraft flying in those areas, and the activities being performed by these aircraft. This includes describing military test and training missions conducted in each sub-range and military operations area within the Nevada Test and Training Range and determining the distances from these areas to the proposed repository surface facilities. The description includes relevant characteristics of each aircraft and ordnance carried by these aircraft. These characteristics will include the aircraft glide ratios and the maximum range of missile ordnance.

The qualitative evaluation will compare the distance a malfunctioning aircraft or missile needs to travel to reach and impact the repository surface facility and the capability of such aircraft or missile to traverse this distance. The distance to be traveled depends on which part of the Nevada Test and Training Range the aircraft is located when the malfunction occurs. Because of the long distances involved, it is expected that many events will be screened out through this evaluation. The qualitative evaluation with regard to airports will also look at the distances involved and most will be screened out through this evaluation.

Quantitative evaluations may be conducted using the same crash frequency models to be used in the more detailed analysis but with best available information for the model parameters. Screening will be done on those events that are sufficiently below the frequency limit such that when all such events are combined, the cumulative frequency of these events will not impact the results of detailed analysis.

10.6.3 Military and Industrial Hazards

10.6.3.1 Scope

Example impacts due to nearby installations and operations were evaluated in the *Preliminary MGR Hazards Analysis* (CRWMS M&O 1996). This determination was conservatively based on limited knowledge of the potential activities ongoing on or off the NTS. It is intended that the Industrial/Military Activity-Initiated Accident Screening Analysis methodology provided herein will meet the requirements of the *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants* (NRC 1987) in establishing whether this external event can be

screened from further consideration or must be included as an initiator in the development of event sequences for the repository.

10.6.3.2 Methodology

The approach recommended is defined in NUREG-0800 (NRC 1987). NUREG-0800 (NRC 1987, Sections 2.2.1 and 2.2.2) address identification of potential hazards in the vicinity of a nuclear facility. The methodology involves identifying facilities within specified criteria, describing these facilities, describing the nature and extent of activities conducted, and providing statistical data about hazardous materials used at these facilities. The criteria in NUREG-0800 (NRC 1987, Section 3.1) include:

- Identified facilities and activities within eight kilometers (five miles) of the plant should be reviewed. Facilities and activities at greater distances should be considered if they otherwise have the potential for affecting plant important to safety features.
- Any facilities which meet the above criteria have to be evaluated in accordance with other sections of NUREG-0800 listed below, as appropriate:
 - Section 2.2.3, Evaluation of Potential Accidents
 - Section 3.5.1.5, Site Proximity Missiles (Except Aircraft)
 - Section 3.5.1.6, Aircraft Hazards

Hazards from an aircraft crash are covered in a separate section of this document while hazards from objects/ordnance falling from aircraft will be covered in this section.

Initiating events may be screened from further consideration if they have a frequency that is less than 1.0×10^{-6} per year (i.e., they are beyond Category 2 event sequence frequencies) or they have no impact on the repository due to the combination of the event magnitude (e.g., minimal overpressure and temperature) and distance from the repository. Types of events that are screened include: explosions, fires, chemical releases, and objects or ordnance falling from aircraft.

Specific evaluations of the overpressure from an explosion and the frequency of a radiological release from the WHB due to dropped objects or ordnance are to be performed to demonstrate that these events can be screened from further event sequence consideration based on either their inability to cause a radiological release or their low frequency of occurrence.

10.6.3.3 Application of NUREG-0800 Proximity Criteria

NUREG-0800 (NRC 1987, Section 2.2.1.III.1) specifies that all identified facilities and activities within 8 kilometers (5 miles) of the plant shall be reviewed. When applying this criterion, surface and subsurface facilities should be considered. DTN: MO9907YMP97128.001 shows the relationship of the surface facilities and the current extent of the subsurface facility with a five-mile perimeter drawn around the both the surface and subsurface areas.

10.6.3.4 Application of NUREG-0800 Plant-Affecting Criteria

NUREG-0800 (NRC 1987, Section 2.2.1.III.1) specifies that facilities and activities at distances greater than five miles should be considered if they otherwise have the potential for affecting plant important to safety features. The area surrounding the 5-mile perimeter includes the balance of the land withdrawal area, the balance of the NTS, Air Force land, and U.S. Bureau of Land Management (BLM) land. The land withdrawal area extends another 2 miles to the west and eight miles to the south. The NTS extends over 30 miles to the north and over 20 miles to the east of the land withdrawal area. The Air Force land is part of the Nellie Air Force Range which extends over 50 miles to the north of the withdrawal area. BLM land extends beyond the withdrawal area to the west and south and includes U.S. Highway 95 providing the major route between Las Vegas and Reno, Nevada. The potential for transportation accidents and Air Force dropped objects affecting the important to safety features should be covered.

Descriptions to be included in this study are the NTS facilities/activities and their potential to impact the repository; facilities/activities on BLM land, and facilities/activities on the Nellis Air Force Range.

10.6.3.5 Parametric Evaluation of Potential Explosions

Some of the NTS and Nellis Air Force Range facilities handle high-explosive materials; in addition, events such as transportation and industrial accidents may result in explosions. The overpressure generated by an explosion (i.e., detonation) is a function of the amount of explosive material involved and the distance between the site of the explosion and the repository.

A methodology is given in Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants*, for evaluating the safe distance from a postulated explosion.

For example, setting the safe radius equal to the five-mile (26,400 ft) criterion (NRC 1987, Section 3.1) and using the methodology in Regulatory Guide 1.91, a value for the mass of explosive can be calculated, and that value compared with any of the explosive inventories currently associated with NTS facilities and any transportation or industrial explosive sources. Data from the Lake Denmark Explosion that occurred at the Picatinny Arsenal in 1926 (Kinney and Graham 1985, p. 13) should also be reviewed for determination of a safe distance from a large-scale explosion.

10.6.3.6 Objects Dropped from Aircraft

Objects inadvertently dropped from aircraft can be screened from further event sequence consideration by demonstrating that the frequency of a release of radiological material is less than 1.0×10^{-6} per year. An event tree (see Section 7.1) can be used to evaluate the frequency of a dropped object causing a radiological release. Some events to consider in the construction of the event tree and sample numbers are listed below:

- **Frequency of Ordnance Drop (per sortie)**—Dropped objects are defined in SAIC (1991, p. 2-48) as items such as screws, bolts, and coverplates. The frequency at which

objects are dropped from military aircraft is given as 1.5 drops per 1,000 sorties (SAIC 1991, p. 2-48).

- **Number of Sorties that Overfly the NTS**—The number of sorties that overfly the NTS is 18,910 per year. This is the 95 percent confidence value as calculated in *MGR Aircraft Crash Frequency Analysis* (CRWMS M&O 1999a, p. V-2).
- **Fraction of Sorties that Fly in the Vicinity of the WHB**—It is estimated that no more than 2 percent (2.0×10^{-2}) of the total sorties that overfly the NTS fly within a 6-mile by 6-mile box centered on the WHB.
- **Probability of an Object being Dropped in the Vicinity of the WHB**—If it is assumed that drop frequency is uniform with respect to the flight path of an aircraft, then the conditional probability that a dropped object falls while an aircraft is within the 6-mile by 6-mile box is the ratio of the flight path length within the box to the total flight path length.
- **Probability of an Object Dropped in the Vicinity of the WHB Striking the WHB**—The conditional probability of an object dropped within the 6-mile by 6-mile box centered on the WHB actually striking the building is equal to the ratio of the WHB footprint (0.01 mi^2) to the footprint of the 6-mile by 6-mile box.

$$(e) = \frac{0.01 \text{ mi}^2}{(6 \text{ miles}) \times (6 \text{ miles})} = 2.78 \times 10^{-4} \quad (\text{Eq. 10-10})$$

- **Probability of an Object that Hits WHB Striking Nuclear Material**—To cause a radiological release, a dropped object that hits the WHB must strike nuclear material; of which the conditional probability is equal to the ratio the available strike area of nuclear material to the area of the WHB footprint.

A calculation that can be reviewed for examples of the treatment of objects dropped from aircraft is *Industrial/Military Activity-Initiated Accident Screening Analysis* (CRWMS M&O 1999b).

10.6.3.7 Ordnance Dropped from Aircraft

Ordnance inadvertently dropped from aircraft can be screened from further event sequence consideration by demonstrating that the frequency of a release of radiological material is less than 1.0×10^{-6} per year. An event tree (see Section 7.1) can be used to evaluate the frequency of dropped ordnance causing a radiological release. Some events to consider in the construction of the event tree and example numbers are listed below:

- **Frequency of Ordnance Drop (per sortie)**—The frequency at which armaments are dropped from military aircraft is given as 0.005 (5.0×10^{-3}) drops per 1,000 sorties (SAIC 1991, p. 2-48).

- **Number of Sorties that Overfly the NTS**—The number of sorties that overfly the NTS is 18,910 per year. This is the 95 percent confidence value as calculated in CRWMS M&O (1999a, p. V-2).
- **Fraction of Sorties that Fly in the Vicinity of the WHB**—It is estimated that no more than 2 percent (2.0×10^{-2}) of the total sorties that overfly the NTS fly within a 6-mile by 6-mile box centered on the WHB.
- **Probability of Ordnance being Dropped in the Vicinity of the WHB**—For dropped ordnance to affect the WHB (and potentially cause a release of nuclear material) it must fall off of the aircraft as its flight path passes near the WHB. If it is assumed that drop frequency is uniform with respect to the flight path of an aircraft, then the conditional probability that dropped ordnance falls while an aircraft is within the 6-mile by 6-mile box is the ratio of the flight path length within the box to the total flight path length.
- **Fraction of Sorties that Fly in the Vicinity of the WHB with Live Ordnance**—Only 10 percent (1.0×10^{-1}) of the sorties flown in the vicinity of the WHB carry live ordnance. Based on “Nellis Airspace and Crash Data for Yucca Mountain” (Tullman 1997), most aircraft flying through the western NTS (i.e., near the repository) are armed with simulated ordnance.
- **Fraction of Sorties that Fly in the Vicinity of the WHB with armed ordnance that could be dropped**—Restrictions imposed by the Air Force on NTS overflights forbid overflight of the NTS with armed live ordnance, unless the ordnance is carried internally and bomb bay doors are confirmed closed (i.e., in a configuration where a drop cannot occur) (Irving 1997). Based on these restrictions and engineering judgement the conditional probability of an inadvertent drop of armed live ordnance is 0.01 (1.0×10^{-2}).
- **Fraction of Dropped Live Ordnance that Explodes Upon Impact**—It is conservatively assumed that any ordnance that is live (i.e., not simulated) and armed will explode upon impact.
- **Probability that Dropped Ordnance Effects the WHB**—The conditional probability of dropped ordnance affecting nuclear material inside the WHB is dependent upon whether or not the ordnance explodes on impact, the probability of which depends on whether the ordnance is live (as opposed to simulated), and whether the ordnance, if live, is armed.

A calculation that can be reviewed for examples of the treatment of ordnance dropped from aircraft is *Industrial/Military Activity-Initiated Accident Screening Analysis* (CRWMS M&O 1999b).

10.6.3.8 Transportation

This section presents a general discussion for assessing transportation hazards. The following paragraphs are considered as an example.

U.S. Highway 95 and roads on the NTS are used to haul large quantities of explosives, munitions, propellants, hazardous materials, and radioactive materials. At its closest point, U.S. Highway 95 is approximately 13 miles from the repository surface facilities (DMA 1995).

Most transportation of hazardous materials on the NTS occurs on roads located at least 15 miles from the repository surface facilities (DMA 1995). The Lathrop Wells Road, which traverses the southeastern area of the proposed repository withdrawal area, is used to support testing in the X and Y tunnels. Assuming that materials are transported onto the NTS via the Lathrop Wells Road for this testing, the transport vehicles will be approximately 10 miles from the repository surface facilities (DMA 1995).

There are no transportation railroad lines within 20 miles of the repository surface facilities (DMA 1995).

These transportation routes are expected to be sufficiently distant from the repository to preclude adverse effects of transportation accidents resulting from explosions. Specific evaluations of the overpressure from an explosion on a nearby transportation route are to be performed to demonstrate that these events can be screened from further event sequence consideration. These distances are also sufficiently distant from the repository to preclude adverse effects of fires associated with transportation accidents. In the case of toxic releases, the NRC regulatory position for evaluating the habitability of a NPP control room can be found in Regulatory Guide 1.78.

10.6.3.9 Evaluation of Application of NUREG-0800, Plant-Affecting Criteria, to Independent Spent Fuel Storage Installations and Nuclear Power Plants

The Safety Analysis Report (Chapter 2.2, Nearby Industrial, Transportation, and Military Facilities) of other NRC-licensed facilities should be reviewed to see if there are any cases where detailed analyses were performed to assess facilities outside the NUREG-0800 (NRC 1987) five-mile evaluation limit. A couple of examples to consider include:

- Idaho National Engineering and Environmental Laboratory TMI-2 Independent Spent Fuel Storage Installation (INEL 1996)
- Rancho Seco Independent Spent Fuel Storage Installation (Shelter 1993).

10.6.3.10 Consequence Analysis

For each applicable credible, either individually or in combination with other events in an event sequence, perform: (1) a frequency analysis that demonstrates the event is not credible (2) a nuclear safety analysis that demonstrates a radiological release does not occur as a result of the event (3) a consequence analysis that demonstrates that the radiological consequences of the event are within regulatory requirements or that identifies required preventative or mitigative SSCs that ensure the radiological consequences are within regulatory requirements.

For each of the credible events identified, dose assessments will be performed to show compliance to requirements as applicable.

The frequency analysis of an event determines if the event is credible. If not credible, no quantitative dose limits are promulgated by 10 CFR Part 63, no further analysis is required, and there is no impact to other repository design or licensing organizations. Event sequences that are beyond Category 2 will be tracked to show safety design margin. If the event is determined to be credible, it is categorized based on the 10 CFR Part 63 definition, and an analysis is performed to determine if the dose limits associated with the applicable event category can be met.

Category 1 event sequences (i.e., frequency greater than 1×10^{-2} events per year) require that the sum of annual doses, exposures, and releases do not exceed limits specified in 10 CFR Part 63 for the public and 10 CFR Part 20 for occupational workers. Category 2 event sequences (i.e., frequency less than 1×10^{-2} and greater than 1×10^{-6} events per year) require that the consequences of a specific Category 2 event sequence not exceed dose limits as specified in 10 CFR Part 63 for the public beyond the preclosure controlled area.

The consequence analysis determines if the calculated doses are within applicable limits. If the calculated dose exceeds applicable limits, SSCs important to radiological safety are designated, new requirements are allocated to the system, assumptions are revised, the design configuration is revised (if necessary), and the dose is recalculated and again compared to applicable dose limits.

10.7 REFERENCES

10.7.1 Documents Cited

CRWMS M&O 1996. *Preliminary MGDS Hazards Analysis*. B00000000-01717-0200-00130 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19961230.0011.

CRWMS M&O 1997. *Engineering Design Climatology and Regional Meteorological Conditions Report*. B00000000-01717-5707-00066 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980304.0028.

CRWMS M&O 1998. *Monitored Geologic Repository Seismic Design Strategy*. B00000000-01717-4600-00122 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980903.0810.

CRWMS M&O 1999a. *MGR Aircraft Crash Frequency Analysis*. ANL-WHS-SE-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19981221.0203.

CRWMS M&O 1999. *Industrial/Military Activity-Initiated Accident Screening Analysis*. ANL-WHS-SE-000004 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000307.0381.

CRWMS M&O 2000a. *MGR External Events Hazards Analysis*. ANL-MGR-SE-000004 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000310.0069.

CRWMS M&O 2000b. *Monitored Geologic Repository Internal Hazards Analysis*. ANL-MGR-SE-000003 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000310.0070.

DMA (Defense Mapping Agency) 1995. *Nellis AFB Range Chart*. St. Louis, Missouri: Defense Mapping Agency. TIC: 243134.

INEL (Idaho National Engineering Laboratory) 1996. *Safety Analysis Report for the INEL TMI-2 Independent Spent Fuel Storage Installation, Revision 0*. Docket 72-20. Idaho Falls, Idaho: U.S. Department of Energy, Idaho Operations Office. TIC: 233637.

Irving, D.E. 1997. "R-4808N Airspace Scheduling." Memorandum from D.E. Irving (USAF) to Distribution List, August 8, 1977, with attachment. ACC: MOL.19990301.0229.

Kimura, C.Y.; Sanzo, D.L.; and Sharirli, M. 1998. *Crash Hit Frequency Analysis of Aircraft Overflights of the Nevada Test Site (NTS) and the Device Assembly Facility (DAF)*. UCRL-ID-131259. Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL.20010724.0327.

Kinney, G.F. and Graham, K.J. 1985. *Explosive Shocks in Air*. 2nd Edition. New York, New York: Springer-Verlag. TIC: 242469.

NRC (U.S. Nuclear Regulatory Commission) 1979. *Single-Failure-Proof Cranes for Nuclear Power Plants*. NUREG-0554. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 232978.

NRC 1986. *Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margins Reviews of Nuclear Power Plants*. NUREG/CR-4482. Livermore, California: Lawrence Livermore national Laboratories. On Order

NRC 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

NRC 1990. *Seismic Margins Review of Plant Hatch Unit 1: Systems Analysis*. NUREG/CR-5632. Livermore, California: Lawrence Livermore National Laboratories. On Order

NRC 2000a. *Standard Review Plan for Spent Fuel Dry Storage Facilities*. NUREG-1567. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 247929.

NRC 2000b. *Safety Evaluation Report Concerning the Private Fuel Storage Facility, Docket No. 72-22*. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249827.

Private Fuel Storage Facility 2000. *Aircraft Crash Impact Hazard at the Private Fuel Storage Facility*. Tooele County, Utah: Private Fuel Storage Facility. Imaging in Process

Ramsdell, J.V. and Andrews, G.L. 1986. *Tornado Climatology of the Contiguous United States*. NUREG/CR-4461. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010727.0159.

SAIC (Science Application International Corporation) 1991. *Special Nevada Report, September 23, 1991*. Las Vegas, Nevada: Science Application International Corporation. ACC: NNA.19920131.0361.

Shelter, J.R. 1993. "Docket No 72-11, Rancho Seco Independent Spent Fuel Storage Installation, Revision 1 to the Rancho Seco Independent Spent Fuel Storage Installation License Application and Safety Analysis Report." Letter from J.R. Shelter (SMUD) to R.E. Cunningham (NRC), October 27, 1993, DAGM/NUC 91-137, with attachments. TIC: 226550.

Smith, C.L.; Wood, S.T.; Kvarfordt, K.L.; McCabe, P.H.; Fowler, R.D.; Hoffman, C.L.; Russell, K.D.; and Lois, E. 2000. *Testing, Verifying, and Validating SAPHIRE Versions 6.0 and 7.0*. NUREG/CR-6688. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249459.

Tullman, E.J. 1997. "Nellis Airspace and Crash Data for Yucca Mountain Hazard Analysis." Letter from E.J. Tullman (USAF/DOE Liaison Office) to W.E. Barnes (DOE/YMSCO), June 5, 1997, with enclosure. ACC: MOL.19970806.0389.

YMP (Yucca Mountain Site Characterization Project) 1997. *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain*. Topical Report YMP/TR-003-NP, Rev 02. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19971009.0412.

10.7.2 Codes, Standards, Regulations, and Procedures

10 CFR 20. Energy: Standards for Protection Against Radiation. Readily available.

10 CFR 50. Energy: Domestic Licensing of Production and Utilization Facilities. Readily available.

10 CFR 60. Energy: Disposal of High-Level Radioactive Wastes in Geologic Repositories. Readily available.

10 CFR 63. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain. Readily available.

10 CFR 100. Energy: Reactor Site Criteria. Readily available.

ANSI/ANS-2.3-1983. *Standard for Estimating Tornado and Extreme Wind Characteristics at Nuclear Power Sites*. La Grange Park, Illinois: American Nuclear Society. TIC: 6420.

ANSI/ANS-2.8-1992. *American National Standard for Determining Design Basis Flooding at Power Reactor Sites*. La Grange Park, Illinois: American Nuclear Society. TIC: 236034.

ASCE 7-98. 2000. *Minimum Design Loads for Buildings and Other Structures*. Revision of ANSI/ASCE 7-95. Reston, Virginia: American Society of Civil Engineers. TIC: 247427.

NFPA (National Fire Protection Association) 299. 1997. *Standard for the Protection of Life and Property from Wildfire*. 1997 Edition. Quincy, Massachusetts: National Fire Protection Association. On Order

Regulatory Guide 1.102, Rev. 1. 1976. *Flood Protection for Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.117, Rev. 1. 1978. *Tornado Design Classification*.
Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.29, Rev. 3. 1978. *Seismic Design Classification*.
Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.59, Rev. 2. 1977. *Design Basis Floods for Nuclear Power Plants*.
Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.76, Rev. 0. 1974. *Design Basis Tornado for Nuclear Power Plants*.
Washington, D.C.: U.S. Atomic Energy Commission. TIC: 2717.

Regulatory Guide 1.78. 1974. *Assumptions for Evaluating the Habitability of a Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release*.
Washington, D.C.: U.S. Atomic Energy Commission. ACC: NNA.19891109.0074.

Regulatory Guide 1.91, Rev. 1. 1978. *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

10.7.3 Source Data

MO9907YMP97128.001. Land Use and Ownership within a 25-Mile Radius of Yucca Mountain. Submittal date: 07/07/1999.

CONTENTS

	Page
ACRONYMS	i
11. CRITICALITY	11-1
11.1 INTRODUCTION	11-1
11.2 REGULATORY REQUIREMENTS.....	11-1
11.3 REPOSITORY PRECLOSURE CRITICALITY SAFETY STRATEGY	11-1
11.4 CRITICALITY RISK ANALYSIS PROCESS	11-1
11.4.1 Identify the Systems, Structures, Components, and Processes Associated with Criticality Hazards	11-6
11.4.2 Identify Those Waste Forms That Have the Potential to Achieve Criticality	11-6
11.4.3 Develop Criticality Event Trees	11-7
11.4.4 Quantify the Criticality Event Trees.....	11-9
11.4.5 Perform Criticality Analysis to Determine k_{eff}	11-9
11.4.6 Perform Criticality Consequence Analyses	11-9
11.4.7 Document the Results	11-10
11.5 REFERENCES	11-10
11.5.1 Documents Cited.....	11-10
11.5.2 Codes, Standards, Regulations, and Procedures.....	11-10

FIGURES

11-1 Criticality Risk Analysis Flow Chart.....	11-3
------------------------------------------------	------

ACRONYMS

BWR	boiling water reactor
DC	disposal container
MCNP	<i>MCNP-A General Monte Carlo N-Particle Transport Code</i>
PWR	pressurized water reactor
SNF	spent nuclear fuel
SSC	systems, structures, and components

INTENTIONALLY LEFT BLANK

11. CRITICALITY

11.1 INTRODUCTION

As part of preclosure safety analysis to support the license application submittal, a preclosure criticality risk analysis is performed to calculate the risks associated with criticality hazards and to prevent and control criticality during surface and subsurface spent nuclear fuel (SNF) handling and high-level radioactive waste operations at the repository. Criticality hazards are hazards associated with handling fissionable materials contained in SNF or other waste forms. The hazards are identified in Section 6.2. The results of the hazard analyses, which identify the systems, structures, components (SSCs), and processes that have the potential for criticality events, serve as input to the criticality risk analysis.

11.2 REGULATORY REQUIREMENTS

Regulatory requirements relating to criticality safety are described in 10 CFR 63.112(e)(6), which requires the preclosure safety analysis to include means to prevent and control criticality. The regulatory requirements applicable to operations involving SNF assemblies or canisters in transportation casks are derived from 10 CFR Part 71, which will not be addressed in Section 11. It is assumed that the transportation casks have been designed in accordance with applicable Certificates of Compliance and have met the criticality safety requirements in 10 CFR Part 71.

11.3 REPOSITORY PRECLOSURE CRITICALITY SAFETY STRATEGY

The repository preclosure criticality safety strategy is described in *Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation* (BSC 2001). The strategy to prevent criticality is to rely, where practicable, on equipment design that uses passive-engineered controls (such as geometry control or fixed neutron absorbers) rather than on administrative controls. Where passive engineering controls alone are not practical or sufficient, administrative controls on fissionable material mass or other reliable and verifiable reactivity control methods, such as minimum burnup requirements on commercial SNF, will be established.

The repository preclosure criticality safety strategy also relies on a defense-in-depth approach. The defense-in-depth approach involves taking advantage of the natural site and engineering design features. These features are expected to reduce the probability of a preclosure criticality event to below the regulatory thresholds established in 10 CFR Part 63. The natural site and engineering design features accounted for in the preclosure criticality safety strategy will be identified and credited in the criticality risk analysis.

11.4 CRITICALITY RISK ANALYSIS PROCESS

Criticality is attained when the effective neutron multiplication factor, k_{eff} , of a system of fissionable material in a given geometry becomes equal to or greater than unity. Conversely, subcriticality is defined by a k_{eff} less than unity. When designing a system (e.g., a waste package) to be subcritical, it must be demonstrated that the calculated k_{eff} conservatively represents the true neutron multiplication of the system. This is accomplished by choosing a

value below unity where nuclear criticality is assumed to occur. This value is known as the upper subcritical limit.

The process for evaluating the risk of the potential criticality events associated with the handling waste forms containing fissionable materials is shown in a flow chart (Figure 11-1). The flow chart is composed of the following steps:

1. Examine the results from the hazard analyses.
2. Identify the SSCs and processes associated with criticality hazards.
3. Identify the types of waste forms that could achieve criticality.
4. Develop a criticality event tree.
5. Quantify the criticality event tree.
6. If an event sequence frequency is less than 1.0×10^{-6} per year, the event sequence is screened from additional analysis per the requirements of 10 CFR Part 63.
7. If an event sequence frequency is equal to, or greater than, 1.0×10^{-6} per year, perform criticality analysis to determine k_{eff} , where k_{eff} is the effective neutron multiplication factor.
8. If the calculated k_{eff} is less than the upper subcritical limit, the event sequence has no potential for criticality and additional analysis is not required.
9. If the calculated k_{eff} is equal to, or greater than, the upper subcritical limit, initiate an appropriate redesign of the SSCs and process, make the appropriate modifications to the criticality event tree, and then repeat steps 5 through 9 until the calculated k_{eff} is below the upper subcritical limit.
10. If practical modifications to the SSCs and processes have been evaluated, the event sequence frequency still exceeds 1.0×10^{-6} per year, and the calculated k_{eff} still equals or exceeds the upper subcritical limit, a consequence analysis of the event sequence will be performed to calculate the doses to members of the public and workers. The calculated doses will be compared with the regulatory dose limits (Table 8-1). It will be shown that the calculated doses are below the regulatory dose limits.

In steps 8, 9, and 10, the upper subcritical limit is defined as:

$$\text{Upper Subcritical Limit} = 1 - \text{bias} - \text{bias uncertainty} - \text{administrative margin}$$

The upper subcritical limit should not be confused with the critical limit that is defined as one minus the bias and the bias uncertainty. The bias is determined by comparison of criticality calculation results using a code such as *MCNP-A General Monte Carlo N-Particle Transport*

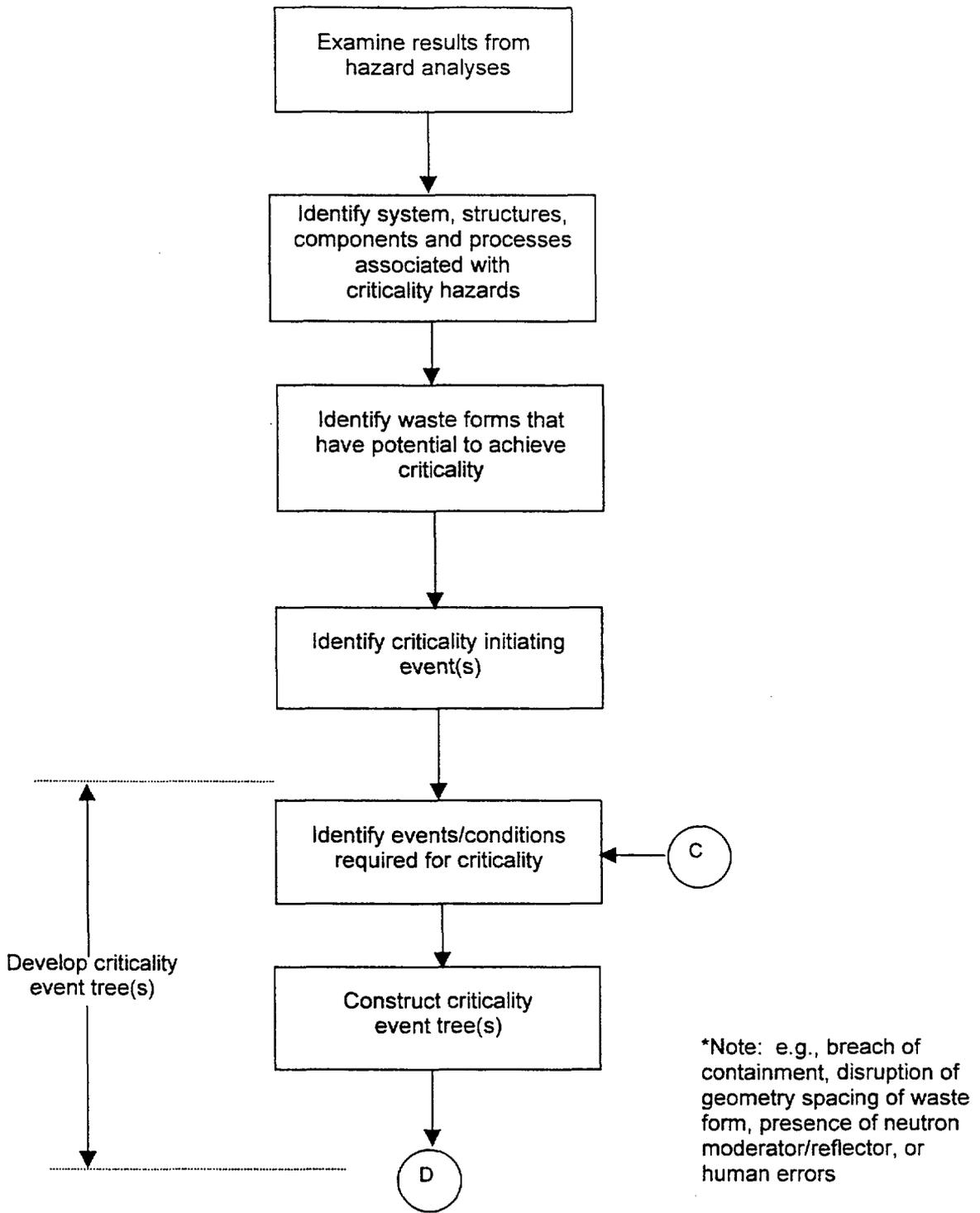


Figure 11-1. Criticality Risk Analysis Flow Chart

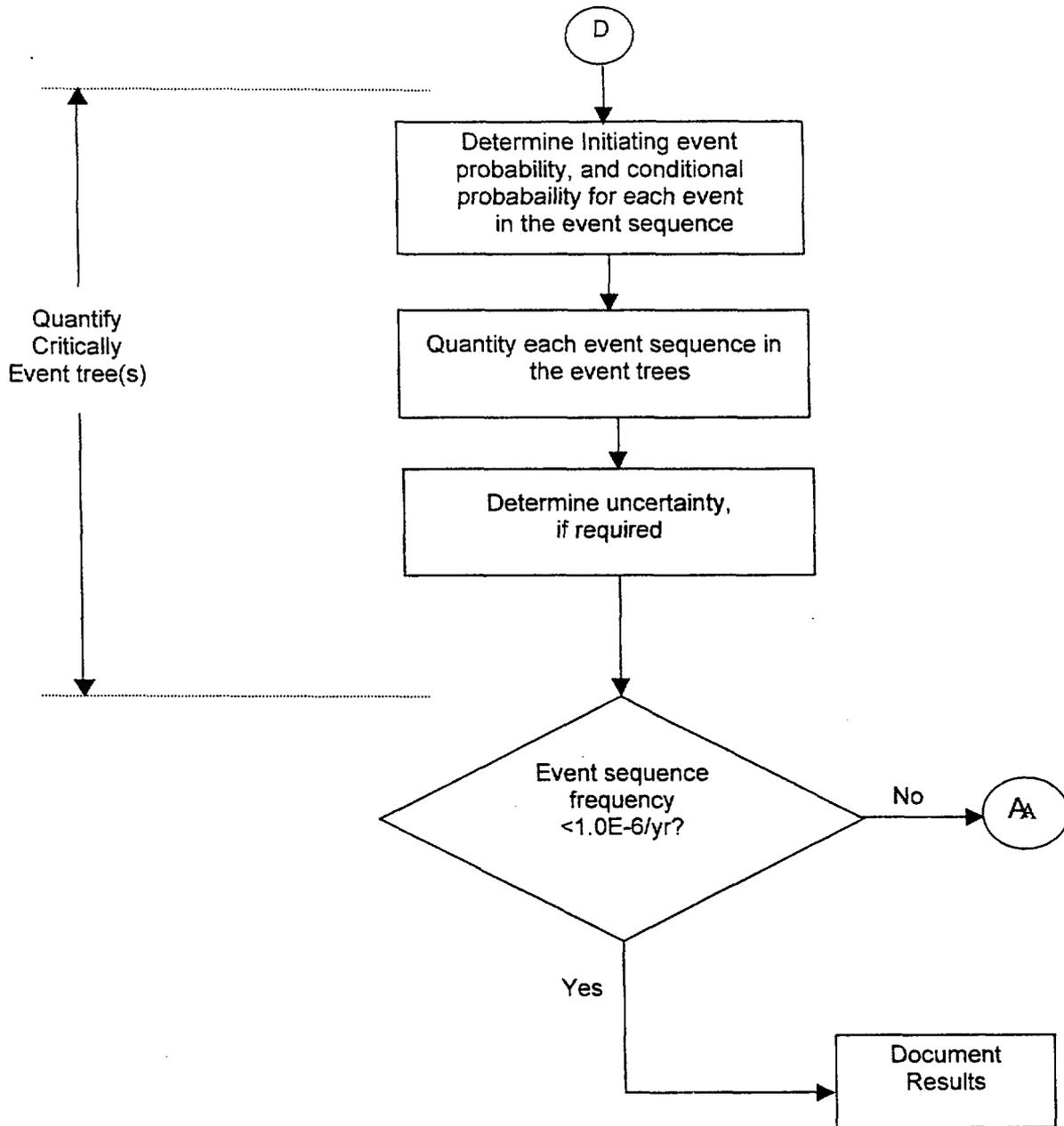


Figure 11-1. Criticality Risk Analysis Flow Chart (Continued)

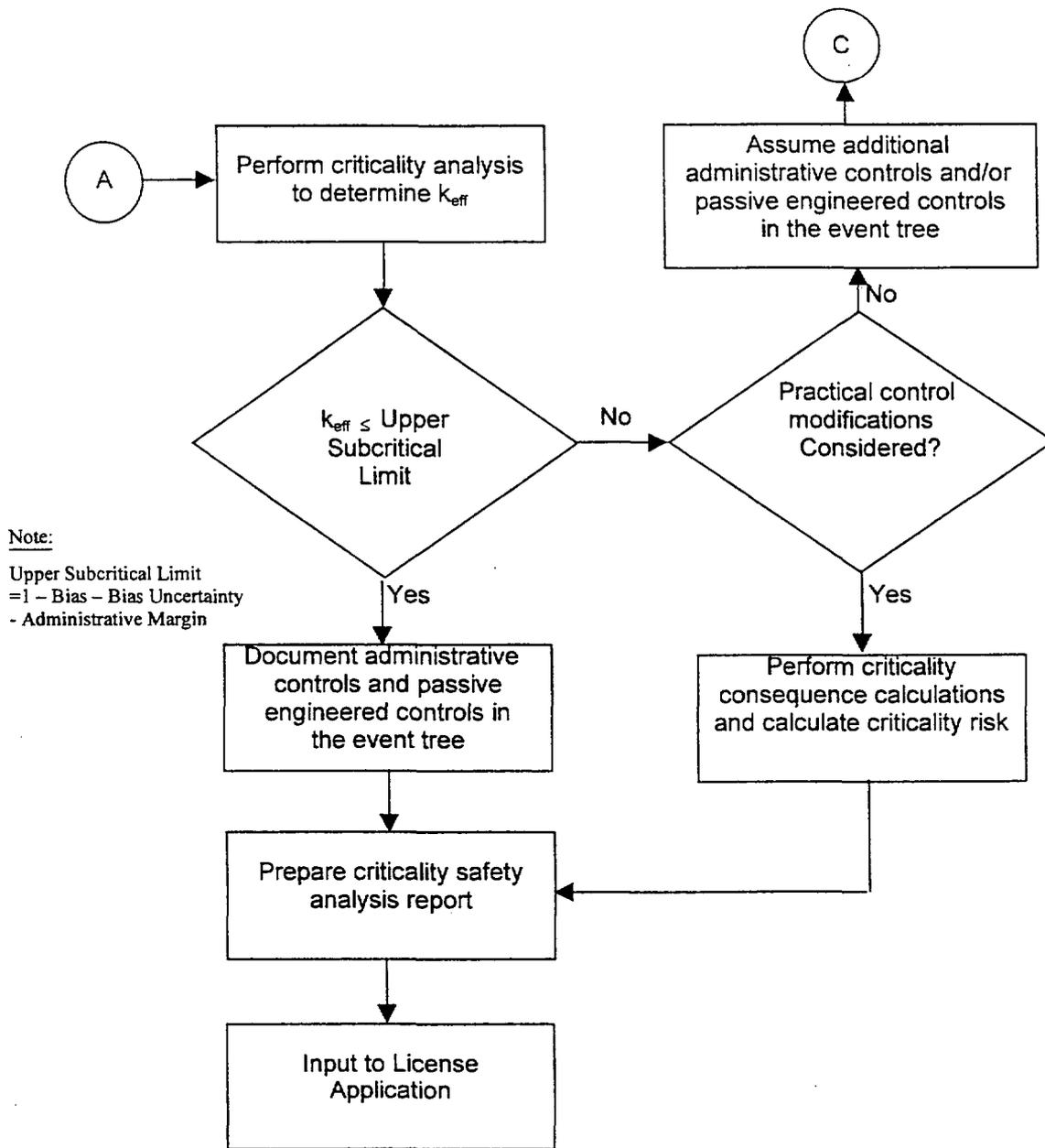


Figure 11-1. Criticality Risk Analysis Flow Chart (Continued)

Code (MCNP; Briesmeister 1997) to critical benchmarks. The administrative margin is an additional arbitrary margin applied to ensure subcriticality.

11.4.1 Identify the Systems, Structures, Components, and Processes Associated with Criticality Hazards

The results of hazard analyses will be reviewed to identify the SSCs and processes associated with the generic criticality hazards.

As an example, the following repository functional areas and processes identified from the site recommendation design would, at a minimum, be considered for criticality risk analysis:

- Waste Receipt and Carrier/Cask Transport
- Waste Handling Building - Carrier Preparation Area
- Waste Handling Building - Carrier Bay
- Waste Handling Building - Transfer Cell (including any waste form staging areas)
- Waste Handling Building - Disposal Container (DC) Handling Cell
- Waste Handling Building - Waste Package Remediation Cell
- Waste Handling Building - Waste Package Transporter Load Cell
- Surface storage facility (vault) (for the storage of steel containers that contain pressurized water reactor [PWR] and boiling water reactor [BWR] SNF assemblies), if a cold repository design is selected.
- Subsurface transport, emplacement, and monitoring.

11.4.2 Identify Those Waste Forms That Have the Potential to Achieve Criticality

Key factors in determining the potential for waste form criticality are the configuration and the quantity and type of fissionable material it contains. Only a fraction of the waste forms in the currently-identified inventory to be received at the repository have the potential to achieve criticality. These waste forms have medium or high reactivity with the characteristics of a high initial enrichment or low burnup. These include some PWR and BWR fuels and canisters with U.S. Department of Energy SNFs (e.g., Fast Flux Test Facility [i.e., FFTF], Enrico Fermi, Training Research Isotope General Atomic [i.e., TRIGA], Shippingport PWR and Light Water Breeder Reactor [i.e., LWBR], Ft. St. Vrain and N-Reactor SNF). Other waste forms such as high-level radioactive waste glass, contain insufficient fissionable material and, therefore, have no potential for criticality. The fraction of each of these waste forms in annual throughput should be determined and included in the criticality event sequence frequency calculation.

11.4.3 Develop Criticality Event Trees

Three potential preclosure criticality events were identified in *Preclosure Design Basis Events Related to Waste Packages* (CRWMS M&O 2000, p. 60). The events identified in this analysis were:

1. Alteration of geometry events
2. Introduction of neutron moderator or reflector events
3. Waste form misload events

These potential events are briefly discussed in the following sections.

11.4.3.1 Event Trees for Alteration of Geometry Events

Initiating events resulting in the drop, tipover and slapdown, or collision of the waste forms or waste form containers could occur during various repository processes. For an event sequence to have the potential for causing a criticality in a waste form container or a waste form handling area, a number of events and conditions must occur. The events and conditions that must occur include the following:

1. The waste form container (transportation cask, canister, or waste package) must be breached.
2. The geometric spacing or configuration of the waste form and the neutron absorber materials of the waste form, waste form container, or waste form handling area must be disrupted or changed. The configuration of a waste form may change after a drop or tip-over/slap-down (e.g., fuel scrap could fall out of a scrap basket in a multi-canister overpack [i.e., MCO] after a drop and slap-down).
3. A significant source of neutron moderator or reflector material must be present at the location where the initiating event occurs. In addition, the neutron moderator and reflector material must be able to remain in close proximity to the waste form.
4. The waste form must have the potential to achieve criticality.

11.4.3.2 Event Trees for Introduction of Neutron Moderator and Reflector Material Events

Initiating events resulting in the introduction of large quantities of a neutron moderator or reflector material (e.g., hydrogenous materials such as water) could occur in the repository surface facility. The current surface facility design philosophy is to preclude any water source in the waste form and DC handling areas. However, the potential for flooding events, such as a pipe break or an inadvertent actuation of the fire suppression system, will be assessed. The conditional probability of internal flooding could be determined using the fault tree methodology described in Section 7.3.

11.4.3.3 Event Trees for Misload Events

Methods for loading waste forms into a DC have been developed such that subcriticality is ensured during the preclosure period. This method may be referred to as the Criticality Loading Curve Evaluation. This evaluation established a simple criterion, in terms of the available waste form information, to determine if a waste form can be loaded into a given DC. The available waste form information used in the determination for commercial SNF consists of four components: bundle identification number, initial enrichment, assembly average discharge exposure, and decay time. With this information, a curve is developed for each commercial SNF (PWR, BWR, and mixed oxide) that represents the required minimum-average assembly burnup as a function of the initial-average assembly enrichment allowable for loading into a particular type of DC. For assemblies that fall below this curve, additional means of reactivity control are utilized. Such reactivity control increases the margin to criticality, either by addition of disposable control rods within the assembly or loading of these assemblies into an alternate DC, which is smaller and possesses a higher negative reactivity component inherent in its design. Adhering to this process ensures that a subcritical configuration exists. However, human errors during loading of the waste form into a DC could potentially lead to a criticality event.

Initiating events resulting in the waste form misload of a waste package or waste form storage area could occur. During the loading of waste forms into a DC, selection and conceptual human errors could occur resulting in an assembly misload event. A selection error simply represents an unintentional selection of the wrong item while trying to select the correct one. The conceptual error represents intentionally selecting the wrong item based on the erroneous belief that it is the correct item. The following paragraphs provide a brief list of the potential human errors that could result in a waste form misload.

- Based on the characterization of the waste form removed from transportation casks, the operator decides what type of DC it is to be loaded into. Deciding on an inappropriate DC type or selecting a wrong DC type is a human error.
- Some fuel assemblies will require the insertion of a neutron absorber rod assembly for permanent disposal. It is expected that these fuel assemblies will be shipped with a neutron absorber rod assembly already in place. For those assemblies that require the insertion of a neutron absorber rod assembly, but are not shipped with one in place, the following two human error scenarios are possible: the operator fails to identify the assembly as requiring the insertion of the neutron absorber assembly, or having identified the assembly as requiring the insertion of the neutron absorber assembly, the operator fails to insert it.
- An additional human error scenario is possible for those fuel assemblies that will require the insertion of a neutron absorber rod assembly for permanent disposal. It is expected that these fuel assemblies will be shipped with an inadequate neutron absorber rod assembly. The operator could fail to recognize that the assembly has an inadequate neutron absorber assembly and, therefore, fail to replace it with an acceptable assembly.
- The selection of the waste form to be placed in the DC is another opportunity for human error. The operator could select an incorrect waste form, or after selecting the correct

waste form for the DC, make a manipulation error with the crane and transfer the wrong one. Only the misload of medium or high reactivity waste forms into a DC would have the potential for criticality.

- After placing the waste forms into the DC, the operator performs a physical verification to ensure that correct waste forms were loaded. Failure to detect a misloaded SNF assembly in the DC during the physical verification process is another possible human error.

Human error probability can be reduced through the use of an independent checker during the physical verification task. Additionally, passive engineering controls have been utilized in the design of the DC internals such that some waste form types will not fit into a DC for which it was not intended. The analysis of human reliability is discussed in Section 7.4.

11.4.4 Quantify the Criticality Event Trees

The event sequence frequency analysis will be performed using the methods in Section 7. Quantification of the initiating event frequency, probabilities of branches, and the event sequence frequency should be performed in accordance with Section 7.1.4.

11.4.5 Perform Criticality Analysis to Determine k_{eff}

The criticality analysis methods for criticality analysis for the repository are detailed for the preclosure period in the *Preclosure Criticality Analysis Process Report* (CRWMS M&O 1999). This report provides the design requirements; applicable regulations, codes, and standards; summary descriptions of the types of computational tools to be used; and the types of analyses to be performed.

Criticality analyses will be performed when an event sequence frequency is determined to equal or exceed 1.0×10^{-6} per year. These criticality analyses will be performed to determine the sequence configuration k_{eff} using criticality analysis tools such as the MCNP code (Briesmeister 1997). MCNP is a general-purpose Monte Carlo N-Particle code that can be used for neutron transport, and has the capability of calculating k_{eff} for generalized systems containing fissionable material. MCNP uses the isotopic compositions of the materials, a detailed representation of the geometry, and a set of nuclear information libraries to calculate k_{eff} for the system. The nuclear information libraries used by MCNP are comprised of continuous-energy cross sections of materials. A full set of these material cross sections has been evaluated and is provided through the MCNP code package.

If the calculated k_{eff} is below the upper subcritical limit, the system is considered to be subcritical and the event sequence is screened out.

11.4.6 Perform Criticality Consequence Analyses

If the criticality event sequence evaluation results in a frequency equal to or exceeding the regulatory threshold of 1.0×10^{-6} per year, and practical steps have been taken to reduce the calculated k_{eff} of sequence configuration to below the upper subcritical limit, then it is necessary to determine the consequences of the criticality event. The doses to members of the public and

workers will be calculated using the methods presented in Section 8. The frequency calculated for the event sequence will determine whether the event sequence is a Category 1 or Category 2 event sequence. The calculated doses will be compared with the regulatory dose limits (Table 8-1). It will be shown that the calculated doses are below the regulatory dose limits.

11.4.7 Document the Results

A criticality safety analysis will be prepared to document the results of the criticality risk analysis. The documentation of the results of the criticality event tree evaluations should include the frequency of each event sequence identified. If administrative controls and natural site and engineered design features are relied on to reduce the criticality event sequence frequency to below the regulatory threshold of 1.0×10^{-6} per year, these controls and features should be documented through the SSCs system description documents.

11.5 REFERENCES

11.5.1 Documents Cited

Briesmeister, J.F., ed. 1997. *MCNP-A General Monte Carlo N-Particle Transport Code*. LA-12625-M, Version 4B. Los Alamos, New Mexico: Los Alamos National Laboratory. ACC: MOL.19980624.0328.

BSC (Bechtel SAIC Company) 2001. *Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation*. TDR-MGR-SE-000009 REV 00 ICN 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20010705.0172.

CRWMS M&O 1999. *Preclosure Criticality Analysis Process Report*. B00000000-01717-5705-00132 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990930.0102.

CRWMS M&O 2000. *Preclosure Design Basis Events Related to Waste Packages*. ANL-MGR-MD-000012 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000725.0015.

11.5.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. Readily available.

10 CFR 71. Energy: Packaging and Transportation of Radioactive Material. Readily available.

CONTENTS

	Page
ACRONYMS.....	ii
12. QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY.....	12-1
12.1 INTRODUCTION.....	12-1
12.2 SUMMARY OF THE PRECLOSURE SAFETY ANALYSIS PROCESS.....	12-2
12.3 DEVELOPMENT OF A RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION PROCESS	12-5
12.4 QUALITY ASSURANCE CLASSIFICATION PROCESS.....	12-12
12.5 FUNCTIONAL FAILURE ANALYSIS IN RISK INFORMED QUALITY ASSURANCE CLASSIFICATION.....	12-12
12.6 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 1 EVENT SEQUENCES	12-13
12.7 COMPLIANCE DEMONSTRATION FOR NORMAL OPERATION RELEASES AND CATEGORY 1 EVENT SEQUENCES.....	12-14
12.8 PROCESS FOR RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IN CATEGORY 1 EVENT SEQUENCES	12-15
12.9 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 2 EVENT SEQUENCES	12-16
12.10 REFERENCES.....	12-19
12.10.1 Documents Cited	12-19
12.10.2 Codes, Standards, Regulations, and Procedures.....	12-19

FIGURES

	Page
12-1 Preclosure Safety Analysis	12-3
12-2 Compliance or Acceptable Risk Region Based on 10 CFR Part 63	12-8
12-3 Example Quality Assurance Classification Risk Regions Developed from 10 CFR Part 63 Performance Objectives	12-10
12-4 Risk Informed Quality Assurance Classification Process	12-13
12-5 Example of the Quality Assurance Classification Process for a Category 2 Event Sequence	12-19

TABLES

	Page
12-1 Development of a Preclosure Safety Analysis.....	12-4
12-2 Relative Risk Significance Based on 10 CFR Part 63	12-6
12-3 Updated Relative Risk Significance	12-8
12-4 Quality Levels Based on Risk Significance.....	12-9
12-5 Risk Significant Screening Criteria	12-11
12-6 Steps for Performing a Quality Assurance Classification Analysis of Structures, Systems, and Components Associated with Category 1	12-18

ACRONYMS

CQ	conventional quality
HLW	high-level radioactive waste
NRC	U.S. Nuclear Regulatory Commission
PRA	probabilistic risk assessment
PSA	preclosure safety analysis
QA	quality assurance
QL	quality level
SSCs	structures, systems, and components
TEDE	total effective dose equivalent

12. QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY

12.1 INTRODUCTION

This section provides an overview of the risk-informed quality assurance (QA) classification process for structures, systems, and components (SSCs) of a high-level radioactive waste (HLW) repository that are important to safety as required by 10 CFR 63.112(e). The screening criteria are based on the risk-informed, performance-based philosophy embodied in the regulation. SSCs are assigned one of four Quality Level (QL) classifications based on the risk significance of the SSC for the purpose of applying the QA program criteria of 10 CFR 63.142. A discussion is provided on how the QA classification process fits into the design process and the overall development of a preclosure safety analysis (PSA). Background information related to the evolution of the QLs and the associated criteria is provided, as well as a discussion of the application of the risk-informed screening criteria through a functional failure analysis.

The QA classification process is applied to the SSCs of a HLW repository that are important to preclosure safety and important to postclosure waste isolation. This section addresses the preclosure portion of the QA classification process; the identification of features important to waste isolation is not included.

QL classifications (QL-1, QL-2, QL-3, or Conventional Quality [CQ]) are assigned to SSCs that represent the relative importance of an SSC to the health and safety of the public or to the radiological safety of workers. The QA classifications will be used to develop a graded application of the QA program requirements. The QA classifications are derived in a risk-informed, performance-based framework. The QA classification process will support a license application for the construction authorization for a HLW repository.

The governing regulation for a HLW repository is 10 CFR Part 63, which states, in part:

[The U.S. Department of Energy] DOE is required by 63.21(c)(20) to include in its safety analysis report a description of the quality assurance program to be applied to all structures, systems, and components important to safety, to design and characterization of the barriers important to waste isolation, and to related activities (63.142(a))

The quality assurance program must control activities affecting the quality of the identified structures, systems, and components, to an extent consistent with their importance to safety. (63.142(c)(1))

The phrase “to an extent consistent with their importance to safety” recognizes that the QA program for a HLW repository should impose graded quality requirements that would be applied to SSCs commensurate with their relative importance to radiological safety.

Importance to safety is defined in 10 CFR 63.2 as:

Important to safety, with reference to structures, systems, and components, means those engineered features of the geologic repository operations area whose function is:

- (1) To provide reasonable assurance that high-level waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of § 63.111(b)(1) for Category 1 event sequences; or
- (2) To prevent or mitigate Category 2 event sequences that could result in radiological exposures exceeding the values specified at § 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site.

The U.S. Nuclear Regulatory Commission (NRC) has published guidelines for applying risk-informed decision making to graded QA program controls for nuclear power plants. The NRC has presented the definition and principles of risk-informed decision making in nuclear power plant regulatory guidance using the results of a probabilistic risk assessment (PRA).

In NUREG-0800 (NRC 1987, Section 19.0), it is stated that "...the decision making process will use the results of the risk analysis in a manner that complements traditional engineering approaches, supports the defense-in-depth philosophy, and preserves safety margins. Thus, risk analysis will inform, but it will not determine regulatory decisions" (NRC 1987). The NRC applies the principles for risk-informed decision making to graded QA program controls for nuclear power plants in Regulatory Guide 1.176. Although the risk measures for nuclear power plants (e.g., core-damage frequency) are not relevant to a HLW repository, the principles provide general guidance for such a repository.

The NRC approach establishes a risk-informed framework for defining a multiple-level QA classification process for SSCs important to safety. The multiple-level QA classification will set the stage for implementation of graded QA program controls. For a HLW repository, the items important to safety are identified and classified using the PSA that employs elements of PRA supplemented by applicable regulatory and industry precedents. The SSCs that are subject to 10 CFR 63.142 QA requirements will be classified as QL-1, QL-2, or QL-3, and SSCs that are not subject to 10 CFR 63.142 QA requirements will be classified as CQ.

12.2 SUMMARY OF THE PRECLOSURE SAFETY ANALYSIS PROCESS

Because 10 CFR Part 63 has been developed as a risk-informed, performance-based rule, the Yucca Mountain Site Characterization Project is adopting a risk-informed, performance-based approach for developing the PSA. Figure 12-1 illustrates the overall process for developing a PSA and defining the event sequences for a HLW repository. While parts of the safety strategy for a HLW repository will be based on deterministic principles and industry and regulatory precedents, much of the safety evaluation of the preclosure operations will apply some of the techniques used in PRA. Section 4 presents a more comprehensive overview, and details of PSA analyses are presented in Sections 7-11.

The development of the PSA is an iterative process that evolves as the repository design develops, as site characteristics are more fully defined, and as operational features are identified. As this evolution progresses (and consistent with the current state of development) potential internal and external hazards are identified, event sequences are developed, frequency assessments are performed, event sequences are categorized, and potential resultant consequences are evaluated. Additional information regarding these steps is described in Table 12-1. If the consequences of an event sequence do not meet the regulatory requirements, preventative or mitigative design features and administrative controls are implemented until the event sequence risk is reduced to meet the performance objectives. Sensitivity and uncertainty analyses are performed, as required, to demonstrate that the categorization of the sequence and potential consequences meet the preclosure performance objectives. The SSCs important to safety are identified through the use of these sensitivity and uncertainty analyses and the use of the QA classification process. The identification of SSCs important to safety is documented in classification analyses and is subject to independent checking and an interdisciplinary review.

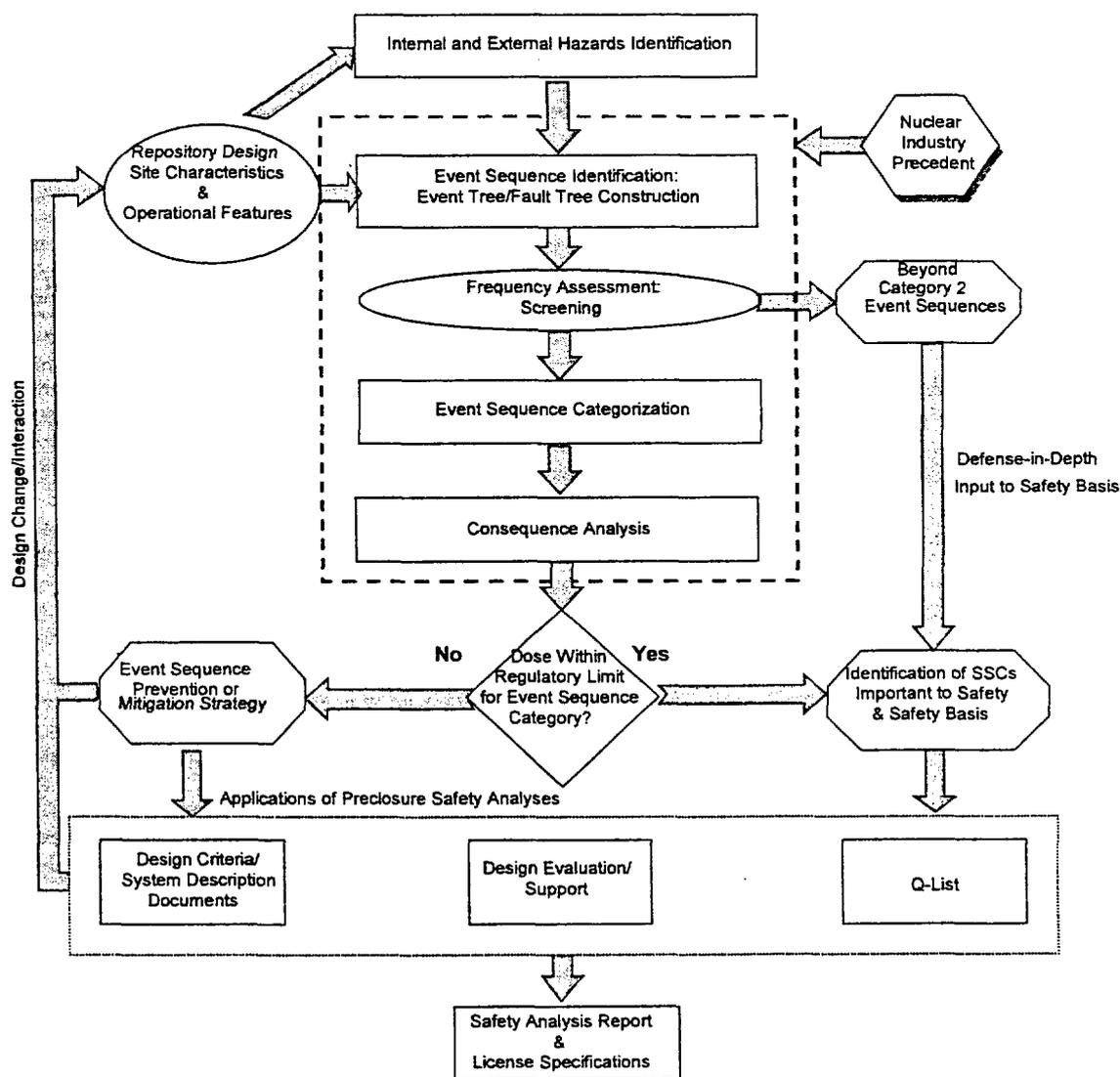


Figure 12-1. Preclosure Safety Analysis

Table 12-1. Development of a Preclosure Safety Analysis

<p>Internal and External Hazards Identification</p>	<p>Hazards analysis is a systematic identification and evaluation of naturally occurring and human-induced hazards. To ensure completeness, the analysis begins with checklists of generic categories of hazards that have been developed for safety and risk analyses of nuclear power plants, spent fuel storage facilities, fuel cycle facilities, and spent fuel transportation. The generic hazards are screened to determine which hazards, either internal or external to the repository facilities, are applicable. The purpose of the hazards analysis is to identify energy-source categories that can potentially interact with a waste form (e.g., collision or crushing, chemical contamination or flooding, explosion or implosion, fire, radiation, thermal, natural phenomena, and potential criticality). Initially, qualitative evaluations are applied to screen out inapplicable or incredible* hazards. Potentially credible** external hazards that are not eliminated in the initial qualitative screening are subjected to quantitative analyses to screen them out, if possible. Otherwise, they are incorporated into the design bases to prevent initiation of a radiological release that would exceed preclosure performance objectives (e.g., earthquakes, winds, tornadoes, and loss of offsite power). Potentially credible internal hazards that are not eliminated in the qualitative screening are evaluated further in accident sequence analyses.</p>
<p>Event Sequence Identification</p>	<p>Potential accident scenarios (or event sequences) may be displayed in the form of event trees that include an initiating event (from an identified hazard) and one or more enabling events that must occur to result in a release of radioactivity, a criticality, or an abnormal exposure of a worker. The event tree format provides a framework for estimating the event sequence frequency by displaying the frequency of the initiating event and the conditional probabilities of contributing (enabling) events. Where necessary and appropriate, fault-tree analysis is used to estimate the frequency of an initiating event or probability of an enabling event. Potential criticality event sequences are subjected to specialized analyses to demonstrate that sufficient design and operational controls will be in place to ensure that the frequency of an accidental criticality will be below 1×10^{-6} events per year (for a 100-year preclosure period).</p>
<p>Frequency Assessment Screening and Event Sequence Categorization</p>	<p>The frequency (or annual probability of occurrence) is estimated for each event sequence. The frequencies of initiating events for internal hazards are estimated from the annual frequency of each operation multiplied by the conditional probability of the initiating event per operation. For example, the frequency of a potential canister drop is estimated by the product of the frequency of canister lifts (i.e., the number per year) and the conditional probability of dropping the canister per lift. Uncertainties in data and models will be addressed in the frequency analyses.</p> <p>This analysis results in a categorization of each event sequence according to its mean frequency as either Category 1, Category 2, or Beyond Category 2. This frequency categorization is important because it establishes which portion of the Preclosure Performance Objectives of 10 CFR 63.111 must be met for each sequence. Note that the frequency categorization is based on the mean frequency of an entire sequence of events and not just the frequency of the initiating event.</p>
<p>Consequence Analysis</p>	<p>In this portion of the PSA the potential mean consequences are calculated for Category 1 and Category 2 event sequences and compared against the regulatory limits of 10 CFR 63.111. For Category 1 event sequences, which includes chronic releases from normal operations, consequences are evaluated from relevant pathways as potential contributors to chronic exposures and are aggregated. For Category 2 event sequences, consequences are evaluated for relevant pathways for each sequence as an acute exposure. Uncertainties will be addressed in the consequence analyses.</p>

* Incredible (derived from 10 CFR Part 63) is defined such that that the event sequence has less than a one in 10,000 chance of occurring before permanent closure (10 CFR 63.2).

** Credible (also derived from 10 CFR Part 63) is defined such that the event sequence has at least one chance in 10,000 of occurring before permanent closure.

The PSA will demonstrate with reasonable assurance that HLW can be received, handled, packaged, stored, emplaced, and retrieved without exceeding regulatory dose limits. The results of the PSA will be included in the license application. The PSA will also include a consideration of the means for providing radiation protection to workers, for detection and suppression of fires, for control of radioactive wastes and effluents, and for implementation of criticality safety principles. The PSA results will demonstrate the ability of SSCs important to safety to perform their intended safety functions based on reliability requirements. The SSCs identified as important to safety are identified on the *Q-List*, YMP/90-55Q (YMP 2001).

12.3 DEVELOPMENT OF A RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION PROCESS

The QA requirements in 10 CFR Part 50, Appendix B, were imposed on the safety-related SSCs in commercial nuclear reactor power plants. The safety-related SSCs for nuclear power plants include complex systems that are relied upon to ensure the integrity of the reactor coolant pressure boundary, ensure the capability to shut down the reactor, and prevent or mitigate the consequences of accidents having significant radiological consequences.

Initially, full Appendix B requirements were imposed on the safety-related SSCs of nuclear power plants on a deterministic basis. However, regulation of nuclear power plants has transitioned from the traditional, deterministic basis to a risk-informed basis. The implementation of NUREG-0800 (NRC 1987, Section 19.0), and Regulatory Guides 1.174 and 1.176 establishes the bases for graded QA requirements for a given nuclear power plant. Through the use of PRA, both safety-related and non-safety-related SSCs are classified into four risk-informed categories that provide the bases for QA grading of SSCs in a nuclear power plant. This graded approach for identifying risk significance provides general guidance for applying risk-informed QA classification to a HLW repository. However, this approach is not directly applicable since, compared to a nuclear power plant, a HLW repository is a low-energy, nonvolatile-hazard facility. The HLW repository important to safety features are basically passive with a limited need for automatic safety response to events. No short-term operator actions are expected to be required to meet the preclosure performance objectives. Also, no major risk-significant receipt, handling, packaging, storage, emplacement, or retrieval events have been identified in the site recommendation safety assessments that have been performed (BSC 2001). Therefore, NUREG-0800 (NRC 1987) and Regulatory Guides 1.174 and 1.176 should not be applied directly to a HLW repository, but do provide conceptual guidance to establish a risk-informed QA classification process. Consistent with this guidance, levels of risk significance (similar to the risk-informed safety significance for a nuclear power plant) can be developed using the event sequence frequency and consequence performance objectives of 10 CFR Part 63. Event sequence definitions and performance objectives from 10 CFR Part 63 provide bases for establishing the risk significance of SSCs.

From a risk perspective, the performance objectives of 10 CFR 63.111(b)(1) and (2) can be interpreted to define acceptable and unacceptable risk regions in terms of event sequence frequency (Category 1 or Category 2) and consequences (performance objectives for Category 1 and Category 2 event sequences). While the absolute risk associated with the performance objectives is small, relative risk regions can be established to identify the relative significance of an SSC. The relative risk regions derived from the 10 CFR Part 63 event sequence

categorization and performance objectives are summarized in Table 12-2. Note that the event sequence frequencies are derived from the definitions of Category 1 and Category 2 event sequences based on a 100-year preclosure period. The use of a 100-year preclosure period results in a frequency of 1×10^{-2} events per year for event sequences that have at least one chance in the life of the facility and a frequency of 1×10^{-6} events per year for event sequences that have one chance in 10,000 for the life of the facility. The consequence values are derived from 10 CFR 63.204 (15 mrem), 10 CFR 63.111(b)(2) (5 mrem) and 10 CFR 20.1301(a)(1) (100 mrem).

Table 12-2. Relative Risk Significance Based on 10 CFR Part 63

Event Sequence Frequency	Consequences (Dose [TEDE])		
	$15 \text{ mrem} \leq d < 100 \text{ mrem}$	$d \geq 100 \text{ mrem}$	$d \geq 5 \text{ rem}$
$\geq 10^{-2}$ per yr	Medium	High	
$\geq 10^{-6}$ per yr	Low	Medium	High

d = dose, TEDE = total effective dose equivalent.

An event sequence complies with the performance objectives when the event sequence frequency and consequences are within the boundaries of the acceptable risk region. Any event sequence with a frequency-consequence ordered-pair outside of these regions is an unacceptable risk. Figure 12-2 displays the acceptable risk regions based on the 10 CFR Part 63 preclosure performance objectives. For simplicity, only the mean Total Effective Dose Equivalent (TEDE) offsite preclosure performance objectives from 10 CFR Part 63 are displayed.

The region in Figure 12-2 between the frequencies of 1×10^{-2} events per year and 1×10^{-6} events per year that is bounded by the vertical consequence line at 5 rem is derived from the 10 CFR 63.2 definition of Category 1 and 2 event sequences and the Category 2 preclosure performance objectives. Category 1 event sequences are defined in 10 CFR 63.2 as:

Those event sequences that are expected to occur one or more times before permanent closure of the geologic repository area...

Assuming a preclosure operating period of 100 years, the sequence frequency separating Category 1 and Category 2 event sequences becomes 1 per 100 years, or a frequency of occurrence greater than or equal to 1×10^{-2} events per year. Event sequences at or above a frequency of 1×10^{-2} events per year are Category 1 event sequences. Those event sequences below a frequency of 1×10^{-2} events per year are Category 2 event sequences. Category 2 event sequences are defined in 10 CFR 63.2 as:

Other event sequences that have at least one chance in 10,000 of occurring before permanent closure...

With an assumed 100 year period before permanent closure, the frequency above which event sequences are defined as Category 2 is $(1/10,000)/(100 \text{ years})$, or 1×10^{-6} events per year. Event sequences with frequencies greater than or equal to 1×10^{-6} events per year, but less than 1×10^{-2} events per year, are defined as Category 2 event sequences.

The Category 2 performance objective stated in 10 CFR 63.111 is 5 rem per event sequence. This objective is represented in Figure 12-2 as a vertical line at 5 rem ending at frequencies of 1×10^{-2} and 1×10^{-6} events per year.

An isorisk line drawn with a slope of 15 mrem per year, ending with a vertical line drawn at 15 mrem, is illustrated in Figure 12-2 for Category 1 event sequences. The points on this isorisk line (i.e., the event sequence frequencies multiplied by the doses) have a constant risk of 15 mrem per year. This risk measure is based on the annual dose performance objective stated in 10 CFR 63.111(a)(2) for the aggregation of Category 1 radiation releases. The truncation of the isorisk line with a vertical line at a dose of 15 mrem reflects an interpretation of the Category 1 performance objective that states that no single event sequence shall exceed 15 mrem in any year.

A second isorisk line with a slope of 100 mrem per year is illustrated in Figure 12-2 for Category 1 event sequences. This line represents the annual dose objective of 100 mrem year from 10 CFR 63.111(a)(1) and the description of the numerical guide given in 10 CFR 63.111(b)(1). The 10 CFR 63.111(a)(1) guidance states that the requirements of 10 CFR Part 20 must be met for Category 1 event sequences; the Part 20 requirements state that the total annual dose cannot exceed 100 mrem per year. The truncation of the isorisk line with a vertical line at a dose of 100 mrem reflects an interpretation of this Category 1 performance objective that states that no single event sequence shall exceed 100 mrem in any year. For the purposes of QA classification, if the results of an SSC functional failure analysis (as explained in Section 5) produce a dose greater than 15 mrem along the 15-mrem isorisk line, the SSC will be classified as QL-2. Similarly, if the results of an SSC functional failure analysis produce a dose greater than 100 mrem along the 100-mrem isorisk line, the SSC will be classified as QL-1.

For simplicity, only the TEDE offsite preclosure performance objectives from 10 CFR Part 63 are displayed in this figure.

A high frequency (more than 1×10^{-2} events per year) low consequence (less than the 10 CFR 63.204 dose limits) risk region can be established that recognizes the potential for the occurrence of a low-risk-significant important to safety SSC. These SSCs can also provide margin (or defense-in-depth) for Category 1 event sequences and provide confidence that normal operations can be maintained while minimizing offsite radiological consequences. The low consequence threshold can be established based on trivial offsite consequences (taken to be less than one percent of the 10 CFR 63.204 dose limits). The updated relative risk significance is presented in Table 12-3.

The resultant relative risk is presented graphically in Figure 12-3, where:

- Risk Region I - High Relative Risk
- Risk Region II - Medium Relative Risk
- Risk Region III - Low Relative Risk
- Risk Region IV - Very Low (or no) Relative Risk

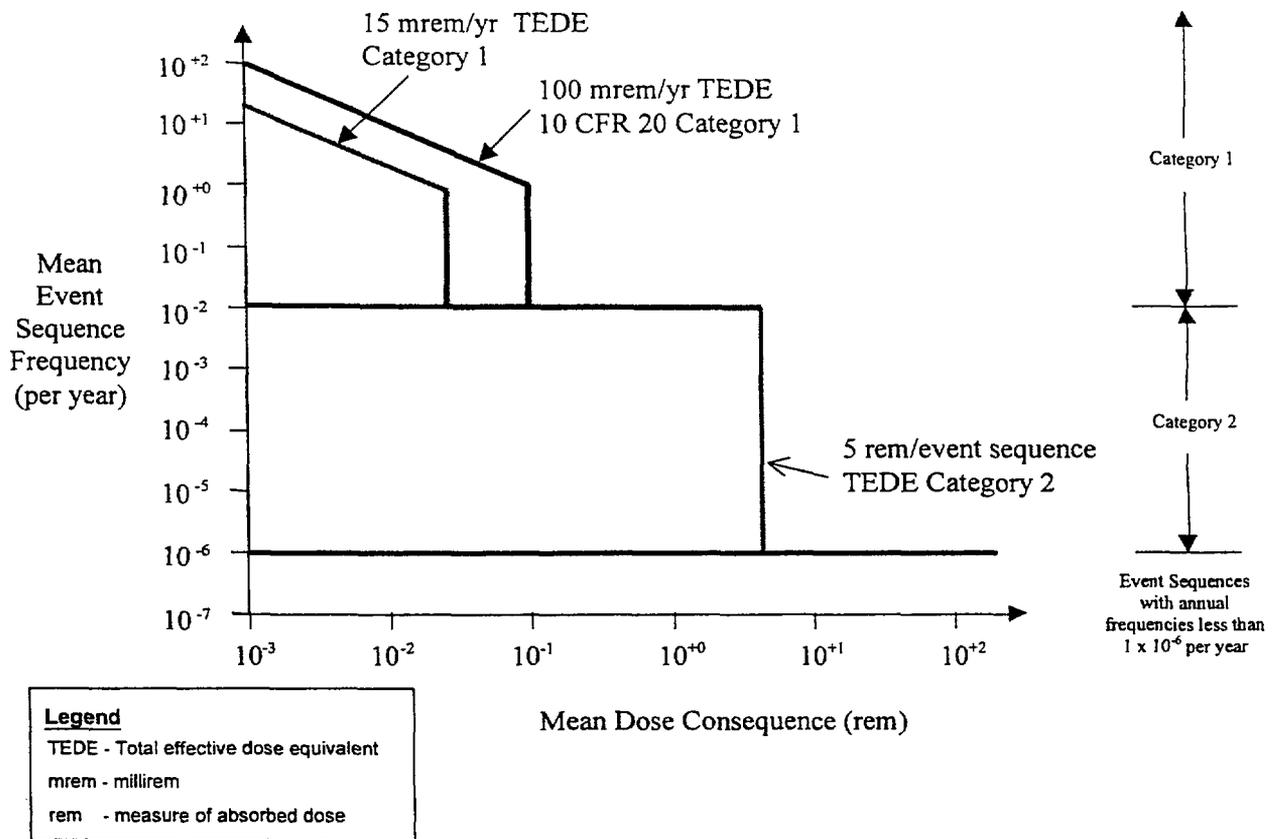


Figure 12-2. Compliance or Acceptable Risk Region Based on 10 CFR Part 63

Table 12-3. Updated Relative Risk Significance

Event Sequence Frequency	Consequences (Dose [TEDE])				
	$d < 0.15$ mrem	$0.15 \text{ mrem} \leq d < 15$ mrem	$15 \text{ mrem} \leq d < 100$ mrem	$d \geq 100$ mrem	$d \geq 5$ rem
$\geq 10^{-2}$ per yr	Very Low	Low	Medium	High	
$\geq 10^{-6}$ per yr		Very Low	Low	Medium	High

d = dose, TEDE = total effective dose equivalent

The risk regions in Figure 12-3 can then be used to define regions of comparable risk significance. Since the level of QA requirements applied should be consistent with the risk significance of the SSC based on a risk-informed, performance-based approach, the QLs (where comparable QA controls are applied) can be established, as presented in Table 12-4.

Table 12-4. Quality Levels Based on Risk Significance

Event Sequence Frequency	Consequences (Dose [TEDE])				
	$d < 0.15$ mrem	$0.15 \text{ mrem} \leq d < 15$ mrem	$15 \text{ mrem} \leq d < 100$ mrem	$d \geq 100$ mrem	$d \geq 5$ rem
$\geq 10^{-2}$ per yr	CQ	QL-3	QL-2	QL-1	
$\geq 10^{-6}$ per yr		CQ	QL-3	QL-2	QL-1

d = dose, TEDE = total effective dose equivalent

Where:

- QL-1 - Quality level associated with highest relative risk significance, full application of 10 CFR 63.142 QA criteria
- QL-2 - Quality level associated with medium relative risk significance; selected application of 10 CFR 63.142 QA criteria, but less than full application of quality requirements
- QL-3 - Quality level associated with low relative risk significance; limited application of 10 CFR 63.142 QA criteria; less rigorous application of quality requirements than those of QL-2
- CQ - Quality level associated with little or no relative risk significance; application of 10 CFR 63.142 criteria not required

The acceptable risk regions are used as a basis to define areas of successively lower relative risk for QA classification of each SSC important to safety. The QA classification process starts after HLW repository event sequences identified by a PSA have been shown to comply with 10 CFR Part 63. The classification of each SSC is then determined through a sensitivity analysis (called an SSC functional failure analysis). This analysis recalculates the frequency and consequences for that event sequence assuming that a specific SSC fails to perform its defined function (i.e., the SSC is hypothetically removed from the event sequence). This classification analysis identifies the importance to safety of the SSC in satisfying the 10 CFR Part 63 radiological performance objectives.

In order to implement a QA classification process, QA classification criteria must be established for each QL consistent with the relative risk regions and the associated functional failure analysis. The quantitative QA classification criteria are derived from the 10 CFR Part 63 preclosure performance objectives for offsite doses and worker exposures. The event sequences are categorized into one of three frequency ranges: Category 1 event sequences, Category 2 event sequences, and beyond Category 2 event sequences (i.e., incredible). The risk-informed, performance-based criteria are established through the use of limiting dose performance coupled with Category 1 and Category 2 event frequency categorizations. The resultant QA classification criteria are summarized in Table 12-5. These risk-informed regulatory performance objectives are an essential element in the QA classification. Models and the results of the PSA are used to

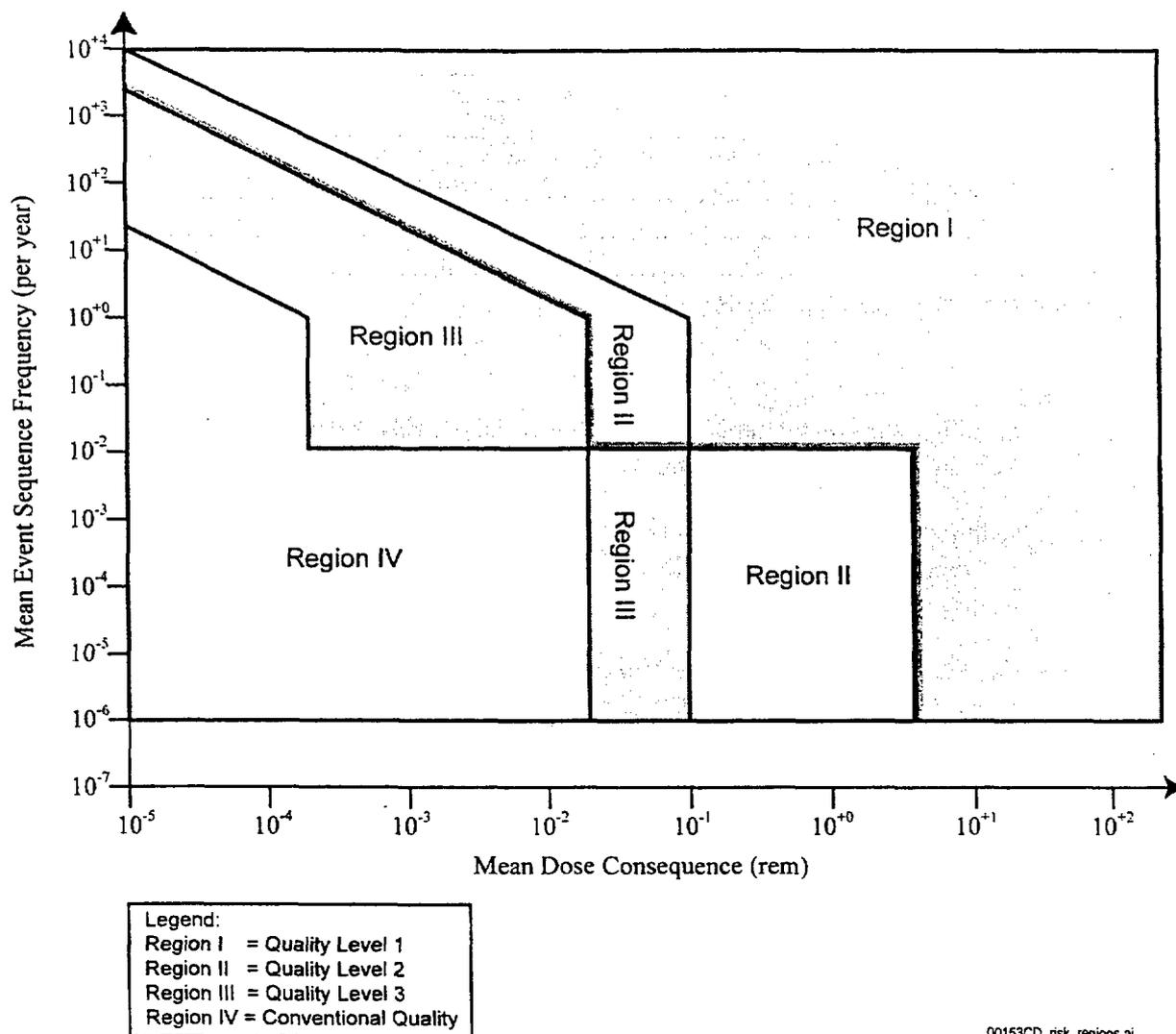


Figure 12-3. Example Quality Assurance Classification Risk Regions Developed from 10 CFR Part 63 Performance Objectives

assess the change in frequency or consequences that occur when a given SSC is assumed to be unavailable. A QL is assigned to an SSC in accordance with the risk region that contains the location of an event sequence, based on frequency and consequence, following the performance of the functional failure analysis for each SSC.

When evaluating the risk significance of an SSC in event sequences, the following factors should be considered:

- Is the SSC required to function to support another SSC that has been classified as important to safety?
- Does the SSC provide input to support a required action?

- Is there an interaction (e.g., seismic) in a portion of the event sequence that must be considered?
- Does the event sequence result in a fire that may impact the performance of an SSC in an event sequence?
- Are failure probabilities based on meeting licensing specifications or technical specifications (i.e., should licensing specification instrumentation be classified consistent with its role in the event sequence evaluation)?

Table 12-5. Risk Significant Screening Criteria

Criteria	Discussion	Basis
QL-1		
Frequency – Category 1 Consequence potential > 100 mrem TEDE	Regulatory Performance Objective Risk: High (High frequency, Medium consequence)	10 CFR 63.2 definition 10 CFR Part 20 limits (invoked by 10 CFR 63.111(a)(1) performance objective)
Frequency – Category 2 Consequence potential > 5 rem TEDE	Regulatory Performance Objective Risk: High (Low frequency, High consequence)	10 CFR 63.2 definition 10 CFR 63.111(b)(2) performance objective
QL-2		
Frequency – Category 1 Consequence potential > 15 mrem TEDE	Regulatory Performance Objective Risk: Medium (High frequency, Low consequence)	10 CFR 63.2 definition 10 CFR 63.204 performance objective
Frequency – Category 2 Consequence potential > 100 mrem TEDE	Risk judgment Risk: Medium (Low frequency, medium consequence)	10 CFR 63.2 definition 10 CFR Part 20 limit
QL-3		
Frequency – Category 1 Consequence potential > 0.15 mrem TEDE	Risk judgment classification for SSCs involved in event sequence Risk: Low (High frequency, low consequence) Supports minimization of normal releases	Engineering judgment to establish trivial offsite consequences (1% of category regulatory limit)
Frequency – Category 2 Consequence potential > 15 mrem TEDE	Risk judgment classification for SSCs involved in event sequence Risk: Low (Low frequency, low consequence)	Engineering judgment to establish trivial offsite consequences for associated event frequency (used QL-2 risk level for Category 1 event sequences)
Frequency – Category 1 Consequence potential > 5 rem to worker	Regulatory Performance Objective Highlights SSCs that contribute to worker dose reduction during category 1 event sequences	10 CFR 63.2 Regulatory Guide 8.8 10 CFR Part 20 limit (invoked by 10 CFR 63.111(a)(1) performance objective)

TEDE = total effective dose equivalent

Many of these factors are derived from industry and regulatory precedents. When evaluating the safety significance of an SSC, a robust, systematic approach is required that ensures that the

relevant factors have been considered. Industry and regulatory guidance such as the Regulatory Guides (e.g., 1.26, 1.29, 1.97, 1.143, 1.189), NUREGs (e.g., NUREG-0800 [NRC 1987]), and standards (e.g., ANSI/ANS-55.1-1992, American Society of Mechanical Engineers, and American National Standards Institute radioactive waste standards) can be used as guidance when evaluating the risk significance of an SSC. The use of precedent as guidance supports a risk-informed QA classification approach by linking the risk determined for an SSC to an identified hazard. Preclosure safety will be based on the SSCs that are required to meet the preclosure safety performance objectives. These SSCs are identified as important to safety in accordance with 10 CFR 63.2. In addition, defense-in-depth SSCs may also be included. By definition, defense-in-depth SSCs are not required in order to demonstrate compliance with preclosure performance objectives and are, therefore, classified as CQ.

12.4 QUALITY ASSURANCE CLASSIFICATION PROCESS

The risk-informed, performance-based QA classification process is presented in Figure 12-4. Because the development of the PSA is an iterative process linked to the development of the design, so is the QA classification process. The PSAs that are based on, and consistent with, the level of development of a repository design provide inputs to the classification of SSCs. Using this information, each SSC is evaluated at the QL-1, QL-2, and QL-3 decision blocks depicted in Figure 12-4. At each decision block, each event sequence (that will become part of the licensing basis) involving the SSC being classified is considered. The QL-1, QL-2, and QL-3 screening criteria are applied sequentially to determine the appropriate QL for each SSC. The first positive response in a decision block yields the QL for the SSC. If the SSC passes through the three decision blocks, it is assigned a classification of CQ.

The QL decision criteria can be answered only with the support of PSA elements: hazards analyses for external and internal events, event sequence analyses, radiological consequence analyses, or discipline-specific analyses such as criticality analyses. Functional failure analyses are used to identify the relative risk significance of SSCs in event sequences.

The resultant SSC classifications are presented in the Q-List. Future updates to the Q-List will reflect the criteria prescribed in Table 12-5 and the process described in Figure 12-4.

12.5 FUNCTIONAL FAILURE ANALYSIS IN RISK INFORMED QUALITY ASSURANCE CLASSIFICATION

The QA classification process is applied to individual SSCs in sequential order. The process is different for Category 1 and Category 2 event sequences due to the differences in the regulatory performance objectives. The steps in the QA classification process for Category 1 event sequences involve evaluating both the consequences of normal operations and Category 1 event sequences, which are then summed to estimate an annual dose. The dose summation provides aggregated consequences prior to permanent closure to show compliance with the performance objectives stated in 10 CFR 63.111(b)(1). Category 2 event sequences are assessed on an individual basis; the process has fewer steps than for Category 1 event sequences.

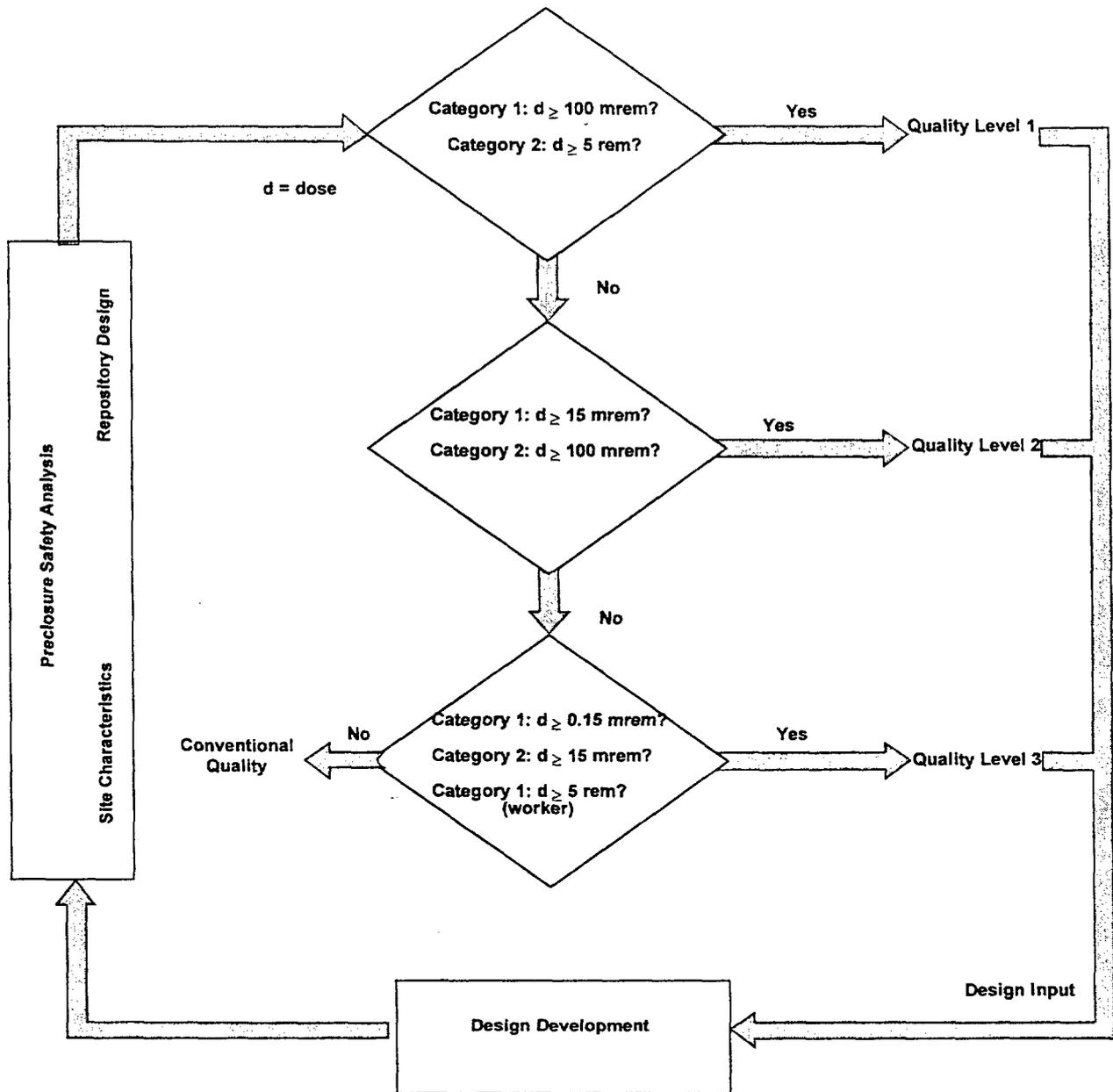


Figure 12-4. Risk Informed Quality Assurance Classification Process

12.6 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 1 EVENT SEQUENCES

As noted previously, before the QA classification process is applied, Category 1 event sequences will have been demonstrated to comply with the performance objectives. Demonstrating compliance for Category 1 event sequences takes into consideration contributions from normal surface and subsurface operational and offsite radiological releases from Category 1 event sequences in the annualized dose estimates. These contributions to the annualized dose estimate are part of the aggregation of exposures required by 10 CFR Part 63.

Compliance with the Category 1 annual dose objectives is performed as follows:

1. Demonstrate that the aggregate radiation exposures and the aggregate radiation levels in both restricted and unrestricted areas, and the aggregate releases of radioactive materials to unrestricted areas from normal operations in addition to the Category 1 event sequences meet the annual dose performance objectives in 10 CFR 63.111(a).
2. Demonstrate that the radiation exposure and the radiation levels in both restricted and unrestricted areas and releases of radioactive materials to unrestricted areas for each Category 1 event sequence meet the annual dose performance objectives in 10 CFR 63.111(a).
3. Demonstrate that the radiation exposure and the radiation levels in both restricted and unrestricted areas, and releases of radioactive material to unrestricted areas resulting from combinations of two or more Category 1 event sequences that could occur in a single year with a mean frequency greater than or equal to a frequency of 1×10^{-2} events per year, meet the annual offsite dose performance objectives in 10 CFR 63.111(a).

The methodology for Category 1 event sequence compliance demonstration is described in the following section.

12.7 COMPLIANCE DEMONSTRATION FOR NORMAL OPERATION RELEASES AND CATEGORY 1 EVENT SEQUENCES

For compliance demonstration of Category 1 event sequences and normal operating releases from the surface and subsurface facilities, the annual offsite dose is calculated as follows:

$$D_{Cat1} = D_{norm} + \sum F_i D_i \quad (\text{Eq. 12-1})$$

where

- D_{Cat1} = total annual offsite doses from Category 1 event sequences and normal operations (mrem per yr)
- D_{norm} = the expected annual offsite dose from surface and subsurface normal releases (mrem per yr)
- F_i = frequency for event sequence i (per year)
- D_i = offsite dose for i^{th} Category 1 event sequences (mrem)
- $\sum F_i D_i$ = sum of the frequency-weighted offsite doses for the Category 1 event sequences in any given year, summed over sequences $i = 1$ to n , where n is the number of Category 1 event sequences (mrem per yr)

Compliance is demonstrated when the performance objectives in 10 CFR 63.111(a) are met (e.g., when D_{Cat1} is demonstrated to be less than 15 mrem per yr TEDE).

Further, to ensure that no single event sequence could exceed the performance objectives in 10 CFR 63.111(a); compliance is also assessed for each individual Category 1 event sequence as follows:

$$D_i < 15 \text{ mrem} \quad (\text{Eq. 12-2})$$

where

$$D_i = \text{offsite TEDE dose for individual Category 1 event sequence } i \text{ (mrem)}$$

Total offsite doses are estimated for compliance demonstration of combinations of two or more Category 1 event sequences. The combinations of event sequences that can occur with an estimated mean frequency of 1×10^{-2} events per year or greater are selected from the list of Category 1 event sequences. The offsite doses for each event sequence in the combination are summed and then compared to the 10 CFR 63.111(a) performance objectives. The doses from the combined event sequences that could credibly occur are evaluated as follows to demonstrate compliance:

$$D_{Comb} = \sum D_i \quad (\text{Eq. 12-3})$$

where

$$D_{Comb} = \text{total offsite dose for credible combinations of individual Category 1 event sequences (mrem)}$$

$$D_i = \text{offsite dose for the } i^{\text{th}} \text{ Category 1 event sequence considered in the combination (mrem)}$$

Compliance is demonstrated when the dose from the combination of two or more Category 1 event sequences that could credibly occur is shown to be less than 15 mrem per yr TEDE.

12.8 PROCESS FOR RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS IN CATEGORY 1 EVENT SEQUENCES

The QA classification of a particular SSC may require several different functional failure analysis iterations. The first analysis is applied to the SSCs involved in individual Category 1 event sequences. The second analysis is applied to those same SSCs that may also appear in credible combinations of Category 1 event sequences. For the classification analysis of each SSC, the offsite doses that result after the assumed functional failure of the SSC are evaluated in the following manner:

$$D_{ce} = [D_{norm} + \sum F_i D_i] + D_e^* \quad (\text{Eq. 12-4})$$

where

D_{norm} and $\sum F_i D_i$ are defined previously

D_{ce} = offsite classification event dose with the assumed functional failure of the SSC (i.e., the SSC is hypothetically removed from the sequence being evaluated) (mrem per yr)

D_e = dose from an event sequence that includes the SSC being classified; however the mitigation function of the SSC is assumed to have failed (the sequence is assumed to occur no more than once per year) (mrem per yr)

NOTE: The Category 1 event sequences are assumed to have an estimated mean frequency of less than once per year. However, for the purpose of QA classification, these event sequences are assumed to have occurred every year and are not annualized.

The offsite classification event dose (D_{ce}) represents the potential dose for Category 1 event sequences if the SSC under study was assumed to fail when called upon to mitigate consequences. The increase in dose resulting from the removal of the SSC is D_e . The D_e is added to aggregate offsite doses of $D_{norm} + \sum F_i D_i$. This approach provides a risk-informed basis for classifying each SSC. If D_{ce} exceeds 15 mrem per year TEDE but is less than 100 mrem per year TEDE, the SSC is classified as QL-2. If D_{ce} exceeds 100 mrem per year TEDE, the SSC is classified as QL-1.

If the SSC is also part of a credible combination of two or more Category 1 event sequences that could occur at a mean frequency of 1×10^{-2} events per year or greater, the QA classification process proceeds considering the unavailability of each SSC that has a mitigation function for that combination of event sequences. The annual offsite dose resulting from the combination of credible Category 1 event sequences after the assumed functional failure of an SSC will determine the QA classification of that SSC. If D_{Comb} exceeds 15 mrem per year TEDE but is less than 100 mrem per year TEDE, the SSC is classified as QL-2; if D_{Comb} exceeds 100 mrem per year TEDE, the SSC is classified as QL-1.

If applicable, each SSC is also evaluated for QA classification according to Category 2 event sequence criteria. The final QA classification for each SSC is the highest classification level resulting from the QA classification process used for Category 1 and Category 2 event sequence evaluations.

The steps for performing the QA classification evaluation of SSCs in Category 1 event sequences are summarized in Table 12-6.

12.9 RISK-INFORMED QUALITY ASSURANCE CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS ASSOCIATED WITH CATEGORY 2 EVENT SEQUENCES

As discussed previously, before the QA classification process is begun, event sequences will have been shown to meet the preclosure performance objectives stated in 10 CFR Part 63. Compliance analyses for Category 2 event sequences will demonstrate, for each event sequence assessed individually, that the offsite dose is less than 5 rem TEDE (10 CFR 63.111(b)(2)). The classification analyses reassess the dose after an SSC functional failure is performed. If the dose

exceeds 5 rem, the SSC is classified as QL-1. If the dose is less than 5 rem but greater than 100 mrem, the SSC is classified as QL-2. If the dose is less than 100 mrem but greater than 15 mrem, the SSC is classified as QL-3. Otherwise, the SSC is not subject to the requirements of the 10 CFR Part 63 QA program (i.e., is classified as CQ).

Figure 12-5 illustrates an example of the QA classification process using the functional failure analysis. Initially, an event sequence is identified and demonstrated to comply with the performance objectives. For example, the square in Figure 12-5 represents an event sequence with a mean frequency of 5×10^{-5} events per year and an offsite dose of 5×10^{-3} rem TEDE. This event sequence complies with the performance objectives based on the performance of one or more SSCs important to safety. After the assumed removal of an SSC considered in the original event sequence evaluation, the consequences are re-estimated. In the illustration in Figure 12-5, the consequence is now shown to be 6 rem TEDE (a value used for illustration only) after the assumed functional failure of the SSC under consideration. This dose exceeds the 10 CFR 63.111(b)(2) performance objective of 5 rem TEDE. The resulting event sequence (represented as a circle in Figure 12-5) now has a mean frequency of 5×10^{-5} events per year and dose of 6 rem TEDE. This analysis demonstrates that the SSC under consideration is important to safety and that without it the event sequence would be in Risk Region I. In this illustration, the SSC under consideration would be classified as QL-1.

If the same SSC appears in more than one event sequence, regardless of whether in Category 1 or Category 2 regions, an appropriate functional failure analysis would be performed. The analysis would be completed for each affected event sequence. The highest QA classification resulting from these analyses would be assigned to the SSC.

Table 12-6. Steps for Performing a Quality Assurance Classification Analysis of Structures, Systems, and Components Associated with Category 1

1. Calculate D_{norm} , the annual offsite dose from surface and subsurface normal operations.
2. Calculate D_i , the offsite dose from a Category 1 event sequence i .
3. Calculate $\sum F_i D_i$, the frequency-weighted offsite dose sum of the Category 1 event sequences [i.e., $i = 1$ to n sequences].
4. Identify event sequences that include the SSC being classified and its associated offsite dose D_e (after the SSC is assumed to be removed).
5. Perform an SSC functional failure analysis for each event sequence that includes the SSC being classified using classification event dose D_{ce} where $D_{ce} = [D_{norm} + \sum F_i D_i] + D_e$.
6. Perform an SSC functional failure analysis for each Category 1 combination of event sequences that includes the SSC being classified (the D_e from each event sequence is included).
7. Classify SSCs based on highest classification level identified based on the functional failure analysis from each Category 1 event sequence or Category 1 combination that includes the SSC being evaluated. If applicable, each SSC is also evaluated for classification according to Category 2 event sequences and consideration of event sequences with annual frequencies less than 1×10^{-6} events per year.

The final SSC QA classification is the highest classification level resulting from applying the QA classification objectives from Category 1, Category 2 and event sequences that are at a lower event sequence frequency than the Category 2 event sequence frequency.

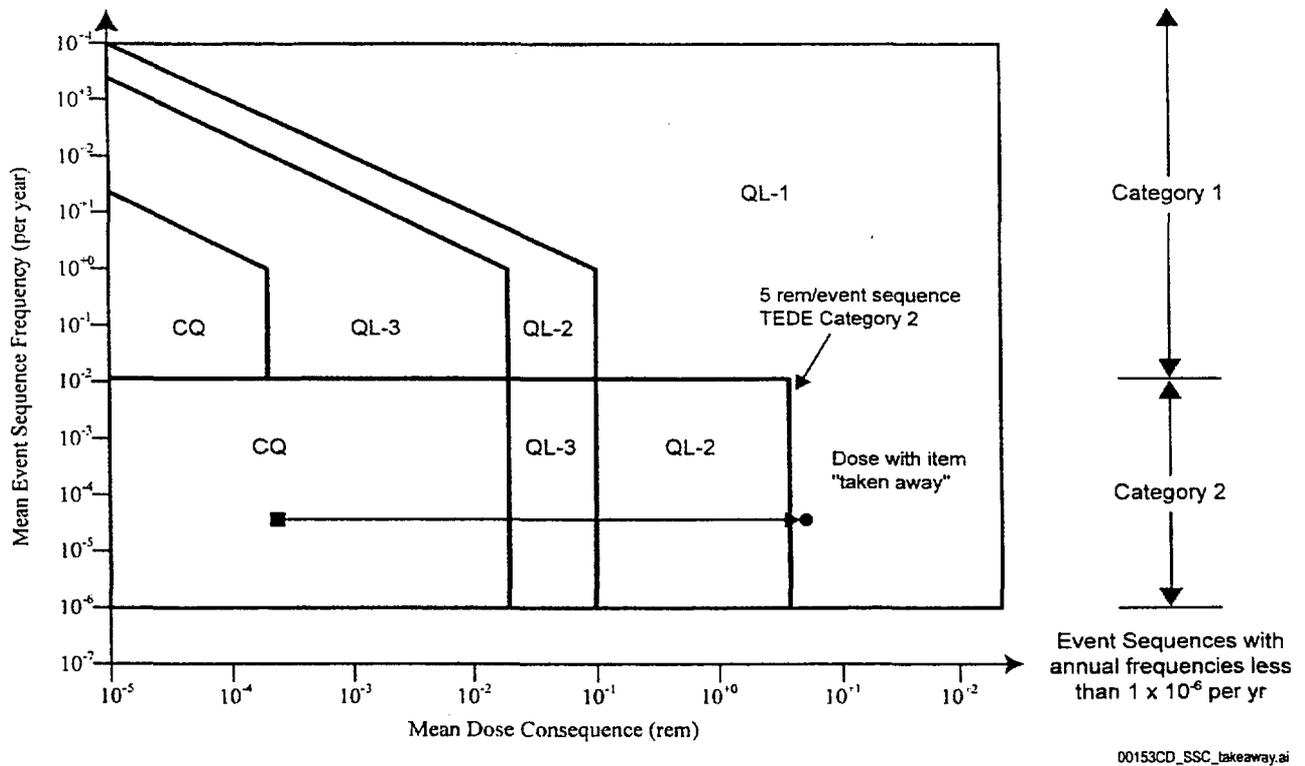


Figure 12-5. Example of the Quality Assurance Classification Process for a Category 2 Event Sequence

12.10 REFERENCES

12.10.1 Documents Cited

BSC (Bechtel SAIC Company) 2001. *Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation*. TDR-MGR-SE-000009 REV 00 ICN 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: MOL.20010705.0172.

NRC (U.S. Nuclear Regulatory Commission) 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

YMP (Yucca Mountain Site Characterization Project) 2001. *Q-List*. YMP/90-55Q, Rev. 7. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.20010409.0366.

12.10.2 Codes, Standards, Regulations, and Procedures

10 CFR 20. Energy: Standards for Protection Against Radiation. Readily available.

10 CFR 50. Energy: Domestic Licensing of Production and Utilization Facilities. Readily available.

10 CFR 63. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. Readily available.

40 CFR 191. Protection of Environment: Environmental Radiation Protection Standards for Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes. Readily available.

ANSI/ANS-55.1-1992. *Solid Radioactive Waste Processing System for Light-Water-Cooled Reactor Plants*. La Grange Park, Illinois: American Nuclear Society. TIC: 241063.

Regulatory Guide 1.143, Rev. 2. 2001. *Design Guidance for Radioactive Waste Management Systems, Structures, and Components Installed in Light-Water-Cooled Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.174, Rev. 01 Draft. 2001. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.176. 1998. *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.189. 2001. *Fire Protection for Operating Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.26, Rev. 3. 1976. *Quality Group Classifications and Standards for Water, Steam, and Radioactive Waste Containing Components of Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.29, Rev. 3. 1978. *Seismic Design Classification*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 1.97, Rev. 3. 1983. *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

Regulatory Guide 8.8, Rev. 3. 1978. *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations Will be as Low as is Reasonably Achievable*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily available.

CONTENTS

	Page
ACRONYMS.....	i
13. SELECTION OF 10 CFR 63.2 DESIGN BASES FOR STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY.....	13-1
13.1 INTRODUCTION	13-1
13.2 BACKGROUND INFORMATION	13-1
13.3 METHOD FOR DEVELOPING 10 CFR 63.2 DESIGN BASES.....	13-3
13.4 EXAMPLES	13-5
13.5 REFERENCES	13-6
13.5.1 Documents Cited	13-6
13.5.2 Codes, Standards, Regulations, and Procedures.....	13-6

FIGURES

	Page
13-1 Relationship of Repository Design Bases to 10 CFR 63.2 Design Bases and the Safety Analysis Report (SAR).....	13-2
13-2 Basic Steps in Developing 10 CFR 63.2 Design Bases.....	13-5

ACRONYMS

PSA	preclosure safety analysis
SAR	safety analysis report
SSCs	structures, systems, and components

INTENTIONALLY LEFT BLANK

13. SELECTION OF 10 CFR 63.2 DESIGN BASES FOR STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY

13.1 INTRODUCTION

This section describes the development of the design bases for structures, system, and components (SSCs) important to preclosure safety. Background information from 10 CFR Part 63 will be presented followed by a general discussion of the methodology for developing the design bases for SSCs and an example.

13.2 BACKGROUND INFORMATION

Important to safety, SSCs will have design bases established as defined in 10 CFR 63.2:

Design bases means that information that identifies the specific functions to be performed by a structure, system, or component of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be constraints derived from generally accepted "state-of-the-art" practices for achieving functional goals or requirements derived from analysis (based on calculation or experiments) of the effects of a postulated event under which a structure, system, or component must meet its functional goals. The values for controlling parameters for external events include:

- (1) Estimates of severe natural events to be used for deriving design bases that will be based on consideration of historical data on the associated parameters, physical data, or analysis of upper limits of the physical processes involved; and
- (2) Estimates of severe external human-induced events to be used for deriving design bases, that will be based on analysis of human activity in the region, taking into account the site characteristics and the risks associated with the event.

The values for the controlling parameters for external events include (1) estimates of severe natural events to be used for deriving design bases that will be based on consideration of historical data on the associated parameters, physical data, or analysis of upper limits of the physical processes involved; and (2) estimates of severe external human-induced events to be used for deriving design bases, that will be based on analysis of human activity in the region, taking into account the site characteristics and the risks associated with the event.

When describing the content of application, 10 CFR 63.21 states that the safety analysis must include among other items:

- (3) (ii) The design criteria used and their relationship to the preclosure and postclosure performance objectives specified at §63.111(b), §63.113(b) and §63.113(c); and (iii) The design bases and their relation to the design criteria.

Design basis requirements are developed from the geologic repository Category 1 and Category 2 event sequences that are identified through a preclosure safety analysis (PSA) (as discussed in Section 7.6 of this guide). The Category 1 and 2 event sequences are evaluated against their respective dose performance objectives. SSC safety functions are identified from these event sequences.

SSCs involved in the event sequences that are required to prevent or mitigate offsite dose from exceeding the 10 CFR Part 63 preclosure performance objectives are selected as important to safety. A design basis is developed for each of these SSCs. The design basis describes the SSC safety function. Design criteria are established for each safety function. Design criteria are bounding values for controlling specific values or ranges of values chosen for controlling parameters as reference bounds for the design. The relationship of each SSC design criteria to the design bases must be tied directly to the preclosure performance objectives specified in 10 CFR 63.111(b).

A distinction is made between the repository design bases and 10 CFR 63.2 design bases for SSCs. SSCs that comprise the repository design will have design bases. However, only SSCs that are important to safety will have design bases developed per 10 CFR 63.2. These 10 CFR 63.2 design bases are a subset of the licensing bases and are required pursuant to 10 CFR 63.112 to be included in the safety analysis report (SAR). The SAR will set forth a safety assessment of the 10 CFR 63.2 repository design bases. Both 10 CFR 63.2 design bases and supporting design information are subjected to design control and other quality assurance criteria of 10 CFR 63.142 as applicable to the quality level classification of the SSCs. The 10 CFR 63.2 design bases and supporting information contained in the SAR are controlled in accordance with 10 CFR 63.44.

Figure 13-1 shows the relationship of 10 CFR 63.2 design bases to the repository design bases and the SAR.

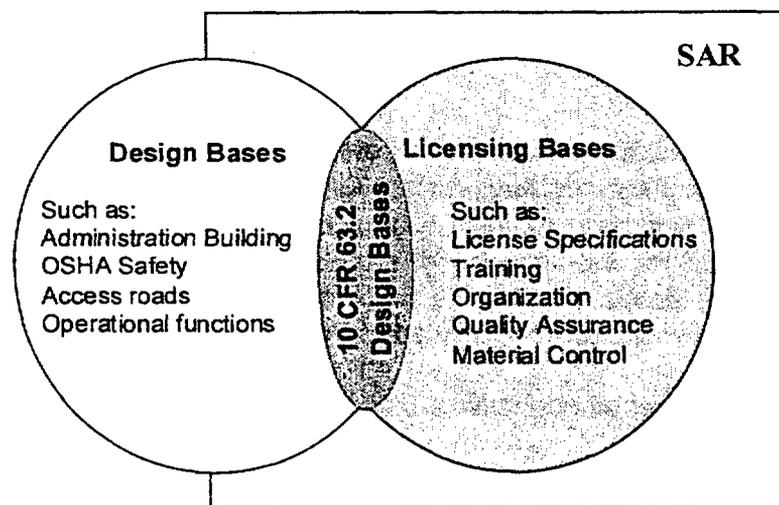


Figure 13-1. Relationship of Repository Design Bases to 10 CFR 63.2 Design Bases and the Safety Analysis Report (SAR)

The white circle represents the design bases for each SSC comprising the repository facility. The dark gray circle represents the complete licensing bases presented in the SAR. The crosshatched region depicts those SSC that are important to safety and have 10 CFR 63.2 design bases.

The assessment of the important to safety SSCs should be in sufficient detail so that the U.S. Nuclear Regulatory Commission staff can make an independent determination that there is reasonable assurance that safe operation will be achieved. Underlying 10 CFR 63.2 design bases is supporting design that includes design inputs, design analyses, and design output documents. Supporting design information may be contained in the SAR or other documents some of which are docketed and some that are retained by the licensee.

13.3 METHOD FOR DEVELOPING 10 CFR 63.2 DESIGN BASES

The basic steps in developing the 10 CFR 63.2 design bases are illustrated in Figure 13-2 and summarized as follows:

1. Identify, through a PSA, the Category 1 and 2 event sequences that are derived from internal, external, and manmade hazards (see Sections 6, 7, 10, and 11).

The list of Category 1 and 2 events form a part of the repository licensing bases and will appear in the SAR. Each Category 1 or 2 event sequence contains SSCs modeled within the PSA to assess the likelihood and consequences of an event sequence.

This list may change as the design matures. Changes in this list will result in a reassessment of the design bases and design criteria. Design iterations, design improvements, or modifications can lead to changes in this list throughout the licensing process and beyond.

2. Identify those SSCs important to safety, based on the Category 1 and 2 event sequences (see Section 12).

Every SSC on this list will require the establishment of 10 CFR 63.2 design bases and design criteria.

3. Select an important-to-safety SSC from the above list and identify the Category 1 and Category 2 event sequences that contain that SSC.

Category 1 and Category 2 event sequence compliance with 10 CFR Part 63 performance requirements are significantly different. Category 1 compliance assessments are based on annual performance requirements that require an aggregation of releases to unrestricted areas, as described in Section 8. Category 2 event sequence compliance assessment is on a per event basis. No aggregations of release are to be done for Category 2 event sequences. Because of these compliance differences, it will be easier to start with SSCs involved in Category 2 event sequences. Develop the design bases and design criteria for these SSCs first.

4. Identify the design criteria by safety function, from the selected Category 2 event sequences for the selected SSC.

Beginning with an SSC identified from Category 2 event sequences, establish the design criteria and safety functions or design bases. Document the relationship between design criteria and design bases and the performance objectives that are met by the SSC in the event sequence under study. Maintain this relationship by SSC within a database or some other organizational tool.

To provide confidence in the repository preclosure design, in some cases, the PSA includes evaluation of the consequences of selected sequences that are below the Category 2 frequency threshold, using the best estimate conditions. The purpose of this evaluation is to ensure that such an event sequence with unacceptable consequences is not arbitrarily excluded, based on probability. Any features added to mitigate the consequences of such events would not be considered as important to safety. Such analysis will not be part of the safety case, but has the potential of providing additional confidence in the repository performance.

5. Select the Category 2 bounding 10 CFR 63.2 design criteria for each safety function identified for the selected SSC.
6. Repeat Steps 3 through 5 until the important-to-safety SSCs have 10 CFR 63.2 design bases developed for Category 2 event sequences.
7. Select an SSC that is important to safety for meeting Category 1 performance criteria.
8. Examine the Category 1 event sequences containing this SSC and develop 10 CFR 63.2 design bases and design criteria.
9. Select the bounding design bases and design criteria for this SSC that will meet the performance objectives.
10. After the bounding Category 1 design bases are established for an SSC, review the Category 2 design bases established and optimize the Category 1 and 2 design bases such that the most limiting performance objectives from 10 CFR 63.111 are met.
11. Repeat Steps 7 through 10 until SSCs in Category 1 event sequences have 10 CFR 63.2 design bases established.
12. Review the total set of bounding design criteria for each important-to-safety SSC for completeness and consistency.

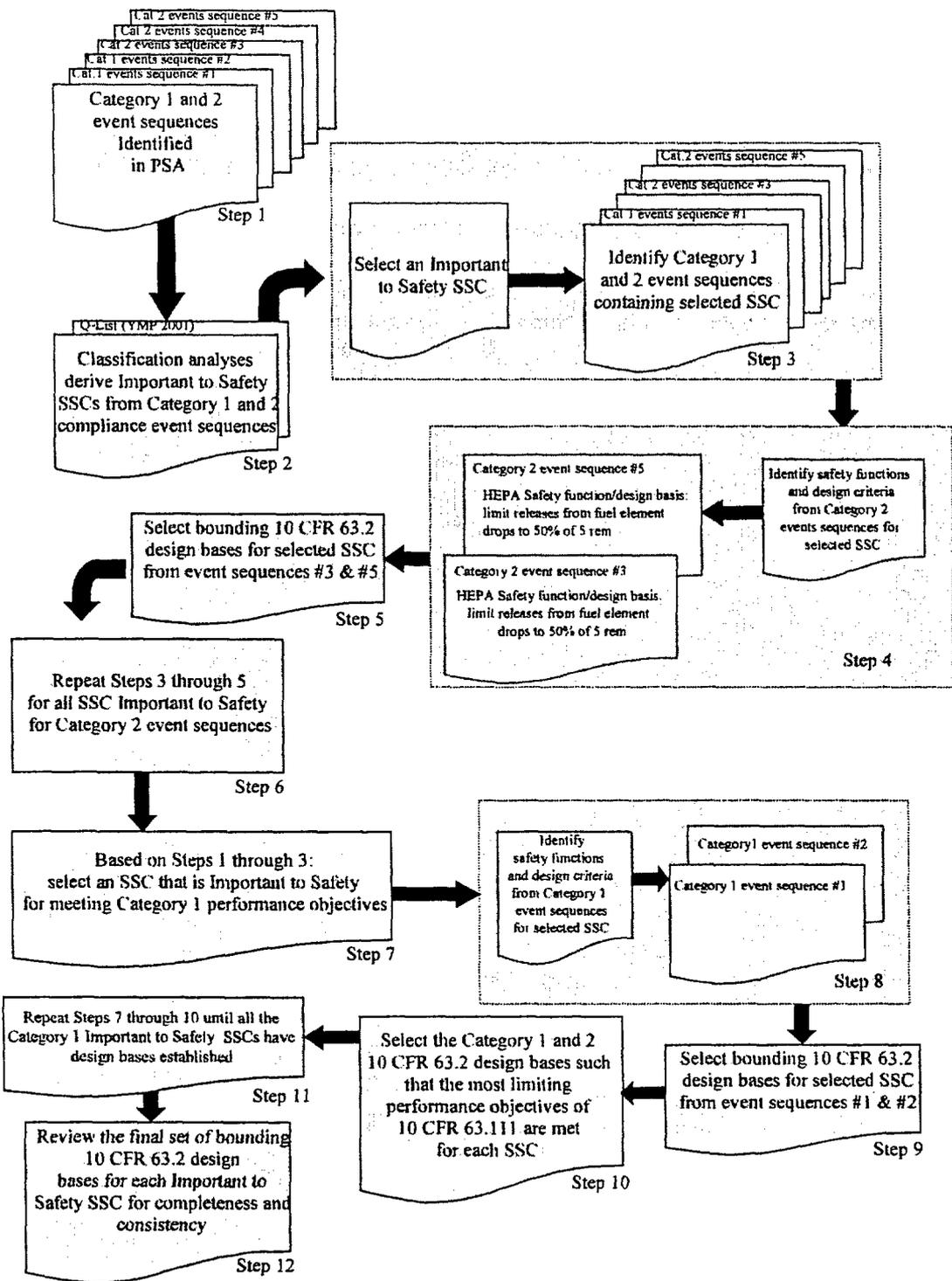


Figure 13-2. Basic Steps in Developing 10 CFR 63.2 Design Bases

13.4 EXAMPLES

[Information for this section is under development and will be provided later.]

13.5 REFERENCES

13.5.1 Documents Cited

YMP (Yucca Mountain Site Characterization Project) 2001. *Q-List*. YMP/90-55Q, Rev. 7. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.20010409.0366.

13.5.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

CONTENTS

	Page
ACRONYMS.....	i
14. DOCUMENTATION AND PREPARATION OF LICENSE APPLICATION	14-1
14.1 PRECLOSURE SAFETY ANALYSIS DOCUMENTATION	14-1
14.1.1 Internal and External Hazards Analyses	14-1
14.1.2 Categorization of Event Frequencies	14-1
14.1.3 Consequence Analysis	14-2
14.1.4 Preclosure Safety Analysis	14-2
14.1.5 Identify Structures, Systems, and Components to Prevent or Mitigate Event	14-3
14.2 PRECLOSURE SAFETY ANALYSIS AND LICENSE APPLICATION SUBMITTAL.....	14-4
14.3 REFERENCES	14-4
14.3.1 Documents Cited.....	14-4
14.3.2 Codes, Standards, Regulations, and Procedures	14-4

ACRONYMS

ALARA	as low as is reasonably achievable
BC2	beyond Category 2
HVAC	heating, ventilation, and air-conditioning
NRC	U.S. Nuclear Regulatory Commission
PSA	Preclosure Safety Analysis
SSCs	structures, systems, and components
YMP	Yucca Mountain Site Characterization Project

INTENTIONALLY LEFT BLANK

14. DOCUMENTATION AND PREPARATION OF LICENSE APPLICATION

14.1 PRECLOSURE SAFETY ANALYSIS DOCUMENTATION

The documents that are required to provide the input for the Preclosure Safety Analysis (PSA) are described in the following sections.

14.1.1 Internal and External Hazards Analyses

The internal and external hazards analyses document the potential hazards that may be present at a repository at Yucca Mountain. These analyses should be consistent with the 10 CFR 63.2 repository design bases. The process used to identify hazards is described in Section 6.

The internal hazards analysis describes the potential hazards that are related to the design and operation of the repository during the preclosure period, including potential chemical and criticality hazards. The external hazards analysis describes the spectrum of potential external events and natural phenomena. The credible hazards (i.e., initiating events) during the preclosure period will be based on historical data or U.S. Nuclear Regulatory Commission (NRC) regulatory guidance.

14.1.2 Categorization of Event Frequencies

Using the results of the internal and external hazards analyses, potential event sequences will be categorized as Category 1, Category 2, or beyond Category 2 (BC2) event sequences by analysis. The analyses will be continually updated as design develops to ensure the categorization, design, and hazards identification are consistent with license application design. The evaluation of potential hazards will be captured in analyses and calculations such as:

Aircraft Hazards Assessment—The credibility of aircraft hazards within the selected vicinity of the general repository operations area, consistent with NUREG-0800 (NRC 1987) and other appropriate NRC guidance, will be analyzed using current flight information. The appropriateness of flight information for the repository operating period is evaluated, and future efforts, if required, to support aircraft hazards categorization are identified.

Wind and Tornado Analysis—The design basis tornado and wind loadings will be identified in accordance with nuclear and regulatory guidance (e.g., NUREG-0800 [NRC 1987] and Regulatory Guide 1.76). The tornado missile spectrum for the Yucca Mountain Site Characterization Project (YMP) will be developed. The features and controls that are required to ensure that design basis tornado and winds will not result in a radiological release that exceeds regulatory requirements will be identified.

Industrial and Military Hazards Assessment—The potential industrial and military hazards for potential consideration in the repository design consistent with nuclear industry precedents (e.g., NUREG-0800 [NRC 1987]) will be identified and evaluated. Any features or controls required to screen or mitigate industrial and military hazards will be identified.

Rainstorm and Flooding Analysis—The rainstorm and flooding criteria is determined in accordance with accepted nuclear precedents (e.g., NUREG-0800 [NRC 1987]). Any features or

controls required to ensure that a rainstorm or flooding event does not result in a radiological release will be identified.

Seismic Analysis—The appropriate SSC seismic design criteria consistent with regulatory requirements and the YMP seismic topical report will be identified. The SSC seismic criteria to ensure that regulatory requirements are met in the event of a seismic event will be identified.

Fire Sequence Analysis—Using the results of the facility fire hazards analyses, credible fires will be evaluated as initiating events for the potential to result in a radiological release. Potential fire scenarios should include surface, subsurface, and external fires (e.g., range fires and lightning-initiated fires). Any features or controls that ensure that fires do not result in a radiological release that exceeds regulatory requirements will be identified.

Loss of Power—Loss of power as an initiating event will be evaluated. It should be demonstrated that loss of power does not result in a radiological release that exceeds regulatory requirements. Any features or controls that are required to ensure loss of power does not result in releases that exceed regulatory requirements will be identified.

Waste Handling Fault Tree Analysis—The reliability of handling systems for use in event trees that include handling branches will be determined.

Component Failure and Reliability Analysis Database—Industry failure rate information to support the development of event trees will be collected and analyzed. Justification for appropriateness of failure rates for use at YMP will be included. An uncertainty analysis of the failure rates that is appropriate to support categorization of event sequences will be included.

14.1.3 Consequence Analysis

Potential consequences from Category 1 and 2 event sequences will be evaluated to demonstrate any radiological releases meet regulatory requirements. Consequence analyses will be available to support the SSC classification. Mean consequences, including the associated uncertainty distribution, will be calculated using the GENII-S computer code (Leigh et al. 1993) or other methods. Any features and controls that are required to limit radiological consequences to within regulatory limits will be identified. The potential radiological consequences of the selected BC2 event sequences will be determined. The basis will be provided for BC2 event sequences that are selected for evaluation. BC2 event sequences will be selected for evaluation to gain risk insights into the design and support identification of defense in depth features. Commercial spent nuclear fuel release fractions analysis will be available. Preclosure safety requirements for atmospheric dispersion factors will be developed. Atmospheric dispersion factors based on site meteorological data through 2001 will be developed. Site data collection will continue to support updates to the dispersion factor calculation. Dispersion factor calculation will be used to support calculations of mean and upper bound consequences from event sequences.

14.1.4 Preclosure Safety Analysis

The PSA will be consistent with 10 CFR Part 63 requirements, the Yucca Mountain Review Plan (when issued by the NRC), and other NRC guidance and interactions. The PSA will demonstrate

compliance with PSA regulatory requirements; summarize hazards analyses, event categorization, consequence analyses, worker dose, ALARA (i.e., as low as is reasonably achievable), radiation protection program, preclosure criticality, and classification processes and results.

Preclosure Safety Analysis Guide—The PSA guide will present the project approach to developing a PSA. The guide will identify PSA project interfaces and responsibilities. It will describe processes for performing hazards analyses and for developing event trees, fault trees, and event scenarios. Guidance on performing uncertainty analyses, Category 1 and 2 consequence analysis approaches, and developing classification analyses will be included. Also, discussions on the integration of PSA work performed in other project areas should be included (e.g., design requirements and criticality). Examples of products to be used in preparation of the PSA include:

- Internal hazards analysis
- External hazards analysis
- Aircraft hazards analysis
- Wind, tornado, and tornado missile analysis
- Industrial and military hazards analysis
- Rainstorm and flooding analysis
- Seismic analysis
- Fire sequence analysis
- Loss of power analysis
- Failure rate and reliability data analysis
- Categorization of event sequences analysis
- Consequence analysis
- BC2 evaluation plan
- Atmospheric dispersion factors calculation
- 10 CFR 63.2 design bases report
- Classification analysis updates (consistent with design needs) and *Q-List* updates

These products will support the final major PSA input into the license application design.

14.1.5 Identify Structures, Systems, and Components to Prevent or Mitigate Event

10 CFR 63.2 design bases, classification analyses, and *Q-List* (YMP 2001) will be maintained consistent with the latest regulatory requirements, Yucca Mountain Review Plan (when issued by NRC), safety analyses, and design concepts. SSCs will be identified and maintained for the *Q-List* and the selection and implementation of quality assurance requirements consistent the risks identified in the preclosure safety analyses. 10 CFR 63.2 design bases report and *Q-List* will be maintained by integrating with the design organizations and updating the products, as appropriate, to ensure consistency between the products and the design.

The classification analyses determine the quality level classification of SSCs based on their role in meeting radiological safety requirements. The *Q-List* is a tabulation of the repository SSCs and their respective quality level classification.

14.2 PRECLOSURE SAFETY ANALYSIS AND LICENSE APPLICATION SUBMITTAL

The license application submittal will be prepared in accordance with "Management Plan for Development of the Yucca Mountain License Application" (in preparation).

[Information for this section is under development and will be provided later.]

14.3 REFERENCES

14.3.1 Documents Cited

Leigh, C.D.; Thompson, B.M.; Campbell, J.E.; Longsine, D.E.; Kennedy, R.A.; and Napier, B.A. 1993. *User's Guide for GENII-S: A Code for Statistical and Deterministic Simulations of Radiation Doses to Humans from Radionuclides in the Environment*. SAND91-0561. Albuquerque, New Mexico: Sandia National Laboratories. ACC: MOL.20010721.0031.

NRC (U.S. Nuclear Regulatory Commission) 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

YMP (Yucca Mountain Site Characterization Project) 2001. *Q-List*. YMP/90-55Q, Rev. 7. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.20010409.0366.

14.3.2 Codes, Standards, Regulations, and Procedures

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada.

Regulatory Guide 1.76, Rev. 0. 1974. *Design Basis Tornado for Nuclear Power Plants*. Washington, D.C.: U.S. Atomic Energy Commission. TIC: 2717.

GLOSSARY

INTENTIONALLY LEFT BLANK

GLOSSARY

Term	Definition	Reference
Acceptance Limit	A value that accounts for uncertainty about the conditions to which structures, systems, and components will be subjected and accounts for variability in the properties of component materials. This value provides a margin for unacceptable conditions. Whether the value is a maximum or a minimum depends on the type of variable being discussed.	
Analysis	A documented study, mathematical process, or evaluation defining, investigating, validating, solving, or reviewing: an engineering problem using formula or computer code for the resulting engineering parameters; the development of design inputs; translation of design input into design output; or performance of engineered structures, systems, and components.	AP-3.12 Q
Assumption	A statement or proposition that is taken to be true or representative in the absence of direct confirming data or evidence.	AP-SIII.9Q
Breach	An opening in a transportation cask, spent nuclear fuel canister, disposal container, waste package, or drip shield caused by corrosion or mechanical stress.	
Calculation	A documented study, mathematical process, or evaluation defining, investigating, validating, solving, or reviewing: an engineering problem using formula or computer code for the resulting engineering parameters; the development of design inputs; translation of design input into design output; or performance of engineered structures, systems, and components.	AP-3.12Q
Calculated Value	Values used as input assumptions for safety analyses or evaluations, or which result from the performance of a safety analysis or evaluation, and which the U.S. Nuclear Regulatory Commission has accepted during its review of a license application.	
Certification	The act of determining, verifying, and attesting in writing to the achievement or compliance with specified requirements.	DOE 2000
Codes and Standards	Applicable industry codes and standards are those codes and standards applicable to the design of the structures, systems, and components	
Computation	A mathematical process of solving a problem by formula or computer code for the resulting engineering or scientific parameters. See the definition of Calculation.	
Confinement	To keep within limits; restrict.	
Committed Effective Dose Equivalent	The sum of products of the weighting factors applicable to each of the body organs or tissues that are irradiated and the committed dose equivalent to those organs or tissues. The committed dose equivalent means the dose equivalent to organs or tissues of reference that will be received from an intake of radioactive material by an individual during the 50-year period following the intake.	10 CFR 20
Conventional Quality	Conventional quality items (i.e., not QL-1, QL-2, or QL-3) are not subject to the requirements of the <i>Quality Assurance Requirements Description</i> (DOE 2000). Program management controls are applied commensurate with regulatory requirements, industry standards, local codes, and good engineering practices.	

Term	Definition	Reference
Conservative	In developing and applying mathematical models of physical systems, choices can be made regarding assumptions, approximations, data values, and data distributions. If these choices are made so that the resulting models and the estimates produced by them tend to make the estimated performance of a safety system worse than might actually be expected, the choices made are considered conservative or pessimistic. If the development and application of the model are such that the estimated performance tends to be better than might actually be expected the choices made are considered optimistic.	Eisenberg et al. 1999
Consequence	Result or effect.	
Containment	The confinement of radioactive waste within a designated boundary.	10 CFR 63.2
Credible Event	An event or event sequence having a probability of occurrence of at least 1 in 10,000 prior to the final closure of the repository.	
Criticality	The condition in which nuclear fuel sustains a chain reaction. It occurs when the effective neutron multiplication factor (the number of fissions in one generation divided by the number of fissions in the preceding generation) of a system equals one.	
Data	As it pertains to Supplement III, information developed as a result of scientific investigation activities associated with site characterization of the Yucca Mountain repository or the results of reducing, manipulating, or interpreting data after its field or laboratory acquisition to prepare it for use in analyses, models, or calculations used in performance assessment, integrated safety analyses, the design process, performance confirmation, or other similar work using data as an input.	Document Action Request D813 to the <i>Quality Assurance Requirements and Description</i> document (DOE 2000)
Defense-In-Depth	(1) A design strategy based on a system of multiple, independent, and redundant barriers, designed to ensure that failure in any one barrier does not result in failure of the entire system. (2) A term used to describe a system of multiple barriers that mitigate uncertainties in conditions, processes, and events.	DOE 2001
	An element of the U.S. Nuclear Regulatory Commission 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.	NRC 1998
Design Agency	The design agency is the organization that performs design activities particularly those associated with design analysis and calculations. The design agency performs design activities at the direction of and under the responsibility of the design authority.	
Design Authority	The design authority is the organization responsible for establishing the design requirements and ensuring that design output documents accurately reflect the design requirements. The design authority is responsible for the design control and ultimate technical adequacy of the design processes.	

Term	Definition	Reference
Design Bases	Design bases are statements that refer to design requirements for structures, systems, and components and identify why the requirement exists, why it is specified in a particular manner, and why a specified value is used. The design bases provide information that identifies the specific functions performed by the structures, systems, and components of a facility and the specified range of values chosen for controlling the parameters that are the referenced boundaries for the design of the structures, systems, and components.	
10 CFR 63.2 Design Bases	<p>That information that identifies the specific functions to be performed by a structure, system, or component of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be constraints derived from generally accepted state-of-the-art practices for achieving functional goals or requirements derived from analysis (based on calculation or experiments) of the effects of a postulated event under which a SSC must meet its functional goals. The values for controlling parameters for external events include:</p> <ol style="list-style-type: none"> (1) Estimates of severe natural events to be used for deriving design bases that will be based on consideration of historical data on the associated parameters, physical data, or analysis of upper limits of the physical processes involved (2) Estimates of severe external human-induced events, to be used for deriving design bases that will be based on analysis of human activity in the region, taking into account the site characteristics and the risks associated with the event. 	10 CFR 63.2
Design Criteria	Design criteria consist of the standards, codes, laws, regulations, general discipline design criteria, event sequences, and hazards that shall be used as a basis for acceptance of design for structures, systems, and components to satisfy requirements.	10 CFR 63.112(f)
Design Input	Design inputs shall be defined as the design requirements, supporting design bases, applied design criteria, and any other design parameters, conditions, boundaries, limits, or values used to develop and complete design configuration(s) and design output documents.	DOE 2000, ASME NOG-1-1995
Design Output	Design outputs shall be defined as the drawings, specifications, and other design documents prepared to present the design configuration(s) of structures, systems and components that satisfy design inputs.	DOE 2000, ASME NOG-1-1995
Design Requirement	<p>Detail design requirements are engineering technical requirements (determined by design processes) that define, for example, the functions, capabilities, capacities, physical size, configurations, dimensions, performance parameters, limits, and setpoints, that are developed and specified by the design authority for structures, systems, and components to satisfy the mission design input requirements. The detail design requirements are the result (often iterative) of design processes.</p> <p>(Example: Lateral load resisting systems elements for surface structure will be designed to withstand 100 mph wind loads.)</p>	

Term	Definition	Reference
Design Verification	Documented, traceable measures (e.g., design review, alternate calculation, and qualification testing) applied to a design package or technical output by qualified individuals or groups other than those who performed the original design work. These measures verify the technical validity, adequacy, and completeness of a design package or technical output in context with the total design, natural or engineered barrier system, or integrated technical work.	AP-3.20Q
Disposal	The emplacement of radioactive waste in a geologic repository with the intent of leaving it there permanently.	10 CFR 63.2
	The emplacement of radioactive material into the Yucca Mountain disposal system with the intent of isolating it for as long as reasonably possible and with no intent of recovering the material. Disposal of radioactive material in the Yucca Mountain disposal system begins when the ramps and other opening into the Yucca Mountain repository are sealed.	10 CFR 63.302
Documentary Material	<ol style="list-style-type: none"> (1) Any information that a party, potential party, or interested governmental participant intends to use or to cite in support of their position in the proceeding for a license to receive and possess high-level radioactive waste at a geologic repository operations area pursuant to 10 CFR Part 60 or 10 CFR Part 63. (2) Any information that is known to, in the possession of, or developed by the party that is relevant to, but does not support, that information or that party's position. (3) Reports and studies, prepared by or on behalf of the potential party, interested governmental participant, or party, including related circulated drafts, relevant to the license application and the issues set forth in Regulatory Guide 3.69, Topical Guidelines, regardless of whether they will be relied upon or cited by a party. The scope of documentary material will be guided by the topical guidelines in the applicable U.S. Nuclear Regulatory Commission Regulatory Guides. 	10 CFR 2.1001
Electrical One-Line Diagrams	Electrical One Line Diagrams are diagrams of single lines showing the electrical power sources, distribution busses, major loads, and associated circuit breakers. Electrical one-line diagrams may be generated based on the general system description and the design information required to perform the safety analyses, such that no additional supporting information will be required.	
Evaluation	<ol style="list-style-type: none"> (1) To examine and judge carefully. (2) To form an opinion about. (3) To determine the significance, worth, or condition, usually by careful appraisal and study. 	
Event Sequence	A series of actions or occurrences within the natural and engineered components of a geologic repository operations area that could potentially lead to radiation exposure. An event sequence includes one or more initiating events and associated combinations of repository system component failures, including those produced by the action or inaction of operating personnel. Those event sequences that are expected to occur one or more times before permanent closure of repository are referred to as Category 1 event sequences. Event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences.	10 CFR 63.2

Term	Definition	Reference
General Arrangement Drawings	General arrangement drawings provide an overall view of a structure, component, or area showing the arrangement of major structural features and major equipment. Only overall dimensions are included. General arrangement drawings may be generated based on the general system description and the design information required to perform the safety analyses such that no additional supporting information will be required.	
General System Description	A general system description provides a summary of the system functions, operations, the system design, concept of operations, and a description of system interfaces, such as in Section 1 of the System Description Documents. This description should include a discussion on any special construction or fabrication techniques, unique testing programs or special design and analysis procedures used for the structures, systems, and components, as applicable.	
Geologic Repository Operations Area	A high-level radioactive waste facility that is part of a geologic repository, including surface and subsurface areas, where waste handling activities are conducted.	10 CFR 63.2
Handling Diagrams	Handling diagrams depict major handling paths and sequence of operations at a summary level (e.g., fuel movement in the Waste Handling Building). Handling diagrams may be generated based on the general system description and the design information required to perform the safety analyses, such that no additional supporting information will be required.	
Important to Safety	<p>With reference to structures, systems, and components, engineered features of the geologic repository operations area, that:</p> <p>(1) Provide reasonable assurance that high-level radioactive waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of 10 CFR 63.111(b)(1) for Category 1 event sequences</p> <p>(2) Prevent or mitigate Category 2 event sequences that could result in doses exceeding the values specified 10 CFR 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site.</p>	10 CFR 63.2
Initiating Event	A natural or human induced event that causes an event sequence.	10 CFR 63.2
Licensing Basis	The currently effective requirements imposed on the facility including the requirements at the time the initial license was applied for and granted, together with requirements subsequently imposed. The licensing bases are contained in U.S. Nuclear Regulatory Commission regulations, orders, license conditions, exemptions, and licensee commitments contained in the safety analysis report and other docketed licensee correspondence.	
Margin	Margin is the difference between the calculated event sequence dose and the prescribed regulatory compliance limit, which provides confidence that the repository design features can adequately protect public health and safety and the environment from any uncontrolled radiological event.	
Model	A representation of a system, process, or phenomenon, along with any hypotheses required to describe the process or system or to explain the phenomenon, often mathematically.	DOE 2000
	Model development typically progresses from conceptual to mathematical models. Mathematical model development typically progresses from process, to abstraction, and to system models.	AP-SIII.10Q
Negligible	So small, unimportant, or of so little consequence as to warrant little or no attention.	

Term	Definition	Reference
Piping and Instrumentation Diagrams (Process and Instrumentation Diagrams)	Piping and instrumentation diagrams are diagrams showing only major flow paths, equipment, and instrumentation (e.g., pumps, tanks, ion exchangers, major valves, and instrumentation used for operation). Interfaces with other systems and seismic and quality interfaces shall be included on the piping and instrumentation diagrams. These piping and instrumentation diagrams may be generated based on the general system description and the design information required to perform the safety analyses, such that no additional supporting information will be required.	
Permanent Closure	The final backfilling of the underground facility, if appropriate, and the sealing of shafts, ramps, and boreholes.	10 CFR 63.2
Postclosure	Refers to the period of time after permanent closure of the repository system.	
Preclosure	Refers to the period of time before and during permanent closure of the repository system.	
Preclosure Safety Analysis	A systematic examination of the site; the design; and the potential hazards, initiating events, and event sequences; and their consequences (e.g., radiological exposures to workers and the public). The analysis identifies structures, systems, and components important to safety.	10 CFR 63.2
Qualification (Personnel)	The capabilities gained through education, training, or experience that qualify an individual to perform a required function.	DOE 2000
Quality Level 1	[Later]	
Quality Level 2	[Later]	
Quality Level 3	[Later]	
Reasonable Assurance	The test of compliance with the standards and criteria. This concept recognizes that absolute assurance of compliance is neither possible nor required.	Eisenberg et al. 1999
Regulatory Commitment	An explicit statement made to ensure compliance, agreed to or volunteered by the U.S. Department of Energy, to take a specific action. Regulatory commitments are made in written correspondence with the U.S. Nuclear Regulatory Commission or the U.S. Environmental Protection Agency.	AP-REG-005, Sections 3.1 and 3.10
Regulatory Limit	Limit specified by U.S. Nuclear Regulatory Commission regulations or other regulatory requirements document (e.g., SRP, Regulatory Guides, and NUREGs). Whether the value is a maximum or a minimum depends on the type of variable being discussed.	
Regulatory Margin	Regulatory margin is the difference between the event sequence dose and the prescribed regulatory compliance limit.	
Retrieval	The act of permanently removing radioactive waste from the underground location at which the waste had been previously emplaced for disposal.	10 CFR 63.2
Risk	(1) The probability that an undesirable event will occur, multiplied by the consequences of the undesirable event. (2) Expected (mean) value of the consequences of an undesirable process or event.	DOE 2001
Risk Informed	An approach to regulatory decision-making whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operation issues commensurate with their importance to public health and safety.	NRC 1998
Risk Insights	The results and findings that come from risk assessments.	NRC 1998

Term	Definition	Reference
Safety Case	The logic, analyses, and calculations that show that the repository system would meet performance objectives.	CRWMS M&O 2001
Significant	More than a minimal increase in the consequences of an accident (e.g., the margin to the regulatory limit is eroded by more than ten percent).	NEI 2000
Technical Information	Information available from drawings, specifications, calculations, analyses, reactor operational records, fabrication records, construction records, other design basis documents, regulatory or program requirements documents, or consensus codes and standards that describe physical, performance, operational, or nuclear characteristics or requirements.	Document Action Request D813 to the <i>Quality Assurance Requirements and Description</i> document (DOE 2000)
Total Effective Dose Equivalent	For purposes of assessing doses to workers, the sum of the deep-dose equivalent (for external exposures) and the committed effective dose equivalent (for internal exposures). For purposes of assessing doses to members of the public (including the reasonably maximally exposed individual), total effective dose equivalent means the sum of the effective dose equivalent (for external exposures) and the committed effective dose equivalent (for internal exposures).	10 CFR 63.2
Traceability	The ability to trace the history, application, or location of an item, data, or sample using recorded documentation. Traceability exists when there is an unbroken chain linking the result of an assessment (e.g., final dose calculation) with models, assumptions, expert opinions, and data used in the formulation of the result.	DOE 2000
Transparent	A document (e.g., a calculation, analysis, or model) is transparent if it is sufficiently detailed as to purpose, method, assumptions, inputs, conclusions, references, and units such that a person technically qualified in the subject can understand the document and ensure its adequacy without recourse to the originator.	DOE 2000, Section 3.2.2
Uncertainty	The interval above and below the measurement, parameter, or result that contains the true value at a given confidence level.	AP-SIII.9Q
	There are two types of uncertainty: 1) Stochastic (or aleatory) uncertainty is caused by the random variability in a process or phenomenon 2) State-of-knowledge (or epistemic) uncertainty results from a lack of complete information about physical phenomena. State-of-knowledge uncertainty is further divided into: i) Parameter uncertainty, which results from imperfect knowledge about the inputs to analytical models ii) Model uncertainty, which is caused by imperfect models of physical systems, resulting from simplifying assumptions or an incomplete identification of the system modeled iii) Completeness uncertainty, which refers to the uncertainty as to whether the important physical phenomena, relationships (coupling), and events have been considered.	Eisenberg et al. 1999
Unrestricted Area	Areas where access is neither limited nor controlled by the licensee.	10 CFR 63.2

Term	Definition	Reference
Validation	A process used to establish confidence that a conceptual model (as represented in a mathematical model, software, or analysis) adequately represents the phenomenon, process, or system in question.	DOE 2000
	A process carried out by comparison of model predictions with field observations and experimental measurements. A model is considered validated when sufficient testing has been performed to ensure an acceptable level of predictive accuracy over the range of conditions over which the model may be applied.	Eisenberg et al. 1999
Verification	The act of reviewing, inspecting, testing, checking, auditing, or otherwise determining and documenting whether items, processes, services, or documents conform to specified requirements.	DOE 2000
	A process of assuring that the implementation of a mathematical model (in the form of a computer code) is free of coding errors, and that the numerical schemes used are within the bounds of required accuracy. The process consists of following established Quality Assurance procedures during the development of the code, comparison of the code with analytic solutions, and comparison with results from other codes.	Eisenberg et al. 1999
Waste Form	The radioactive waste materials and any encapsulating or stabilizing matrix.	10 CFR 63.2

GLOSSARY REFERENCES

GLOSSARY DOCUMENTS CITED

ASME (American Society of Mechanical Engineers) NOG-1-1995. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 238309.

CRWMS M&O 2001. *Repository Safety Strategy: Plan to Prepare the Safety Case to Support Yucca Mountain Site Recommendation and Licensing Considerations*. TDR-WIS-RL-000001 REV 04 ICN 01. Two volumes. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20010329.0825.

DOE (U.S. Department of Energy) 2000. *Quality Assurance Requirements and Description*. DOE/RW-0333P, Rev. 10. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20000427.0422.

DOE 2001. *Yucca Mountain Science and Engineering Report*. DOE/RW-0539. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20010524.0272.

Eisenberg, N.A.; Lee, M.P.; Federline, M.V.; Wingefors, S.; Andersson, J.; Norrby, S.; Sagar, B.; and Wittmeyer, G.W. 1999. *Regulatory Perspectives on Model Validation in High-Level Radioactive Waste Management Programs: A Joint NRC/SKI White Paper*. NUREG-1636. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246310.

NEI (Nuclear Energy Institute) 2000. *Guidelines for 10 CFR 50.59 Implementation*. NEI 96-07, Rev. 1. Final Pre-publication Draft. Washington, D.C.: Nuclear Energy Institute. TIC: 249183.

NRC 1998. "White Paper on Risk-Informed and Performance-Based Regulation." Correspondence from L.J. Callan (NRC) to the Commissioners, June 22, 1998, with attachment. SECY-98-144. Washington, D.C.: U.S. Nuclear Regulatory Commission. Accessed August 24, 1998. TIC: 240107. <http://www.nrc.gov/NRC/COMMISSION/SECYS/1998-144scy.html>.

GLOSSARY CODES, STANDARDS, REGULATIONS, AND PROCEDURES

10 CFR 2. 1998. Energy: Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders. Readily available.

10 CFR 20. Energy: Standards for Protection Against Radiation. Readily available

10 CFR 63. 2002. Energy: Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada. Readily available.

AP-3.12Q, Rev. 1. *Design Calculations and Analyses*. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20020102.0198.

AP-3.20Q, Rev. 0, ICN 1. *Technical/Design Verification*. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20010403.0149.

AP-REG-005, Rev. 0, ICN 0. *Managing External Recommendations and Commitments*. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20010514.0165.

AP-SIII.9Q, Rev. 0, ICN 0. *Scientific Analyses*. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20020102.0199.

AP-SIII.10Q, Rev. 0, ICN 0. *Models*. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20020102.0197.

INTENTIONALLY LEFT BLANK