SUMMARY OF PRECLOSURE SAFETY ANALYSIS RELIABILITY ASSESSMENT METHODOLOGY

AUGUST 2006

Table of Contents

Table of Contents (Cont'd)

List of Figures

List of Tables

List of Acronyms

Acronyms

AIChE	American Institute of Chemical Engineers
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event Analysis
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety
CES	Categorization of Event Sequences
CFR	Code of Federal Regulations
COV	Coefficient of Variation
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
EF	Error Factor
EOPs	Emergency Operating Procedures
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HEP	Human Error Probability
HEPA	High Efficiency Particulate Air or High Efficiency Particulate Arrestor
HFE	Human Failure Event
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
ITS	Important to Safety
LA	License Application
LERs	License Event Reports
MOVs	Motor Operated Valves
NRC	U.S. Nuclear Regulatory Commission
OREDA	Offshore Reliability Data
PCSA	Preclosure Safety Analysis
PDF	Probability Density Function
PFDs	Process Flow Diagrams
P&IDs	Piping & Instrumentation Diagrams
PRA	Probabilistic Risk Assessment
PSCs	Procedural Safety Controls
PSFs	Performance Shaping Factors (used in HRA)
SAPHIRE	System Analysis for Hand-on Integrated Reliability Evaluation software
SHARP1	Systematic Human Action Reliability Procedure 1
SOPs	Standard Operating Procedures
SPAR-H	Standardized Plant Analysis Risk - Human Reliability Analysis
SRS	Savannah River Site
SSCs	Systems, Structures and Components

List of Acronyms (Cont'd)

Acronyms

THERP	Technique for Human Error Rate Prediction
VFDs	Ventilation Flow Diagrams
V&IDs	Ventilation & Instrumentation Diagrams
YMP	Yucca Mountain Project
YMRP	Yucca Mountain Review Plan

EXECUTIVE SUMMARY

This report was prepared to provide a summary of the methodology that is used to conduct reliability assessments and data management to support the Yucca Mountain repository Preclosure Safety Analysis (PCSA) event sequence quantification and categorization.

The reliability assessment methodology supports the following activities:

- Estimation of the frequency of occurrence for initiating events identified in the event-sequence categorization
- Estimation of the probability of human-failure events if identified in the event-sequence categorization
- Estimation of the reliability of important to safety (ITS) Structures, Systems, and Components (SSCs) and Procedural Safety Controls (PSCs) that are credited to prevent or mitigate the consequence of event sequences

The reliability assessment methodology follows a graded approach wherein the assessment starts with the most straightforward way to obtain reliability values (i.e., accepted engineering practices, expert judgment, codes and standards); makes use of empirical data; and, where empirical data is unavailable, reliability modeling (fault-tree analysis, human-reliability analysis, etc.) are performed to provide technical justification of the reliability estimate.

The reliability estimates are obtained at the highest level (i.e., systems) if appropriate analogs are available, and, where these analogs are not available, the reliability estimates are based on the aggregate of subsystem- and component-level reliability information.

The report provides a brief overview of the event-sequence generation and categorization, and the linkage between the event sequences and the reliability assessments that support the event-sequence categorization. It provides a description of the methodologies that are used to conduct fault-tree analysis; uncertainty and sensitivity analysis; human reliability analysis; and to evaluate the reliability of passive SSCs and PSCs that are credited in event-sequence categorization. The methodologies and technical bases are presented in the report with illustrative examples.

Summary of Preclosure Safety Analysis Reliability Assessment Methodology

1. INTRODUCTION

1.1 BACKGROUND

A Preclosure Safety Analysis (PCSA) is a required element of the License Application (LA) for the high-level radioactive waste repository. As described in 10 CFR Part 63, the PCSA requirements were developed as part of a risk-informed, performance-based regulatory framework. Specifically, in 10 CFR 63.111(c), the U.S. Nuclear Regulatory (NRC) specifies that a PCSA of the geologic repository operations area that meets the requirements of 10 CFR 63.112 must be performed, and it must demonstrate compliance with the performance objectives delineated in 10 CFR 63.111(a) and 10 CFR 63.111(b).

The PCSA, through its hazard analysis, identifies the potential Yucca Mountain repository hazards due to natural phenomena and operational activities for the period before permanent closure. Where possible, potential hazards from natural phenomena and external events are screened out based on the absence of a credible presence at the site (e.g., tsunami) or through probabilistic analysis (e.g., demonstrating the low probability of an aircraft crash on the site.) Otherwise, potential hazards are treated as potential initiating events for event sequences that could result in exposure to, or release of, radioactive materials.

Through event tree analysis and/or event sequence (or scenario) descriptions, the PCSA identifies and evaluates potential events and event sequences for each initiating event. Each event sequence is categorized by probability of occurrence during the preclosure operating period in accordance with the definitions of Category 1 and Category 2 event sequences in 10 CFR 63.2. The consequences (radiological dose) to workers and to the public are evaluated for each Category 1 and Category 2 event sequence for purposes of demonstrating compliance with the performance objectives of 10 CFR 63.111.

From these analyses, the PCSA provides a basis for identifying important to safety (ITS) structures, systems, and components (SSCs) and procedural safety controls (PSCs) that are used to prevent or mitigate potential accidents or event sequences. Within this framework for the PCSA , the conduct of reliability assessments is used to support the following:

- Establishing the likelihood of initiating events identified in the hazard analysis and providing the basis for event sequence development and categorization (quantified as a frequency or probability, see Section 2.3).
- Establishing the reliability values for credited safety functions of ITS SSCs identified in the event sequences to verify that the sequences are categorized properly as Category 1, Category 2 or Beyond Category 2 (BC2).
- Establishing the reliability values for PSCs (credited for preventing or mitigating event sequences).

Although 10 CFR 63 does not provide explicit guidance for consideration of uncertainties in the analysis of event sequence probabilities for purposes of categorization, the Yucca Mountain Review Plan (YMRP) (NRC, 2003) requires a discussion of uncertainty as specified in Sections 2.1.1, 2.1.1.3.2, 2.1.1.3.3, 2.1.1.5.1.2, 2.1.1.5.1.3, 2.1.1.6.2, and 2.1.1.6.3.

Therefore, as part of the demonstration of compliance with 10 CFR 63.111(a), (b), and (c), the PCSA will provide reliability analysis and technical justifications for the probability values of ITS SSCs and PSCs that are credited in the event sequence categorization.

1.2 PURPOSE

This document was prepared to provide a summary of the methodology that is used for performing reliability analysis and data management to support event sequence quantification, categorization, and screening for the PCSA in support of the License Application.

1.3 SCOPE

The scope of the reliability assessment covers all ITS SSCs and PSCs that are credited in the PCSA for prevention or mitigation of event sequences during the repository preclosure period and also covers the establishment of the frequency (or probability) of the initiating events.

1.4 DEFINITIONS

hazard: An underlying condition that might manifest into an undesired end state (or damage state) by means of an accident scenario. Occurrence of a hazard is not synonymous with damage to SSCs or an undesired end state.

external hazard or *external event*: An event, such as earthquake, windstorm, flood, or aircraft crash, which is not derived from failure of components owing to normal or abnormal operation.

accident scenario: A set of sequential and/or coincident events that begins with an initiating event and ends in a damage state to SSCs. An accident scenario describes one manifestation of an underlying hazard.

initiating event: A perturbation from normal operation that alone or in concert with pivotal events causes a damage state to SSCs.

pivotal event: A set of events that follows an initiating event and characterizes potential facility responses to the initiating event. Pivotal events may be aggravative or mitigative.

event sequence: According to 10 CFR 63.2, the term "event sequence" can be defined as a series of actions and/or occurrences within the repository that could lead to potential exposure of individuals to radiation. An event sequence can include one or more initiating events and associated combinations of system component failures, including those produced by the action or inaction of operating personnel.

Category 1 event sequences: According to 10 CFR 63.2, event sequences that are expected to occur one or more times before permanent closure of the repository are referred to as Category 1 event sequences.

Category 2 event sequences: As stated in 10 CFR 63.2, event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences.

Beyond Category 2 (BC2) event sequence: BC2 event sequences are those that have less than one chance in 10,000 of occurring before permanent closure.

important to safety (ITS): According to 10 CFR 63.2, ITS SSCs are defined as those engineered features of the 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 10 CFR 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 10 CFR 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site.

passive components are those that function in a static manner within a system. Such components may act as a means to transfer energy, or matter from place to place such as a wire carrying a current, a pipe carrying a liquid, or a steam line transferring heat energy. They could also be used to transmit loads such as a structural member.

active components are those that contribute in a dynamic sense to the system function. For example, a valve, which opens or closes allows liquid to move or stop within the system, or a pump, which provides motive force for the transfer of liquid from place to place. At YMP, certain active components could also be a passive component depending on the functions they provide. For example, a cask transporter is an active component when it is used as a means to move a cask from point A to point B; it becomes a passive component when it is used as a barrier for protecting the cask during a rockfall event.

2. PRECLOSURE EVENT SEQUENCE ANALYSIS

2.1 OVERVIEW

The PCSA process includes a suite of analyses that pertain to the identification and screening of hazards, development and quantification of event sequences, categorization of event sequences (CES), and radiological dose consequence analyses. The process applies methods commonly used in the probabilistic risk assessment (PRA) community NASA and Nuclear Power Plant licensee 's. The PCSA process can be summarized as follows:

- An external events hazards analysis is performed to identify and screen potential hazards. In some cases, the hazard analyses provide input to the development of initiating and pivotal events as part of an event sequence analysis. In other cases, the hazards are deterministically analyzed to show adverse effects on the repository are physically unrealizable. Identified external hazards are subjected to a multi-level process to screen out as many hazards as possible using both qualitative and quantitative evaluations of site-specific characteristics. The screening criterion is presented in Section 2.3.2. For example, a detailed probabilistic analysis is used to screen out aircraft crashes as a potential initiating event. Design features and/or potential PSCs that prevent or reduce the likelihood of an initiating event are specified for external events that cannot be screened out. For example, design features are specified for the following external events: loss of offsite power, severe windstorms, tornadoes, flooding, and earthquakes. An event sequence can be initiated only if the SSC credited with prevention fails in conjunction with the occurrence of an external event.
- An internal events hazard analysis provides input to the development of initiating and pivotal events as part of the event sequence analysis. It does so by identifying in each operational area, credible events that could potentially initiate an accident sequence. The types of internal hazards analyzed in the PCSA include: chemical contamination, collision/crushing, electrical, explosion, fire, fissile, flooding, implosion, magnetic, radiation, thermal.
- The event sequence analysis identifies in detail events that must occur to result in a radiological release or exposure or criticality, and evaluates their credibility and potential consequences. The event sequence analysis may incorporate analyses and design strategies from safety-specific disciplines (e.g., criticality and fire-protection) and across disciplines (e.g., criticality, fire, and radiological exposure). Event sequence analysis also incorporates random failures of equipment and external event driven failures of structures, passive equipment, and active equipment.
- The screening of initiating events and quantification of the probabilities of event sequences require a variety of techniques of reliability assessment that are the primary subject of this document.

2.2 SEQUENCE IDENTIFICATION – EVENT TREE AND FAULT TREE CONSTRUCTION

The internal hazards are classified by potential energy sources associated with each facility operation 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) are displayed in the form of event trees that include an initiating event (from an identified hazard) and one or more pivotal events (associated combinations of repository system component failures from random sources, from hazards, and from those produced by the action or inaction of operating personnel) that must occur to result in a release of radioactivity, a criticality, or offsite public 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 (pivotal) events.

Figure 1 shows a hypothetical event tree.

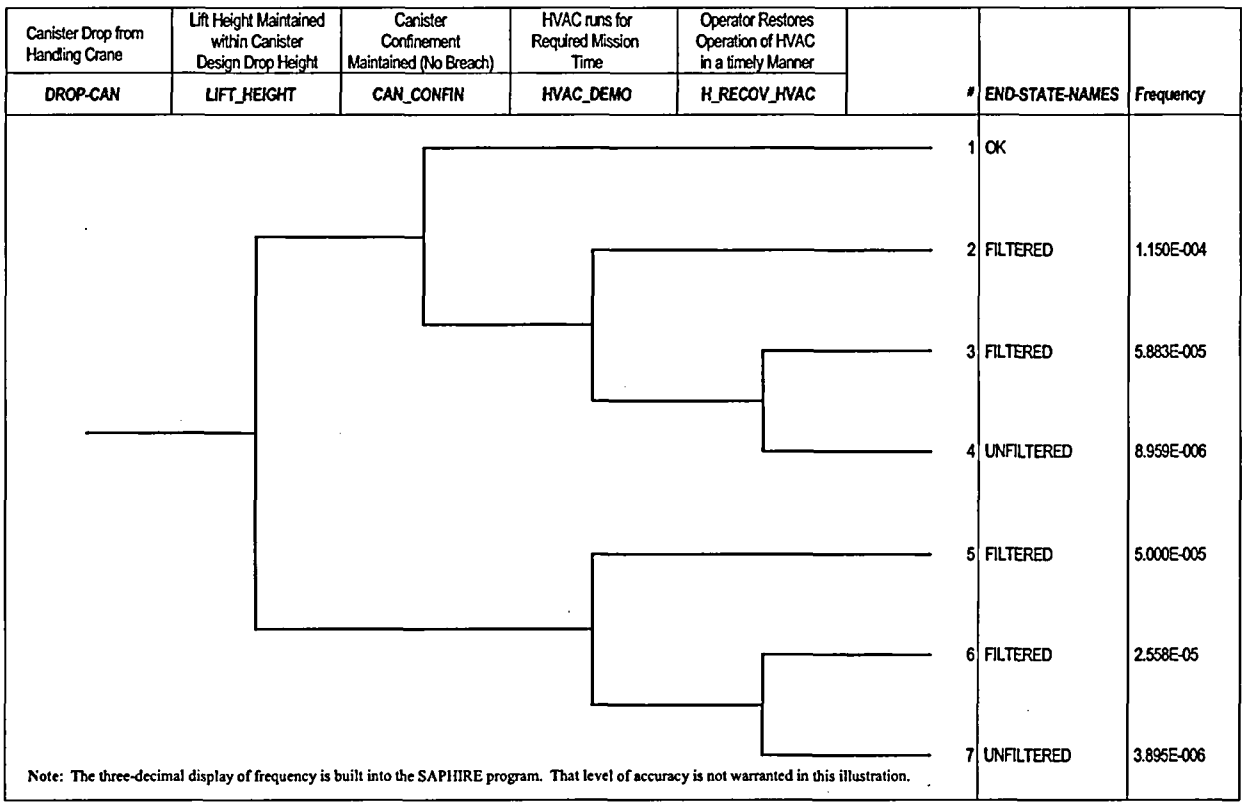

Figure 1. Hypothetical Event Tree

A reliability assessment is required for the initiating event and all of the branch points (or nodes) illustrated in the event tree, using one of the methods described in Section 3.

In some cases, the failure probability of a node may be estimated from empirical data. When the failure node represents the failure of an active system, a fault tree analysis (FTA) may be performed (see Section 3.5.1 for a definition of "fault tree"). When the failure node represents a human failure event (HFE), then a human reliability analysis (HRA) may be performed. When the failure node represents the failure of a confinement barrier of a waste form (or some other passive barrier such as a tornado missile barrier), an appropriate reliability analysis is performed.

Potential criticality event sequences are subjected to analyses, not described in detail in this document, that demonstrate that sufficient design and operational controls are in place to ensure event sequences with at least one chance in 10,000 of occurring before permanent closure result in a configuration that is subcritical. The YMRP recognizes that methodologies in accordance with NUREG-1567 and regulatory guide 3.71 are acceptable. In brief, the evaluation of the frequency of a criticality event is similar to the evaluation of other event sequences. For example, an HRA may be conducted to determine the probability that a canister or waste package is misloaded with fissile material. The difference, however, is that the end state condition of interest is not an exposure to radiation but whether or not a criticality could occur. The event sequence analysis (for events that could lead to a critical event) concludes with a criticality analysis to demonstrate that the k_{eff} value is less than 0.95 for any Category 2 event sequence.

2.3 QUANTIFICATION OF EVENT SEQUENCE FREQUENCY

In general terms, each pathway through the event tree from the initiating event to the end state represents an event sequence. In PCSA usage, per the definition in 10 CFR 63.2, the term "event sequence" means only those sequences of events "that could potentially lead to exposure of individuals to radiation."

Each event sequence is quantified in terms of probability of occurrence during the period before permanent closure (either in terms of frequency, or annual probability of occurrence). Generally, PRAs use the term frequency for quantification of event sequence likelihood; to facilitate comprehension, the same meaning is used in this document. The framework of the event tree is used to display the frequency of the initiating event and the conditional probabilities of each pivotal event in a sequence. The frequency of each event sequence is calculated as the product of the initiating event frequency and the probabilities of the pivotal events. The event tree construction and quantification of event sequences are performed with the SAPHIRE software program (Smith, 2005) (see Section 2.3.1) or other qualified software appropriate for these activities.

The frequencies of initiating events for internal hazards are estimated from the frequency of each operation multiplied by the conditional probability of the initiating event per operation.

EXAMPLE: The frequency of a canister drop is estimated as the product of the frequency of canister lifts (defined as the number of lifts per year or the number of lifts over the total period before permanent closure) and the per lift conditional probability of dropping the canister. The conditional probability of each pivotal event (usually a failure of some preventive or mitigative feature), such as "maintaining a lift height within a canister design basis drop height," is derived from applicable empirical data or from a FTA. 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 a waste form confinement barrier breaches in a drop sequence, irrespective of the drop height).

However, another objective of the event sequence analysis is to define where prevention or mitigation controls are needed to prevent the potential for an unacceptable worker or public dose. For example, to demonstrate prevention, the quantification of a given event sequence that has the potential for an unacceptable public dose requires that the probability of failure of the SSC be less than or equal to a quantified value necessary to demonstrate that the event sequence is BC 2. Therefore, one application of the event sequence analysis is to define reliability goals for the required safety functions of ITS SSCs. A reliability assessment for the safety function must be performed, using one of the methods described in this document to verify that the required reliability can be achieved.

EXAMPLE: The frequency of the initiating event in the hypothetical event tree (Figure 1) is 5E-3/yr, based on a preliminary estimated probability of 1 drop per 100,000 lifts (or 1E-5 drops/lift) and 500 lifts/year. The probability of drops/lift and the frequency of lifts must be verified to support the initial screening value assigned to the initiating event frequency. In this example, the verification effort would entail a reliability modeling of the crane (or lift) systems to determine whether the probability of 1E-5 drop/lift is achievable. Such reliability modeling could be obtained from the equipment vendor, or performed by the PCSA staff. In addition, a more detailed assessment of the operational throughput requirements and design would be performed to determine whether the lift frequency of 500 lifts/year or 50,000 lifts per 100 years is correct. For purposes of this example, the lift frequencies would need to be verified based on the operational plans developed for the repository.

The event sequence frequency quantification will include consideration of uncertainties. The uncertainty distributions in input parameters used in the fault tree basic events and event tree headings are propagated through the cut sets that are generated for the fault trees and event sequences. If all input values are represented by probability distributions, the output value is also expressed as a probability distribution and summarized by a mean value and upper and lower bound. If the input values include some bounding values (e.g., the maximum throughput rate), the output value must be appropriately interpreted as a "maximum throughput weighted" result for the frequency and uncertainty distribution of a given event sequence.

2.3.1 Event Sequence/Fault Tree Linkage

The SAPHIRE software program employs the method known as event-tree/fault-tree linking. This means the initiating event, and each pivotal event under each event heading in an event tree, can be automatically linked to a fault tree logic model. The SAPHIRE code performs all of the logical linking of pivotal events from several fault trees to establish the combinations of component and/or HFEs (e.g., event sequence cut sets) that are required to cause each event sequence to occur. The SAPHIRE code also inserts the failure probability defined for each component or HFE and the frequency of the initiating event into the event sequences to produce the frequency of a given event sequence. Uncertainties in input data are also propagated through the event sequence frequency calculation.

Reliability data that are obtained for each failure mode of an SSC that is modeled in the event tree are input into various "basic event" data entry forms in the SAPHIRE program. The data entry forms permit the analyst to select the probability model that is applied to a given failure event and to specify all of the parameters and uncertainty factors required to support the reliability model. For example, in a very basic model, a point-estimate value may be used for which a single frequency or probability value is the required input. However, the exponential model, which is commonly used in nuclear reliability estimation, requires input of two values, a mean failure rate and a mission or operation time. The analyst specifies the probability distribution that is used to characterize the uncertainties in the failure rate. For example, if the failure rate is defined to be a normal (Gaussian) distribution, then an associated uncertainty data field is opened for inserting the standard deviation. Similarly, if the failure rate is defined to be lognormal distribution, then an uncertainty data field is opened for entering the error factor (EF) (i.e., the ratio of the 95^{th} and 50^{th} percentile).

EXAMPLE: The event "HVAC_DEMO" in Figure 1 represents the top-event of a fault tree that was constructed to evaluate system failure based on a detailed analysis. Once the system failure probability is calculated, the value is then fed directly to the event tree entry that has the same name. The uncertainties in the parameters in the basic events in the fault tree are propagated through the event tree and combined with the uncertainties of other parameters appearing in the event tree or other linked fault trees. All these steps are done automatically in SAPHIRE.

When an event tree heading does not require linking to a fault tree model, the heading event is treated in SAPHIRE as a basic event and is automatically linked to a data-entry form.

2.3.2 Initiating Event and Event Sequence Screening

10 CFR 63.2 defines Category 2 event sequences as those that have a probability of occurrence of at least one chance in 10,000 during the period before permanent closure (or preclosure period). For a 100-year preclosure period, the corresponding frequency of occurrence is:

$$F = [(1/10{,}000) \text{ chance/preclosure period}] * [\text{preclosure period}/100 \text{ years}]$$

$= 1/1{,}000{,}000$ chance/year or 1×10^{-6} per year

Quantitative screening 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 period before permanent closure (or less than 1×10^{-6} per year). Initiating events or event sequences whose probabilities are less than one chance in 10,000 before permanent closure (or a frequency of less than 1×10^{-6} per year) are termed BC 2 event sequences and are screened out. No radiological consequence analysis is performed for BC 2 event sequences.

During the preliminary screening of event sequences, conservative point estimates may be used to demonstrate that certain event sequences are BC 2. In more refined analyses, the mean value of an event sequence frequency is used for screening and categorization. That is, if the estimated mean frequency of an initiating event or a full event sequence is less than 10^{-6} per year, the event sequence is categorized as BC 2 and is screened out. In other cases, it may be shown from physical arguments that a given hazard is not a credible initiating event.

EXAMPLE: A very detailed probabilistic screening analysis has been performed for aircraft crash on the repository site (BSC,2005[b]) to screen out an aircraft crash as an initiating event. On the other hand, a deterministic screening analysis has been performed for industrial and military external hazards to demonstrate that separation distance provides adequate safeguards against these hazards and, as a result, these hazards can be screened out (BSC,2005[c]).

It should also be noted that, depending on the magnitude of uncertainty associated with a given event sequence, a screening margin may be applied to ensure high confidence that the sequence is properly categorized or screened out.

External events such as earthquakes, severe windstorms and tornadoes, floods, and loss of offsite power cannot be screened out on the basis of initiating event frequency of occurrence. Screening will occur on the basis of event sequence frequency or dose.

2.4 EVENT SEQUENCE CATEGORIZATION

In this step of the analyses, the frequency of each event sequence that is not determined to be BC 2 is categorized as Category 1 or Category 2 as defined by 10 CFR 63.2. This categorization establishes which portion of the performance objectives of 10 CFR 63.111 governs the consequence analyses. Category 1 event sequences require dose aggregation; doses for Category 2 are applied on a per-event-sequence basis, as summarized in Section 2.5.

2.5 CONSEQUENCE ANALYSIS

The potential radiological consequences of releases or exposures are calculated for Category 1 and Category 2 event sequences.

Compliance to performance criterion in 10 CFR 63.111(b)(1) requires aggregation of worker, on-site public, and off-site public doses due to normal operations and Category 1 event sequences. Normal operations are defined as the potential events that are considered part of normal operations that will not lead to further degradation or failure of spent nuclear fuel (SNF) cladding. Exposure of workers to radiation will be managed as a normal operations dose by procedures for monitoring radiation doses and assigning work, which ensure worker doses will be kept as low as are reasonably achievable. This requires a frequency-weighted summation of doses over all Category 1 event sequences and normal operations.

By contrast, the radiological consequence analysis for Category 2 event sequences will be evaluated for off-site public and will be performed on a per-event-sequence basis, in accordance with 10 CFR 63.111(b)(2). There is no frequency-weighted evaluation of doses for Category 2 event sequences.

There is no requirement for performing consequence analysis for BC 2 event sequences.

Methods for consequence analyses, which may be bounding-type analyses using single-parameter values, are not described in this document.

3. RELIABILITY ASSESSMENT METHODOLOGY

3.1 INTRODUCTION

Depending on the specific SSC and the safety function being credited, a variety of techniques will be employed to assess the reliability of an ITS SSC to perform the credited safety function. Section 3 describes each method and its application within the PCSA.

For the purposes of determining the category of an event sequence the following are represented numerically in the appropriate branches of an event sequence:

- Estimate of the frequency of occurrence for the initiating event;
- Estimate of the reliability of the human operator, if involved;
- Estimate of the reliability of the ITS SSCs to perform the safety function relied upon in the event sequence to decrease the frequency of the event sequence or to mitigate the consequences of the event sequence.

The numerical reliability estimates to be included in the event sequences are developed using a graded approach (i.e., using the most straight forward methodology or combination of methodologies, as appropriate, with a sound technical basis). Where empirical data from similar SSCs in similar applications exist (e.g., data from existing nuclear plant risk assessments), they are used as such. Where empirical data are unavailable, data modeling (e.g., Bayesian analysis and HRA) and system reliability modeling (e.g., FTA) are performed to provide technical justification of the reliability estimate.

If appropriate analogs are available, the reliability estimates are obtained at the highest level (i.e., systems). Where such analogs are not available, the reliability estimates will be based on the aggregate of subsystem- and component-level reliability information.

For passive components, accepted engineering practice (i.e., application of codes and standards and a quality assurance program) is used as the basis for a reasonable estimate of reliability for passive components of specific types, unless it is impractical to do so. The need to develop different estimates to address the various types of passive components (e.g., structural, piping, vessels) will be determined. The approach to developing the estimate will also consider existing quantitative reliability estimates in nuclear plant and spent nuclear fuel storage facility risk assessments, and empirical reliability data, where available and appropriate.

For active components, data modeling (using empirical data, if available) for similar functions within a fault tree analysis is used to develop the numerical reliability estimates.

The overall probability of an event sequence must be evaluated to determine: (1) proximity to an event sequence category limit when considering uncertainties and assumptions, and (2) severity of the consequence of the event sequence.

Regardless of the approach, a technical basis for the selected methodology will be provided.

3.2 OVERVIEW OF RELIABILITY ASSESSMENT METHODOLOGY

Figure 2 illustrates the information and decision processes associated with the PCSA reliability analysis.

The reliability assessment process begins with the results from the initiating event development (as supported by the hazard analysis), subsequent scenario development and quantification and the event sequence categorization activities (i.e., identified ITS SSCs and PSCs). It ends with a documented estimate for the reliability associated with the credited safety functions of the analyzed SSCs and PSCs with uncertainties as appropriate. Generally, the first step is to determine whether empirical data exist for, and whether they are applicable to the failure mode of interest for a particular SSC. If applicable data do not exist or are not available, modeling is required to estimate the reliability values and uncertainty. It is important to determine whether human interactions are implicitly and/or adequately addressed in the empirical data. If there is no need to consider explicit human interactions, the empirical data can be documented and applied in the event sequence categorization process. If consideration of explicit human interaction is required, HRA modeling is performed to quantify the contribution by potential HFEs included in the final reliability estimate, and documented for application in the event sequence categorization.

Because PSCs are procedure related, the reliability assessment process leads directly to an HRA for the derivation of the reliability values. However, in certain cases in which the PSCs may involve manipulation of ITS equipment or instrumentation, the HRA of the PSCs will be incorporated into a system reliability model (i.e., as part of an FTA). HRA derived human errors may be included in either a fault tree or event tree in order to adequately represent the dependencies among events.

The reliability assessment process is applicable to the reliability estimation of all ITS SSCs and PSCs that are credited in the PCSA for prevention or mitigation of event sequences during the repository preclosure period and to the establishment of the frequency (or probability) of the initiating events.

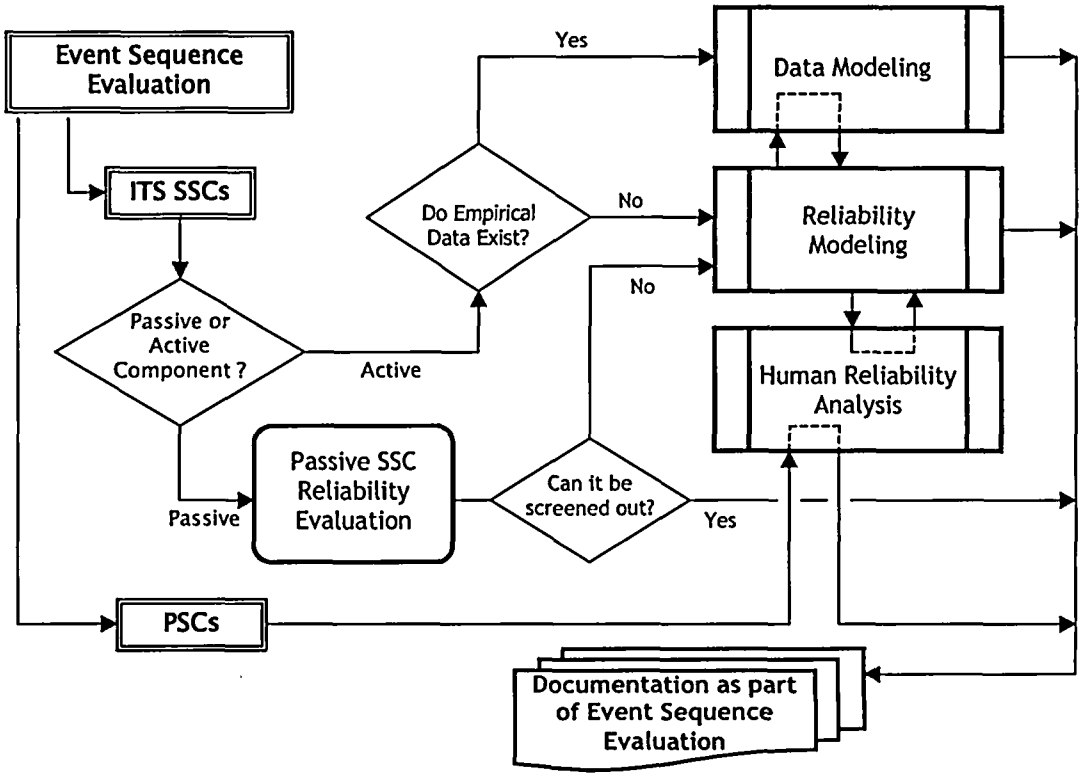

Figure 2. Flow Diagram for PCSA Reliability Assessment Process

As discussed in Section 1.3, the reliability assessment process is applied to the ITS SSCs, and PSCs identified and credited in the CES analysis (BSC, 2005[a]). [**NOTE**: the CES is regarded as a "living" document that will be updated when there is a significant change in the design or operations of the repository]. Results from the reliability assessment are fed back to the CES as verification that the reliability requirements and/or initiating event frequencies used to categorize the event sequences are achievable by the design and properly applied. If such verification is not demonstrated, the affected SSCs and/ or PSCs may be redesigned or reevaluated to meet the CES requirements and reconfirmed through the reliability assessment process; or the affected event sequences may be re-categorized.

3.3 PERTINENT TECHNICAL INFORMATION

After the purpose and scope of the analysis are established for a given SSC or PSC, pertinent technical information for the to-be-analyzed ITS SSCs and PSCs is collected. This may include but is not necessarily limited to the following:

- Safety functions credited in the CES
- Success/failure criteria

- Mission time
- P&IDs, V&IDs, and VFDs
- Instrument and control logic diagrams
- System and facility descriptions
- Electrical single-line diagrams
- Nuclear radiation and contamination zone drawings
- Mechanical handing diagrams
- The environment in which the SSCs and PSCs are required to function and remain functional during the mission time
- Normal and Emergency Operating procedures (if available; if not, surrogate procedures from licensed ISFSI are used)
- Operating parameters and conditions
- Personal protective equipment (for use during recovery activities or mitigating actions)
- Structure layout

3.4 DATA MODELING FOR ACTIVE COMPONENTS

Previous sections of this document have summarized scenario modeling using event trees and event sequences. The current state-of-practice in the nuclear industry also requires modeling to develop the frequencies and probabilities that populate the fault tree basic events and event tree pivotal events of the scenario model. This is called data modeling.

The basis of data modeling practice in the nuclear industry is Bayes' Theorem (Apostolakis, 1978; Apostolakis, 1981; NRC, 1983). This is because Bayes' Theorem allows development of frequencies and probabilities with appropriate consideration of uncertainties for situations of interest. This includes, for example, the following situations:

- No failures.
- Sparse data.
- Multiple data sources.
- Perfectly applicable data and partially applicable data.
- Handbook data (often called generic data).
- Combinations of the above, all with consideration of uncertainties.

Data about equipment may be characterized as one of the following types:

1. Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (an example of this is operational experience of equipment to be used in the repository).

2. Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (an example of this is test data on an identical piece of equipment to be used in the repository).

3. Historical performance of successes and failures of a similar piece of equipment or similar category of equipment under conditions that may or may not be those under analysis (an example of a similar piece of equipment is similar functioning equipment used on another program, or tested on another program). An example of a similar category of equipment is data from handbooks or field data compilations.

4. General engineering or scientific knowledge about the design, manufacture and operation of the equipment, or an expert's experience with the equipment.

Bayes' Theorem

Data is often found from more than one of the above sources. Bayes' Theorem has been proven to be a coherent method that is able to combine data (Lindley, 1965). It mathematically expresses a decrease in uncertainty gained by an increase in knowledge. Equation 3.4.1 is one formulation of Bayes' Theorem commonly used when combining judgment (data type 4) with directly applicable data (data type 1).

Let λ_j be one failure rate of a set of possible failure rates of an SSC and E be type 1 data actually observed about the SSC. The probability of λ_j given E is represented as $P(\lambda_j/ E)$. Bayes' Theorem gives us:

$$P(\lambda_j / E) = \frac{P(\lambda_j)L(E / \lambda_j)}{\sum_j P(\lambda_j)P(E / \lambda_j)} \qquad (3.4.1)$$

In Equation 3.4.1, $P(\lambda_j)$ is called the "prior probability", $L(E / \lambda_j)$ is called the "likelihood". For this example, the prior probability is determined by the judgment of those who are knowledgeable about the SSC failure characteristic (i.e. type 4 data). The likelihood is the conditional probability that the type 1 data would actually be observed if the failure rate were truly λ_j. In summary, Equation 3.4.1 states that the knowledge of the "updated" $P(\lambda_j/ E)$equals the "prior" probability of λ_j before the type 1 data is known times the likelihood, $L(E / \lambda_j)$. This is all divided by a normalization factor.

The normalization factor must be such that the sum of the probabilities over the entire set of λ_j equals unity. In order to account for uncertainties, Equation 3.4.1 is integrated over all λ_j and each factor in the equation becomes a probability distribution. The "prior" distribution may be any form that fits the expert knowledge. In this formulation, the likelihood distribution (often called likelihood function) is either a binomial distribution or a Poisson distribution. The former is used for failure on demand; the latter is used for failures over time.

A typical application of Bayes' Theorem for directly applicable SSC data would be to:

- Estimate the "prior" probability using engineering analysis, simulation, previously developed generic priors (for example, "Reliability Data Analysis for Space Station Freedom (External Maintenance Task Team)", SAIC Project Number 1-265-07-840-00, July 11, 1990 provides generic prior distributions for mechanical, electro-mechanical, electrical, and electronic equipment), maximum entropy (Jaynes, 1982; Jaynes, 1988), and/or expert opinion,
- Obtain new information in the form of observed operation,
- Characterize operational data in the form of a likelihood function, and
- Perform the calculation in accordance with the above equation to infer the updated probability.

Consider the following example in Figure 3.

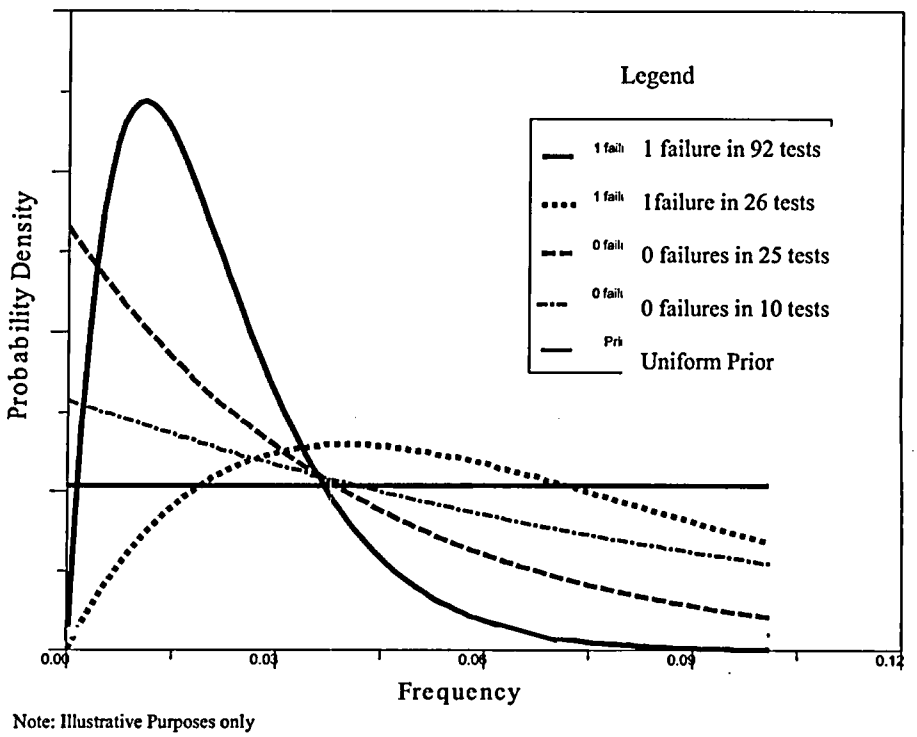

Figure 3. Example Effect of Test Data on Prior Uniform Distribution

Suppose, a new system has been designed. In thinking about the failure characteristics of the system, design and reliability engineers estimate that the probability of failure will be between 0 and 0.1. This is denoted by the horizontal line labeled "Uniform Prior". They

then start a series of reliability tests simulating the operational environment and stresses. After 10 tests, there has not been a failure and the integral of Equation 3.4.1 gives the distribution labeled "0 failures in 10 tests". Note that the data supports the opinion that the probability of failure might indeed be zero. The left portion of the curve is elevated with respect to the original uniform prior.

Tests continue and on the 26^{th} test a failure occurs. The integral of Equation 3.4.1 produces the current updated probability distribution labeled as "1 failure in 26 tests." Note application of Bayes' Theorem shows that system failure probability must be greater than zero and cannot be zero.

Tests continue up to 92 tests and the application of Bayes Theorem produces the curve labeled "1 failure in 92 trials." Notice that the probability distribution shows a clear preference, based on the test data, that the actual failure rate has a central tendency (represented by the mode of the curve) of approximately 0.01. This is approximately the same point estimate that would be expected from simply dividing the number of failures by the number of trials. It is seen that for zero failure, weak data and strong data Bayes' Theorem obtains a completely intuitive result with uncertainties inherently considered.

Other Bayes Methods

Different combinations of data require modeling with a different Bayes' methods. Although the method for analysis of a specific SSC cannot be selected in advance, general guidelines for application have been developed. Table 1 provides examples of these guidelines.

Table 1. Example Method Guidance for Analysis of Different Data Combinations

Data Combination	Method	Bayesian Method Reference
On-site data only	Equation 3.4.1 with previously developed or judgment prior.	Martz, 1991
Multiple failure rates from handbooks with on-site operational data	Two-Stage Bayes, Empirical Bayes, or Hierarchical Bayes	Kaplan, 1983; Martz, 1991; Atwood, 2003
Multiple failure rates from handbooks without on-site operational data	Two-Stage Bayes, Empirical Bayes, or Hierarchical Bayes Development of prior only.	Kaplan, 1983; Martz, 1991 Atwood, 2003
Multiple failure rates from handbooks with on-site equipment test data	Two-Stage Bayes, or Hierarchical Bayes	Kaplan, 1983; Atwood, 2003
Multiple failure rates from other waste repositories with on-site operational data	Two-Stage Bayes, Empirical Bayes, or Hierarchical Bayes	Kaplan, 1983; Martz, 1991 Atwood, 2003

Mathematical details of the tabulated methods are described in the references in Table 1, and are not discussed. All needed electrical, mechanical, and electronic equipment

frequencies and probabilities for the event trees and fault trees will be modeled using Bayesian methods.

3.4.1 Active Component Reliability Data Sources

Reliability data or values generally refer to the failure rate per unit of time or failure probability per demand (or challenge) to the SSCs. Reliability data and values are generally expressed as mean values with associated uncertainty.

Reliability data and values can be obtained from a variety of sources including:

- Empirical data collected from industrial reliability/ monitoring/ testing studies for specific components and structures, or empirical modeling (i.e., computer-based design and simulation) conducted by equipment vendors or generally available in the industry. This data may be from nuclear and non-nuclear sources.

- Reliability modeling using data from generic reliability databases such as those listed in Section 3.4.3.

- Accepted engineering practices and expert judgments.

3.4.2 Treatment of Empirical Data

Empirical reliability data are defined as data obtained through testing or in-service observations of systems, subsystems, or equipment behavior (success and failure) during a period of time or through a number of challenges. Such empirical databases include reliability data for both active and passive components. When available, empirical data of the specific equipment slated for use in the repository, or for similar equipment from the same vendor, may be used in the reliability assessments. In many cases, it may be necessary to use handbook data from other industrial applications that have been collected for similar (surrogate) components and systems used in the nuclear (or other applicable industries). In all cases, the application of the data will be accounted for as an epistemic uncertainty.

Ordinarily, data specific to the Yucca Mountain Project (YMP) equipment are not readily available. However, generic data may be applicable if it serves the same functions under similar environmental conditions. Generic databases can therefore sometimes provide equipment level data that may be of use. Some databases (such as MIL-HDBK-217 and Nuclear Plant Reliability Data System [NPRDS]) have factors to facilitate adjustment for operating conditions and environments.

If empirical or generic data are available for the SSCs in question, the issues noted in the following questions must be addressed:

- Are the data directly applicable to SSCs, and for the safety function in question (e.g., same manufacturer, same construction [materials and methods], same usage,

same exposure environment, same maintenance practices)? If not, the uncertainties would include an assessment of applicability.
- Are human interactions included in the empirical data? If not, human interactions must be analyzed (as discussed in Section 3.7) and documented as part of the overall reliability assessment for that particular SSC.
- Do the empirical data come with an associated uncertainty value (e.g., EF, standard deviation, error band)? If not, an uncertainty analysis must be performed as discussed previously and in Section 3.5.1.4.

3.4.3 Generic Active Component Databases

Reliability data that are needed for the reliability assessment could be derived from various sources such as applicable licensee event reports, empirical data or generic component reliability databases. This section provides information related to these reliability data sources.

3.4.3.1 Application of Event Reports

In some instances, it might be necessary for reliability analysts to acquire and process raw data from incident reports from the nuclear, chemical, mining, or transportation industries. For example, the aircraft analysis used aircraft crash event reports.

Although such event reports provide insights into causal factors that can be considered in the development of reliable systems and operations for the repository, they do not directly provide failure rate or failure probability values, and they do not provide exposure durations. The analyst must estimate these parameters and their uncertainty, and justify the values used. The collection of event reports provides the number of failures observed, but might not provide any information on the total number of opportunities for failure, or on the time-in-service per component represented by the number of failures. Therefore, the reliability analyst would process the information as follows:

- Review each event report for its applicability to a given reliability assessment for a specific repository SSC

- Discard the events determined not to be applicable, but include partially applicable events based on similarity of failure mode or failure mechanism

- Develop a probability distribution with the median value obtained as a count of the number of remaining events including partially applicable fractions (this provides the "numerator" for an expression of failure rate or probability)

- Estimate the number of challenges (or component service hours) represented by the span of relevant event reports as a probability distribution (this provides the "denominator" for an expression of failure rate or probability).

Once the numerator and denominator probability distributions are obtained, by a suitable statistical sampling technique, the analyst can quantify the estimated mean failure rate with uncertainties.

The U.S. Department of Transportation (DOT) database on railway accident causes provides a similar application of empirical data from industry. The DOT collects data on the number of accidents (on a "per million miles traveled per year" basis) that occur for individual railroad companies and for entire commercial railways. The data are then processed in several sorting schemes, including a sorting by the category of equipment whose failure caused or contributed to the accidents. The database does not, however, provide component failure rate data. Therefore, if a repository reliability analyst intended to estimate the failure rate for various components of a rail-based waste package transporter system (e.g., engine-to-car couplers), or of an air-brake system or its components, the analyst would have to perform a detailed review of the raw data and make inferences as to both the relevance and applicability of the data, and develop appropriate supporting technical justifications, including justification for excluding data. Once the data are so processed, to estimate the appropriate failure rate for a given component or system, the analyst must estimate the number of miles traveled by the transporter per year. Again, uncertainties in both the numerator and denominator are expressed as probability functions.

3.4.3.2 Generic Component Reliability Databases

Although the repository reliability analyses may derive reliability data from LERs and other industrial event reports, most of the reliability data used in the fault tree modeling will be derived from published generic databases, including the following:

- Offshore Reliability Data (OREDA) (SINTEF, 2002),
- MIL-HDBK-217F (DOD, 1991),
- Center for Chemical Process Safety (CCPS) (CCPS, 1989)
- Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) (Gertman, 1989)
- NPRDS (Denson, 1991)

These databases include both active and passive components. As an example, component failure rates or demand failure probabilities derived from some of the generic sources are tabulated below:

Table 2. Examples of Component Reliability Data Obtained from Generic Databases

Systems, Subsystems, or Components	Failure Mode	Failure Rate or Demand Failure Probability	Unit (/hr) or (/d)	Upper bound	Lower bound	Error Factor	Data Source	Reference	SSC Classification
Substation Transformer Liquid Filled Three Phase	All modes – catastrophic, degraded, incipient	2.23E-6	/hr	3.25E-6	9.3E-7		IEEE – Std 500, 1991	p. 392	Active
Power Cables	All modes	4.84E-6	/hr	1.75E-4	7.1E-7		IEEE – Std 500, 1991	p. 747	Passive
Thermoplastic electrical joints – 601 – 15 kV	All modes	9.0E-8	/hr	1.4E-7	5.0E-8		IEEE – Std 500, 1991	p. 792	Passive
Switches, general	Fail to open/ close	1.0E-5	/d			5	Eide & Calley, 1993	p. 1179	Active
	Spurious Operations	1.0E-6	/hr			10	Eide & Calley, 1993	p. 1179	Active
Fans – Ventilators	Fail to start	5.0E-3	/d			5	Eide & Calley, 1993	P. 1178	Active
	Fail to run	3.0E-5	/hr			10	Eide & Calley, 1993	p. 1178	Active
Air Filter	Plugged	1.0E-5	/hr			10	Eide & Calley, 1993	p. 1178	Passive
AC Motors	Fail to start	2.5E-5	/d	6.9E-5	4.5E-6		CCPS, 1989	p. 138	Active
	Fail to run	1.5E-5	/hr	4.7E-5	2.2E-8		CCPS, 1989	p. 138	Active
Gear Box	Failure	3.3E-4	/hr	N.G.	N.G	N.G.	NPRDS-91	p. 2-69	Active
Piping – straight metal sections	Catastrophic	2.7E-8	/(mile-hr)	1.0E-7	4.7E-10		CCPS, 1989	p. 183	Passive
Fire Suppression System - Water	Catastrophic	9.7E-6	/hr	3.7E-5	1.7E-7		CCPS, 1989	p. 207	Active

NOTES: N.G. = Not Generated; NPRDS-91 = Nuclear Plant Reliability Data System 1991

Often, different failure rates are provided for the same type of component in the same reference or a similar type of component in different references. The analyst may view this as an indication of the epistemic uncertainty of the failure rate and develop a probability distribution for it, even if the uncertainty bounds are not provided in the references. The NPRD-95 is an example of a reference that provides multiple failure rates (from field data) for the same non-electronic component, and EPRD-97 coupled with MIL-HDBK-217F may be used to derive failure rate uncertainties for electronic components.

OREDA

The OREDA project has a collection of reliability data obtained from several offshore oil platform operations. The reliability data were analyzed, processed and published in the ORED Handbook (SINTEF, 2002). The data are organized by:

- Machinery
- Electrical generators
- Mechanical equipment
- Control and safety equipment
- Valves
- Subsea equipment

The handbook provides mean estimates for both component failure rates and demand failure probabilities with lower and upper bounds and the associated standard deviations. A limitation in the use of this database for the repository is that the environmental conditions on offshore oil platforms are more severe than those expected at the repository. However, within an uncertainty analysis framework, these data may be an indication of failure rates greater than a median or mean value at the repository.

MIL-HDBK-217F

The Department of Defense has collected and published reliability estimates for electronic equipment in Military Handbook MIL-HDBK-217F (DOD, 1991). The reliability estimates are divided into the following categories:

- Microcircuits
- Discrete semiconductors
- Tubes
- Lasers
- Resistors
- Capacitors
- Inductive devices
- Rotating devices
- Relays
- Switches
- Connectors
- Interconnection assemblies
- Connections
- Meters
- Quartz crystals
- Lamps
- Electronic filters
- Fuses
- Miscellaneous parts

The handbook provides a base failure rate for electronic components, and potential correction factors involving quality, environment, construction, etc. These correction factors, when appropriately applied to the base failure rate, will provide component

failure rate estimates that reflect the conditions at the operating sites or facilities. The estimates do not have associated uncertainties.

CCPS Reliability Data

The CCPS of the American Institute of Chemical Engineers (AIChE) has collected reliability data for equipment used in the chemical processing industry, and published them in "Guidelines for Process Equipment Reliability Data" (CCPS, 1989). The generic data provided in the document represent the final aggregated data set from a lognormal distribution of raw data inputs. The reliability data are documented for electrical components, piping systems, rotating equipment, etc., with mean values for both failure rates and demand failure probabilities. Lower and upper bounds are also provided.

NUCLARR

NUCLARR was developed as a repository of human error and hardware failure information that could be used to support a variety of analytical techniques for assessing risk. NUCLARR was documented in five volumes as NUREG/CR-4639 (Gertman, 1989).

NPRDS

The NPRDS was developed by Southwest Research Institute and was later maintained by the Institute of Nuclear Power Operations (INPO) (Denson, 1991). The objective of this effort was to collect and provide reliability data (failure rates, mean-time-between-failures, mean-time-to-restore) for safety related systems and components. Nuclear power plants participating in this program began reporting data on a voluntary basis in 1974, and continued until reporting was terminated at the end of 1996.

Data reported to the NPRDS consisted of:

- Engineering reports providing detailed design and operating characteristics for each reportable component.
- Failure reports providing information on each reportable component whenever the component was unable to perform its intended function. These reports used a standard set of component boundaries and failure mode definitions.

The NPRDS has some limitations, which include: 1) the program was discontinued; 2) the reliability parameters such as number of component demands and exposure time are estimated; 3) provided information is too brief to determine the exact failure cause; and 4) maintenance rates and repair time are not provided.

Other Databases

In addition to the previously discussed reliability databases, other generic databases are available such as the Savannah River Site Generic Database that was established by the

Savannah River Site (SRS) to upgrade their safety analysis methodologies (Blanchard, 1998). The SRS generic database contains reliability data estimates for components of systems, such as the following:

- Water system
- Chemical process system
- Compressed gas system
- HVAC/ exhaust system
- Electrical distribution system
- Instrumentation and control system

The failure rates and demand failure probabilities are provided as lognormal distribution means with EFs.

In addition, Eide and Calley have compiled a mechanical and electrical component failure rate database, whose data are primarily based on information in the NUCLARR database. The Eide and Calley database also provides a comparison of the recommended mechanical component failure rate against data from other reliability databases such as NUREG-1150, IEEE-500 Standard. The reliability data are provided as mean failure rates with EFs (Eide, 1993).

The Reliability Analysis Center provides generic data handbooks from field experience for non-electronic components (NPRD-95) and electronic components (EPRD-97). They also provide a compilation of failure mechanisms and causes (FMD-95).

3.4.4 Data Uncertainties

Discussion on data uncertainties is provided in Section 3.4 (use of Bayes' Theorem) and Section 3.5.1.4.

3.5 RELIABILITY MODELING

Generally, FTA or failure modes and effects analysis (FMEA), among other techniques, is used to assess the reliability of a system containing many components that can fail either through various failure modes intrinsic to a given component, or through some extrinsic cause such as a human-induced event.

FMEA is a method by which failure modes of components and their effects on the system or facility, are tabulated and analyzed. FMEA is an inductive, bottom-up logic model. One by one, each specific failure mode of a given component is postulated (e.g., switch fails to open, switch fails to close) and the impacts of the failure modes on the overall SSC performance are tabulated (e.g., fan motor overspeeds, bypassed HEPA filters). Ordinarily, FMEA is applied to single failure modes; it is not efficient to evaluate combinations of equipment failures that lead to accidents (AIChE, 1992). An FMEA may be conducted by design engineers (in consultation with safety analysts) as a

qualitative analysis of SSC reliability for the purpose of identifying potential weaknesses and defenses against failures. Such an FMEA may then be used in the PCSA as a basis for developing an FTA, or for identifying required PSCs.

In contrast to an FMEA, FTA is a top-down, deductive technique that looks at a particular system failure, and provides a means to explore the potential causes for that failure. It is a graphical tool that can be used to model the various combinations of equipment failures and HFEs that can lead to the system failure (AIChE, 1992). The "top event" (see Section 3.5.1 for definition) in a given fault tree may represent a heading event in an event tree, which permits the event tree/ fault tree linkage.

Due to the complexity of the system design and the potential of human interactions, FTA is preferred over FMEA as the technique for assessing the reliability of ITS SSCs. The methodology for deriving the model and obtaining reliability data for systems and subsystems using FTA is described and illustrated in Sections 3.5.1.

As noted, FMEA and FTA techniques are generally associated with analysis of system reliability. For structures and certain passive components, other techniques are required for deriving a reliability estimate. The methodology for deriving reliability estimates for ITS structures and passive components is described in Section 3.6. Reliability data estimation for PSCs is described in Section 3.8.

3.5.1 Fault Tree Analysis for Systems and Subsystems

FTA is an accepted methodology for assessing the reliability of a system; it has been used widely within the nuclear industry, and within other industries (e.g., aeronautic, chemical processing, automobile manufacturing). The methodology used at YMP follows that described in the NRC's *Fault Tree Handbook*, NUREG-0492 (Vesely, 1981).

A fault tree is a logic model (of a physical system) that helps to define the various ways a system can fail to provide a given safety function. The fault tree is based on deductive logic that starts with a well-defined undesired event, called the "top event", and systematically decomposes the top event into intermediate failure events of subsystems that, in turn, are decomposed into lower level events. The standard graphical symbols used to represent fault tree logic are defined in Reference (Vesely, 1981).

The decomposition of events is terminated at the lowest level of assembly for which data are available. In general, the events at the lowest level of assembly are called basic events. Each basic event represents a specific failure mode for a given component or HFE. A common-cause failure of two or more identical components is also represented as a basic event.

Figure 4 depicts a hypothetical fault tree that was constructed to model the potential failure of the HVAC system denoted in Figure 1 (hypothetical event tree).

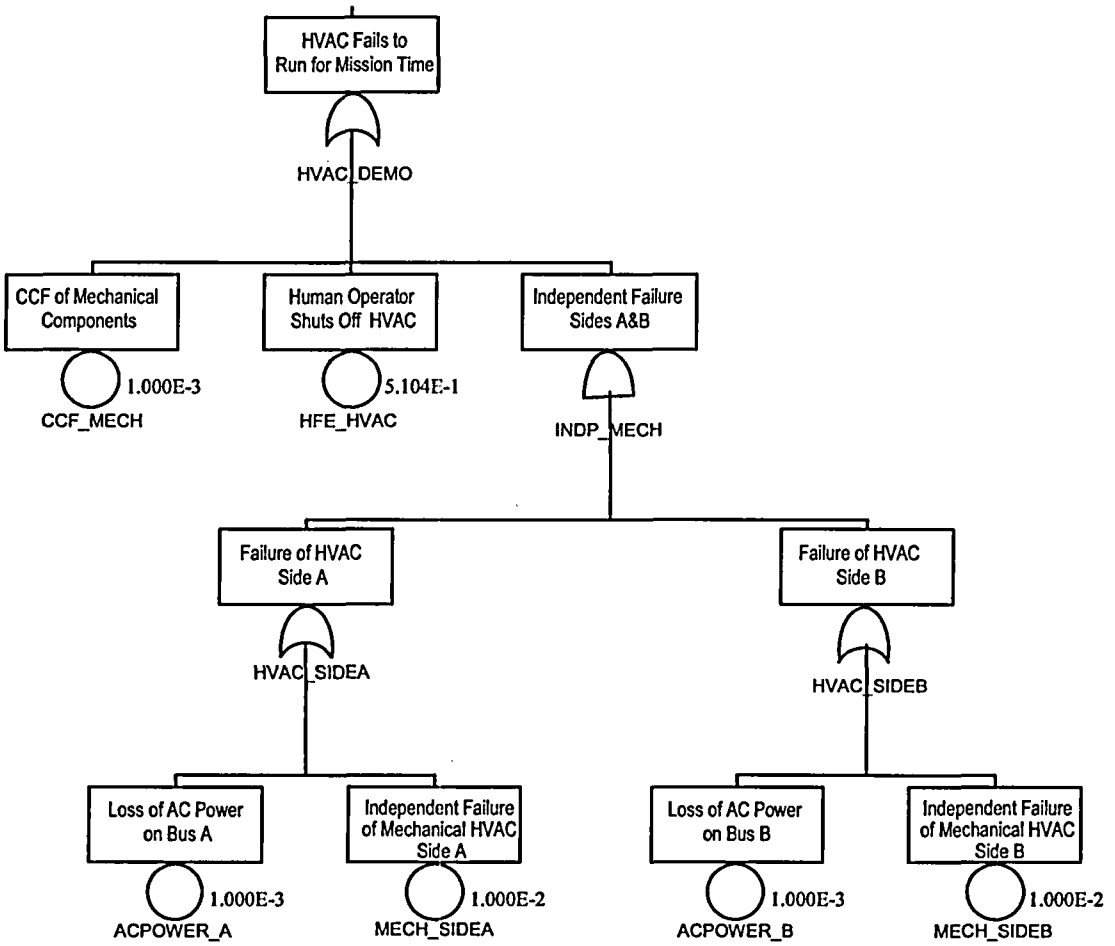

Figure 4. Hypothetical Fault Tree for the HVAC System Failure

It should be noted that the top event of the fault tree ("HVAC_DEMO") has the same name as one of the conditional pivotal events in Figure 1. This naming convention provides the linkage that the SAPHIRE software uses to transfer the estimated failure probability of the system into the event tree where the system failure is modeled and uses it to quantify the event sequences.

The solution of the fault tree model is derived using the rules of Boolean algebra. Simple fault trees may be solved by hand to determine the minimal cut sets; complex trees are generally evaluated using computer analysis (e.g., using SAPHIRE).

The qualitative results are expressed in the form of a list of minimal cut sets. Each minimal cut set represents a single basic event or a combination of two or more basic events (e.g., a logical union of basic events) that could result in the occurrence of the top event. Minimal cut sets are minimal in the sense that they contain no redundant basic

events (i.e., if any basic event were removed from a minimal set, the remaining basic events together would not be sufficient to cause the top event).

For quantification of the probability of the top event, failure probabilities are developed for each basic event (hardware or HFE) and are used to compute the probability of each cut set. Using the rare-event approximation, the mean probabilities of the cut sets are added together to approximate the probability of the top event. Other approximations may also be used to solve the event tree. Failure probabilities of basic events are expressed in terms of uncertainty distributions in SAPHIRE. The uncertainty distributions are propagated through the cut set quantification to yield the uncertainty distribution of the top event. The mean of the uncertainty distribution of the top event is the best point estimate of the probability of the top event. For more information on FTA modeling, please refer to Reference (Vesely, 1981).

Issues that are addressed in the fault trees, in addition to the mapping of the descriptions of the physical system into a fault tree logic diagram based on explicit effects of mechanical and hardware failures, include the following:

- Basic event data
- Common cause and common mode failures such as failures induced by common training, maintenance practices, fabrication, common electrical supplies, etc.
- Support systems and subsystems such as cooling (HVAC, cooling water), electrical, etc.
- System interactions
- Human failure events – the methodology for assessing and quantifying HFEs is provided in Section 3.7.
- Control logic malfunctions

The following discussions focus on the basic event data used in FTA, the common cause failure, the fault tree quantification process, and the uncertainty analysis.

3.5.1.1 Basic Event Data for Component Failures

Basic event data are typically represented in the FTA as component failure rates or component demand failure probabilities (see Section 3.4.3.2). As presented in NUREG-0492, the typical model of failure probability for a component is depicted as a "bathtub curve" as illustrated in Figure 5. The curve is divided into three distinct phases. Phase I represents the component failure probability during the "burn-in" period. Phase II corresponds to the "constant failure rate function," where the exponential distribution can be applied to calculate the probability of failure within a specified "mission time." Toward the end of the component life or the wear-out period, which is represented by Phase III of the curve, the probability of failure increases.

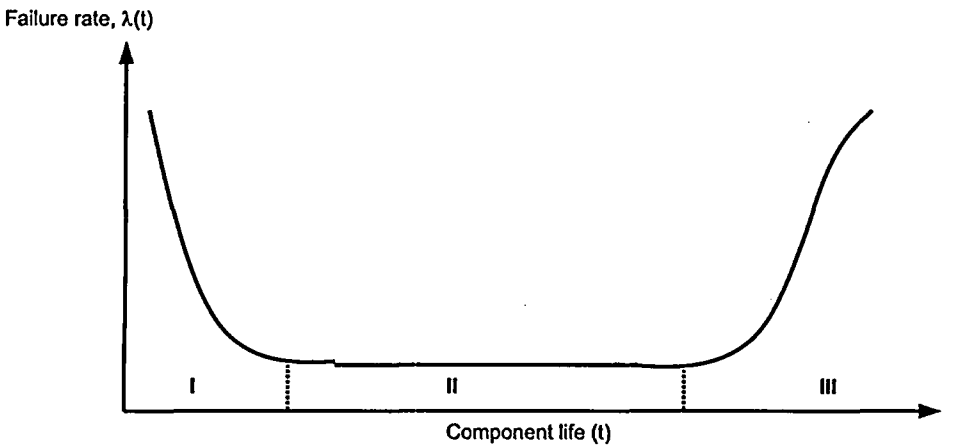

Figure 5. Component Failure Rate "Bathtub Curve" Model

If the component failure rate is assumed to be constant in time with no burn-in or wear-out (e.g., the Phase II region of the curve, assuming the burn-in testing of components has been conducted, and preventive maintenance replaces components before they are worn out), then the component time-to-failure probability can be represented with the exponential distribution. The probability of failure of a given component (or system) depends on the value of the constant failure rate, λ, and the mission time, t_m, as follows:

$$P_F(\lambda,t_m) = 1 - \exp(-\lambda t_m)$$

Component failure databases provide a mean or median value for λ and its variability. The mission time, t_m, is determined by the PCSA analyst.

The probability of failure increases with an increase in either λ or t_m, or both. When the product λt_m is small (<0.1), the failure probability may be calculated by the following approximation, which introduces less than a 10% error:

$$P_F(\lambda,t_m) \cong \lambda t_m$$

This fundamental exponential is called the "no-repair, continuous operation" model. When repair is feasible, other failure models that are modifications of the basic exponential model can be used. The "with repair" model includes a factor for both time between failures and time to repair given a failure.

If a probability of failure during Phase I or II is needed, then it is necessary to use other time-to-failure models such as a two-parameter Weibull distribution. Refer to Reference (Vesely, 1981) and Reference (Smith, 2005) for more information on the component failure models.

In SAPHIRE, the basic event input screen allows the analyst to specify the failure model to be applied to the component. Based on the specific system and component being

evaluated, the analyst may select the "no-repair" option (exponential model) and be asked to provide λ and t_m, or the analyst may select the "with repair" option, which will require values for λ, t_m, and a mean repair time. This information may become the basis for a technical specification.

Other applications of the constant failure rate model include estimates of the unavailability of standby components or systems that are periodically tested and/or repaired. Reliability theory assumes that after each test the component or system is "good as new" with a "resetting" of the time-to-failure "clock" for the exponential failure model. The unavailability factor is evaluated as the probability of failure during the time between tests, τ. The average unavailability factor, or failure on demand of the standby unit, q_d, is calculated as:

$$q_d(\lambda,\tau) = \frac{1}{2}(\lambda\tau).$$

Again, λ is obtained from component databases, but the mean time between tests, τ, is determined by the analyst. The value of τ may become the basis for a technical specification. This is a highly simplified model that assumes the component is continuously running between tests, the test does not require any time, and the test neither introduces another failure mode nor changes the failure rate of the component.

The concept of the bathtub curve also applies to the failure-on-demand probability of components or systems. This probability is often symbolized as q_d. This model is not based on time in service; it is based on the number of times the component or system is called upon to perform its safety function. For various reasons (including physical mechanisms), each challenge to the component/system may leave it degraded, such that, after several challenges it may be degraded to the point of failure that is unknown until the next challenge (or test).

Component databases sometimes provide a mean or median value for the q_d and its variability. The PCSA analyst must determine whether the value is appropriate.

For YMP, a constant component failure rate per unit of time, or a constant component failure probability per challenge, has been determined to be applicable for the FTA and event sequence categorization. As noted in the *Fault Tree Handbook* (Vesely, 1981), it is common practice to select a constant failure rate model, because most of the reliability data are "order of magnitude" accurate. It is assumed, by following vendor recommendations for useful lifetime and normal refurbishment, the component is routinely replaced before wear-out can occur. In addition, most of the empirical reliability databases assume the collected data represent the constant failure rate region of the bathtub curve and report the failure rate, λ, or the failure-on-demand value, q_d. Some databases report only point values λ or q_d, others also provide uncertainty parameters.

EXAMPLE: As shown in Figure 4, the basic events modeled in the hypothetical HVAC fault tree include:

ACPOWER_A	Loss of power on HVAC train A
MECH_SIDEA	Independent failure of mechanical HVAC train A
ACPOWER_B	Loss of power on HVAC train B
MECH_SIDEB	Independent failure of mechanical HVAC train B
CCF_MECH	Common cause failure of HVAC mechanical components
HFE_HVAC	Human failure event due to operator shutting off HVAC

The basic event "MECH_SIDEA" mean failure probability is estimated at 1E-2, which is the product of a hypothetical mean constant failure rate λ of 1E-3/hr and a hypothetical mission time t_m of 10 hours. The associated uncertainty is represented by an EF of 3 for the log normal distribution. This means that the 95th percentile is 3 times the median value, or approximately 3E-2 in this example.

The constant failure rate data are normally obtained from generic reliability databases as described in Section 3.4.3.2.

3.5.1.2 Dependent and Common Cause/ Common Mode Failure

Component failures modeled in the fault tree may not necessarily be independent. There are two broad classes of dependent failures among multiple components: dependence on common support systems, and common-cause failures.

The hypothetical fault tree shown in Figure 4 illustrates the explicit dependence of each side (A or B) of the HVAC system on the respective side of the electrical supply system (bus A or B). However, a more significant dependence would occur if both sides A and B of the HVAC system were connected to the same electrical supply (e.g., bus A). Loss of power from that bus will result in the loss of function of multiple components of the HVAC system. Such dependent failures would be modeled explicitly in the FTA.

EXAMPLE: In Figure 4, the dependence is shown in the "OR" gate logic linking to the bus failure, which is treated as a basic event in the example quantification. However, the underlying supply to a particular bus can be a complex electrical system. A fault tree model can be developed for each of the respective top events "loss of power on Bus A" or "loss of power on Bus B." Using a program such as SAPHIRE, the dependence on Bus A or Bus B in the HVAC fault tree may be linked to the fault trees for the electrical supply system.

A CCF is a single failure that could lead to multiple failures that may result in a failure of the system, but which cannot be explicitly mapped from a physical system's description or drawings into fault tree logic. The quantification of the probability of a CCF is treated by implicit methods discussed below. The issue of CCF is important when redundancy of components or subsystems is included in a system design with the intent of improving reliability. Because of the probability of CCF, the resulting reliability (i.e., probability of success) is reduced relative to that which is calculated by assuming complete independence of the components (or subsystem).

Generally, a common-cause failure among multiple components (or subsystems) can occur when there is some agent that can link a failure in one component (subsystem) to another. The linking agent can be a physical interaction, such as a spray or missile generated by the first component failure that results in failure of the others. By using barriers or separation in the design, the potential for such interactions can be eliminated or significantly reduced in probability. Other agents of CCFs are common environment, common specification, common vendor, common maintenance and testing practices, common installation and handling, etc., that can degrade a component and all redundant components that share the agents. A defective maintenance procedure (missing steps in the procedure) leading to failure of all HVAC dampers, which in turn, could result in a HVAC system failure in a waste handling cell is an example of a maintenance agent.

Although design and programmatic controls can be established to eliminate identified CCFs in systems in which high-reliability is necessary, experience has shown there remains a small probability that a CCF could occur among redundant components. Various models and supporting empirical data have been collected for the purpose of analyzing the probability of CCFs.

Among them, two of the most common methods used to estimate the CCF contribution to the system reliability are:

- β-factor model for preliminary screening of all levels of redundancy
- α-factor model for more refined analysis of more than 2 redundant components with k-of-n (e.g., 1-of-3, 2-of-3) success criteria

β-Factor Model: The probability of CCF contribution is expressed as a fraction of the total probability of one component:

$$q_{total} = q_{ind} + q_{ccf}$$

where

$$q_{ind} = q_{total}(1-\beta)$$
$$q_{ccf} = \beta \cdot q_{total}$$

In a redundant system of two identical components A and B, where the system success is the success of either A or B, the probability of the system failure is:

$$q_{sys} = (q_{A,ind} * q_{B,ind}) + q_{ccf} \qquad = q_{ind}^2 + q_{ccf}$$

Typically, a generic β factor of 0.1 (as suggested in NUREG/CR-4780 [Mosleh, 1988]) is used as a first approximation for most components. Therefore, if q_{total} for each component A and B is 10^{-2}, then the system failure probability is:

$$q_{sys} = [q_{total}(1-\beta)]^2 + q_{ccf} \qquad = (1-\beta)^2 q_{total}^2 + q_{ccf}$$
$$= (1-0.1)^2 (10^{-2})^2 + (0.1)(10^{-2}) \qquad = (0.9)^2 (10^{-4}) + 10^{-3}$$
$$= 0.00108 \text{ or } \cong 0.001$$

If CCF were ignored and the system failure mode includes only independent failure, the system failure probability would be 10^{-4}. The effect of the β factor in this example is to increase the failure probability by a factor of 10.

A limitation of the β-factor model is that it gives no credit for redundancy greater than 2. That is, even if the number of multiple components in the above example were increased to 3 or 4, the system failure probability would still be dominated by the term q_{ccf}, and would still remain at 0.001.

α-Factor Model: As described in NUREG/CR-5485 (Mosleh, 1998), when the success criterion becomes more complex such as one-of-three or two-of-three, the α-factor model is applied to estimate the CCF probabilities. Furthermore, the α-factor model permits a reduction in q_{ccf} when staggered testing is credited. For example, the α-factor model is reduced to that of the β-factor when the success criterion is 1-of-2 in a non-staggered testing scheme. However, in a staggered testing scheme, the CCF contribution is reduced by half (i.e., instead of $\alpha = \beta = 0.1$, $\alpha = 0.05$). So, for the preceding 1-of-2 example, in a staggered testing scheme, the system failure probability is:

$$q_{sys} = [q_{total}(1-\alpha)]^2 + q_{ccf} = (1-\alpha)^2 q_{total}^2 + q_{ccf}$$
$$= (1-0.05)^2 (10^{-2})^2 + (0.05)(10^{-2}) = (0.95)^2 (10^{-4}) + 0.0005$$
$$= 0.0005902 \cong 0.0006$$

NUREG/CR-5497 provides tabulated values of α factors for various types of components and subsystems commonly available in nuclear power plants (Marshall, 1998). In the FTA quantification process, the q_{ccf} values are inserted into the fault tree model with their associated uncertainty values. Basic event data and their uncertainties are then processed with the α-factor uncertainties, to obtain the overall probability distribution propagated through the fault tree.

EXAMPLE: The basic event "CCF_MECH" shown in Figure 4 represents the hypothetical failure of the HVAC system due to CCF that can knock out both HVAC train A and train B. Because the HVAC system success is 1-of-2 trains, the β-factor model was applied to estimate the common cause contribution to system failure, q_{ccf}. In this example, a β factor of 0.1 was used in the analysis and the estimated failure probability is:

$$q_{ccf} = \beta \cdot q_{component} = 0.1 * 1E\text{-}2 = 1E\text{-}3$$

It should be noted the CCF of the HVAC is modeled in the fault tree as a basic event (with an estimated value of 1E-3) that is shown via the "OR" gate logic of the top event, as alternative failure mode, independent of the failure of both HVAC trains. However, the event "CCF_MECH" could be inserted as a basic event under both of the intermediate event gates "Failure of HVAC Side A" and "Failure of HVAC Side B." The result of the Boolean algebra development of minimal cut sets, however, would show the event CCF_MECH as a single-element cut set, which is equivalent to modeling the event as shown in Figure 4.

3.5.1.3 Fault Tree Quantification

The FTA modeling and quantification are performed using the SAPHIRE computer software (Smith, 2005).

Results of the FTA are presented in the form of cut sets and the probability distribution of the top event. The cut sets are evaluated and discussed in a reliability assessment document for each analyzed SSC using the FTA methodology. Within the analysis, if there is a possibility of cut set recoveries, it will be applied and documented appropriately.

EXAMPLE: Assuming all reliability data are available for and populated in the hypothetical fault tree (Figure 4), the quantification process performed by SAPHIRE shows a mean failure probability of 5E-1 for the hypothetical HVAC system with a upper and lower bound of 8E-1 and 2E-1, respectively. The uncertainty analysis is based on a Latin hypercube sampling of 1000 samples and a random seed of 8769. (In practice, more than 1000 samples would be used, depending on the complexity of the fault tree, the desired accuracy, and the convergence required). The uncertainty analysis is discussed in more detail in subsection 3.5.1.4. The cut sets generated from SAPHIRE computation of the HVAC fault tree are tabulated below:

Table 3. Sample Cut Sets for the Hypothetical Fault Tree

Cut No.	% Total	% Cut Set	Prob./Frequency*	Cut Sets
1	99.89	99.89	5.104E-001	HFE_HVAC
2	100.00	0.20	1.000E-003	CCF_MECH
3	100.00	0.02	9.999E-005	MECH_SIDEA, MECH_SIDEB
4	100.00	0.00	1.000E-005	ACPOWER_B, MECH_SIDEA
5	100.00	0.00	1.000E-005	ACPOWER_A, MECH_SIDEB
6	100.00	0.00	1.000E-006	ACPOWER_A, ACPOWER_B

*The three-decimal accuracy is a hard-wired feature of SAPHIRE

As shown in the Table 3, the top contributor to the system failure is a single element cut set "HFE_HVAC" denoting an HFE (operator shutting off both HVAC trains) that leads to a complete shutdown of the HVAC system. This cut set accounts for 99.89% of the HVAC system failure. The next cut set is a CCF of the HVAC component ("CCF_MECH") that accounts for 0.2% of the system failure. The rest of the cut sets have negligible impact on the system failure. Based on this information, it is clear that the primary focus area for system reliability improvement (in this hypothetical example) is operator training, with CCF of the HVAC system being a secondary consideration.

3.5.1.4 Treatment of Uncertainties and Sensitivity Analysis

An important element of the event sequence frequency analysis is that it invariably includes a degree of uncertainty associated with the final results, due to the incomplete understanding of the performance of the designed systems and components, the human interactions, and the uncertainties in the data used in the system modeling. In many cases, the magnitude of uncertainty in the event sequence frequency does not matter with

respect to categorization, because the mean value of the calculated frequency is sufficiently far from an event sequence category boundary. In other cases, the mean may be judged to be too close to the categorization boundary and, an uncertainty analysis is therefore needed to accompany the main reliability and event sequence quantification, to provide a perspective on the results, and to justify the categorization.

Uncertainty analysis for a risk analysis, in general, is defined in the American Society of Mechanical Engineers (ASME) standard for PRAs of reactor plants (ASME, 2002). Sources of uncertainty are characterized as being either aleatory or epistemic.

Aleatory uncertainties refer to the inherent randomness or variability of events or processes. Aleatory uncertainty cannot be reduced by the acquisition of more data or information. An example of aleatory uncertainty is weather, wind speed and wind direction. When doing an analysis that projects possible future dose release scenarios, the actual weather, wind speed and direction at any time in the future cannot be predicted because it is variable.

Epistemic uncertainty refers to uncertainties that arise because of lack of knowledge about a process, materials, systems, models, and applicable data. Where appropriate, examples of aleatory and epistemic uncertainties will be provided in this discussion. As is noted, many of the uncertainties associated with the PCSA reliability estimates are epistemic.

For purposes of PCSA reliability modeling, the performance of uncertainty analyses addresses the following:

- There are two categories of uncertainties that are addressed in PCSA reliability modeling: modeling uncertainties and data uncertainties. Modeling uncertainties pertain to the level of detail used in the system modeling, the knowledge of failure modes, and the adequacy of mapping a complex system into a fault-tree logic model. These are examples of epistemic uncertainties. In addition, various portions of a given event sequence analysis may be conducted at a different level of detail. As noted below, modeling uncertainties are usually investigated via sensitivity analyses in which a portion of a logic model is assessed with different values for selected parameters.

  Data uncertainties refer to the fact that exact values of failure rates that are applicable to a specific repository SSC are not known. One form of data uncertainty is implicit in the variability that exists in measured or statistically processed data. This is an example of aleatory uncertainty. In some cases, databases or specific values of a failure rate use pooled data from multiple basic sources. The pooling process also introduces additional intrinsic uncertainty because the data may not all be of the same population. The basic and pooled databases present the mean and uncertainty spreads for each failure rate.

Another form of epistemic uncertainty is the judgment regarding its applicability for the repository. In this case, it is similar to modeling uncertainty because the analyst makes a judgment. In applying available empirical data, the analyst may adjust the failure rate up or down as appropriate. In addition, the analyst may employ Bayesian Analysis, which formalizes the application of subjective probability in the development of failure rates and uncertainty factors from generic empirical data.

Both modeling and data uncertainties are addressed in SSC reliability assessment and event sequence frequency categorization. The specific uncertainty in each portion of the data is propagated through a reliability or event sequence quantification as described below.

- Combination of Uncertainties: Epistemic uncertainties are propagated through the model, using the event tree/fault tree logic. A stratified sampling method, Latin hypercube sampling, is used to sample the probability distributions defined for the many input parameters. The results of the propagation are a probability distribution of conditional probabilities of each fault tree top event, and a probability distribution of the frequency of each scenario. Monte Carlo calculations have intrinsic calculational uncertainty inversely proportional to the square root of the number of trials. Because the Latin Hypercube method forces trials to be taken at each probability interval, including the extremes, this method provides for a better treatment of the extremes (e.g., less than the 5^{th} percentile and greater than the 95^{th} percentile of the Monte Carlo technique). By inputting correlation coefficients, each method can also treat correlation of variables that might not have been covered by the explicit modeling of dependent events.

Additional discussion of uncertainty analysis methods is provided in NUREG/CR-6823 (Atwood, 2003).

The uncertainty analysis is accomplished by obtaining uncertainty values directly from the data sources or by estimation. Propagation of uncertainties within the fault trees and event trees will be performed by the SAPHIRE software.

EXAMPLE: An uncertainty analysis of the hypothetical HVAC fault tree (Figure 4) was performed by SAPHIRE with the following tabulated results:

Table 4. Hypothetical Fault Tree Quantification SAPHIRE Results

Name	Mean	Min. Cut Upper Bound	Median	Std. Dev.	5th %	95th %	Min.	Max.	Seed	Size
HVAC_DEMO	5.110E-01	5.110E-01	5.121E-01	1.871E-01	2.027E-01	8.167E-01	4.632E-02	9.582E-01	8769	1000

As shown in Table 4, the system (HVAC_DEMO) failure probability has a mean value of 5.11E-1, a standard deviation of 1.871E-01, and 5^{th} and 95^{th} percentile values of 2.03E-1 and 8.17E-1, respectively. This is based on a Latin hypercube sampling of

1000 samples (size) and a random seed of 8769. This is the result of the propagation of uncertainty values provided with each of the basic events modeled in the fault tree.

As noted, sensitivity analysis will be performed for some of the fault trees and event sequences, to investigate effects of modeling uncertainties and/or the application of surrogate empirical data. Sensitivity to modeling involves changing the logic of a fault tree or event tree, and re-analyzing. For example, the effect of increasing redundancy or introducing diversity into a system can be studied with a change to an FTA. Sensitivity to data uncertainties can be evaluated by varying the reliability values of the dominant contributors into the fault trees and event sequences. This provides insights as to what and how a component or a system or a PSC may contribute to the overall reliability of the fault tree or event sequence.

3.6 RELIABILITY ESTIMATION FOR PASSIVE STRUCTURES AND COMPONENTS

When a bounding assumption, for example, failure of a component, is used, probabilities of occurrence of that event are not appropriate. For such an assumption, a consequence analysis is performed to determine whether dose requirements are met. When bounding assumptions are not used, the methods below can be used to develop reliability estimates.

Passive components may fail from manufacturing defects, normal and abnormal use, and external hazards such as earthquakes, windstorms, tornado missiles, floods etc. Industry codes, such as ASCE 7 and ASME Boiler and Pressure Vessel establish design load combinations for passive structures (such as building supports) and components (such as canisters). These codes specify design basis load combinations and provide the method to establish allowable stresses. Typical load combinations for buildings involve snow load, dead (mass) load, live occupancy load, wind load and earthquake load. Typical load combinations for canisters and casks are found in the ASME Boiler and Pressure Vessel Code, Section III and would include, for example, preloads or pre-stresses, internal pressurization and drop loads, which are specified in terms of acceleration. Design basis load combinations are purposefully specified to conservatively encompass anticipated normal operational conditions as well as uncertainties in material properties and analysis. Therefore, passive components, when designed to codes and standards and in the absence of significant aging, generally fail because of load combinations or individual loads that are much more severe than those anticipated by the codes. Fortunately, the conservative nature of establishing the design basis coupled with the low probability of multiple design basis loads occurring concurrently often means a significant margin or factor of safety exists between the design point and actual failure. The approaches described in this section take advantage of the design margins (or factor of safety) and show how failure probability is derived from them.

The approaches described are graded to allow for less complexity where that is justified and supportable arguments for compliance to 10 CFR 63 can be made. A number of screening approaches is suggested below:

- Screening of event sequences or SSCs can take place on the basis of a frequency below the Category 2 threshold if generic or surrogate information is available and able to be justified as sufficiently representative of repository equipment. The information base may include expert judgment, with an associated technical basis.

- Bounding dose calculations with a conservative postulate of failure of passive components or structures may be substituted for development of failure probabilities, if such analyses clearly conclude that regulatory dose limits are met. Similarly, for event sequences that might lead to criticality, a demonstration that reactivity of the configuration is below the upper subcritical limit with doses less than the applicable dose requirements completes the evaluation. For event sequences that lead to a fire, demonstration that there is no release completes the evaluation.

- Screening event sequences may also be achieved on the basis of low probability with assumption of a passive component or structure failure.

Event sequences that could lead to criticality should be handled in the same way as other event sequences. If a component is assumed to fail without evaluation of the probability of failure, then the preclosure safety analysis must evaluate the consequences of its failure. These consequences could be, for example, dose to the public or a possibly critical configuration. Similarly, consequence of a fire will be calculated deterministically.

If these screening methods cannot clearly demonstrate compliance with 10 CFR 63, then failure probabilities for entire event sequences including passive components and structures would be calculated. If such an event sequence is demonstrated to be less than the Category 2 threshold, then this event sequence is screened out.

One method for a passive failure reliability estimate is to employ conservative deterministic calculations the result of which may be converted to probabilities. An example of such a method (developed for seismic analysis) leads to development of a high confidence of low probability of failure (HCLPF) value. The HCLPF value is commonly thought of as a conservative capacity indicating that there is only a 1% or less probability of failure. The Conservative Deterministic Failure Margin (CDFM) method derives a HCLPF value for seismic risk assessment, using design calculation methods but with modified input parameters, that is the base point for a probability distribution. This probability distribution is often called a "fragility curve". To obtain a failure frequency, the fragility curve is combined with an earthquake acceleration-based hazard function.

Another method, which has been applied to waste storage casks, derives a median capacity directly from the designed factor of safety relative to code-allowable stresses. The remainder of the fragility curve is developed by expert judgment. The use of a factor

of safety and expert judgment is acceptable because past experience has shown that the dispersion parameter (e.g., a standard deviation) falls within well defined limits.

The screening methods and more rigorous probabilistic methods need not occur in any particular order. The analyst may select the appropriate methods or combinations of methods. The remainder of this section provides further explanation of passive component and structure reliability estimation and seismic fragility estimation.

3.6.1 Screening Analysis

Sections 3.6.2 and 3.6.3 outline rigorous methods to obtain the failure probabilities of passive equipment and structures. The repository will contain a large number of SSCs. It is neither practical nor necessary to analyze each one with the rigor indicated in Sections 3.6.2. and 3.6.3.

Two types of screening analysis may be performed. One will screen out scenarios based on low frequency and the other will screen out SSCs based on low failure probability. Only those SSCs and scenarios that survive the screening will be quantified rigorously because these will be the most important contributors to total risk. Such an approach is at the very essence of the concept of risk-informed regulation.

Screening Type 1

As described in previous sections, scenarios are developed from initiating events to consequences. Conservative point estimate quantification of scenarios will give a strong indication of their relative risk. Those event sequences that are evaluated to have a frequency that is conservatively below the lower bound for Category 2 can be screened out from further consideration. An example of this would be a finding that the probability of a fire or of tornado missile impact of sufficient severity to cause a release of radionuclides is very low.

Screening Type 2

Typically, codes and standards of buildings provide large factors of safety because loads (such as snow and rain, wind, dead, live occupancy, and earthquake) are assumed to occur simultaneously at their conservative design basis magnitudes, and because known uncertainties in load estimation and strength measurements are considered. It is expected, therefore, that comparison with similarly designed equipment for which probabilities of failure have already been calculated, will allow many equipment items to be screened out. For example, NUREG/CR-3558 (Cover, 1985) provides the following generic seismic capacities for nuclear power plant equipment.

Table 5 lists categories of equipment at nuclear power plants, their median capacity and the lognormal standard deviation of that capacity. The fourth column is derived from the information of the previous two columns using the best estimate equation for a lognormally distributed capacity curve (Cover, 1985). It should be clear the many

categories of equipment would be screened out when combined with the hazard curve using Equation 3.6.16. By similarity arguments, repository equipment within these categories may be shown to be robust against earthquakes and need not be rigorously analyzed.

Table 5. Example Generic Seismic Capacities and Failure Probability at 1.2g

Equipment	*Median Capacity*	*Lognormal Standard Deviation*	*Conditional Probability given 1.2g Acceleration*
Air Handling Units	6.9	0.4	1E-05
Auxiliary Relay Cabinets	7.6	0.8	1E-02
Circuit Breaker Trip	7.6	0.9	2E-02
Control Panels and Racks	11.5	0.9	5E-03
Horizontal Motors	12.1	0.4	1E-08
Large Horizontal Vessels	3	0.6	7E-02
Large Manual, Check, and Relief Valves	8.9	0.4	3E-07
Large Motor Operated Valves (>4")	6.5	0.7	5E-03
Large Pneumatic and Hydraulic Valves	6.5	0.4	4E-05
Local Instruments	7.7	0.4	2E-06
Motor Control Centers	7.6	0.9	2E-02
Relay Chatter	4	0.9	9E-02
Small Miscellaneous Valves	12.5	0.5	8E-06
Small Motor Operated and Air Operated Valves	4.8	0.7	2E-02
Switchgear	6.4	0.7	1E-02
Transformers	8.8	0.4	6E-07

3.6.2 Failure Probability Formulations for Passive Structures and Components

This section describes three formulations for development of failure probabilities from designs that follow current codes and standards. The first formulation is used when the output of structural and component design is represented in terms of actual loads and capacities. The second formulation is useful when the output of the design process yields a factor of safety and standard deviation. Both of these formulations are useful for obtaining a factor of safety with respect to a defined limit state failure criterion. The third is a simplified, conservative approach in which the median capacity is produced from the designed factor of safety relative to code allowables and the remainder of a fragility curve is developed by judgment. All formulations are based on a factor of safety derived from accepted codes and standards that include uncertainties in the calculation and measurement of loads and capacities, and are therefore very conservative.

Probability of Failure from Loads and Capacities

The development of code requirements for minimum design loads in buildings and other structures in the late 1970's considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of American National Standard A58

(Ellingwood, 1980). This document refers to classic structural reliability theory. In this theory, each structure has a limit state (e.g. yield or ultimate) such that loads and resistances may be characterized by an equation of the form:

$$g(x_1,x_2,....x_i,...x_n) = 0 \tag{3.6.1}$$

In Equation 3.6.1, g is termed the limit-state variable where failure is defined as $g < 0$ and the x_i are resistance (sometimes called capacity or fragility) variables or load (sometimes called stress or demand) variables. The probability of failure of a structure is given, in general, by:

$$P_f = \int...\int f_x(x_1,x_2,...x_i...x_n)dx_1dx_2...dx_n \tag{3.6.2}$$

Where f_x is the joint probability density function of x_i and the integral is over the region in which $g < 0$. The fact that these variables are represented by probability distributions implies that absolutely precise values are not known. In other words, the variable values are uncertain. This concept is illustrated in Figure 6. Codes and standards, such as ASCE 7-98 (ASCE, 2000), guide the process of designing structures such that there is a margin, often called a factor of safety, between the load and resistance. The factor of safety is established in recognition that quantities, methods used to evaluate them, and tests used to ascertain material strength give rise to uncertainty.

In the case in which Equations 3.6.1 and 3.6.2 are approximated by one variable representing resistance and the other representing load, each of which is a function of the same independent variable y, the more familiar load-capacity interference integral results as shown in Equation 3.6.3.

$$P_f = \int F(y)h(y)dy \tag{3.6.3}$$

P_f is the mean probability of failure and is appropriate for use when comparing to a probability criterion such as one in a million. In Equation 3.6.3, F(y) represents the cumulative density function (CDF) of structural capacity and h(y) represents the probability density function (PDF) of the load. The former is sometimes called the fragility function and the later is sometimes called the hazard function. For example, in wind risk analysis, y is typically wind generated pressure on structures, F is typically a fragility function, which provides the conditional probability of structural or passive equipment failure given a pressure, and h is the probability density function of wind-generated pressure.

If load and capacity are known, then Equations 3.6.2 and 3.6.3 provide a single valued result, which is the mean probability of failure. Codes and standards guide the design and engineering effort toward development of capacities given the design-to loads. Equation 3.6.3 constitutes one method of developing the reliability of structures. An example of this method is provided in Appendix A, Example 2 for structure reliability under tornado conditions.

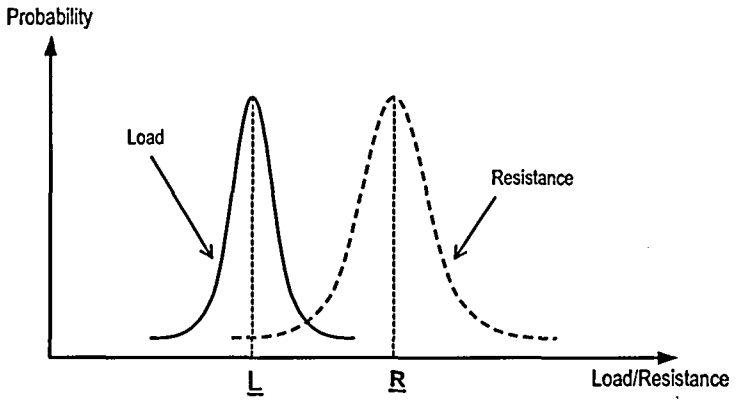

Figure 6. Concept of Uncertainty in Load and Resistance

Each function in Figure 6 is characterized by a mean value, $\overline{L}$ and $\overline{R}$, and a measure of the uncertainty, generally the standard deviation, usually denoted by σ_L and σ_R for L and R, respectively. The spread of the functions may be expressed, alternatively, by the corresponding coefficient of variation (V) given by the ratio of standard deviation to mean, or $V_L = \sigma_L/\overline{L}$ and $V_R = \sigma_R/\overline{R}$ for load and resistance, respectively. The coefficient of variation may be thought of as a measure of dispersion expressed in terms of the number of means.

Probability of Failure From Factor of Safety and Standard Deviation

Another common formulation results from assuming that the probability distributions of Figure 6 are lognormal and is useful if a factor of safety, FS, is provided by the structural analysis. FS is defined as:

$$FS = R/L \tag{3.6.4}$$

FS is also lognormally distributed with median, FS_{50}, and logarithmic standard deviation, β_{FS} given by:

$$FS_{50} = R_{50}/L_{50} \tag{3.6.5}$$

$$\beta_{FS} = \left[\beta_R^2 + \beta_L^2\right]^{1/2} \tag{3.6.6}$$

A median margin and mean margin may be defined as:

$$M_{50} = ln(FS_{50}) \tag{3.6.7}$$

$$\overline{M} = \ln(FS_{mean})$$

Similar to above, a coefficient of variation, V_M, is as follows:

$$1/V_{\overline{M}} = \frac{\overline{M}}{\beta_{FS}} \tag{3.6.8}$$

When V is small, the mean approaches the median and,

$$1/V_{M50} \cong \frac{M_{50}}{\beta_{FS}} \tag{3.6.9}$$

The mean value of FS is:

$$FS_{mean} = FS_{50} e^{\beta_{FS}^2/2} \tag{3.6.10}$$

and the lognormal standard deviation is given in terms of V as:

$$\beta_X = \left[\ell n\left(V_X^2 + 1\right)\right]^{0.5} \tag{3.6.11}$$

Failure occurs when $M < 0$. The adaptation of Equation 3.6.3 for this formulation is:

$$P_f = P(M < 0) = \Phi[-1/V_M] \tag{3.6.12}$$

P_f generates the mean probability of failure when mean inputs are used. In Equation 3.6.12, Φ is the cumulative normal distribution function. Examples of failure probabilities are provided in Table 6 for a variety of values for mean factor of safety and coefficient of variation. This table shows conditional failure probabilities of typical structures designed to current codes.

Table 6. Estimated Passive Structure or Equipment Failure Probability Given Mean Factor of Safety and Coefficient of Variation

FS	$V_L=V_R$	β_{FS}	P_f
3.0	0.2	0.28	8×10^{-5}
4.0	0.2	0.28	8×10^{-7}
3.0	0.15	0.21	2×10^{-7}

Simplified Approach Using Code Allowables

Codes typically provide design basis load combinations and a method for developing the code allowable values. Suppose a design basis load specified a load drop of, for example, X g where g is gravitational acceleration. The design process analysis performed to demonstrate that this load combination is acceptable yields a stress of S_D. The code allowable stress for this load is calculated to be S_A. The factor of safety, using the code allowable stress, would then be (Canavan, 2004):

$$FS = S_A/S_D \tag{3.6.13}$$

Typically, a lognormal distribution for the capacity curve is assumed. If a capacity, C_{50}, at the 50th percentile of the lognormal distribution is defined, then the median capacity may be expressed as:

$$C_{50} = (FS)(X) \tag{3.6.14}$$

However, the code allowable may be at any justified percentile. Equation 3.6.15 presents the equation for the capacity at the nth percentile in a lognormal distribution.

$$C_{50} = C_n e^{K_n \sigma_l} \tag{3.6.15}$$

In equation 3.6.15, K_n is the normal cumulative distribution function value of the nth percentile, and σ_l is the lognormal standard deviation. For example, $K_n = 2.33$ if n is 1%. As mentioned previously, the standard deviation is estimated by expert judgment. SSCs are built to codes to ensure a very low probability of failure. The conditional probability of failure given a drop acceleration, a, is:

$$P_f = \phi[\ln(a/C_{50})/\sigma_l] \tag{3.6.16}$$

In Eq. 3.6.16, ϕ is the standard Gaussian cumulative distribution function. One approach is to very conservatively assume n to be the 50th percentile. With additional justification, n can be chosen to be much lower than the 50th percentile.

3.6.3 Calculation of Probability of Structural or Passive Equipment Failure from Earthquakes

Earthquake risk analysis typically develops fragility functions to represent the structural resistance of structures and components to earthquakes and seismicity functions to represent the earthquakes (Ellingwood, 2001; Kennedy, 1980). Equation 3.6.3 may be rewritten as:

$$P_f^e = \int F(a) \frac{dH(a)}{da} da \tag{3.6.17}$$

In Equation 3.6.17, "a" is ground acceleration (either peak ground or spectral acceleration). The function H(a) is developed from a detailed study of the regional seismic activity and ground faulting conducted by seismologists and geologists (Savy, 2002; Budnitz, 1997). The function, F(a), is called the fragility function and is developed by structural engineers from experiments, codes and standards (Kennedy, 1984).

Application of Eq. 3.6.17 to quantification of seismically initiated event sequences is detailed in a forthcoming revision to a seismic topical report (STR) (DOE, 2004). The following paragraphs present a brief introduction to the method. The revised STR should be used for details of the preclosure seismic safety design and probabilistic evaluation.

A mean fragility cumulative distribution function is typically assumed to be lognormal and can be characterized by a median acceleration (A_m) at which there is a 50% chance that the structure or equipment will fail and a β, the lognormal standard deviation of the CDF. Another anchor point on the CDF is called the HCLPF (high confidence of low probability of failure) and usually set at the 1 percentile of the mean fragility curve. Figure 7 illustrates an example of a fragility curve that shows the HCLPF and median values.

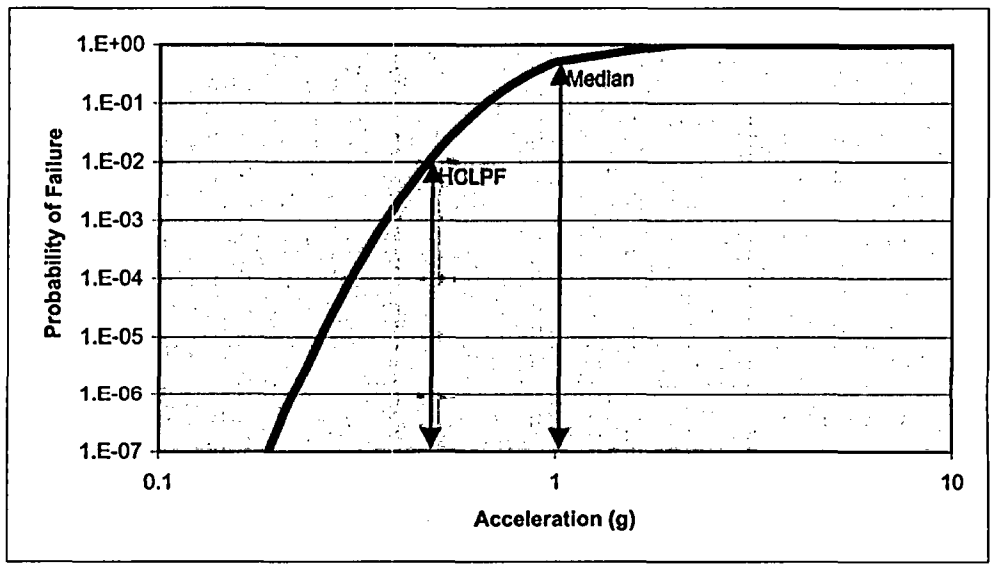

Figure 7. Example Fragility Curve Showing Median and HCLPF

There are two common methods for determining a fragility curve. The first method, developed by Kennedy and Ravindra, relies on a study of the design basis, the assumption in the use of codes and standards, and relevant test data (Kennedy, 1984). An expert opinion is then rendered on the values of A_m and β.

The second method relies on a conservative calculation, based on codes and standards, to develop a HCLPF. This calculation is called the CDFM (conservative deterministic

failure margin) method (Kennedy, 2001; EPRI, 1991). The method also develops a β by judgment recognizing that typical β's range from 0.3 to 0.5 for structures and passive mechanical components at ground level, and 0.4 to 0.6 for active components at high elevation. Furthermore, the method recognizes that the probability of failure is mildly sensitive to β values between 0.3 and 0.6. For example, variations in β within this range change the ratio of the median to the HCLPF capacity by only a factor of 2. Given the uncertainty in the seismicity at the site, it is acceptable to estimate β within this range.

The unconditional probability of failure of the given SSC is calculated via Eq. 3.6.17 using the site-specific H(a) and the fragility curve in Figure 7. The combined site-specific H(a) and fragility curve integral can be solved analytically or numerically, and in the latter case, employing hand computations or the use of computer codes. The convolution integral will be numerically integrated from the design level (5×10^{-4} annual probability of exceedance) to less than Category 2 performance goal (to approximately 10^{-7} annual probability of exceedance) to capture the full range of interest.

3.7 HUMAN RELIABILITY ANALYSIS

Generally, an event sequence analysis is not complete without evaluating the HFEs associated with the analyzed system. If there are human interactions that are typically associated with the operation, calibration, or maintenance of a certain type of component/system (e.g., a controller with a limit setting), then effects of HFEs may be implicit in the empirical data. The analyst is tasked with determining whether that is the case. Otherwise, the analyst must include explicit modeling and quantification of the probability of HFEs. In many situations in which human interaction is considered extremely important to safety, the analyst may include explicit HFE analysis in addition to whatever implicit effects are believed to exist in the empirical data.

In many cases, the HFEs (e.g., failure to follow procedures and maintenance errors) are modeled directly in the fault trees. In other cases, an HFE may be used as an event tree heading. However, it is not always necessary to construct a fault tree or an event tree to analyze HFEs. Regardless of whether the HFE occurs in the event tree or fault tree, the HRA is conducted as a stand-alone evaluation, with the resulting probability of human error appropriately placed in the overall event tree/fault tree model.

3.7.1 Review of Potentially Applicable Human Reliability Analysis Methodologies

A review of NRC's NUREG-1792 "Good Practices for Implementing Human Reliability Analysis (HRA)" (Kolaczkowski, 2005) and NUREG-1842 "Evaluation of Human Reliability Analysis Methods Against Good Practices" (Forester, 2006) indicates that, among other techniques, Technique for Human Error Rate Prediction (THERP) (Swain, 1983), Accident Sequence Evaluation Program (ASEP) (Swain, 1987), Standard Plant Analysis Risk HRA (SPAR-H) (Gertman, 2005), and A Technique for Human Event Analysis (ATHEANA) (NRC, 2000), are suitable for analyzing HFEs in the nuclear

power industry. NUREG-1842 also outlines the strengths and limitations of each of the HRA techniques.

In general, the framework for performing HRA for PCSA consists of the following steps:

- Identification and logic modeling
- Screening
- Task analyses
- Representation, models, and quantification

Technique for Human Error Rate Prediction

Per the description provided in NUREG/CR-1278 (Swain, 1983) THERP is a method for identifying, modeling and quantifying HFEs in nuclear power plant PRAs.

According to NUREG-1842, THERP does not provide explicit guidance on how to model an HFE, but its qualitative approach is useful to derive HFE data. THERP decomposes non-diagnostic HFE into lower level errors and identifies important performance shaping factors (PSFs) through task analysis. This task is graphically represented with an HRA tree. The HRA tree used in THERP is a specialized event tree that shows the successes, failures, and recoveries for each step in a multi-step procedure to which probabilities are assigned to each failure, success, and recovery.

THERP also provides an extensive database of nominal HEPs for many situations encountered in the operations and control of a complex facility (such as a nuclear power plant). THERP presents a series of tables that describe situations that can be used as surrogates by the analyst. Some of the data have an empirical basis while others are based on the expert judgment of the authors.

Experience in performing PRAs for nuclear power plants has shown that the THERP method generally requires use of extensive resources for the HRA and is not normally used in full-scale PRAs. Instead, a simplified method, ASEP, has been derived from the THERP data. ASEP presents two levels of HRA analysis: screening and detailed.

Accident Sequence Evaluation Program HRA Technique

NUREG/CR-4772, "Accident Sequence Evaluation Program Human Reliability Analysis Procedures," provides a description of the ASEP HRA technique (Swain, 1987). Essentially, ASEP is less-resource-intensive than THERP, and it is simple enough that system analysts who are not HRA experts could use it to complete the PRA. However, because of its simplified approach, ASEP HRA results tend to be conservative.

According to NUREG-1842, ASEP addresses pre-accident and post-accident HFEs, and provides guidance for deriving screening and nominal values for both of these HFEs. Although it is based on THERP, ASEP is almost self-contained; it does not require knowledge of THERP or the use of THERP models and data to complete the HRA. In

that regard, ASEP is a useful tool for quantifying HFEs, assuming the HFEs have been identified and modeled. ASEP is not a tool for HFE identification and modeling.

Standardized Plant Analysis Risk Human Reliability Analysis

SPAR-H, documented in NUREG/CR-6883, is an HRA quantification tool for both pre-initiator and post-initiator HFEs (Gertman, 2005). Like ASEP, SPAR-H is not a tool for HFE identification and modeling. It assumes the HFEs have already been identified and modeled in event trees or fault trees. Also like ASEP, SPAR-H, in an earlier version, provided conservative screening estimates. However, the current version of SPAR-H produces detailed "best estimate" values for the analyzed HFEs.

SPAR-H treats HFEs as diagnostic failures and action failures, and quantifies the two types of failures differently. Nominal HFEs for each type of failure are used as the starting point of the quantification process; as the analysis progresses, additional PSFs with specific application guidance are added to the process (as multipliers), to arrive at the final estimate for the HFEs. SPAR-H also provides a worksheet, which allows for proper documentation and transparency of the analysis.

Another advantage to SPAR-H is that the worksheets with PSFs are built into SAPHIRE version 7.26.

A Technique for Human Event Analysis

As described in NUREG-1624, ATHEANA is an HRA method for identifying and modeling HFEs (NRC, 2000). It was developed by NRC to explore why errors occur based on realistic evaluation of the kind of human behaviors observed during accidents or near misses at nuclear power plants and the results due to errors of commission. It is analogous to a root cause analysis for human errors.

According to NUREG-1842, ATHEANA provides guidance for a formal and systematic roadmap for describing context and error forcing contexts, which, in some regard, provides an understanding of how a situation occurs and the causal relationship to human performance that could lead to the error(s) being committed. In this context, ATHEANA can be used to analyze both pre-initiator and post-initiator HFEs; however, in the past, it was used primarily for analysis of post-initiator HFEs. With respect to the quantification, ATHEANA does not provide a database of basic HEPs, and it does not supply a preset list of PSFs as in other HRA techniques; it is left to the HRA analyst to provide this information. Furthermore, ATHEANA does not provide a specific method for quantification of HFEs; it allows the analyst to apply any method that is deemed appropriate.

3.7.2 Selected HRA Methodology for YMP

Based on the information provided in NUREG-1842 and NUREG-1792, it is clear that many methods could be used to conduct a successful HRA. After a review of the type of

analyses conducted at YMP, it appears the HRAs types fall into two categories: (1) those identified in the event trees or fault trees, and (2) those addressed in PSCs, or as initiating events. In this context, HFEs that are identified in the event trees or fault trees may be preliminarily evaluated, using screening values such as those provided in SPAR-H. If the accident scenario of which they are a part is a major contributor to the overall event sequence frequency, then, they will be analyzed with more rigor, using any appropriate method. Because HFEs that are identified in PSCs and initiating events are important to the risk profile, they will be analyzed in detail.

For the screening of HFEs identified in event trees or fault trees, ASEP and SPAR-H are similar, and both are good screening tools. However, the latest version of SPAR-H has incorporated improvements that provide some realism in the estimation of HFE values, thereby making it less conservative than either ASEP or the older version of SPAR. SPAR-H has the following strong points:

- Screening values (nominal values) provided
- Use of PSFs to fine-tune the HEP results
- Uncertainty values associated with the HEP, and propagation of uncertainty
- Applications of recovery
- Documentation with sample worksheet for transparency
- SAPHIRE software has built-in computational module for the HEP quantification based on SPAR-H worksheet.

As a result, SPAR-H was selected over ASEP as the preferred methodology for the screening of simple HFEs.

For complex situations in which detailed HRA is required, an approach that generally follows the steps outlined in the ATHEANA methodology will be used. The approach includes the following:

- Complex task or selected complex PSCs and human error initiating events
- Establish procedural steps
- Conduct talk-thru with operators and designers
- Identify potential indications and cues
- Identify potential time/space interactions
- Prepare action trees
- Assess potential HEPs for each steps in the action tree using SPAR-H methodology
- Documentation using sample worksheet

Although SPAR-H and ATHEANA have been selected as the preferred methodologies to be used to analyze and quantify most of the identified HFEs, THERP and ASEP may also be used when appropriate, if justified by the analyst.

Illustrations of the application of the selected HRA methodology are provided below.

EXAMPLE: As modeled in the hypothetical HVAC fault tree (Figure 5), the top contributor to the HVAC system failure is the HFE "HFE_HVAC", which represents the action taken by the operator to inadvertently turn off both sides of the HVAC system. The HFE was modeled by using the SPAR-H methodology as shown below and the information was entered directly into SAPHIRE for computation.

"HFE_HVAC": this HFE is assumed to be a diagnostic error wherein the operator, somehow, turns off both HVAC trains due to a hypothetical mis-diagnosis of the operating situation. As a result, the following information was entered in the SPAR-H worksheet (automated by SAPHIRE):

Nominal diagnostic HEP: **1E-2**

PSFs			
Time availability:	expansive	**0.01**	(operator has ample time to look into the operating conditions)
Stress:	nominal	**1**	(not in an emergency situation)
Complexity:	moderate	**2**	(many operating parameters to monitor and analyze)
Experience/ training:	nominal	**1**	(operator has received basic training and have HVAC experience at similar facility)
Procedure:	incomplete	**20**	(system was newly installed, operating procedures not updated)
Ergonomics:	50% Poor		0.5*10 = 5
	50% Nominal		0.5*1 = 0.5
	total	**5.5**	(Control panel layout is good, but no accessibility to certain control buttons)
Fitness for duty:	Nominal	**1**	
Work Process:	50% Nominal		0.5*1 = 0.5
	50% Good		0.5*0.8 = 0.4
	total	**0.9**	(Good safety culture, management support, but nominal in planning and scheduling)

The HEP value without dependency can be estimated as the product of the nominal HEP and all PSFs:

$$HEP = (1E\text{-}2)\bullet(0.01)\bullet(1)\bullet(2)\bullet(1)\bullet(20)\bullet(5.5)\bullet(1)\bullet(0.9) = \mathbf{1.98E\text{-}2}$$

In situations where SPAR-H methodology is not equipped to model the cognitive decision process, a root-cause analysis using a methodology such as ATHEANA is more applicable. The ATHEANA technique would call for an assemblage of a multidisciplinary team led by a human reliability assessment expert for the analysis, the availability of applicable procedures, a list of appropriate equipment and design drawing, etc. Once the event is properly analyzed and dissected, and the HFEs are identified, the HEF quantification can be completed with any of the suggested methods including THERP, and SPAR-H.

3.8 RELIABILITY VALUE ESTIMATION FOR PSCs

Generally, PSCs are defined as procedures that can be used to prevent or minimize the chance of events to occur. In most cases, these PSCs rely on human interactions to maintain a safety function. Thus, in order to derive reliability values for these controls, an HRA is required. The general process involved in this type of analysis includes:

- Identify and define the PSC (i.e., clarifications of what is to be accomplished and any time constraints and cues available).
- Determine whether a mechanical or hardware interface is involved. If it is, determine whether an FTA has been performed for the mechanical portion. If not, conduct one as outlined in Section 3.5.1
- Determine whether a procedure related to the control has been written and, if appropriate, whether training on the procedure has been conducted. If a procedure has not been established, develop a surrogate procedure for the analysis. [Note: Due to the parallel development of the license application and the design, a completely developed procedure may not be available at the time of the analysis. In such a case, surrogate procedures from similar operations and controls could be used as a basis for the analysis. As actual procedures are developed, the analysis would be updated as appropriate].
- Assemble a team to review the procedures and conduct the HRA.
- Follow the HRA methodologies outlined in Section 3.7.
- Document the analysis as discussed in Section 4.0.

The following is an example of the evaluation of a PSC.

EXAMPLE: The event sequence under analysis is a brush fire started by lightning striking vegetated area. If the brush fire occurs close to an ITS facility, it could impact the ITS building.

The event sequence analysis of, a PSC is identified that calls for establishment of a vegetation control program around the facility to prevent brush fire events. The source of ignition is limited to natural event – lightning. No man-made ignition sources (e.g., smoking, welding, uncontrolled hot works) are considered because these sources are controlled by different PSCs. A surrogate procedure has been established for the vegetation control program with the following clearly defined steps:

1. The procedure calls for a non-vegetation area 150 feet around the facility to be maintained clear at all times.
2. The non-vegetation area will be controlled, inspected weekly and maintained by the site maintenance crew.
3. The vegetation control task will be done by one person. No supervision will be required.
4. Tools for vegetation control are available and accessible to the maintenance crew at all times.
5. Inspection and maintenance records will be prepared and documented.

The reliability assessment of this PSC is performed with the following assumptions:

1. No other combustible materials besides wild vegetation are considered.
2. Vegetation grows all year long.
3. During the growth period, it takes one month for vegetation to grow to sufficient height and density to cause a problem. A monthly maintenance schedule is therefore sufficient to control vegetation.
4. Vegetation growth of more than 2 months cannot be ignored, and therefore, must be controlled.
5. Vegetation control tools and materials are always available, accessible and maintained properly.
6. The procedure has been written and validated.
7. Proper training on the established procedure has been completed.
8. Time and motion coordination impact on the vegetation control task is negligible.

A brief evaluation of the PSC yields the following potential HFEs that could lead to a "failure to control vegetation in the controlled area" event:

1. HFE-1: The maintenance staff member could forget to perform the monthly vegetation control task for some reason (illness, too busy doing other tasks, etc.)
2. HFE-2: The maintenance staff member fails to spot growing vegetation while doing his or her inspection of the controlled area.
3. HFE-3: The maintenance staff member fails to use proper tools or chemicals to control the vegetation.

HFE-1, HFE-2, and HFE-3 are considered as independent events that could result in the failure of the PSC. The final estimate of the PSC failure probability is equal to the summation of HFE-1, HFE-2, and HFE-3. Because these HFEs are "simple" in nature, the HRA will be conducted using SPAR-H methodology.

The following is an illustration of HEP estimation for HFE-2:

HFE-2: Operator fails to spot vegetation (diagnosis)

Nominal HEP:	1E-2	
PSFs:		
Time availability:	0.01	(expansive >30 mins)
Stress:	1	(none)
Complexity:	0.1	(obvious diagnostic)
Exp./training:	1	(nominal)
Procedures:	1	(nominal)
Ergonomics:	1	(nominal)
Fitness for duty:	1	(nominal)
Work process:	1	(nominal)

Final estimation for HFE-2:
HEP: (1E-2) • (0.01) • (1) • (0.1) • (1) • (1) • (1) • (1) • (1) = 1E-5

Similarly, the estimated probability for HFE-1 is 5E-4, based on the assumption that this is an action task of a nominal probability of 1E-3, and effective training (PSF of 0.5). HFE-3 is also an action task, which starts with a nominal probability of 1E-3, and the associated PSFs of 0.01 for ample time availability, with the rest of the PSFs as nominal; thus, the final estimation for HFE-3 is 1E-5.

As a result, the estimated failure probability of this PSC is:

(HEP-1) + (HEP-2) + (HEP-3) = 5E-4 + 1E-5 + 1E-5 = 5.2E-4

For purposes of this example, a point estimate analysis with no uncertainties is illustrated. The PCSA will include the uncertainties.

Since this task is performed monthly, and assuming that the vegetation growth cannot be ignored if it is older than 2 months, then the exposure period is estimated at 2 months. For the lifetime of the facility, assuming 100 years, there will be (100 years × 12 months /year × 1 exposure period/ 2 months =) 600 exposure periods. If it is assumed that the subsequent failure is independent on the initial failure, then the failure probability in the second month is also 5.2E-4, and the resulting failure probability per exposure period is 5.2E-4 • 5.2E-4 = 2.7E-7.

The lightning frequency is assumed to be the same as that presented in Reference (NRC, 2006) or 11 strikes/yr-mile^2. If the area of vegetation control is represented by an annulus of 150 feet wide around the site, which is approximately 2 mile long and 1 mile wide, the effective area vegetation control area can be estimated as follows:

Site area =1 mile × 2 mile = 2 mile^2
Site and surrounding vegetation control dimensions:
Length = 2 mile + (2 × 150 ft ×1 mile/5280 ft) = 2.057 miles
Width = 1 mile + (2 ×150 ft × 1mile/5280 ft) = 1.057 miles
Site and surrounding vegetation control area:
A = 2.057 mile × 1.057 mile = 2.174 mile^2
Effective vegetation control area:
A_{VC} = 2.174 mile^2 – 2 mile^2 = 0.174 mile^2

The estimated lightning strike frequency at the effective vegetation control area is:

F_{strike} = (11 strikes/yr-mile^2) × 0.174 mile^2 = 1.9 or 2 strikes/yr

The number of strikes that could lead to brush fire events due to the failure of the PSC for the 100 year operations period before permanent closure is:

$N_{strikes}$ = 2 strikes/yr × 100 yrs = 200 strikes.

If the number of exposure periods during the preclosure period is 600, then the frequency of lightning strikes per period is:

$F_{strikes}$ = 200 strikes/600 exp periods = 3.3E-1 strikes/period

Given the estimated frequency of lightning strikes of 3.3E-1 strikes/period and a failure probability of the PSC as 2.7E-7, the event sequence frequency is approximately 9E-8/period. Since the exposure period is renewed over the duration of the preclosure period (e.g., the likelihood of a brush fire due to uncontrolled vegetation starts at 0 at the beginning of the period and reach a maximum probability at the end of the 2 month period; at this point, the vegetation must be controlled, and the cycle begins again). Thus, the final probability estimate for a brush fire event over the preclosure period is the same as that calculated for the period. In this case, the probability of PSC failure is 9.E-8, and therefore, the event sequence is categorized as BC 2.

3.9 RELIABILITY INFORMATION BASED ON EXPERT JUDGMENTS

As described in NUREG-1563 (Kotra, 1996), expert judgment is information that is provided by a technical expert, in his or her subject matter area of expertise, based on opinion, or on a belief based on reasoning. Expert judgments can be based on many factors such as evaluations of theories, models, experiments, or knowledge of the bases for industry codes and standards associated with a given SSC. Expert judgments can be either qualitative or quantitative relating to the expected (or mean) value of a reliability value, or regarding the expected value of parameters that affect a reliability assessment. Expert judgments can provide estimates of uncertainties or judgments about applicability of existing data.

Although expert judgments are often obtained informally (e.g., a staff member asks his or her supervisor for an expert opinion), only a formal documented process will be used to support the PCSA. The formal process is required to preserve transparency, and to provide technical justifications. This process is typically called "expert elicitation". It is a highly structured, formal, and well-documented process whereby expert judgments, usually of multiple experts, are obtained. A formal expert elicitation usually involves the following team members:

- Subject-matter experts who are the experts from whom judgments are elicited. These are individuals who are at the forefront of a specialty relevant to the subject matter(s) in question, and are recognized by their peers as authorities because of their sustained and significant research on the topic.
- Experts who have training and experience in statistics, decision analysis, and probability encoding; the primary function of such an expert is to structure the formal elicitation and train the subject-matter experts in probability encoding.
- A generalist who understands the context in which the results of the expert elicitation will be used, guides the structure of the elicitation to produce the necessary results, provides relevant information and documentation to the subject-matter experts, and helps to train them.

As outlined in NUREG-1563 (Kotra, 1996), formal methods of expert elicitation may be appropriate to be considered in the following situations:

- Empirical data are not reasonably obtainable or the analyses are not practical to perform;
- Uncertainties are large and significant to a demonstration of compliance;
- More than one conceptual model can explain, and be consistent with, the available data; or
- Technical judgments are required to assess whether bounding assumptions or calculations are appropriately conservative.

If expert elicitation is deemed appropriate to obtain reliability information based on expert judgment, project procedures that are based on NUREG-1563 will be implemented.

3.10 EXAMPLE APPLICATIONS

To illustrate the application of various reliability assessment techniques, sample evaluations were conducted and documented in Appendix A. The first example provides an analysis of the reliability of a wall or a steel plate against tornado missiles, providing that the structure is built to codes and standards. The second example illustrates how reliability data can be obtained for passive ITS component such as a structure built to withstand tornado wind force.

4. DOCUMENTATION

The reliability assessment should be documented in such a way that it provides transparency and traceability. To accomplish this goal, the document will provide the following information:

- An introduction
- A brief system narrative describing the ITS SSCs or PSCs
- A description of the scope of the analysis, constraints, and assumptions
- A methodology used for deriving the reliability data (empirical or modeling)
- A presentation of the bulk of the analysis (equations, fault tree structure, fault tree cut sets, uncertainty and sensitivity analysis, HRA, etc.)
- Results and conclusions

PCSA reliability analyses and documentation that supports the License Application will be prepared in accordance with procedures for performing quality-affecting work.

5. REFERENCES

5.1 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. [DIRS 103763]

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. [DIRS 149921]

Apostolakis, G. 1978. *Probability and Risk Assessment: The Subjective Viewpoint and Some Suggestions.* Nuclear Safety, Vol. 19, No.3, May – June, 1978, 305-315

Apostolakis, G. 1981. *Bayesian Methods in Risk Assessment.* Advances in Nuclear Science and Technology. J. Lewis and M. Becker (eds), Plenum Press

Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment.* NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121. [DIRS 177316]

Blanchard, A. 1998. *Savannah River Site Generic Data Base Development.* WSRC-TR-93-262, Rev.1. WSMSC-98-0162. Aiken, South Carolina: Westinghouse Safety Management Solutions. [DIRS 177322]

BSC (Bechtel SAIC Company) 2005[a]. *Categorization of Event Sequences for License Application.* 000-00C-MGR0-00800-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050808.0003; ENG.20050929.0003. [DIRS 174467]

BSC (Bechtel SAIC Company) 2005[b]. *Frequency Analysis of Aircraft Hazards for License Application.* 000-00C-WHS0-00200-000-00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050825.0036. [DIRS 174428]

BSC (Bechtel SAIC Company) 2005[c]. *Monitored Geologic Repository External Events Hazards Screening Analysis.* 000-00C-MGR0-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050829.0012. [DIRS 174235]

Budnitz, R.J.; Apostolakis, G.; Boore, D.M.; Cluff, L.S.; Coppersmith, K.J.; Cornell, C.A.; and Morris, P.A. 1997. *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on the Uncertainty and Use of Experts.* NUREG/CR-6372. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 235076; 235074. [DIRS 103635]

Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.* 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542

CCPS (Center for Chemical Process Safety) 1989. *Guidelines for Process Equipment Reliability Data with Data Tables.* G-07. New York, New York: American Institute of Chemical Engineers. [DIRS 177321]

Cover, L.E.; Bohn, M.P.; Campbell, R.D.; and Wesley, D.A. 1985. *Handbook of Nuclear Power Plant Seismic Fragilities: Seismic Safety Margins Research Program.* NUREG/CR-3558. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: NNA.19890713.0155. [DIRS 177338]

Denson, W.; Chandler, G.; Crowell, W.; and Wanner, R. 1991. *Nonelectronic Parts Reliability Data 1991.* NPRD-91. Rome, New York: Reliability Analysis Center. TIC: 245475. [DIRS 160541]

DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment.* MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828. [DIRS 157646]

DOE (U.S. Department of Energy) 2004. *Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain.* Topical Report YMP/TR-003-NP, Rev. 3. Las Vegas, Nevada: U.S. Department of Energy, Office of Repository Development. ACC: MOL.20041103.0002. [DIRS 172373]

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. [DIRS 146564]

Ellingwood, B.; Galambos, T.V.; MacGregor, J.G.; and Cornell, C.A. 1980. Development of a Probability Based Load Criterion for American National Standard A58: Building Code Requirements for Minimum Design Loads in Buildings and Other Structures. Washington, D.C.: U.S. Department of Commerce, National Bureau of Standards. [DIRS 177339]

Ellingwood, B.R. 2001. "Earthquake Risk Assessment of Building Structures." *Reliability Engineering and System Safety, 74,* 252-262. [Barking, England]: Elsevier. [DIRS 177340]

EPRI (Electric Power Research Institute) 1991. *A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1).* EPRI NP-6041-SL, Rev. 1. Palo Alto, California: Electric Power Research Institute. TIC: 253771. [DIRS 161330]

Forester, J.; Kolaczkowski, A.; and Lois, E. 2006. *Evaluation of Human Reliability Analysis Methods Against Good Practices, Draft Report for Public Comment.* NUREG-1842. Washington, D.C.: U.S. Nuclear Regulatory Commission. [DIRS 177324]

Gertman, D.; Blackman, H.; Marble, J.; Byers, J.; and Smith, C. 2005. *The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883. Washington, D.C.: U.S. Nuclear Regulatory Commission. [DIRS 177326]

Gertman, D.I.; Gilbert, B.G.; Gilmore, W.E.; and Galyean, W.J. 1989. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations.* NUREG/CR-4639, Vol. 5, Part 4, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252112. [DIRS 157687]

Jaynes, E.T. 1982. "On the Rationale of Maximum Entropy Methods." Proceedings of the IEEE, Vol. 70, No. 9, September 1982

Jaynes, E.T. 1988. *The Relation of Bayesian and Maximum Entropy Methods.* Maximum Entropy and Bayesian Methods in Science and Engineering, G. J. Erickson and C.R. Smith (eds), Kluwar Academic Publishers, 1988

Kaplan, S., 1983 "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data." IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 1, January 1983.

Kennedy, R.P. 2001. "Overview of Methods for Seismic PRA and Margin Analysis Including Recent Innovations." Proceedings of the OECD/NEA Workshop on Seismic Risk, Committee on the Safety of Nuclear Installations PWG3 and PWG5, Hosted by the Japan Atomic Energy Research Institute under the Sponsorship of the Science Technology Agency, 10-12 August, 1999, Tokyo, Japan. NEA/CSNI/R(99)28, 33-63. Paris, France: Organization for Economic Co-operation and Development, Nuclear Energy Agency. TIC: 253825. [DIRS 155940]

Kennedy, R.P.; Cornell, C.A.; Campbell, R.D.; Kaplan, S.; and Perla, H.F. 1980. "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant." *Nuclear Engineering and Design, 59,* 315-338. [Amsterdam, The Netherlands]: North-Holland. TIC: 254898. [DIRS 164660]

Kennedy, R.P. and Ravindra, M.K. 1984. "Seismic Fragilities for Nuclear Power Plant Risk Studies." *Nuclear Engineering and Design, 79,* 47-68. Amsterdam, The Netherlands: Elsevier. TIC: 243985. [DIRS 102182]

Kolaczkowski, A.; Forester, J.; Lois, E.; and Cooper, S. 2005. *Good Practices for Implementing Human Reliability Analysis.* NUREG-1792. Washington, D.C.: U.S. Nuclear Regulatory Commission. [DIRS 177323]

Kotra, J.P.; Lee, M.P.; Eisenberg, N.A.; and DeWispelare, A.R. 1996. *Branch Technical Position on the Use of Expert Elicitation in the High-Level Radioactive Waste Program.* NUREG-1563. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 226832. [DIRS 100909]

Lindley, D.V. 1965. *Introduction to Probability and Statistics from a Bayesian Viewpoint.* Part 1 and Part 2. Cambridge: Cambridge University Press

Marshall, F.M.; Rasmuson, D.M.; and Mosleh, A. 1998. *Common-Cause Failure Parameter Estimations.* NUREG/CR-5497. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0105. [DIRS 167710]

Martz, H. and Waller, R.A. 1991. *Bayesian Reliability Analysis.* Krieger Publishing Company, Malabar, FL, 1991

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. [DIRS 149512]

Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques.* Volume 2 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. [DIRS 141035]

Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.* NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106. [DIRS 167711]

NRC (U.S. Nuclear Regulatory Commission) 1983. *Probabilistic Risk Assessment Procedure Guide.* NUREG-2300. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (U.S. Nuclear Regulatory Commission) 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116. [DIRS 157661]

NRC (U.S. Nuclear Regulatory Commission) 2003. *Yucca Mountain Review Plan, Final Report.* NUREG-1804, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards. TIC: 254568. [DIRS 163274]

NRC (U.S. Nuclear Regulatory Commission) 2006. *A Pilot Probabilistic Risk Assessment of A Dry Cask Storage System At A Nuclear Power Plant.* Draft Report. Washington, D.C.: U.S. Nuclear Regulatory Commission, July 20, 2006

Savy, J.B.; Foxall, W.; Abrahamson, N.; and Bernreuter, D. 2002. Guidance for Performing Probabilistic Seismic Hazard Analysis for a Nuclear Plant Site: Example Application to the Southeastern United States. NUREG/CR-6607. Washington, D.C.: U.S. Nuclear Regulatory Commission. [DIRS 177341]

SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook.* 4th Edition. Trondheim, Norway: OREDA. TIC: 257402. [DIRS 174994]

Smith, C.; Knudsen, J.; and Wood, T. 2005. *Modeling Methods for Probabilistic Risk Assessment via the Systems Analysis for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software, Version* 7.26. Idaho Falls, Idaho: Idaho National Laboratory. [DIRS 177320]

Swain, A.D. 1987. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure.* NUREG/CR-4772/SAND86-1996. Washington, D.C.: U.S. Nuclear Regulatory Commission. [DIRS 177325]

Swain, A.D. and Guttmann, 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. [DIRS 139383]

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. [DIRS 128494]

5.2 CODES, STANDARDS, REGULATIONS, AND PROCEDURES

10 CFR 63. 2006 Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. Internet Accessible. [DIRS 176544]

ASME RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.* New York, New York: American Society of Mechanical Engineers. TIC: 255508. [DIRS 167891]

APPENDIX A

DETAILS OF EXAMPLE APPLICATIONS

EXAMPLE 1

Credit for Extreme Wind and Missile Penetration Resistance

The external events hazard analysis could not screen out tornadoes as a credible hazard for the site, although the annual probability of tornadoes is extremely small in Nevada, and in the 1-degree and 5-degree latitude-longitude box that the site resides within. Using regional statistical data for tornadoes and a screening criterion of frequency of exceedance of 1×10^{-6} per year, an analysis was performed to determine a maximum wind speed of 189 mph (translational and rotational). Furthermore, a probabilistic analysis was performed to estimate the probability that a tornado-generated missile would strike at least one important to safety (ITS) structure on the site.

Following the precedent for licensing of nuclear power plants in accordance with NUREG-0800, and associated Regulatory Guides, the maximum tornado wind speed (translational and rotational) and tornado missile spectrum was defined as part of the Nuclear Safety Design Basis. The structural design proceeds in accordance with applicable codes and standards, wherein wind loading is combined with other known and potential loads to determine the bounding design conditions, and the appropriate design margins and material properties.

For purposes of this example, it is assumed that the partial safety factor approach to structural design ensures reliability index β exceeds 3 and, therefore, the conditional probability of failure (given the design-basis wind) is at least 0.001 for structures in normal commercial application. For an ITS structure, a reliability index greater than 3 may be assumed. In as much as the design basis wind for ITS structures of the repository is based on a frequency of exceedance of 1×10^{-6} per year, the joint probability of having significant damage to a concrete ITS structure and potentially initiating an event sequence is significantly less likely than 1×10^{-6} per year, and may be screened out.

Design against missile penetration follows the guidance from NUREG-0800 (NRC, 1996), which specifies the minimum concrete thickness that is accepted as an adequate barrier for the specified missile spectrum. It is specified in NUREG-0800 (Section 3.5.3) that for Region III, a concrete thickness of 6 inches is sufficient to prevent perforation. However, other design considerations, such as seismic, mandate the concrete wall thickness to be greater than 2 feet, which greatly exceeds (by a factor of more than 4) the minimal values cited in NUREG-0800.

With a margin of safety greater than 4 and typical coefficient of variations (Vs), the load-resistance factor model would indicate the conditional probability of perforation of such a wall, given the impact of a tornado missile is much less than 0.001; coupled with the fact that the frequency of exceedance for a tornado that could generate heavier or faster missiles was selected to be at the Category 2 screening level of 1×10^{-6} per year, it is concluded that the joint probability of generating a tornado missile, striking a concrete ITS structure, and penetrating the concrete is at least an order of magnitude less than $1 \times$

10^{-6} per year (i.e., less than 1×10^{-7} per year), and therefore can be screened out as a potential initiator of an event sequence.

If the estimate of potential event sequence frequency using this coarse-screening approach indicates the frequency can be adequately characterized as being much less than 1×10^{-6} per year, then no additional evaluations would be performed. Otherwise, analyses would be undertaken to characterize a fragility function for either wind loading or tornado missile penetration that would have to be combined probabilistically with a respective hazard function (i.e., annual probability of exceedance) for wind speed and missile energy, respectively. The analysis for establishing a fragility function is similar to that used in the PCSA seismic analysis.

REFERENCE

NRC (U.S. Nuclear Regulatory Commission) 1996. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Draft Report for Comment.* NUREG-0800. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 255324. [DIRS 177328]

EXAMPLE 2

Structural Reliability Estimate Under Tornado Conditions

Tornados damage buildings in three ways: direct wind forces as expressed as dynamic pressure, external low static pressure associated with rotational storms, and wind generated missile impact. Wind generated missiles are debris on the site that may be picked up by the wind and thrust at a structure. This example treats dynamic pressure owing to winds passing by and over a small building. Of particular interest is the probability of damage associated with the spectrum of tornado wind speeds.

Wind speed induced pressure (called dynamic pressure) is characterized by:

$$P_w = \tfrac{1}{2}\rho V^2 \qquad \text{(B-1)}$$

where, P_w = pressure; ρ = air density; and V = wind velocity relative to the building.

The probability of failure is given by the resistance/load interference integral given in Equation B-2:

$$P_f = \int_0^v F(y)g(y)dy \qquad \text{(B-2)}$$

In Equation B-2, y represents wind speed; g(y) represents the probability density function of the frequency of wind speed; F(y) = the cumulative distribution function for failure given wind speed and is sometimes called the fragility function.

Design basis winds in nuclear power plants in the U.S. are based on tornados because of their greater wind speeds, higher pressure drops, and higher potential to generate missiles. NUREG/CR-4461(Ramsdell, 2005) provides regional and local tornado wind speeds and recurrence intervals. Figure B-1, for example, shows a complementary cumulative distribution function (CCDF-frequency on the y-axis of exceeding the corresponding value on the x-axis) for four large regions in the U.S.

Local maximum tornado wind speeds are provided in NUREG/CR-4461 by longitude and latitude grids. Figure B-2 is an example grid for a recurrence frequencies of 1E-07/year. The Yucca Mountain site is located at approximately 36° N and 115° W. The figure provides the maximum tornado wind speed for the 2° cell in which the site is located.

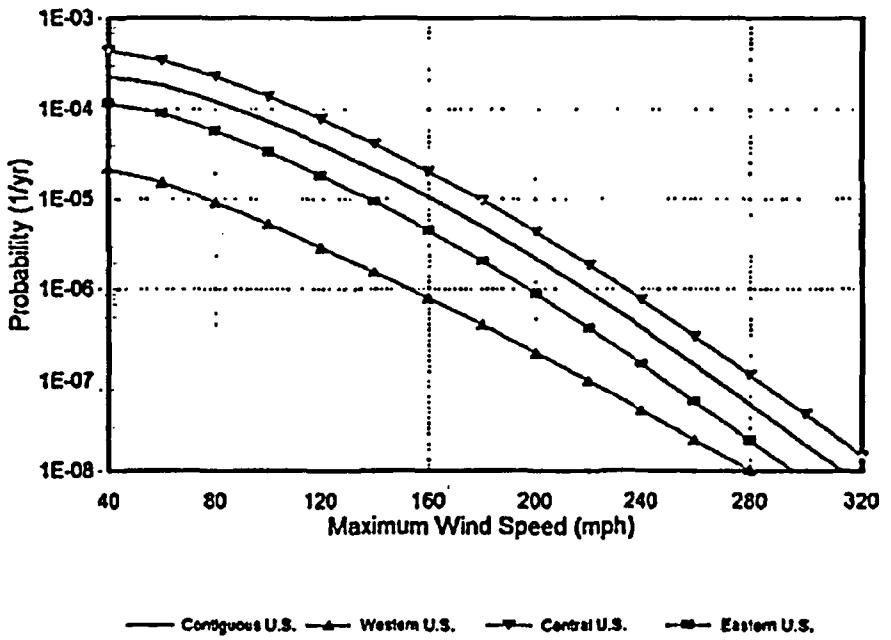

Figure B-1. Regional Tornado Exceedance Frequencies vs. Wind Speed

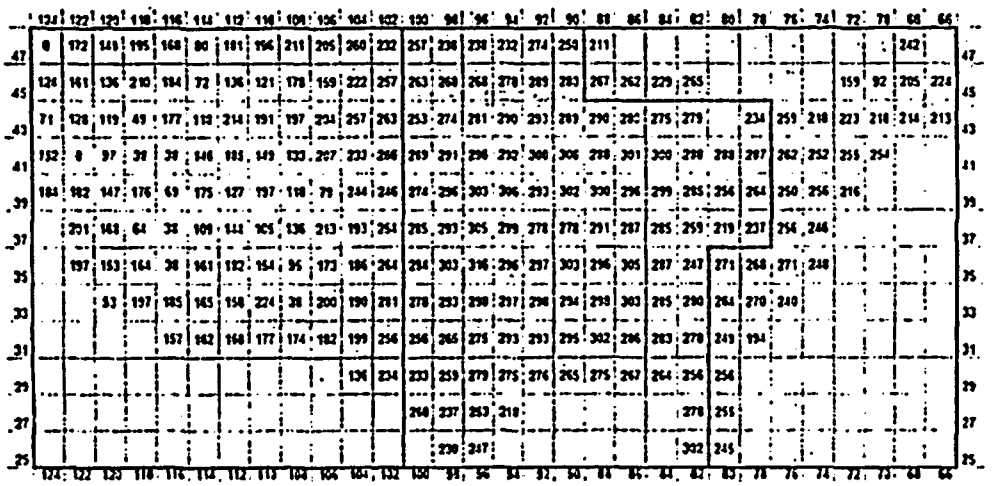

Figure B-2. Maximum Tornado Wind Speeds with a 1E-07/year Probability of Occurrence

Hazard Function

For this example, the western regional CCDF is used from Figure B-1. The hazard function is the cumulative distribution function of pressure (as a function of wind speed)

vs. frequency. It is developed by combining the western regional curve of Figure B-1 with Equation B-1. The results are tabulated in Table B-1.

Table B-1. Hazard Function: Cumulative Frequency of Pressure Generated by Tornado Wind

Exceedance Frequency (/year)	Wind Generated Pressure (psi)
2.0E-05	0.03
1.5E-05	0.06
1.0E-05	0.11
7.0E-06	0.18
3.0E-06	0.25
1.5E-06	0.35
8.0E-07	0.45
4.0E-07	0.57
2.0E-07	0.71
1.0E-07	0.86
5.0E-08	1.02
3.0E-08	1.20
1.0E-08	1.39

Fragility Function

The fragility function represents the conditional probability of failure given a pressure. This example uses a generic fragility for 10-inch thick reinforced concrete walls provided by IAEA NS-G-1.5 (IAEA, 2003). This standard provides a median capacity, *m*, and the high confidence of low probability of failure (HCLPF) of 3.9 psi and 2.0 psi, respectively. IAEA Standard defines HCLPF as the 1 percent probability of failure with 50% confidence.

One can define a lognormal standard deviation, typically denoted by β for a composite fragility curve. It is also typical to assume a lognormal variation of capacity. The following relationship among the median, HCLPF value and lognormal standard deviation allows a solution for β:

$$\beta = -\ln(HCLPF / m) / 2.326 \qquad \text{(B-3)}$$

In Equation B-3, the constant –2.326 is the 1% value of the cumulative normal distribution.

Using Equation B-3 with the values for m and HCLPF provides a lognormal fragility curve, shown in Figure B-3. It is generated by a lognormal distribution with a lognormal standard deviation of β and a lognormal median of $\ln(m)$.

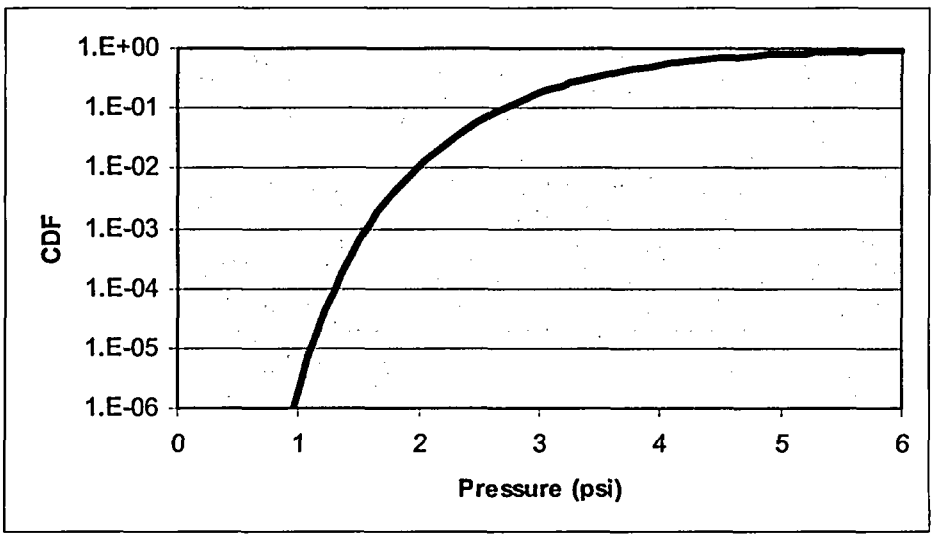

Figure B-3. Example Reinforced Concrete Fragility Curve

Failure Probability

Equation B-2 prescribes integrating the product of the fragility cumulative distribution function with the probability density function for wind speed. The latter is the derivative of the hazard function shown in Table B-1. This is easily done numerically to obtain a failure probability associated with dynamic pressure of much less than 1E-06/year. By comparing Figure B-3 with Table B-1, it is seen that the dynamic pressure of a 280 mph wind has a low probability of failing a reinforced concrete building.

REFERENCES

Ramsdell J.V., Jr. 2005. *Tornado Climatology of the Contiguous United States*, NUREG/CR-4461, Rev. 1, Washington D.C.: U.S. Nuclear Regulatory Commission. ACC: MOI. 20050711.0016. [DIRS 174119]

IAEA (International Atomic Energy Agency) 2003. *External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide.* IAEA Safety Standards Series No. NS-G-1.5. Vienna, Austria: International Atomic Energy Agency. [DIRS 177342]