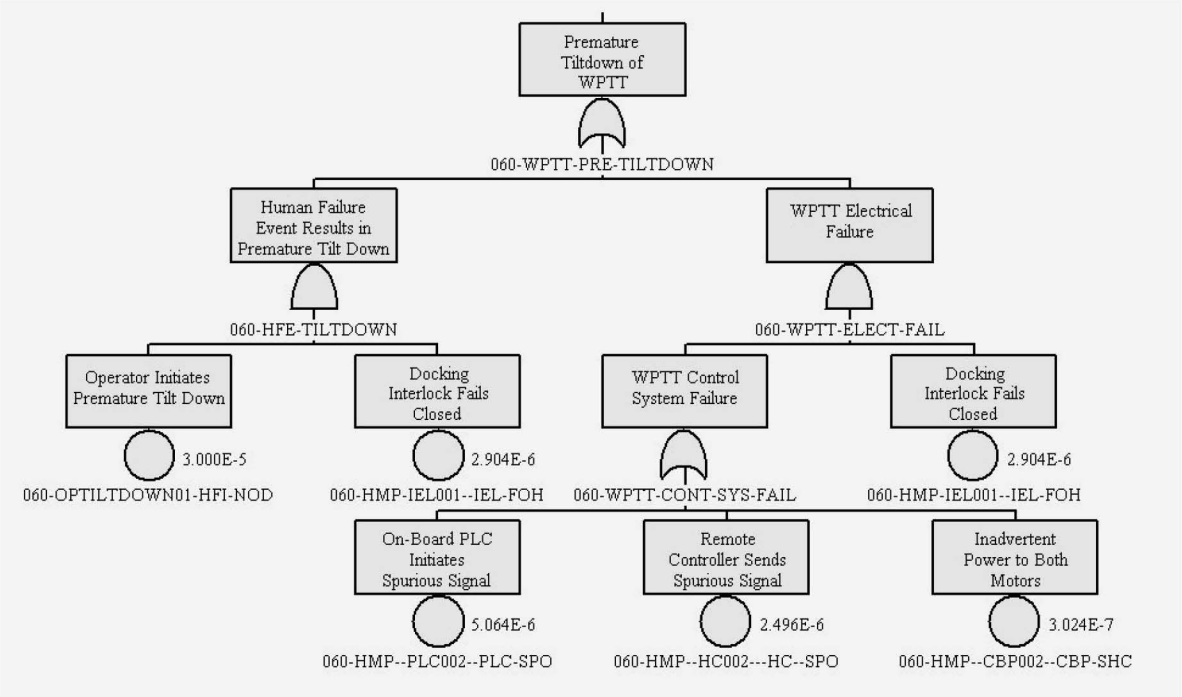


NOTE: This fault tree is presented for illustrative purposes only and is not intended to represent results for the present analysis.

PLC = programmable logic controller; WPTT = waste package transfer trolley.

Source: Original

Figure 4.3-7. Example Fault Tree

As the name implies, fault tree events are usually failures or faults. Fault trees use logic or Boolean gates. Figure 4.3-7 shows two types of gates: the AND gate (mound shaped symbol with a flat bottom) and the OR gate (mound shaped symbol with a concave bottom). An AND gate passes an output up the tree if all events immediately attached to it occur. An OR gate passes an output up the tree if one or more events immediately attached to it take place. An AND gate often implies components or system features that back each other up; if one fails, the other continues to perform the function adequately. The success criterion of the SSC or equipment being analyzed is important in determining the appropriate use of gates.

The bottom level of the fault tree contains events with bubbles beneath them indicating a *basic event*. Basic events are associated with frequencies from industry-wide active equipment reliability information, passive equipment failure analysis, or human reliability analysis.

Fault trees are Boolean reduced to minterm form, which expresses the top event in terms of the union of minimal cut sets. Minimal cut sets, which are groups of basic events that must all occur to cause the top event in the fault tree, result from applying the Boolean Idempotency and Absorption laws. Fault tree analysis, as used in the PCSA, is well described in the *Fault Tree Handbook*. NUREG-0492 (Ref. 2.2.87). Each minimal cut set represents a single basic event or a combination of two or more basic events (e.g., a logical intersection of basic events) that could result in the occurrence of the event sequence. 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). Section 4.3.6 continues the discussion about utilization of minimal cut sets in the quantification of event sequences.

As illustrated in Figure 4.3-7, the organization of the fault trees in the PCSA is developed to emphasize two primary elements, which together result in the occurrence of the top event: (1) human failure events, and (2) equipment failures. The human failure events include postulated unintended crew actions and omissions of crew actions. Identification and quantification of human failure events (HFEs) are performed in phases. Initial identification of HFEs led to design changes to either eliminate them or reduce the probability that they would cause the fault tree top event. For example, Figure 4.3-7 shows an HFE logically intersected with an electro-mechanical interlock such that both a crew error of commission and failure of the interlock must occur for premature WPTT tiltdown to occur.

Event trees and fault trees are complementary techniques. Often used together, they map the system response from initiating events through damage levels. Together, they delineate the necessary and sufficient conditions for the occurrence of each event sequence (and end state). Because of the complementary nature of using both inductive and deductive reasoning processes, combining event trees and fault trees allow more comprehensive, concise, and clearer event sequences to be developed and documented than using either one exclusively. The selection of and division of labor among each type of diagram depends on the analyst's opinion. In the PCSA, the choice was made to develop event trees along the lines of major functions such as crane lifts, waste container containment, HVAC and building confinement, and introduction of moderator. Fault trees disaggregate these functions into equipment and component failure modes for which unreliabilities or unavailabilities were obtained.

4.3.2.2 Passive Equipment Failure Analysis

Passive equipment (e.g., transportation casks, storage canisters, waste packages) may fail from manufacturing defects, material variability, defects introduced by handling, long-term effects such as corrosion, and normal and abnormal use. Industry codes, such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.5) and Section III, Subsection NCA of *ASME Boiler and Pressure Vessel Code* (Ref. 2.2.7) 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 Section III, Subsection NCA of the *ASME Boiler and Pressure Vessel Code* (Ref. 2.2.7) 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 approach used in the PCSA takes advantage of the design margins (or factor of safety).

The development of code requirements for minimum design loads in buildings and other structures in the late 1970s considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures* (Ref. 2.2.50). 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 are characterized by Equation 5:

$$g(x_1,x_2,\ldots x_i,\ldots x_n) = 0 \qquad \text{(Eq. 5)}$$

In Equation 5, 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 Equation 6:

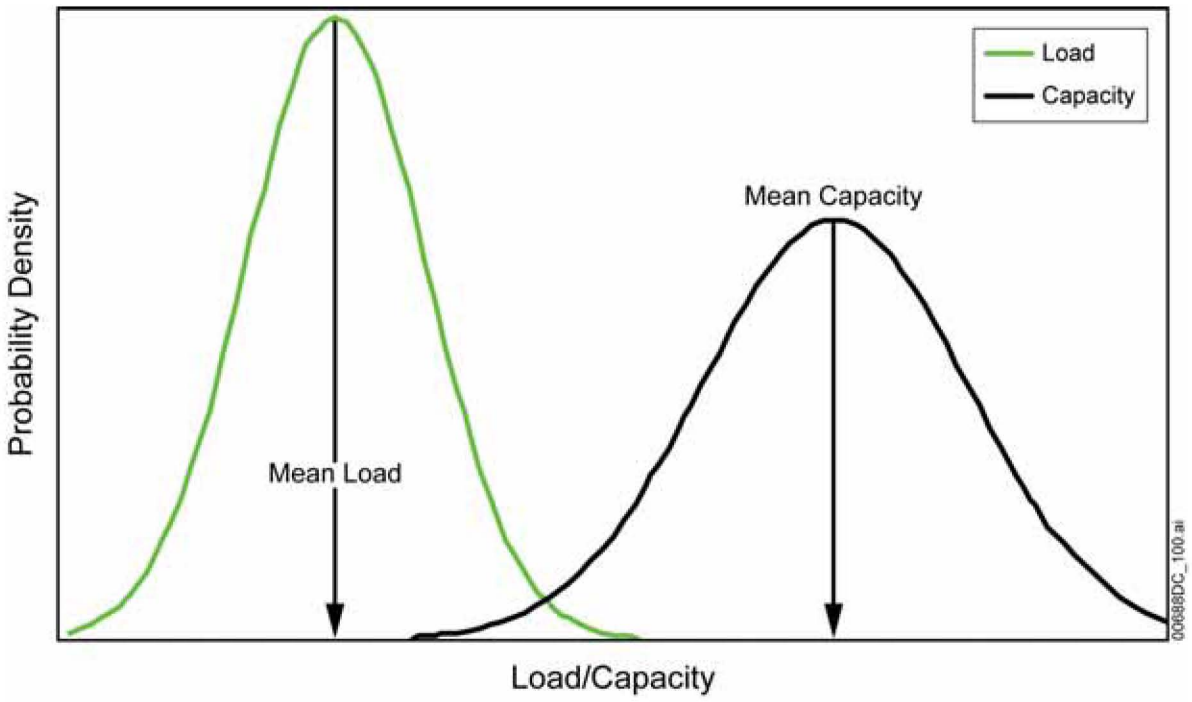
$$P_f = \int \ldots \int f_x(x_1, x_2, \ldots x_i \ldots x_n) dx_1 dx_2 \ldots dx_n \qquad \text{(Eq. 6)}$$

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 4.3-8. Codes and standards such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.5), guide the process of designing structures such that there is a margin, often called a factor of safety, between the load and capacity. 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. A heuristic measure of the factor of safety is the distance between the mean values of the two curves.

In the case in which Equations 5 and 6 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 7.

$$P_f = \int F(y)h(y)dy \qquad \text{(Eq. 7)}$$

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 7, $F(y)$ represents the cumulative density function (CDF) of structural capacity and $h(y)$ represents the probability density function of the load. The former is sometimes called the fragility function and the later is sometimes called the hazard function.



Source: Original

Figure 4.3-8. Concept of Uncertainty in Load and Resistance

To analyze the probability of breach of a dropped canister, y is typically in units of strain, F is typically a fragility function, which provides the conditional probability of breach given a strain; and h is the probability density function of the strain that would emerge from the drop. For seismic risk analysis, h represents the seismic motion input, y is in units of peak ground acceleration, and F is the seismic fragility. The seismic analysis of the YMP structures is documented separately in *Seismic Event Sequence Quantification and Categorization* (Ref. 2.4.4). Degradation of shielding owing to impact loads uses a strain to failure criterion within the simplified approach of Equation 8, described below. For analysis of the conditional probability of breach owing to fires, y is temperature, F is developed from fire data for non-combustible structures, and h is developed using probabilistic heat transfer calculations. Analysis for heating up casks, canisters, and waste packages associated with loss of building forced convection cooling was similarly accomplished, but Equation 8 was used.

If load and capacity are known, then Equations 6 and 7 provide a single valued result, which is the mean probability of failure. Each function in Figure 4.3-8 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.

In the PCSA, the capacity curve for developing the fragility of casks and canisters against drops was constructed by a statistical fit to tensile elongation to failure tests (Ref. 2.2.39). The load curve may be constructed by varying drop height. A cumulative distribution function may be fit to a locus of points each of which is the product of drop height frequency and strain given drop height.

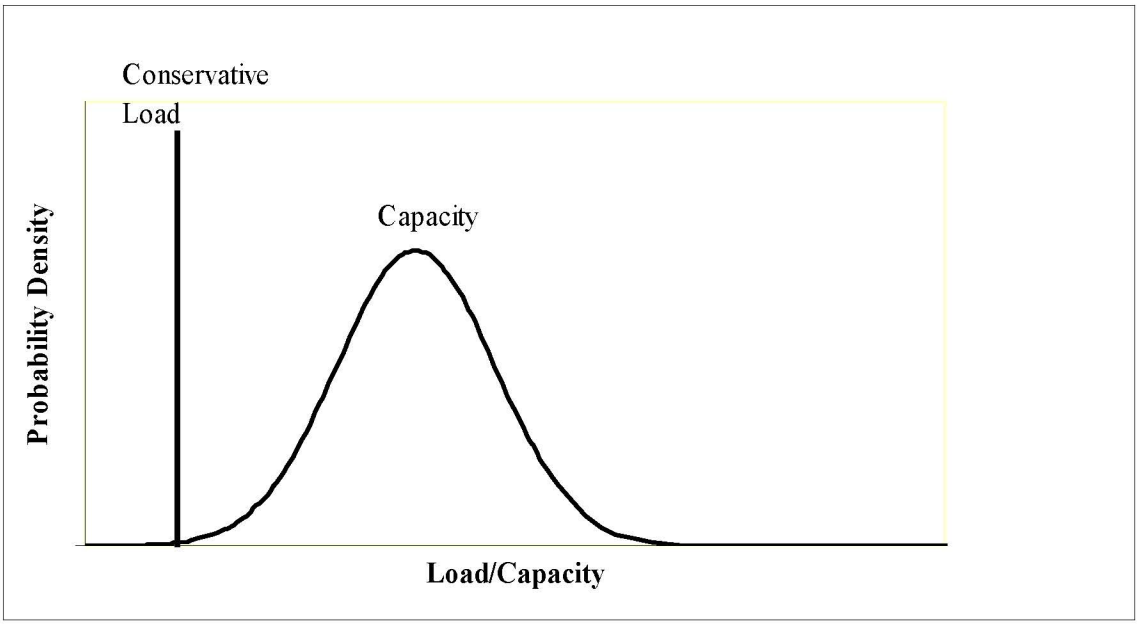
Impact Events Associated with Containment Breach

A simplification of Equation 7, consistent with *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73), and shown in Equation 8, is used in the PCSA. It is illustrated in Figure 4.3-9.

$$P_f = \int_0^h F(y)dy \qquad \text{(Eq. 8)}$$

In Equation 8, h is a single value conservative load.

The load is a single value estimated by performing a calculation for a condition more severe than the mean. For example, if the normal lift height of the bottom of a canister in a handling facility 23 feet, a drop height of 32.5 feet is more severe and may be conservatively applied to all drop heights equal to or below this height. This can be conservatively applied to all drop heights equal to or below this height, such as for the maximum drop heights for the transport and emplacement vehicle (TEV). The conditional probability of breach is an increasing function of drop height. Strain resulting from drops is calculated by dynamic finite element analysis using Livermore Software–Dynamic Finite Element Program (LS-DYNA) for canisters and transportation cask drops (Ref. 2.2.39). Therefore, use of a higher than mean drop height for the load for all drop heights, results in a conservative estimate of breach probability. As an additional conservatism, a lower limit of breach probability of 1E-05 was placed on drops of casks, canisters, and waste packages. To perform the analyses, representative canisters and casks were selected from the variety of available designs in current use which were relatively thin walled on the sides and bottom. This added another conservative element.



Source: Original

Figure 4.3-9. Point Estimate Load Approximation Used in PCSA

The PCSA applies PEFAs to a wide variety of event sequences including those associated with:

- Canister drops
- Canister collisions with other objects and structures
- Other objects dropped on canisters
- Transportation cask drops and subsequent slap-downs (analyzed without impact limiters)
- Conveyance derailments and collisions when carrying transportation casks and canisters (conveyances would be trucks, railcars, cask transfer trolley, and site transporters)
- Other objects dropped on transportation casks
- Waste package drops
- Waste package collision with other waste packages
- TEV collisions with structures and another TEV when carrying a waste package
- Objects dropped on waste packages
- Objects dropped on TEV.

Many of these, such as collisions, derailments, and objects dropped onto casks/canisters, involve far lower energy loads than drop events. For impact loads that are far less energetic than drops, the drop probability is ratioed by impact energy to estimate the less energetic situation.

Shielding Degradation Events

Impact loads (such as drops) may not be severe enough to breach a transportation cask, but might lead to degradation of shielding such that onsite personnel are exposed. The waste package does not provide shielding; worker protection from direct radiation is provided by the TEV. In this analysis, the TEV is considered to function as a transportation cask in providing shielding protection, and thus, all discussions regarding transportation cask shielding is applicable to the TEV shielding function. According to *Conceptual Shielding Study for Transport Emplacement Vehicle* (Ref. 2.2.13, Table 1, Configuration B), the TEV shielding consists of a steel shell with a sandwich of depleted uranium and polymer. This shielding is similar to the steel/depleted uranium truck cask noted below.

The shielding degradation analysis is based primarily on results of finite-element modeling (FEM) performed for, four generic transportation casks types for transportation accidents as reported in NUREG/CR-6672 (Ref. 2.2.83). The results of the FEM analysis were used to estimate threshold drop heights and thermal conditions at which loss of shielding (LOS) may occur in repository event sequences. The four cask types include steel monolith rail cask, steel/depleted uranium truck cask, steel/lead/steel (SLS) truck cask and SLS rail cask. The study performed structural and thermal analyses for both failure of containment boundaries and LOS for accident scenarios involving rail cask and truck cask impacting unyielding targets at various impact speeds from 30 mph to greater than 120 mph. Impact orientations included side, corner, and end. The study also correlated the damage to impacts on real targets, including soil and concrete.

NUREG/CR-6672 (Ref. 2.2.83) addresses two modes of shielding degradation in accident scenarios: Deformations of lid and closure geometry that permit direct streaming of radiation; and/or reductions in cask wall thickness, or relocation of the depleted uranium or lead shielding. The shielding degradation due to lid/closure distortion can be accompanied by air-borne releases if the inner shell of the cask is also breached.

The structural analyses do not credit the energy absorption capability of impact limiters. Therefore, the results are deemed applicable to approximate the structural response of transportation and similar casks in drop scenarios.

Principal insights reported in NUREG/CR-6672 (Ref. 2.2.83) are the following:

- Monolithic steel rail casks do not exhibit any shielding degradation, but there may be some radiation streaming through gaps in closures in any of the impact scenarios. This result can be applied to both transportation casks.

- Steel/depleted uranium/steel truck cask exhibited no shielding degradation, explained by modeling that included no gaps between forged depleted uranium segments so that no displacement of depleted uranium could occur.

- The SLS rail and truck casks exhibit shielding degradation due to lead slumping. Lead slump occurs mostly on end-on impact, with a lesser amount in corner orientation. For side-on orientation, there is no significant reduction in shielding.

Since the TEV shielding construction is similar to the steel/depleted uranium truck cask, no shielding degradation would occur following an impact to the TEV under similar conditions listed in the study.

Fire Events Associated with Possible Containment Breach

Fire initiated events are included in the PCSA, which probabilistically analyzes the full range of possible fires that can occur, as well as variations in the dynamics of the heat transfer and uncertainties in the failure temperature of the target. This analysis focuses on fires that might directly impact the integrity of cask, canister, and waste package containment. Equation 7 is used for this purpose. The fragility analysis includes the uncertainty in the temperature that containment will be breached, and the uncertainty in the thermal response of the canister to the fire. In calculating the thermal response of the canister, variations in the intensity and duration of the fire are considered along with conditions that control the rate of heat transfer to the container, e.g., convective heat transfer coefficients, view factors, emissivities, etc. In calculating the failure temperature of the canister, variations in the material properties of the canister are considered, along with variations in the loads that lead to failure. The load or demand is associated with uncertainty in the fire severity.

Fire severity is characterized by the fire temperature and duration, since these factors control the amount of energy that the fire could transfer to a cask, canister, or waste package. (In this analysis, these are referred to as targets.) The duration of the fire is taken to be the amount of time a particular container is exposed to the fire, and not necessarily the amount of time a fire burns. Probability distributions of the fire temperature and fire duration are based on the unavailability of manual or automatic fire suppression, which leads to an assessment that significantly overstates the risk of fires.

4.3.2.2.1 Uncertainty in Fire Duration

An uncertainty distribution for the fire duration is developed by considering test data and analytical results reported in several different sources; some specific to the YMP facilities and some providing more generic information. In general, the fire durations are found to depend upon the amount, type, and configuration of the available combustible material.

Based on a review of the available information, it is determined that two separate uncertainty distributions would be needed: one for conditions without automatic suppression and one for conditions with automatic suppression. The derivation of these two distributions is discussed below.

Uncertainty in fire duration was developed from:

- *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. 2.2.85)

- *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report.* NUREG/CR-4680 (Ref. 2.2.64)

- *Quantitative Data on the Fire Behavior of Combustible Material in Nuclear Power Plants: A Literature Review.* NUREG/CR-4679 (Ref. 2.2.65).

The derivation of the distribution of fire duration is described in Attachment D, Sections D2.1.1.2 and D2.1.1.3.

The fire temperature used in this calculation is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. 2.2.78, p. 2-56). Fires within a YMP facility may involve both combustible solid and liquid materials. A probability distribution for the fire temperature was derived by combining fire severity information for compartment fires discussed in *SFPE Handbook of Fire Protection Engineering* (Ref. 2.2.78, Section 2, Chapter 2) with information about liquid hydrocarbon pool fires (Ref. 2.2.2) and (Ref. 2.2.78, p. 2-56). The derivation of this distribution is described in Attachment D, Section D2.1.2. The fire temperature is normally distributed with a mean of 1,072 K (799°C) and a standard deviation of 172 K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C specified in 10 CFR 71.73 (Ref. 2.3.3).

Fire temperature and duration are negatively correlated. Intense fires with high fire temperatures tend to be short-lived because the high temperature results from very rapid burning of the combustible material. In determining the joint probability distribution of fire duration and temperature, a negative correlation coefficient of –0.5 was used (Attachment D, Section D2.1.3).

The thermal response of the canister is calculated using simplified radiative, convective, and conductive heat transfer models, which have been calibrated to more precise models. The simplified models are found to accurately match predictions for heating of the canister in either a cask or waste package. The heat transfer models are simplified in order to allow a probabilistic analysis to be performed using Monte Carlo sampling. The models consider radiative and convective heat transfer from the fire to the canister, cask, waste package, or shielded bell. This analysis conservatively models the fire completely engulfing the container.

When calculating the heat load on the target for a fully engulfing fire, radiation is the dominant mode of heat transfer between the fire and the target. The magnitude of the radiant heating of the container depends on the fire temperature, the emissivity of the container, the view factor between the fire and the container, also the duration of the fire.

The total radiant energy deposited in the container can be roughly estimated using Equation 9:

$$Q_{rad} = \varepsilon F_{cf} \sigma (T_{fire})^4 At \qquad \text{(Eq. 9)}$$

where

Q_{rad} = incident radiant energy over the fire duration (J)

ε = emissivity of the container

F_{cf} = container-to-fire view factor

σ = Stefan-Boltzmann constant ($W/m^2 K^4$)

T_{fire} = equivalent blackbody fire temperature (K)

A = container surface area (m^2)

t = duration of the fire (sec)

The following variables in this equation are treated as uncertain: fire temperature, view factor, and fire duration. In the case of a canister inside a waste package, cask, or shield bell, a more complicated set of equations is used to simulate outer shell heat up and subsequent heat transfer to layers of containment or shielding and then to the canister itself. The model also includes heating of the canister by decay heat from the spent fuel or high-level radioactive waste.

To estimate the uncertainty associated with target fragility, two failure modes were considered:

1. *Creep-Induced Failure.* Creep is the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load. This mode of failure is possible for long duration fires.

2. *Limit Load Failure.* This failure mode occurs when the load exerted on a material exceeds its structural strength. As the temperature of the canister increases in temperature, its strength decreases. Failure is generally predicted at some fraction (usually around 70%) of the ultimate strength.

Failure is considered to occur when either of the failure thresholds is exceeded.

Equation 7, along with the heat transfer equations, are solved using Monte Carlo simulation (described in Section 4.3.7) with the above described fragility and target fire severity probability distributions, and distributions for the uncertain heat transfer factors. For each Monte Carlo trial, the calculated maximum canister temperature is compared to the sampled target failure temperature. If the maximum temperature of the target exceeds the sampled failure temperature, then target failure is counted. The failure probability in this method is equal to the fraction of the samples for which failure is calculated.

Uncertainty in the calculated canister failure probability is given by a calculated mean and standard deviation, where the mean is simply the number of failures divided by the total number of samples and the standard deviation is given by Equation 10 for the standard deviation of a binomial distribution:

$$\sigma = \sqrt{\frac{\frac{n_{fail}}{N}\left(\frac{N - n_{fail}}{N}\right)}{N}} \qquad \text{(Eq. 10)}$$

where n_{fail} is the number of trials in which failure occurs and N is the total number of Monte Carlo trials.

Fire Event Associated with Shielding Degradation

The thermal analyses in NUREG/CR-6672 (Ref. 2.2.83) indicates that the probability of shielding degradation in a fire scenario should be based on the probability of having a fire that is equivalent to a 1,000°C engulfing fire that lasts for more than a half-hour. However, TEV shielding degradation does not occur unless the depleted uranium layer is broken into pieces and drops out of the steel shell. Although TEV gamma radiation shielding provided by depleted uranium layer is expected to remain in place, the neutron shielding provided by the polymer layer would be destroyed and considered a loss under fire scenario. As a result, it is conservatively considered that TEV shielding function would be a loss under fire scenarios.

4.3.3 Utilization of Industry-Wide Reliability Data

4.3.3.1 Use of Population Variability Data

The quantification of event sequence probabilities via event tree and fault tree modeling requires information on the reliability of active equipment and components, as usually represented in fault tree basic events. The PCSA attempts to anticipate event sequences before they happen, which means that associated equipment reliabilities are uncertain.

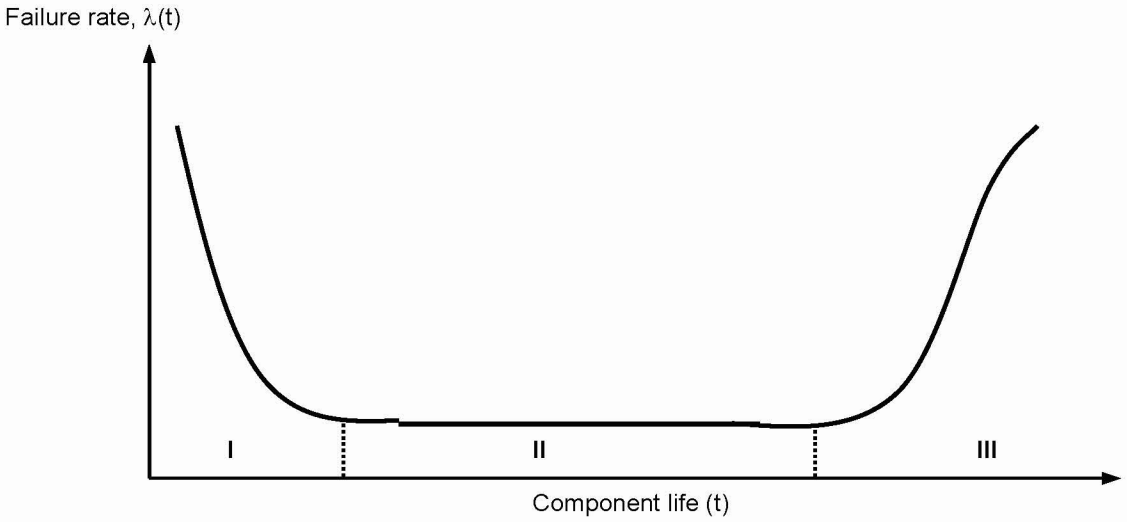
As presented in NUREG-0492 (Ref. 2.2.87, Figure X-8, p. X-23), the typical model of failure probability for a component is depicted as a "bathtub curve" illustrated in Figure 4.3-10. The curve is divided into three distinct phases. Phase I represents the component failure probability during the "burn-in" 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.

As is usually done in PRA, the PCSA uses Phase II because Phase I failures are identified by burn-in testing of equipment before repository operations occur and Phase III failures are eliminated by preventive maintenance which includes manufacturer recommended replacement intervals. In Phase II, 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 in Equation 11:

$$P_F(\lambda,t_m) = 1 - \exp(-\lambda t_m) \quad \text{(Eq. 11)}$$

When the product λt_m is small (<0.1), the failure probability may be calculated by the following Equation 12 approximation, which introduces less than a 10% error:

$$P_F(\lambda,t_m) \cong \lambda t_m \quad \text{(Eq. 12)}$$



Source: NUREG-0492 (Ref. 2.2.87, Figure X-8, p. X-23)

Figure 4.3-10. Component Failure Rate "Bathtub Curve" Model

The PCSA also uses the concept of unavailability to estimate basic event probabilities. This applies to standby equipment such as the emergency diesel generators and fire suppression. 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 shown in Equation 13:

$$q_d(\lambda,\tau) = \tfrac{1}{2}(\lambda\tau) \qquad \text{(Eq. 13)}$$

In this model the component failure rate is constant 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.

Failure on demand is also needed for equipment, such as cranes, that is challenged in discrete steps. 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.

Information about hardware failure is characterized as one of the following:

1. Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (e.g., operational experience).

2. Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (e.g., test data).

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 (e.g., another program's test data or data from handbooks or compilations).

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

The YMP repository has not yet operated, and test information on prospective equipment has not yet been developed. It is assumed that equipment and SSCs designed and purchased for the Yucca Mountain repository will be of the population of equipment and SSCs represented in U.S. industry-wide reliability information sources (Assumption 3.2.1). Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population. Attachment C contains the list of industry-wide reliability information sources used in the PCSA.

The lack of actual operating experience, the use of industry-wide data, and the consideration of uncertainties (Ref. 2.2.73) suggested that a Bayesian approach was appropriate for the PCSA. A Bayesian approach and the use of judgment in expressing the state-of-knowledge of basic event unreliability is a well-recognized and accepted practice (Ref. 2.2.59, Ref. 2.2.9, and Ref. 2.2.66). Furthermore, *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* includes the use of engineering judgment, supported by sufficient technical basis, as a means of justifying reliability estimates for certain SSCs (Ref. 2.2.73).

Let λ_j be one failure rate of a set of possible failure rates of a component and E be a new body of evidence. Knowledge of the probability of λ_j given E, is represented by $P(\lambda_j/E)$. For a failure rate, frequency, or probability of active equipment, Bayes' theorem is stated as follows in Equation 14:

$$P(\lambda_j / E) = \frac{P(\lambda_j)L(E / \lambda_j)}{\sum_j P(\lambda_j)P(E / \lambda_j)} \qquad \text{(Eq. 14)}$$

In summary, this states that the knowledge of the "updated" probability of λ_j, given the new information E, equals the "prior" probability of λ_j, before any new information, times the likelihood function, $L(E/\lambda_j)$. The likelihood function is a probability that the new information really could be observed, given the failure rate λ_j . The numerator in Equation 14 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of λ_j equals unity. If there is actual operational experience available, then the steps in an application of Bayes' theorem would be as follows: (1) estimate the prior probability using one or more of the four reliability data types; (2) obtain new information in the form of tests or experiments; (3) characterize the test information in the form of a likelihood function; and (4) perform the calculation in accordance with Equation 14 to infer the updated probability.

The PCSA used industry-wide reliability data to develop Bayesian prior distributions for each active equipment/component failure mode in the fault trees. Updates per Equation 14 will await actual test and operations. The following summarizes the methods used to develop the Bayesian prior distributions.

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution, *g*, representing the source-to-source variability, also called population variability, of the component reliability (Ref. 2.2.9, Section 8.1). In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. The population-variability distributions developed in this analysis attempt to encompass the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the PCSA. As indicated in "Bayesian Parameter Estimation in Probabilistic Risk Assessment" (Ref. 2.2.79, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

Applying the parametric empirical Bayes method requires first, to categorize the reliability data sources into two types: those that provide information on exposure data, (i.e., the number of failures that were recorded over an exposure time (in case of a failure rate)), or over a number of demands (in case of a failure probability), and those that do not provide such information. In the latter case, reliability estimates for a failure rate or failure probability are provided in the form of a mean or a median value, along with an uncertainty estimate, typically an error factor.

For each data source, the reliability information about a component's failure rate or failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. 2.2.79, Section 4.2). When no exposure data is available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution (Ref. 2.2.79, Section 4.4) and (Ref. 2.2.57, pp. 312, 314, and 315).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. 2.2.9, Section 8.2.1), which have the advantage of resulting in relatively simpler calculations. This technique, however, is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of "The Combined Use of Data and Expert Estimates in Population Variability Analysis" (Ref. 2.2.57, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the

population-variability distribution in its lognormal form is noted $g(x,\nu,\tau)$, where x is the reliability parameter for the component (failure rate or failure probability), and ν and τ, the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided in the latter case that any tail truncation above $x = 1$ has a negligible effect (Ref. 2.2.79, p. 99). The validity of this can by confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1 of Attachment C, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98 % of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

To determine ν and τ, it is first necessary to express the likelihood for each data source as a function of ν and τ only, (i.e., unconditionally on x). This is done by integrating, over all possible values of x, the likelihood function evaluated at x, weighted by the probability of observing x, given ν and τ. For example, if the data source i indicates that r failures of a component occurred out of n demands, the associated likelihood function $L_i(\nu,\tau)$, unconditional on the failure probability x, is as follows in Equation 15:

$$L_i(\nu,\tau) = \int_0^1 Binom(x,r,n) \times g(x,\nu,\tau)dx \qquad \text{(Eq. 15)}$$

where $Binom(x,r,n)$ represents the binomial distribution evaluated for r failures out of n demands, given a failure probability equal to x, and $g(x,\nu,\tau)$ is defined as previously indicated. This equation is similar to that shown in "Bayesian Parameter Estimation in Probabilistic Risk Assessment" (Ref. 2.2.79, Equation 37). If the component reliability is expressed in terms of a failure rate and the data source provides exposure data, the binomial distribution in Equation 15 would be replaced by a Poisson distribution. If the data source provides expert opinion only (no exposure data), the binomial distribution in Equation 15 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine ν and τ (Ref. 2.2.79, p. 101). The maximum likelihood estimators for ν and τ are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each data source (Ref. 2.2.57, Equation 4). To find the maximum likelihood estimators for ν and τ, it is equivalent and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of ν and τ completely determines the population-variability distribution g for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution g, which are calculated using the formulas given in NUREG/CR-6823 (Ref. 2.2.9, Section A.7.3). Specifically, the mean of the

lognormal distribution is equal to $\exp(\nu + \tau^2/2)$ and the error factor is equal to $\exp(1.645 \times \tau)$. A discussion of the adequacy of the empirical Bayes method for the YMP analysis is found in Attachment C.

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom" (Ref. 2.2.54, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between 2×10^{-8}/hr (5th percentile) and 6×10^{-5}/hr (95th percentile), using the definition of the error factor given in NUREG/CR-6823 (Ref. 2.2.9, Section A.7.3), this corresponds to an error factor of $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$. Therefore, in the PCSA, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55, are too diffuse to adequately represent the population-variability distribution of a component. In such instances (i.e., the two cases in the entire PCSA database when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution, and therefore is unaffected by the value taken by the error factor. Based on the NUREG/CR-6823 (Ref. 2.2.9, Section A.7.3), the median is calculated as $\exp(\nu)$, where ν is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the PCSA is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in NUREG/CR-6823 (Ref. 2.2.9, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution, and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using the data source that yields the most diffuse likelihood using one of the two methods described in the next paragraph.

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean, and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data, i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities, the

probability distribution for the reliability parameter is developed through a Bayesian update using Jeffreys' noninformative prior distribution as indicated in NUREG/CR-6823 (Ref. 2.2.9, Section 6.2.2.5.2). This noninformative prior conveys little prior belief or information, thus allowing the data to speak for itself.

4.3.3.2 Dependent Events

Dependent events have long been recognized as a concern for those responsible for the safe design and operation of high-consequence facilities because these events tend to increase the probability of failure of multiple systems and components. Two failure events, A and B, are dependent upon when the probability of their coincidental occurrence is higher than expected if A and B were each an independent event. Dependent events occur from four dependence mechanisms: functional, spatial, environmental, and human:

1. **Functional dependence** is present when one component or system relies on another to supply vital functions. An example of a functional dependence in this analysis is electric power supply to HVAC. Functional dependence is explicitly modeled in the event tree and fault tree logic.

2. **Environmental dependence** is in play when system functionality relies on maintaining an environment within designed or qualified limits. Here, an example is material property change as a result of temperature change. Environmental effects are modeled in the system reliability analyses as modifications (e.g., multiplying factors) to system- and component-failure probabilities and are also included in the passive equipment failure analyses. External events such as earthquakes, lightning strikes, and high winds that can degrade multiple SSCs are modeled explicitly as initiating events and are discussed in other documents ((Ref. 2.2.34) and (Ref. 2.4.4)).

3. **Spatial dependence** is at work when one SSC fails by virtue of close proximity to another. For example, during an earthquake one SSC may impact another because of close proximity. Another example is inadvertent fire suppression actuation which wets SSCs below it. Spatial dependences are identified by explicitly looking for them in the facility layout drawings. Inadvertent fire suppression is modeled explicitly in the event trees and fault trees.

4. **Human dependence** is present when an SSC or function fails because humans intervene inappropriately or failed to intervene. In the YMP, most human errors are associated with initiating events (inadvertent actuation) or are pre-initiator failures (failure to restore after maintenance). The PCSA includes an extensive human reliability analysis which is described later in this section, in Section 6.4 and in Attachment E. The results of the human reliability analysis (HRA) are integrated into the event tree and fault tree models for a complete characterization of event sequence frequency.

4.3.3.3 Common-Cause Failures

Common-cause failures (CCF) can result from any of the dependence mechanisms described above. The term common-cause failure is widely employed to describe events in which the same

cause degrades the function of two or more SSCs that are relied upon for redundant operations, either at the same time or within a short time relative to the overall component mission time. Because of their significance to overall SSC reliability when redundancy is employed, CCFs are a special class of dependent failures that are addressed in the PCSA.

Because CCFs are relatively uncommon, it is difficult to develop a statistically significant sample from monitoring only one system or facility, or even several systems. The development of CCF techniques and data, therefore, rely on a national data collection effort that monitors a large number of nuclear power systems. Typically, the fraction of component failures associated with common causes leading to multiple failures ranges between 1% and 10% ((Ref. 2.2.53), (Ref. 2.2.62), and (Ref. 2.2.58)). This fraction depends on the component; level of redundancy (e.g., two, three, or four); duty cycle; operating and environmental conditions; maintenance interventions; and testing protocol, among others. For example, equipment that is operated in cold standby mode (i.e., called to operate occasionally on demand) with a large amount of preventive maintenance intervention tends to have a higher fraction of CCFs than systems that continuously run.

It is not practical to explicitly identify all CCFs in a fault tree or event tree. Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. 2.2.53), the Multiple Greek Letter method (Ref. 2.2.61), and the Alpha Factor method (Ref. 2.2.62). These methods do not require an explicit knowledge of the dependence failure mode.

The PCSA uses the Alpha Factor method (Ref. 2.2.62), which is summarized below. After identifying potential CCF events from the fault trees, appropriate alpha factors are identified according to the procedure described in NUREG/CR-5485 (Ref. 2.2.62). The general equations for estimating the probability of a CCF event in which k of m components fail are as follows in Equation 16, Equation 17, and Equation 18:

$$Q(k,m) = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad \text{for staggered test} \qquad \text{(Eq. 16)}$$

$$Q(k,m) = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad \text{for non-staggered test} \qquad \text{(Eq. 17)}$$

where α_k denotes the alpha factor for size k, Q_t denotes the total failure probability, and:

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \qquad \text{(Eq. 18)}$$

Industry-wide alpha factors used in the PCSA are taken from NUREG/CR-5801 (Ref. 2.2.60). The process of applying these alpha factors is explained further in Attachment C, Section C3.

4.3.4 Human Reliability Analysis

Human interactions that are typically associated with the operation, test, calibration, or maintenance of an SSC (e.g., drops from a crane when using slings) are implicit in the empirical data. If this is the case, empirical data may be used, provided human errors that cause the SSC failures are explicitly enumerated and determined to be applicable to YMP operations. When this was the case in the PCSA, the appropriate method of Section 4.3.3.1 was applied. Otherwise, an HRA was performed, the methodology of which is summarized in this section. The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6) and incorporates the guidance in HLWRS-ISG-04, *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. 2.2.72). It emphasizes a comprehensive qualitative analysis and uses applicable quantitative models.

The HRA task identifies, models, and quantifies HFEs postulated for YMP operations to assess the impact of human actions on event sequences modeled in the PCSA. YMP operations differ from those of traditional nuclear power plants, and the HRA reflects these differences. Appendix E.IV of Attachment E includes further discussion of these differences and how they influence the choice of methodology.

The overall steps to the PCSA HRA are identification of HFEs, preliminary analysis (screening), and detailed analysis. The HRA task ensures that the HFEs identified by the other tasks (e.g., HAZOP evaluation, MLD development): (1) are created on a basis that is consistent with the HRA techniques used, (2) are appropriately reincorporated into the PCSA (modeled HFEs derived from the previously mentioned PCSA methods), and (3) provide appropriate human error probabilities (HEPs) for all modeled HFEs. The HRA work scope largely depends on boundary conditions defined for it.

4.3.4.1 HRA Boundary Conditions

Unless specifically stated otherwise, the following general conditions and limitations are applied throughout the HRA task. The first two conditions always apply. The remaining conditions apply unless the HRA analyst determines that they are inappropriate. This judgment is made for each individual action considered:

1. Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior, deliberate acts of sabotage, and the like are not considered in this task.

2. All personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard operating procedures is made because the employee believes their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.

3. Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include SNF handling at reactor sites having independent spent fuel storages, chemical

munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the GROA facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.

4. The YMP is initially operating under normal conditions and is designed to the highest quality human factor specifications. The level of operator stress is optimal unless the analyst determines that the human action in question cannot be accommodated in such a manner as to achieve optimal stress.

5. In performing the operations, the operator does not need to wear protective clothing unless it is an operation similar to those performed in comparable facilities where protective clothing is required.

6. The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are to be experienced and have functioned in their present positions for a sufficient amount of time to be proficient.

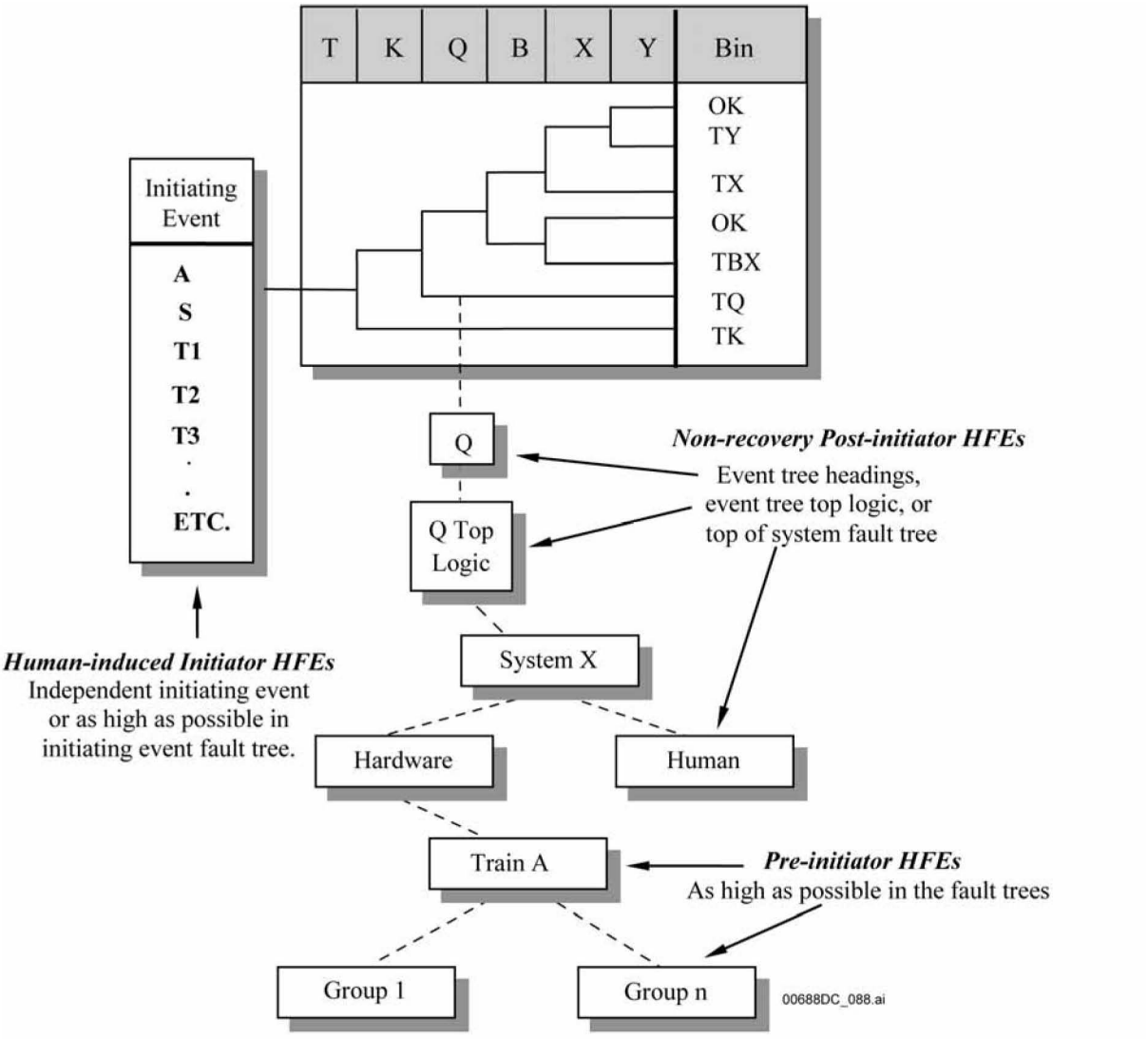
7. The environment inside each YMP facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination, and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made regarding optimal weather conditions.

8. While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

4.3.4.2 HRA Methodology

The HRA consists of several steps that follow the intent of ASME RA-S-2002, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6) and the process guidance provided in *Technical Basis and Implementation Guidelines for Technique for Human Event Analysis (ATHEANA),* NUREG-1624 (Ref. 2.2.70). The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt material that is based on nuclear power plants to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. 2.2.70). Section 10.3 of NUREG-1624 (Ref. 2.2.70) provides an overview of the method for incorporating HFEs into a PRA. Figure 4.3-11 illustrates this integration method.



NOTE: HFE = human failure event.

Source: Original

Figure 4.3-11. Incorporation of Human Reliability Analysis within the PCSA

Step 1: Define the Scope of the Analysis—The objective of the YMP HRA is to provide a comprehensive qualitative assessment of the HFEs that can contribute to the facility's event sequences resulting in radiological release, criticality, or direct exposure. Any aspects of the work that provide a basis for bounding the analysis are identified in this step. In the case of the YMP, the scope is bounded by the design state of the facilities and equipment.

Step 2: Describe Base Case Scenarios—In this step, the base case scenarios are defined and characterized for the operations being evaluated. In general, there is one base case scenario for each operation included in the model. The base case scenario represents the description of expected facility, equipment, and operator behavior for the selected operation.

Step 3: Identify and Define HFEs of Concern—Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then becomes the error-forcing context (EFC) for a specific HFE. As defined by ATHEANA (Ref. 2.2.70), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses. The analyses performed in later steps (e.g., Steps 6 and 7) may identify the need to define additional HFEs or unsafe actions.

Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis—The preliminary analysis is a type of screening analysis used to identify HFEs of concern. This type of analysis is commonly performed in HRA to conserve resources for those HFEs that are involved in the important event sequences. The preliminary quantification process consists of the following subtasks:

1. Identification of the initial scenario context.
2. Identification of the key or driving factors of the scenario context.
3. Generalization of the context by matching it with generic, contextually anchored rankings or ratings.
4. Discussion and justification of the judgments made in subtask 3.
5. Refinement of HFEs, associated contexts, and assigned HEPs.
6. Determination of final preliminary HEP for HFE and associated context.

Once preliminary values have been assigned, the model is run, and HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, that sequence is Category 1 or Category 2 according to the performance objectives in 10 CFR 63.111 (Ref. 2.3.2).

Step 5: Identify Potential Vulnerabilities—This information collection step defines the context for Step 6 in which scenarios that deviate from the base case are identified. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in the HFEs and/or unsafe actions identified in Step 4. The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). The HRA analysts rely on experience in other similar operations.

Step 6: Search for HFE Scenarios—In this step, the analyst must identify deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These deviations are referred to as HFE scenarios. The method for identifying HFE scenarios in the YMP HRA is stated in Step 3. This process continues throughout the event sequence development and quantification. The result is a description of HFE scenarios, including system and equipment conditions, along with any resident or triggered human factor concerns (e.g., PSFs). These combinations of conditions and human factor concerns then become the EFC for a specific HFE.

Step 7: Quantify Probabilities of HFEs—Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with 10 CFR 63.111 performance objectives (Ref. 2.3.2) performance objectives after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CRF 63.111 performance objectives (Ref. 2.3.2). The activities of a detailed HRA are as follows:

- Qualitative analysis (e.g., identification of PSFs, definitions of important characteristics of the given unsafe action, assessment of dependencies)
- Selection of a quantification model
- Quantification using the selected model
- Verification that HFE probabilities are appropriately updated in the PCSA.

The four quantification approaches that are in the PCSA, either alone or in combination, follow:

1. Cognitive Reliability and Error Analysis Method (CREAM) (Ref. 2.2.56)
2. Human Error Assessment and Reduction Technique (HEART) (Ref. 2.2.88)/ Nuclear Action Reliability Assessment (NARA) (Ref. 2.2.43)
3. Technique for Human Error Rate Prediction (THERP) with some modifications (Ref. 2.2.84).

When an applicable failure mode cannot be reasonably found in one of the above methods, then the following HRA method is used:

4. ATHEANA expert elicitation approach (Ref. 2.2.70).

The selection of a specific quantification method for the failure probability of an unsafe action(s) is based upon the characteristics of the HFE quantified. Appendix E.IV of Attachment E provides a discussion of why these specific methods were selected for quantification, as well as a discussion of why some methods, deemed appropriate for HRA of nuclear power plants, are not suitable for application in the PCSA. It also gives some background about when a given method is applicable based on the focus and characteristics of the method.

Step 8: Incorporate HFEs into PCSA—After HFEs are identified, defined, and quantified, they must be reincorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. 2.2.70) provides an overview of the state-of-the-art method for performing this step in PRAs. The term "reincorporated" is used because some HFEs are identified within the fault tree and event tree analysis. All event sequences that contain multiple HFEs are examined for possible dependencies. Figure 4.3-11 shows how the different types of HFEs discussed previously are incorporated into the model based on their temporal phase, which determines where in the model each type of HFE is placed. More detailed discussion of how this is done is provided in Attachment E.

Step 9: Evaluation of HRA/PCSA Results and Iteration with Design—This last step in the HRA is performed after the entire PCSA is quantified. HFEs that ultimately prove to be important to categorization of event sequences are identified. Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is not in compliance with the performance objectives of 10 CFR 63.111 (Ref. 2.3.2) because the probability of a given HFE dominates the probability of that event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or completely eliminate the HFE. An example of such iteration includes the interlocks that ensure that cask lids are securely grappled in a waste handling facility. The interlocks might have a bypass feature when a yoke is attached to a grapple. An operator might fail to void the bypass when attempting to grapple a heavy load. The design changed such that the bypass would automatically be voided (by an electromechanical interlock) as soon as a yoke is attached to a grapple.

4.3.4.3 Classification of HFEs

HFEs are classified to support the HRA preliminary analysis, selection of HRA quantification methods, and detailed quantification. A combination of four classification schemes is used in the YMP HRA. The first three schemes are familiar standards in HRA. The fourth scheme has its basis in behavioral science and has been used in some second-generation HRA methods. The four classification schemes are as follows:

1. The three temporal phases used in PRA modeling:

    A. Pre-initiator
    B. Human-induced initiator
    C. Post-initiator.

2. Error modes:

    A. Errors of omission (EOOs)
    B. Errors of commission (EOCs).

3. Human failure types:

    A. Slips/lapses
    B. Mistakes.

4. Informational processing failures:

    A. Monitoring and detection
    B. Situation awareness
    C. Response planning
    D. Response implementation.

These classification schemes are used in concert with each other. They are not mutually exclusive. The first three schemes have been standard PRA practice; additional information on these three schemes can be found in Section E5.1 of Attachment E. The fourth scheme is summarized below.

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is used for the YMP HRA guidelines is based on the discussion in Chapter 4 of NUREG-1624 (Ref. 2.2.70) and consists of the following elements:

- Monitoring and detection–Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.

- Situation awareness–This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents the operator's understanding of the present situation and their expectations for future conditions and consequences.

- Response planning–This term is defined as the process by which operators decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.

- Response implementation–This term is defined as the activities involved with physically carrying out the actions identified in response planning.

- When there are short time frames for response and the possibility of severely challenging operating conditions (e.g., environmental conditions) exists, then failures in all information processing stages must be considered. Also, slips/lapses and mistakes are considered for each information processing stage. Response implementation failures are expected to dominate the pre-initiator failures that are modeled. Post-initiator failures and failures that initiate event sequences can occur for all information processing stages, although detection failures are likely to be important only for events requiring response in very short time frames.

4.3.5 Fire Analysis

Fire event sequence analysis consists of four parts:

1. Development of fire ignition frequencies for each location in the facility or operations area. These are all called fire initiating event frequencies.

2. Development of the fire severity in terms of both temperature and durations. This was discussed in Section 4.3.2.

3. Development of the conditional probability of fire damaging a cask, canister, or waste package target. This was also discussed in Section 4.3.2.

4. Development of and quantification of fire event sequence diagrams and event trees. Development of the ESDs and event trees was discussed in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40). Quantification of fire event trees is conducted exactly like quantification of any other event tree and is described in Section 4.3, Section 4.3.1, and Section 4.3.7.

This section summarizes the method for the fire initiating event analysis performed as a part of the PCSA. The analysis was performed as part of an integrated analysis of internal fires in the subsurface facilities. This section only discusses those aspects of the fire analysis methodology that apply directly to the analysis for subsurface operations. The full fire analysis and detail on the methods and data are documented in Attachment F to this volume. The fire analysis is subject to the boundary conditions described in the following section.

4.3.5.1 Boundary Conditions

The general boundary conditions used during this analysis are compatible with those described in Section 4.3.10. The principal boundary conditions for the fire analysis are listed below:

- Plant Operational State. Operation initial state conditions are normal with each system operating within its limiting condition of operation limits.

- Number of Fire Events to Occur. Operations are analyzed to respond to one fire event at a given time. Additional fire events as a result of independent causes or of re-ignition once a fire is extinguished are not considered.

- Relationship to Process Buildings. Fires included in the analysis occur outside of the main process buildings. With regard to the frequency of such fires based on historical fire ignition frequencies from other facilities, the fire frequency across the site is proportional to the number of main process buildings (i.e., for the YMP, the waste handling facilities) on the site. That is, the number of opportunities for fires outside buildings is affected by the number of waste handling facilities being serviced. The number of waste handling facilities for the YMP is six: Initial Handling Facility (IHF), Receipt Facility (RF), WHF, and three CRCFs.

- Irrelevancy of Industrial Facility Type to Subsurface Fire Frequency. The frequency of subsurface fires at YMP is expected to be similar to industrial facilities. The specific type of facility, the type of construction of the buildings and other features, are not considered relevant to the frequency of outside fires since the ignition sources that exist outside of the buildings are considered to be generic to any industrial facility. This does not extend to the assessment of fire severity, since the type of facility could affect the type and availability of combustibles. Fire severity is addressed in Attachment D.

- Component Failure Modes. The failure mode of a SSC affected by a fire is the most severe with respect to consequences. For example, the failure mode for a canister could be the over pressurization of a reduced strength canister.

4.3.5.2 Analysis Method

Nuclear power plant fire risk assessment techniques have limited applicability to repository operations in the GROA. The general methodological basis of the PCSA fire analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76). Chemical agent disposal facilities are similar to those in the GROA in that these facilities are handling and disposal facilities for highly hazardous materials. This is a "data based" approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the YMP waste handling facilities. To the extent applicable to a non-reactor facility, NUREG/CR-6850 Volumes 1 (Ref. 2.2.51) and 2 (Ref. 2.2.52) are also considered in the development of this analysis method. The method complies with the applicable requirements of *Fire PRA Methodology* (Ref. 2.2.3) that are relevant to a non-reactor facility. The steps in the analysis are summarized below and described in detail in Attachment F, Section F4.

1. Identification of initiating events. Subsurface fire initiating events for the YMP are considered for the potential for a fire to directly affect the waste containers. The fire analysis therefore, focused on the potential for a fire to directly affect the waste containers. The initiating events for subsurface operations are identified in the event sequence development analysis (Ref. 2.2.40). The steps of this process are detailed below:

   A. Identify subsurface areas where waste containers can be present.

      The processes for the movement of waste forms on site, while outside of buildings, are evaluated and the areas where the waste forms either sit or traverse are identified. Each area where waste can be present, even if only for a brief time, is listed.

   B. Correlate the areas with the National Fire Protection Association (NFPA) historical database for outside fires.

      The NFPA historical database identifies the areas outside buildings where fires have occurred. These have been grouped into broader categories for use in this study.

C. Define initiating events.

Fire ignition occurrences are identified for each outside area where a waste form can be present.

2. Quantification of fire ignition frequency. In order to assess the total fire frequency, two pieces of information are required: the number of facilities and the number of fires at these facilities. The first piece of data is maintained by the U.S. Census Bureau, which conducts an economic census (Ref. 2.2.86). The second piece of data is tracked by NFPA. This approach uses historical data over a 10 year period (1988 to 1997) from these databases. Specifically, the fire data used in this report were taken from a report authored by the NFPA – Division of Fire Analysis and Research on fires in or at industrial chemical, hazardous chemical, and plastic manufacturing plants (Ref. 2.2.1). These data are used to develop estimates for the total frequency of fires and the distribution of fires on the grounds of the facility:

   A. *Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Facilities: 1988 – 1997 Unallocated Annual Averages and Narratives* (Ref. 2.2.1)

   B. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76)

   C. "Manufacturing United States." *1997 Economic Census: Summary Statistics for the United States* (Ref. 2.2.86).

3. Determine initiating event frequency. The next step is to determine where these subsurface fires start, since the initiating events are defined in terms of fires that start in specific outside areas where waste forms reside. One analysis performed by the NFPA provided information for this (Ref. 2.2.1, Section 5). With some interpretation, these data can be used to estimate the fraction of the total fire frequency that should be assigned to the various onsite areas outside the building. By multiplying the appropriate fraction representing areas where waste forms will be times the total frequency of outside fires per facility-year, the frequency is determined for a fire in a particular area where a waste form resides (per facility year).

   The frequency is expressed in terms of facility-year, since the number of NFPA fires is divided by the number of North American Industry Classification System (NAICS) facilities. There is some uncertainty as to what is meant by a "facility" in this context. The NAICS does not make clear whether multiple process buildings can be considered a single facility; although, noting in this context that the purpose of the NAICS is an economic census, it implies that the number of main process buildings (i.e., the throughput of a given site) is more important than the number of sites. Because of this and in order to avoid potentially nonconservative probabilistic results, a boundary condition has been established that each main process building in the GROA constitutes a facility, and that the outside fire frequency pertains to each of them (i.e., each of these buildings generates the necessary conditions to contribute a full measure

of potential fire ignitions). The aging pads, buffer areas, and subsurface will not be considered as separate facilities, but rather as support areas for the process buildings (i.e., they are an integral part of a typical facility in that they supply the "raw materials" to the process and take the "product" from the process). In addition, the other balance of plant support buildings will also not be considered facilities for the purpose of determining the overall frequency of outside fires, for a similar reason. Therefore, the overall frequency of outside fires for the GROA will be the frequency per facility-year, times the number of main process buildings (i.e., number of waste handling facilities), which is six: IHF, WHF, RF, and three CRCFs. Multiplying by 50 yields the frequency over the preclosure period.

4.3.6 Event Sequence Quantification

4.3.6.1 Overview of Quantification

Event sequences are represented by event trees and are quantified via the product of the initiating event frequency and the pivotal event probabilities. Event sequences that lead to a successful end state (designated as "OK") are not considered further. The result of quantification of an event sequence is expressed in terms of the number of occurrences over the preclosure period. This number is the product of the following factors:

1. The number of demands (sometimes called trials) or the time exposure interval of the operation or activity that gives rise to the event sequence. For example, this could be the total number of transfers of a cask in a facility preparation area.

2. The frequency of occurrence per demand or per time interval of the initiating event. For example, this could be the frequency of cask drop per transfer by a crane. Initiating event frequencies are developed either using fault trees or by direct application of industry-wide data, as explained in Section 4.3.2. Factors one and two are represented in the initiator event trees.

3. The conditional probability of each of the pivotal events of the event sequence, which appear in the associated system-response event tree. These probabilities are the results of a passive equipment failure analyses, fault tree analyses (e.g., HVAC), and direct probability input (e.g., moderator introduced), or judgment.

Calculated fault tree top event frequency or probability is input directly into the Excel spreadsheet containing the event sequence logic. The event sequence frequency is then estimated by calculating the product of the three factors mentioned above. This methodology can be applied here due to the simplicity of the event sequence, and there is no dependence between pivotal events.

SAPHIRE Version 7.26 (Section 4.2), developed by Idaho National Laboratory, stands for "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations." It is 32-bit software that runs under Microsoft Windows. Features of SAPHIRE that help an analyst build and quantify fault trees are as follows:

- A listing of where a basic event appears, including within cut sets. Conversely, the basic events that are *not* used are known and can be easily removed when it comes time to "clean" the database.

- Context-driven menu system that performs actions (report cut sets, view importance measures, display graphics, etc.) on objects such as fault trees, event trees, and event sequences.

Fault trees can be constructed and analyzed to obtain different measure of system unreliability. These system measures are:

- Overall initiating or pivotal event failure frequency

- Minimal cut sets size, number, and frequency

- Built in features include:

  - Generation, display, and storage of cut sets
  - Graphical editors (fault tree and event tree)
  - Database editors
  - Uncertainty analysis
  - Data Input/Output via ASCII text files (MAR-D)
  - Special seismic analysis capability.

SAPHIRE is equipped with two uncertainty propagation techniques: Monte Carlo and Latin Hypercube sampling. To take advantage of these sampling techniques, twelve uncertainty distributions are built such that the appropriate distribution may be selected. SAPHIRE contains a cross-referencing tool, which provides an overview of every place a basic event, gate, initiating, or pivotal event is used in the model.

4.3.6.2 Propagation of Uncertainties and Event Sequence Categorization with Uncertainties

The fundamental viewpoint of the PCSA is probabilistic in order to develop information suitable for the risk informed nature of 10 CFR Part 63 (Ref. 2.3.2). Any particular event sequence may or may not occur during any operating time interval, and the quantities of the parameters of the models may not be precisely known. Characterizing uncertainties and propagating these uncertainties through the event tree/fault tree model is an essential element of the PCSA. The PCSA includes both aleatory and epistemic uncertainties. Aleatory uncertainty refers to the inherent variation of a physical process over many similar trials or occurrences. For example, development of a fragility curve to obtain the probability of canister breach after a drop would involve investigating the natural variability of tensile strength of stainless steel. Epistemic uncertainty refers to our state of knowledge about an input parameter or model. Epistemic uncertainty is sometimes called reducible uncertainty because gathering more information can reduce the uncertainty. For example, the calculated uncertainty of a SSC failure rate developed from industry-wide data will be reduced when sufficient GROA specific operational information is included in a Bayesian analysis of the SSC failure rate.

As described in Section 4.3.1, event sequence categorization is performed using the mean value of event sequences emanating from the large circle in Figure 4.3-4. By the definition of the term, mean values are derived solely from probability distributions.

Using the screening criteria set out in 10 CFR 63.2 (Ref. 2.3.2), the categorization of an event sequence that is expected to occur m times over the preclosure period (where m is the mean or expected number of occurrences) is carried out as follows:

- A value of m greater than or equal to one, places the corresponding event sequence into Category 1.

- A value of m less than one indicates that the corresponding event sequence is not expected to occur before permanent closure. To determine whether the event sequence is Category 2, its probability of occurrence over the preclosure period needs to be compared to 10^{-4}. A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to m. The probability, P, that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution, $P = 1 - \exp(-m)$, a value of P greater than or equal to 10^{-4} implies that value of π is greater than or equal to $-\ln(1 - P) = m$, which is numerically equal to 10^{-4}. Thus, a value of m greater than or equal to 10^{-4}, but less than one, implies the corresponding event sequence is a Category 2 event sequence.

- Event sequences that have a value of m less than 10^{-4} are designated as Beyond Category 2.

Using either Monte Carlo or Latin Hypercube methods allows probability distributions to be arithmetically treated to obtain the probability distributions of minimal cut sets and the probability distributions of event sequences. The PCSA used Monte Carlo simulation with 10,000 trials and a standard seed so the results could be reproduced. The number of trials for final results was arrived at by increasing the number of trials until the median, mean, and 95th percentile were stable within the standard Monte Carlo error.

The adequacy of categorization of an event sequence is further investigated if its expected number of occurrences m over the preclosure period is close to a category threshold.

If m is greater than 0.2, but less than 1, the event sequence, which a priori is Category 2, is reevaluated differently to determine if it should be recategorized as Category 1. Similarly, if m is greater than 2×10^{-5}, but less than 10^{-4}, the event sequence, which a priori is Beyond Category 2, is reevaluated to determine if it should be recategorized as Category 2.

The reevaluation begins with calculating an alternative value of m, designated by m_a, based on an adjusted probability distribution for the number of occurrences of the event sequence under consideration. The possible distributions that are acceptable for such a purpose would essentially have the same central tendency, embodied in the median (i.e., the 50th percentile), but relatively more disparate tails, which are more sensitive to the shape of the individual distributions of the

basic events that participate in the event sequence. Accordingly, the adjusted distribution is selected as a lognormal that has the same median M as that predicted by the Monte Carlo sampling. Also, to provide for a reasonable variability in the distribution, an error factor $EF = 10$ is used, which means that the 5th and 95th percentiles of the distribution are respectively lesser or greater than the median by a factor of 10.

If the calculated value of m_a is less than 1, the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., Category 2. Similarly, if the calculated value of m_a is less than 10^{-4}, the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., Beyond Category 2.

In contrast, if the calculated value of m_a is greater than 1, the alternative distribution indicates that the event sequence is Category 1, instead of Category 2 found in the original determination. In such a case, the conflicting indications are resolved by conservatively assigning the event sequence to Category 1.

Similarly, if the calculated value of m_a is greater than 10^{-4}, the alternative distribution indicates that the event sequence is Category 2, instead of Beyond Category 2 found in the original determination. In such a case, the conflicting indications are resolved by conservatively assigning the event sequence to Category 2.

The calculations carried out to quantify an event sequence are performed using the full precision of the individual probability estimates that are used in the event sequence. However, the categorization of the event sequence is based upon an expected number of occurrences over the preclosure period given with one significant digit.

4.3.7 Identification of ITS SSCs, Development of Nuclear Safety Design Bases, and Development of Procedural Safety Controls

4.3.7.1 Identification of ITS SSCs

ITS SSCs are subject to nuclear safety design bases that are established to ensure that safety functions and reliability factors applied in the event sequence analyses are explicitly defined in a manner that assures proper categorization of event sequences.

ITS is defined in 10 CFR 63.2 (Ref. 2.3.2) as:

> *"Important to safety*, with reference to structures, systems, and components, means those engineered features of the geologic repository operations area whose function is:
>
> (1) To provide reasonable assurance that high-level radioactive waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of § 63.111(b)(1) for Category 1 event sequences; or

> (2) To prevent or mitigate Category 2 event sequences that could result in radiological exposures exceeding the values specified at § 63.111(b) (2) to any individual located on or beyond any point on the boundary of the site."

Structures are defined as elements that provide support or enclosure such as buildings, free standing tanks, basins, dikes, and stacks. Systems are collections of components assembled to perform a function, such as HVAC, cranes, trolleys, and TEVs. Components are items of equipment that taken in groups become systems such as pumps, valves, relays, piping, or elements of a larger array, such as digital controllers.

Implementation of the regulatory definition of ITS has produced the following specific criteria in the PCSA to classify SSCs: A SSC is classified as ITS if it is relied upon to reduce the frequency of an event sequence or mitigate the consequences of an event sequence and at least one of the following criteria apply:

- The SSC is relied upon to reduce the frequency of an event sequence from Category 1 to Category 2.
- The SSC is relied upon to reduce the frequency of an event sequence from Category 2 to Beyond Category 2.
- The SSC is relied upon to reduce the aggregated dose of Category 1 event sequences by reducing the event sequence mean frequency.
- The SSC is relied upon to perform a dose mitigation or criticality control function.

A SSC is classified as ITS in order to assure safety function availability over the operating lifetime of the repository. The classification process involves the selection of the SSCs in the identified event sequences (including event sequences that involve nuclear criticality) that are relied upon to perform the identified safety functions such that the preclosure performance objectives of 10 CFR Part 63 (Ref. 2.3.2) are not exceeded. The ITS classification extends only to the attributes of the SSCs involved in providing the ITS function. If one or more components of a system are determined to be ITS, the system is identified as ITS, even though only a portion of the system may actually be relied upon to perform a nuclear safety function. However, the specific safety functions that cause the ITS classification are delineated.

Perturbations from normal operations, human errors in operations, human errors during maintenance (preventive or corrective), and equipment malfunctions may initiate Category 1 or Category 2 event sequences. The SSCs supporting normal operations (and not relied upon as described previously for event sequences) are identified as non-ITS. In addition, if an SSC (such as permanent shielding) is used solely to reduce normal operating radiation exposure, it is classified as non-ITS.

4.3.7.2 Development of Nuclear Safety Design Bases

Design bases are established for the ITS SSCs as described in 10 CFR 63.2 (Ref. 2.3.2):

> "Design bases means that information that identifies the specific functions to be performed by a structure, system, or component of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be constraints derived from generally accepted "state-of-the-art" practices for achieving functional goals or requirements derived from analysis (based on calculation or experiments) of the effects of a postulated event under which a structure, system, or component must meet its functional goals..."

The safety functions for this analysis were developed from the applicable Category 1 and Category 2 event sequences for the SSCs that were classified as ITS. In general, the controlling parameters and values were grouped in, but were not limited to, the following five categories:

1. Mean frequency of SSC failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of failure (e.g., failure to operate, failure to breach), with consideration of uncertainties, less than or equal to the stated criterion value.

2. Mean frequency of seismic event-induced failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of a seismic event-induced failure (e.g., tipover, breach) of less than 1E-04 over the preclosure period, considering the full spectrum of seismic events less severe than that associated with a frequency of 1E-07/yr.

3. High confidence of low mean frequency of failure. It shall be demonstrated by analysis that the ITS SSC will have a high confidence of low mean frequency of failure associated with seismic events of less than or equal to the criterion value. The high confidence of low mean frequency of failure value is a function of uncertainty, expressed as β_c, which is the lognormal standard deviation of the SSC seismic fragility.

4. Preventive maintenance and/or inspection interval. The ITS SSCs shall be maintained or inspected to assure availability, at intervals not to exceed the criterion value.

5. Mean unavailability over time period. It shall be demonstrated by analysis that the ITS SSCs (e.g., HVAC and emergency electrical power) will have a mean unavailability over a period of a specified number of days, with consideration of uncertainties, of less than the criterion value.

These controlling parameters and values ensure that the ITS SSCs perform their identified safety functions such that 10 CFR Part 63 (Ref. 2.3.2) performance objectives are met. The controlling parameters and values include frequencies or probabilities in order to provide a direct link from the design requirements for categorization of event sequences. The PCSA will demonstrate that these controlling parameters and values are met by design of the respective ITS SSCs.

Table 6.9-1 in Section 6.9 presents a list of ITS SSCs, the nuclear safety design bases of the ITS SSCs, the actual value of the controlling parameter developed in this analysis, and a reference to that portion of the analysis (e.g., fault tree analysis), which demonstrates that the criterion is met.

4.3.7.3 Identification of Procedural Safety Controls

10 CFR 63.112(e) (Ref. 2.3.2) requires that the PCSA include an analysis that "identifies and describes the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences" and "identifies measures taken to ensure the availability of safety systems." This section describes the approach for specifying and analyzing the subset of procedural safety controls (PSCs) that are required to support the event sequence analysis and categorization.

The occurrence of an initiating or pivotal event is usually a combination of human errors and equipment malfunctions. A human reliability analysis is performed for the human errors. Those human actions that are relied upon to reduce the frequency of or mitigate the consequence of an event sequence are subject to procedural safety controls.

The approach for deriving PSCs from the event sequence analysis is outlined in the following:

1. Use event tree and supporting fault tree models for initiating events and pivotal events to identify HFEs.

2. Identify the types of PSCs necessary to support the HRA analysis for each of the HFEs. For example, provide clarifications about what is to be accomplished, time constraints, use of instrumentation, interlock and permissives that may back-up the human action.

3. Perform an event sequence analysis using screening HRA values. Identify the PSCs that appear to be needed to reduce the probability of or mitigate the severity of event sequences. The same criterion is used to identify ITS SSCs.

4. Work with the design and engineering organizations to add equipment features that will either eliminate the HFE or support crew and operators in the performance of the action. In effect, this step entails the development of design features that appear instead of a human action or appear under an AND gate with a human action.

5. Quantify event sequences again, identifying HFEs for which detailed HRA must be performed. The detailed HRA would lead to specific PSCs that are needed to reduce the frequency of event sequences or mitigate their consequences.

As indicated previously and outlined in item 3 above, those human actions that are relied upon to reduce the frequency or mitigate the consequence of an event sequence are subject to PSCs. Not all human actions are required to be identified as PSCs. A human failure event could be a minor contributor to an event sequence such that the proper execution of the corresponding human action may not need to be relied upon to maintain the event sequence in an adequate category. In this case, the use of a PSC is unnecessary.

If, on the contrary, a human error probability is a significant contributor to an event sequence, the proper execution of the corresponding human action is likely to be decisive in maintaining the event sequence in its proper event sequence categorization category or in ensuring that the consequences of the event sequence meets the 10 CFR 63.111 (Ref. 2.3.2) performance objectives. In this case, the use of a PSC may prove necessary.

An illustration of this approach is given by comparing two event sequences; one in which a human action is proceduralized (as a PSC) and the other in which no control is invoked. The first event sequence involves a low speed collision of a railcar or truck trailer loaded with a transportation cask with a moving or fixed object. A principal cause for this initiating event is an operator error. However, the intrinsic sturdiness of the transportation cask ensures that the probability of a breach of the cask after such a collision is very small. In such a case, there is no need to specifically rely on the proper execution of railcar or truck trailer movements to maintain the event sequence in a proper event sequence category. The categorization of the event sequence is essentially governed by the robustness of the transportation cask. No PSC is needed.

The second event sequence involves the direct exposure of a facility worker during the transfer of a waste package from a waste package transfer trolley (WPTT) to a TEV. To ensure that no radiological exposure occurs, personnel should not be present in the loadout room when this operation takes place. Assurance that this is the case, however, is dependent on personnel following procedures. This, therefore, is an example of a situation in which adherence to procedures is directly relied upon to ensure that the corresponding event sequence is maintained in the proper event sequence category. In such a case, a PSC is relied upon in the categorization of this event sequence.

4.3.8 Event Sequence to Dose Relationship

Outputs of the event sequence analysis and categorization process include tabulations of event sequences by expected number of occurrences, end state, and waste form. The event sequences are sorted by Category 1, Category 2 and Beyond Category 2. Summaries of the results are tabulated in Section 6.8 with the following information:

1. Event sequence designator—A unique designator is provided for each event sequence to permit cross-references between event sequence categorization and consequence and criticality analysis.

2. End state conditions—One of the following is provided for each event sequence:

   A. DE-SHIELD-DEGRADE or DE-SHIELD-LOSS (Direct Exposure). Condition leading to potential exposure due to degradation of shielding provided by the TEV, cask or the aging overpack.

   B. RR-FILTERED (Radionuclide Release, Filtered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister). However, the availability of the secondary confinement (structural and HVAC with HEPA filtration) provides mitigation of the consequences. This end state is not used for

the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.

C. RR-UNFILTERED (Radionuclide Release, Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister), and a breach in the secondary confinement boundary (e.g., no HEPA filtration to provide mitigation of the consequences or breach of the structural confinement).

D. RR-FILTERED-ITC and RR-UNFILTERED-ITC (Radionuclide Release, Important to Criticality, Filtered or Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister) with or without HEPA filtration. In addition, the potential of exposing the unconfined waste form to moderator could result in conditions important to criticality. This characteristic of the end state is used by both the dose consequence analysts and the criticality analysts. The RR-FILTERED-ITC end state is not used for the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.

E. ITC (Important to Criticality). This end state is not used for the IHF because all potential criticality initiators are associated with a radiological release (i.e., end state RR-UNFILTERED-ITC).

3. General description of the event sequence—This is a high-level description that will be explained by the other conditions described above. For example, "Filtered radionuclide release resulting from a drop from the TEV that causes a breach of both sealed waste package and sealed canister."

4. Material at risk—Identify and define the number of each waste form that contributes to the radioactivity or criticality hazard of the end state (e.g., number of TAD canisters, DPCs, uncanistered commercial SNF assemblies, etc., involved in the event sequence).

5. Expected number of occurrences—Provide the expected mean number of occurrences of the designated event sequences over the preclosure period and associated median and standard deviation.

6. The event sequence categorization—Provide the categorization of the designated event sequence and the basis for the categorization.

7. The bounding consequences—Provide the bounding consequence analysis cross-reference, as applicable, for each Category 1 or Category 2 event sequence to the bounding event number from the preclosure consequence analysis.

10 CFR 63.111 (Ref. 2.3.2) requires that the doses associated with Category 1 and Category 2 event sequences meet specific performance objectives. There are no performance objectives for Beyond Category 2 event sequences. Dose consequences associated with each Category 1 and Category 2 event sequence are evaluated in preclosure consequence analyses, by comparison, to

pre-analyzed release conditions (or dose categories) that are intended to characterize or bound the actual event sequences (Ref. 2.2.36). As such, the results of the event sequence analysis and categorization serve as inputs to the consequence analysis for assignment to dose categories.

4.3.9 Event Sequence to Criticality Relationship

The requirements for compliance with preclosure safety regulations are defined in 10 CFR 63.112 (Ref. 2.3.2). Particularly germane to criticality considerations, is the requirement in 10 CFR 63.112, Paragraph (e) and Subparagraph (e) (6). Paragraph (e) requires an analysis to identify the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. This is a general requirement imposed on all event sequence analyses. Subparagraph (e) (6) specifically notes that the analyses should include consideration of "means to prevent and control criticality." The PCSA criticality analyses (Ref. 2.2.38) employs specialized methods that are beyond the scope of the present calculation. However, the event sequence development analyses inform the PCSA criticality analyses by identifying the event sequences and end states that may have a potential for criticality. As noted in Section 4.3, some event sequence end states include the phrase "important to criticality." This indicates that the end state implies the potential for criticality and that a criticality investigation is indicated.

To determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity of variations in each of the parameters important to criticality during the preclosure period, that is, waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor (k_{eff}) to variations in any of these parameters as a function of the other parameters. The criticality calculations demonstrate that one of the following is true for each parameter:

- It is bounded (i.e., its analyzed value is greater than or equal to the design limit) or its effect on k_{eff} is bounded and does not need to be controlled. This is designated as a no in Table 4.3-1.

- It needs to be controlled if another parameter is not controlled (conditional control). This is designated as a Conditional in Table 4.3-1.

- It needs to be controlled because it is the primary criticality control parameter. This is designated as a yes in Table 4.3-1.

The criticality control parameters analysis, which comprises the background calculations that led to Table 4.3-1, is presented in detail in the *Preclosure Criticality Safety Analysis* (Ref. 2.2.38). Event sequences that impact the criticality control parameters that have been established as needing to be controlled are identified, developed, quantified, and categorized. These event sequences are referred to as event sequences ITC. The following matrix elements, indicating the need for control, are treated in the current event sequence analysis:

- Conditional: needs to be controlled if moderator is present
- Conditional: needs to be controlled during a boron dilution accident

- Yes: moderation is the primary criticality control
- Yes: interaction for DOE standardized SNF canisters needs to be controlled.

Table 4.3-1. Criticality Control Parameter Summary

Operation / Parameter	Commercial SNF (Dry Operations)	Commercial SNF (WHF Pool and Fill Operations)	DOE SNF	HLW
Waste form characteristics	No[a]	No[a]	No[b]	No[c]
Moderation	Yes[d]	N/A	Yes[d]	No
Interaction	No	Conditional[g]	Yes[e]	No
Geometry	Conditional[f]	Conditional[g]	Conditional[f]	No
Fixed neutron absorbers	Conditional[f]	Conditional[g]	Conditional[f]	No
Soluble neutron absorber	N/A	Yes[h]	N/A	N/A
Reflection	No	No	No	No

NOTE: [a]The *Preclosure Criticality Safety Analysis* (Ref. 2.2.38) considers bounding waste form characteristics. Therefore, there is no potential for a waste form misload.
[b]The *Preclosure Criticality Safety Analysis* (Ref. 2.2.38) considers nine representative DOE SNF types. Because the analysis is for representative types and loading procedures for DOE standardized SNF canisters have not been established yet, consideration of waste form misloads is not appropriate.
[c]Criticality safety design control features are not necessary for HLW canisters because the concentration of fissile isotopes in an HLW canister is too low to have criticality potential.
[d]Moderation is the primary criticality control parameter.
[e]Placing more than four DOE standardized SNF canisters outside the staging racks or a codisposal waste package needs to be controlled.
[f]Needs to be controlled only if moderator is present.
[g]Needs to be controlled only if the soluble boron concentration in the pool and transportation cask/dual purpose canister fill water is less than the minimum required concentration.
[h]Minimum required soluble boron concentration in the pool is 2500 mg/L boron enriched to 90 atom % ^{10}B.
DOE = U.S. Department of Energy; HLW = high-level radioactive waste; SNF = spent nuclear fuel; WHF = Wet Handling Facility.

Source: Ref. 2.2.38, Table 6

4.3.10 Boundary Conditions and Use of Engineering Judgment Within a Risk Informed Framework

4.3.10.1 Boundary Conditions

The initiating events considered in the PCSA define what could occur within the site GROA and are limited to those events that constitute a hazard to a waste form while it is present in the GROA. Initiating events include internal events occurring during waste handling operations conducted within the GROA and external events (e.g., seismic, wind energy, or flood water events) that impose a potential hazard to a waste form, waste handling systems, or personnel within the GROA. Such initiating events are included when developing event sequences for the PCSA. However, initiating events that are associated with conditions introduced in SSCs before they reach the site are not within the scope of the PCSA. The excluded from consideration offsite conditions include drops of casks, canisters, or fuel assemblies during loading at a reactor site; improper drying, closing, or inerting at the reactor site; rail or road accidents during transport; tornado or missile strikes on a transportation cask; or nonconformances introduced during cask or canister manufacture that result in a reduction of containment strength. Such potential precursors are subject to deterministic regulations such as 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4) and associated quality assurance programs. As a result of compliance to such regulations, the SSCs are deemed to pose no undue risk to health and safety. Although the analyses do not address quantitative probabilities to the aforementioned excluded precursors, it is clear that conservative design criteria and QA controls result in unlikely exposures to radiation.

Other boundary conditions used in the PCSA include:

- Plant operational state. Initial state of the facility is normal with each system operating within its vendor prescribed operating conditions.

- No other simultaneous initiating events. It is standard practice to not consider the occurrence of other initiating events (human-induced and naturally occurring) during the time span of an event sequence because, (a) the probability of two simultaneous initiating events within the time window is small and, (b) each initiating event will cause operations in the waste handling facility to be terminated which further reduces the conditional probability of the occurrence of a second initiating event, given the first has occurred.

- Component failure modes. The failure mode of a SSC corresponds to that required to make the initiating or pivotal event occur.

- Fundamental to the basis for the use of industry-wide reliability parameters within the PCSA, such as failure rates, is the use of SSCs within the GROA that conform to NRC accepted consensus codes and standards, and other regulatory guidance.

4.3.10.2 Use of Engineering Judgment

10 CFR Part 63 (Ref. 2.3.2) is a risk-informed regulation rather than a risk-based regulation. The term risk-informed was defined by the NRC to recognize that a risk assessment can not always be performed using only quantitative modeling. Probabilistic analyses may be supplemented with expert judgment and opinion, based on engineering knowledge. Such practice is fundamental to the risk assessment technology used for the PCSA.

10 CFR Part 63 (Ref. 2.3.2) does not specify analytical methods for demonstrating performance, estimating the reliability of ITS SSCs (whether active or passive), or calculating uncertainty. Instead, the risk-informed and performance-based preclosure performance objectives in 10 CFR Part 63 (Ref. 2.3.2) provide the flexibility to develop a design, and demonstrate that it meets performance objectives for preclosure operations including the use of well established (discipline-specific) methodologies. As exemplified in the suite of risk-informed regulatory guides developed for 10 CFR Part 50 (Ref. 2.3.1) facilities (e.g., Regulatory Guide 1.174 (Ref. 2.2.75) and NUREG-0800 (Ref. 2.2.67, Section 19), such methodologies use deterministic and probabilistic inputs and analysis insights. The range of well established techniques in the area of PRA, which is used in the PCSA, often relies on the use of engineering judgment and expert opinion (e.g., in development of seismic fragilities, human error probabilities, and the estimation of uncertainties).

As described in Section 4.3.3, for example, active SSC reliability parameters will be developed using a Bayesian approach; and the use of judgment in expressing prior state-of-knowledge is a well-recognized and accepted practice ((Ref. 2.2.59), (Ref. 2.2.4), (Ref. 2.2.9), and (Ref. 2.2.66)).

The NRC issued *Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73) to provide guidance for compliance to 10 CFR 63.111 and 112 (Ref. 2.3.2). This document states that "treatment of uncertainty in reliability estimates may depend on the risk-significance (or reliance) of a canister system in preventing or reducing the likelihood of event sequences." Furthermore, *Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73) indicates that reliability estimates for high reliability SSCs may include the use of engineering judgment supported by sufficient technical basis; and empirical reliability analyses of a SSC could include values based on industry experience and judgment (Ref. 2.2.73).

In a risk-informed PCSA, therefore, the depth, rigor of quantitative analysis and the use of judgment depends on the risk-significance of the event sequence. As such, decisions on the level of effort applied to various parts of the PCSA are made, based on the contribution to the frequency of end states and the severity of such end states. An exhaustive analysis need not be performed to make this resource allocation. Accordingly, the PCSA analyst has flexibility in determining and estimating the reliability required for each SSC, at the system or component level, and in selecting approaches in estimating the reliability. The quantified reliability estimates used to reasonably screen out initiating events, support categorization, or screening of event sequences must be based on defensible and traceable technical analyses. The following summarizes the approaches where judgment is applied to varying degrees.

All facility safety analyses, whether or not risk-informed, take into account the physical conditions, dimensions, materials, human-machine interface, or other attributes such as operating conditions and environments to assess potential failure modes and event sequences. Such factors guide the assessment of what can happen, the likelihood, and the potential consequences. In many situations, it could be considered obvious that the probability of a particular exposure scenario is very small. In many cases, it is impractical or unnecessary to actually quantify the probability when a non-probabilistic engineering analysis provides sufficient assurance and insights that permit the event sequence to be either screened out, or demonstrated to be bounded by another event sequence. Examples of such are provided in Section 6.0.

When Empirical Information is not Available

There is generally no or very little empirical information for the failure of passive SSCs such as transportation casks and spent fuel storage canisters. Such failures are postulated in predictive safety and risk analyses and then the SSCs are designed to withstand the postulated drops, missile impacts, seismic shaking, abnormal temperatures and pressures, etc. While in service, few if any SSCs have been subjected to abnormal conditions that approach the postulated abnormal scenarios so there is virtually no historical data to call on.

Therefore, structural reliability analyses are used in the PCSA to develop analysis-based failure probabilities for the specific event sequences identified within the GROA. Uncertainties in the calculated stresses/strains and the capacity of the SSCs to withstand those demands include the use of judgment, based on standard nuclear industry practices for design, manufacturing, etc., under the deterministic NRC regulatory requirements of 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), or 10 CFR Part 72, (Ref. 2.3.4). It is standard practice to use the information basis associated with the consensus standard and regulatory requirement information as initial conditions of a risk-informed analysis. This approach is acceptable for the PCSA subject to the following:

1. The conditions associated with the consensus codes and standards and regulatory requirements are conservatively applicable to the GROA.

2. Equivalent quality assurance standards are applied at the GROA.

3. Operating processes are no more severe than those licensed under the aforementioned deterministic regulations.

Use of Empirical Reliability Information

In those cases where applicable, quantitative historical component reliability information is available, the PCSA followed Sections 4.3 including the application of judgment that is associated with Bayesian analysis. Similarly, as described in Sections 4.3.5, 4.3.6, and 4.3.7, historical data is applied in human reliability, fires, and flooding analyses with judgment-based adjustments as appropriate for subsurface operations and GROA operating conditions.

Use of Qualitative Information When Reliability Information is Not Available

In those cases where historical records of failures to support the PCSA are not available, qualitative information may be used to assign numerical failure probabilities and uncertainty. This approach is consistent with the Bayesian framework used in the PCSA, consistent with HLWRS-ISG-02 (Ref. 2.2.73), and involves the use of judgment in the estimation of reliability or failure probability values and their associated uncertainties. In these cases, the PCSA analyst may use judgment to determine probability and reliability values for components.

The following guidelines are used in the PCSA when it is necessary to use judgment to assess the probability of an event. The analyst will select a median at the point believed to be just as likely that the "true" value will lie above as below. Then, the highest probability value believed possible is conservatively assigned as a 95th percentile or error factor (i.e., the ratio of the 95th percentile to median), rather than a 99th or higher percentile, with a justification for the assignments. A lognormal distribution is used because it is appropriate for situations in which the result is a product of multiple uncertain factors or variables. This is consistent with "A Central Limit Theorem for Latin Hypercube Sampling." (Ref. 2.2.74). The lower bound, as represented by the 5th percentile, is checked to ensure that the distribution developed using the median and 95th percentile does not cause the lower bound to generate values for the variable that are unrealistic compared to the knowledge held by the analyst.

In some cases, an upper and lower bound is defensible, but no information about a central tendency is available. A uniform distribution between the upper and lower bound is used in such cases.

Another way in which risk-informed judgment is applied to obtain an appropriate level of effort in the PCSA, involves a comparison of event sequences. For example, engineering judgment readily indicates that a 23-foot drop of a canister onto an unyielding surface would do more damage to the confinement boundary, than a collision of a canister with a wall at maximum crane speed (e.g., 40 ft/min). A rigorous probabilistic structural analysis of the 23-foot drop is performed and these results may be conservatively applied to the relatively benign slow speed collision.

INTENTIONALLY LEFT BLANK

5. LIST OF ATTACHMENTS

		Number of Pages
Attachment A	Event Trees	34
Attachment B	System/Pivotal Event Analysis – Fault Trees	326
Attachment C	Active Component Reliability Data Analysis	58
Attachment D	Passive Equipment Failure Analysis	96
Attachment E	Human Reliability Analysis	68
Attachment F	Fire Analysis	20
Attachment G	Event Sequence Quantification Summary Tables	22
Attachment H	EXCEL and SAPHIRE Model and Supporting Files	4 + CD

INTENTIONALLY LEFT BLANK

6. BODY OF ANALYSIS

The *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40, Section 6.1.2, Attachment A, and Attachment B), which describes the Subsurface Operations and equipment should be consulted in conjunction with the present analysis.

6.0 INITIATING EVENT SCREENING

The NRC's interim staff guidance for its evaluation of the level of information and reliability estimation related to the Yucca Mountain repository, HLWRS-ISG-02 (Ref. 2.2.73, p. 3), states that there are multiple approaches that DOE could use to estimate the reliability of SSCs that contribute to initiating events or event sequence propagation (i.e., pivotal events), including the use of judgment. By the definition provided in 10 CFR 63.102(f) (Ref. 2.3.2) initiating events are to be considered for inclusion in the PCSA for determining event sequences only if they are reasonably based on the characteristics of the geologic setting and the human environment, and are consistent with the precedents adopted for nuclear facilities with comparable or higher risks to workers and the public.

This section provides screening arguments that eliminate extremely unlikely initiating events from further considerations. Screening of initiating events is a component of a risk-informed approach that allows attention to be concentrated on important contributors to risk. The screening process eliminates those initiators that are either incapable of initiating an event sequence having radiological consequences or are too improbable to occur during the preclosure period. The screening arguments are based on either a qualitative or quantitative analysis documented under separate cover, or through engineering judgment based on considerations of site and design features documented herein.

Initiating events are screened out and are termed Beyond Category 2 if they satisfy either of the following criteria:

- The initiating event has less than one chance in 10,000 of occurring during the preclosure period.
- The initiating event has less than one chance in 10,000 over the preclosure period of causing physical damage to a waste form that would result in the potential for radiation exposure or inadvertent criticality.

In other instances, initiating event screening analysis is based on engineering or expert judgment. Such judgment is based on applications of industry codes and standards, comparison to results of analyses for more severe, or plausibility arguments based on the combinations of conditions that must be present to allow the initiating event to occur or the event sequence to propagate.

6.0.1 Boundary Conditions for Consideration of Initiating Events

6.0.1.1 General Statement of Boundary Conditions

Manufacturing, loading, and transportation of casks and canisters are subject to regulations other than 10 CFR Part 63 (Ref. 2.3.2) (e.g., 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4)) and associated quality assurance programs. As a result of compliance with such regulations, the affected SSCs provide reasonable assurance that the health and safety of the public are protected. However, if a potential precursor condition could result in an airborne release that could exceed the performance objectives for Category 1 or Category 2 event sequences, or a criticality condition, then a qualitative argument that the boundary condition is reasonable is provided. A potential initiating event that is outside of the boundary conditions but has been found to require a qualitative discussion is the failure to properly dry a SNF canister prior to sealing it and shipping it to the repository.

6.0.1.2 Specific Discussion of Receipt of Properly Dried SNF Canisters

Under the boundary conditions stated for this analysis, canisters shipped to the repository in transportation casks are received in the intended internally dry conditions. Shipments of SNF received at the repository, whatever their origin, are required to meet the requirements of 10 CFR Part 71 (Ref. 2.3.3). NUREG-1617 (Ref. 2.2.69) provides guidance for the NRC safety reviews of packages used in the transport of spent nuclear fuel under 10 CFR Part 71 (Ref. 2.3.3). The review guidance, NUREG-1617 (Ref. 2.2.69, Section 7.5.1.2), instructs reviewers that, at a minimum, the procedures described in the safety analysis report should ensure that:

> Methods to drain and dry the cask are described, the effectiveness of the proposed methods is discussed, and vacuum drying criteria are specified.

NUREG-1536 (Ref. 2.2.68, Chapter 8, Section V) refers to an acceptable process to evacuate water from SNF canisters. No more than about 0.43 gram-mole of water (about 8 grams) is left in the canister if adequate vacuum drying is performed (Ref. 2.2.68). The following example is cited as providing adequate drying (Ref. 2.2.68, Chapter 8, Section V):

> The cask should be drained of as much water as practicable and evacuated to less than or equal to 4E-4 MPa (3.0 mm Hg or Torr). After evacuation, adequate moisture removal should be verified by maintaining a constant pressure over a period of about 30 minutes without vacuum pump operation. The cask is then backfilled with an inert gas (e.g., helium) for applicable pressure and leak testing. The cask is then re-evacuated and re-backfilled with inert gas before final closure. Care should be taken to preserve the purity of the cover gas, and after backfilling, cover gas purity should be verified by sampling.

The procedure described appears to ensure that very little water is left behind. However, the probability of undetected failure when performing the process is not addressed in the deterministic regulation 10 CFR Part 71 (Ref. 2.3.3) or in NUREG-1536 (Ref. 2.2.68). Indeed, there is no after-the-fact water or error detection method in NUREG-1536 or the regulation. Therefore, some unknown number of canisters may arrive in the GROA with more residual water than is expected with proper drying. Because the canisters are welded and are not required to provide for sampling the inside of the canister, nondestructive measurement of the residual water content would be difficult. The following discussion provides reasonable assurance that no significant risks are omitted from the analysis due to adoption of the boundary condition that canisters shipped to the repository in transportation casks are received in the intended internally dry conditions:

1. The YMP will be accepting, handling, and emplacing TAD canisters in a manner consistent with the specifications laid out in the TAD canister system performance specification (Ref. 2.2.47) which prescribes the use of consensus codes and standards along with design requirement associated with GROA specific event sequences.

2. **Criticality**. GROA operating processes are similar to those of nuclear power plant sites with respect to the use of cranes, and there are no processes or conditions that would exacerbate adverse effects associated with abnormal amounts of water retention. Event sequences involving the drop and breach of a naval canister are Beyond Category 2 as shown in Section 6.8. To receive a license to transport SNF, 10 CFR 71.55 (Ref. 2.3.3) requires the licensee to demonstrate subcriticality given that "the fissile material is in the most reactive credible configuration consistent with the damaged condition of the package and the chemical and physical form of the contents" under the hypothetical accident conditions specified in 10 CFR 71.73 (Ref. 2.3.3). Drop events, which are unlikely to breach the canister, are also unlikely to impart sufficient energy to the fuel to reconfigure it so dramatically that criticality would be possible even if water is present. It is concluded that existing regulations that apply to the canister and transportation cask for transportation to the repository provide reasonable assurance that a criticality event sequence that depends on the presence of residual water inside the canister and reconfiguration of the fuel would not occur under conditions that could reasonably be achieved during handling at the repository.

3. **Hydrogen explosion or deflagration**. Radiation from SNF can generate radiolytic hydrogen and oxygen gas in a SNF canister if water is inadvertently left in the canister before it is sealed. Given a processing error that leaves enough residual water, the gas concentrations could conceivably reach levels where a deflagration or explosion event could occur. However, precautions taken at the generator sites are expected to make receipt of a canister that was improperly dried unlikely. In addition, an ignition source would be required for an explosion or deflagration to occur. High electrical conductivity of the metal canister would dissipate any high voltage electrical discharge (which is unlikely in any case) and preclude arcing within the canister. Normal handling operations do not subject the canisters to energetic impacts that could cause frictional sparking inside the canister. Therefore, an unlikely event during handling, such as a canister drop would have to occur to ignite the gas. Considering the combination of unlikely events that must occur, event sequences involving this

combination of failures are screened out from further consideration on the judgment that they contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.

4. **Overpressurization due to residual water**. Given a processing error that leaves an excessive amount of residual water, the internal pressure due to vaporization of water could conceivably breach the canister. If sufficient water were to be left in the canister, overpressurization would occur within hours of the canister being welded closed. Therefore, overpressurization would occur while the canister is still in the supplier's possession and not in the GROA. Ambient environmental conditions in the GROA are similar to those that would be encountered by the canister while it is on the supplier's site and during transportation to the GROA. If there is not enough water to cause overpressurization before the canister reaches the GROA, then overpressurization would not occur in the GROA. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable for loaded canisters that are received from off-site.

6.0.2 Screening of External Initiating Events

6.0.2.1 Initial Screening of External Initiating Events

The *External Events Hazards Screening Analysis* (Ref. 2.2.34) identifies potential external initiating events at the repository for the preclosure period and screens a number of them from further evaluation based on severity or frequency considerations. The four questions that constitute the evaluation criteria for external events screening are:

1. Can the external event occur at the repository?

2. Can the external event occur at the repository with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

3. Can the external event, severe enough to affect the repository and its operation, occur at the repository with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

4. Can a release that results from the external event severe enough to affect the repository and its operations occur with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

The screening criteria are applied for each of the external event categories listed in Table 6.0-1. Each external event category is evaluated separately with a definition and the required conditions for the external event to be present at the repository. Then the four questions are applied. Those external event categories that are not screened out are retained for further evaluation as initiating events in the event sequences for the preclosure safety analysis.

As noted in Table 6.0-1, the potential external initiating event categories that are retained for further evaluation are seismic activity and loss of power. Seismically induced event sequences