

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 are developed, categorized, and documented in a separate analysis. Loss of power is analyzed separately for facility impact but is not an initiating event for Intra-Site Operations (Section 6.0.9).

Table 6.0-1. Retention Decisions from External Events Hazards Screening Analysis

External Event Category	Retention Decision. If Not Retained, Basis for Screening.
Seismic activity	YES. Retained for further analysis. ¹
Nonseismic geologic activity	NO. Except for drift degradation, the external events in this category are not applicable to the site or do not occur at a rate that could affect the repository during the preclosure period. The chance of drift degradation severe enough to affect the repository and its operation over the preclosure period is less than 1/10,000.
Volcanic activity	NO. The chance of volcanic activity occurring at the repository over the preclosure period is less than 1/10,000.
High winds / tornadoes	NO. The chance of a high wind or tornado event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
External floods	NO. The chance of a flood event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Lightning	NO. The chance of a lightning event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Loss of power event	YES. Retained for further analysis. Facility event sequence categorization analyses provides disposition. ²
Loss of cooling capability event	NO. The primary requirements for cooling water at the Yucca Mountain site during the preclosure period are makeup water for the WHF pool and cooling of HVAC chilled water. The chance of a loss of cooling capability occurring at the repository over the preclosure period is less than 1/10,000.
Aircraft crash	NO. The chance of an accidental aircraft crash occurring at the repository over the preclosure period is less than 1/10,000.
Nearby industrial/military facility accidents	NO. The chance of an industrial or military facility accident occurring at the repository over the preclosure period is less than 1/10,000.
Onsite hazardous materials release	NO. The chance of an accident event sequence initiated by the release of onsite hazardous materials at the repository over the preclosure period is less than 1/10,000.
External fires	NO. The chance of an external fire severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Extraterrestrial activity	NO. Extraterrestrial activity is defined as an external event involving objects outside the earth's atmosphere and enters the earth's atmosphere, survive the entry through the earth's atmosphere and strike the surface of the earth. Extraterrestrial activity includes: meteorites, asteroids, comets, and satellites. The chance of an occurrence at the repository over the preclosure period is less than 1/10,000.

NOTE: ¹ Seismic events are analyzed separately.

² Loss of power events do not affect Intra-Site Operations in a way that threatens a waste container.
HVAC = heating, ventilation, and air conditioning; WHF = Wet Handling Facility.

Source: Adapted from Ref. 2.2.26, Sections 6 and 7

6.0.3 Screening of Internal Initiating Events

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

Potential initiating events were qualitatively identified in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29) for quantitative treatment in the present analysis. For completeness, some events that were identified in the event sequence development analysis are extremely unlikely or physically unrealizable and reasonably can be qualitatively screened from further consideration. A qualitative screening argument for certain internal initiating events is developed in the present analysis as documented in Table 6.0-2. The first column of Table 6.0-2 indicates the branch of the IET (where applicable) that pertains to the screened initiating event. Each branch of an IET represents an initiating event or an initiating event group that includes other similar initiating events and corresponds to a small circle on an ESD (Ref. 2.2.29, Attachments F and G). Some of the initiating events that are addressed in Table 6.0-2 were implicitly screened out in the event sequence development analysis, and for that reason there is no applicable event tree. The screening argument for internal flooding is presented in Section 6.0.4. Sections 6.0.4 and 6.0.5 provide detailed screening arguments for internal flooding and diesel fuel oil tank explosions, which are too long for inclusion in Table 6.0-2.

Table 6.0-2. Bases for Screening Internal Initiating Events

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
ISO-ESD05-LLWLIQ (Branch 3)	Impact to a single (liquid) LLW container	Liquid LLW release for this event is not analyzed for categorization because the consequences to a worker for this type of release are a small fraction of the performance objectives. It is classified as an off-normal event in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Appendix IV).
ISO-ESD06-LLW (Branch 3)	Non-fire event involving all LLW containers	Collapse of the LLWF due to a seismic event is analyzed for consequence in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Table 2, Section 6.3.4, and Section 6.8.1), and is bounding. No further analysis for collapse of the LLWF is needed.
ISO-ESD08- LLWLIQ, (Branches 3, 4, and 5)	Structural challenges to a Liquid LLW container or containment boundary during transfer from GROA facilities, resulting in an unfiltered radiological release due to impact or to equipment failure.	Liquid LLW release for this event is not analyzed for categorization, because the consequences to a worker for this type of release are a small fraction of the performance objectives. It is classified as an off normal event in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Appendix IV)

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
ISO-ESD01-HLW (Branch 4) ISO-ESD01-MCO (Branch 4) ISO-ESD01-DSTD (Branch 4) ISO-ESD01-UCSNF (Branch 4)	Truck trailer collision leading to rollover/drop of transportation cask	PEFA values described in Section 6.3.2.2 and Attachment D, Section D1 do not account for buffer cars and impact limiters, which are always in place for Intra-Site Operations activities. This value is overly conservative, as detailed in Section 6.0.6.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened from further analysis. Section 6.0.4 provides the detailed screening argument.
No applicable event trees	Tipover of site transporter	<p>The site transporter is a crawler-type vehicle with four tank-type treads designed to preclude tipover. The size and weight of a loaded site transporter, along with the low center of gravity, precludes tipover if hit by a general service vehicle, the forces for which would be enveloped by the seismic spectrum described in the sliding/rocking calculation (Ref. 2.2.17). If impacted by another mover (cask tractor, site prime mover, or other site transporter), tipover would still be precluded because all of these vehicles are mechanically speed limited to reduce the frequency of severity of collisions (Ref. 2.2.20, Sections 3.2.1 and 3.2.2)</p> <p>The routes defined in <i>GROA North Portal Site Plan</i> and <i>GROA Aging Pad Site Plan</i> are evenly graded across gentle terrain (Ref. 2.2.28) and (Ref. 2.2.27) and are paved or compacted aggregate. Employing standard construction practices ensures that any culverts required along the transportation paths are barricaded to prevent vehicles from driving off at those points. Therefore, tipover of a site transporter is not analyzed further for categorization.</p>
No applicable event trees	Site transporter, cask tractor, cask transfer trailer collisions at speeds in excess of 2.5 mph	The site transporter, cask tractor, and cask transfer trailer are designed with speed limiters (Ref. 2.2.20, Section 2.2).
No applicable event trees	SPM collisions at speeds in excess of 9 mph in the GROA	The SPM is used to move waste containers in casks similar to or the same as casks moved by the cask tractor/cask transfer trailer. A design requirement of 9 mph is applied to the SPM (Table 6.9-1). It is reasonable to apply similar design requirements, such as speed limiters, as on other vehicles that are used to transport waste containers in the GROA, in order to reduce the severity of collisions (Ref. 2.2.20); (Ref. 2.2.14); (Ref. 2.2.17); and (Ref. 2.2.15).
No applicable event trees	High-speed collisions	YMP vehicles involved in the movement of waste containers are speed limited to reduce frequency and severity of collisions. Traffic control is also established to limit the speed of vehicles other than waste container transporters or conveyances operating in the vicinity of roads and areas used for waste container transit.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Cask transfer trailer punctures HTC, HSTC, or HDPC	The ram unit on the cask transfer trailer is designed such that the ram is positioned to preclude puncture of the HTC or HSTC during a collision or seismic event. In addition, the ram is designed to have insufficient force to deform a DPC (Ref. 2.2.25, Section 2.1.3); (Ref. 2.2.14); and (Ref. 2.2.15). Therefore, further consideration of this initiating event is not required.
No applicable event trees	Fuel tank explosion involving site transporter, cask tractor, cask transfer trailer, or SPM	Fuel tank design for equipment used to move casks or aging overpacks containing high-level waste shall include a requirement for the tank construction to use a low-temperature melt material. The low-temperature melt material precludes tank explosion as an initiating event. Therefore, fuel tank explosions for these movers are not analyzed further for categorization.
No applicable event trees	Floods affecting areas within the GROA	Flood controls will divert up to 55,000 cubic feet per second. These controls are required to divert a flood capacity of 40,000 cubic feet per second measured at the hydrological concentration point (identified as Collection Point 9 in <i>Yucca Mountain Project Drainage Report and Analysis</i> (Ref. 2.2.24, Table 7-1), which is the external flood event analyzed in the <i>External Events Hazards Screening Analysis</i> (Ref. 2.2.26)). The frequency of exceeding 40,000 cubic feet per second is less than 1E-06 per year (Ref. 2.2.24) and (Ref. 2.2.26). Refer also to Table 6.0-1, above.
No applicable event trees	Blocked vents on aging overpack or HAM cause overheating	<p>In NUREG-1864 (Ref. 2.2.11, p. 4-14), the NRC analyzed the maximum canister temperature that would result from blockage of all storage overpack vents. The analysis shows that vent blockage results in a maximum canister temperature that is hundreds of degrees below the temperature at which the canister would fail (canister failure temperature is analyzed in Attachment D, Section D2). The storage overpack and canister configuration analyzed in the NUREG report are very similar to the YMP canister and aging overpack configuration, so these results can be applied in the PCSA. Though the canister would remain well below its failure temperature and failure would be precluded, a conservative failure probability of 1E-06 is used in the PCSA.</p> <p>Due to design differences, complete blockage of HAM vents is much less likely to occur than in aging overpacks. However, if such a blockage were to occur, the large thermal capacity of the surrounding concrete would result in a similarly low maximum canister temperature and canister failure probability.</p> <p>Canister overheating that leads to breach due to blocked vents is, therefore, not analyzed further for categorization.</p>
No applicable event trees	Diesel fuel oil tank (Area 70A) or tanker truck explodes	The facility layout is such that the waste handling facilities and the waste container transportation paths are well beyond the estimated stand-off distance for these explosions (Ref. 2.2.28) and (Ref. 2.2.27). Estimated stand-off distances are provided in Table 6.0-5.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Moderator intrusion into a transportation cask containing uncanistered CSNF breached due to a thermal challenge	The breach path created due to a thermal challenge would not permit intrusion of moderator for a transportation cask (Section 6.0.7 provides a detailed discussion).
No applicable event trees	Thermal challenge to uncanistered CSNF in a transportation cask results in direct exposure of personnel or unfiltered release of radionuclides	The probability of fuel rod failure (in a transportation cask) at 750°C combined with frequency of a fire event in the buffer area during Intra-Site Operations activities is about 8E-05 (Section 6.0.8 provides a detailed discussion).
No applicable event trees	Loss of power causes equipment failure leading to direct exposure of personnel or unfiltered release of radionuclides	Activities associate with Intra-Site Operations occur outside of waste handling facilities. Failure of AC power to equipment during Intra-Site Operations activities does not result in an initiating event (Section 6.0.9 provides a detailed discussion).

NOTE: Initiator event trees, with branch numbers shown, are provided in Attachment A.

AC = alternating current; °C = degree Celsius; CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; GROA = geologic repository operations area; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; NRC = U.S. Nuclear Regulatory Commission; NUREG = Nuclear Regulation (U.S. Nuclear Regulatory Commission); PCSA = preclosure safety analysis; PEFA = passive equipment failure analysis; SPM = site prime mover; YMP = Yucca Mountain Project.

Source: Original

6.0.4 Screening of Flooding as an Initiating Event for Intra-Site Operations

Transportation casks and canisters are not physically susceptible to short-term effects of flood water. Therefore, flood water from sources other than the external events analyzed separately (Ref. 2.2.26) cannot breach a transportation cask or canister. Drains, ordinary housekeeping practices, evaporation, and relatively short handling times ensure that corrosion does not threaten the integrity of the containers over the longer term of the preclosure period.

As indicated in Table 6.0-1, external flooding events that might affect site transportation activities within the GROA and Aging Facility activities are screened from further analysis (Table 6.0-1, "Retention Decisions from External Events Screening Analysis"). No significant source of water exists at the Aging Facility, and water supply line breaks (e.g., damage to a fire hydrant or failure of water main) would not provide a sufficient amount of water or sufficient force to damage a transportation cask. Design and total mass of a transportation cask on conveyance, an aging overpack on a site transporter, or a cask on a cask transfer trailer is sufficient to preclude an initiating event of this type of flooding that would lead to a breach of a cask or canister. (Similarly, internal flooding to the drifts is also screened from further analysis.) Moderator intrusion into canisters resulting from Intra-Site Operations event sequences that might breach a waste container are treated quantitatively, as described in the pivotal event descriptions of Section 6.2.

6.0.5 Screening of Diesel Fuel Oil Storage Tank (Area 70A) and Tanker Truck Explosions

The following provides an assessment of a potential explosion in diesel fuel oil resupply trucks or in the diesel fuel storage tank (Area 70A), in order to determine if the possible truck routes and the Area 70A tank are situated a safe distance from the waste handling facilities and other SSCs such that no event sequences result from such an explosion. The increased external pressure generated by such an explosion is a function of the amount of explosive material and the distance between the site of the deflagration and the target (i.e., waste container or waste handling facility).

The parameters defined in Table 6.0-3 are used for the purpose of conservatively estimating the hazards associated with a diesel fuel vapor cloud explosion in a diesel fuel oil storage tank in Area 70A or in a tanker truck used for resupplying the tank in Area 70A. These parameters are appropriate to provide a conservative and bounding estimation of the hazards associated with such explosions.

Table 6.0-3. Parameters Used to Estimate Stand-Off Distances for Explosion Involving the Area 70A or a Tanker Truck

Parameter No.	Parameter Description	Applicable Equation No(s).	Input Value
6.0.5-1	A vapor cloud explosion occurs within the vapor space of the diesel storage tank, regardless of the ignition source. Vapor cloud explosions may occur in unconfined areas, although some degree of congestion is still required. Vapor cloud explosions can only occur in relatively large gas clouds (Ref. 2.2.60, p. 49). An ignition source is required to ignite such a vapor cloud, however, none is specified, because it is evaluated as if ignition is a given event.	—	—
6.0.5-2	The pressure in the vapor space above the tank is approximately atmospheric pressure. Bulk diesel fuel tanks are commonly vented. Therefore, the vapor mixture in the vapor space above the liquid in the tank will not be pressurized.	Eq. 21	P=101,325 Pa, equivalent to approximately P=14.70 psi (Ref. 2.2.88, p. F-335)
6.0.5-3	The temperature in the vapor space above the liquid in the storage tank is approximately equal to the flash point typical for a low-sulfur diesel fuel blend. The flash point of a liquid corresponds roughly to the lowest temperature at which the vapor pressure of the liquid is just sufficient to produce a flammable mixture at the lower limit of flammability (Ref. 2.2.33, p. 5-31). For this reason, the flash point was chosen as the temperature of the diesel fuel-air vapor mixture within the tank. This is conservative and bounding.	Eq. 21	T _F =140°F, equivalent to approximately T_R=600°R (Ref. 2.2.52, p. 2)
6.0.5-4	The diesel fuel vapor concentration is equal to the UFL for diesel fuel, which is 7.0%. The UFL and LFL for diesel fuel will vary depending on the concentrations of the components that comprise the grade of the fuel. A typical LFL for a low-sulfur diesel fuel is 0.9%; the UFL for the blend analyzed is 7.0% (Ref. 2.2.52). To provide a bounding quantity of diesel fuel in the diesel fuel-air vapor mixture, the UFL concentration of 7.0% is used.	Eq. 22	0.07 (Ref. 2.2.52, p. 2)
6.0.5-5	The space filled by the diesel fuel vapor is equivalent to the tank capacity. Under normal circumstances, the storage tank and tanker will always have liquid remaining, and a vapor mixture of diesel fuel and air will occupy the tank in the area above the liquid (including the freeboard area above the liquid). In order to conservatively estimate bounding TNT equivalencies for the diesel fuel vapor in the storage tank and in the tanker truck, the vapor mixture for each is calculated as if it occupies the equivalent volume of the liquid capacity.	Eq. 21	120,000 gal equivalent to approximately 16,044 ft³ for the Area 70A storage tank (Ref. 2.2.18, p. 1) 10,000 gal, equivalent to approximately 1,337 ft³ for the tanker truck

Table 6.0-3. Parameters Used to Estimate Stand-Off Distances for Explosion Involving the Area 70A or a Tanker Truck (Continued)

Parameter No.	Parameter Description	Applicable Equation No(s).	Input Value
6.0.5-6	The molecular weight of diesel fuel is equivalent to that of JP-5 jet fuel. The molecular weight of diesel varies with carbon and hydrogen content. Jet fuel JP-5, which is in the same family of gas oils or fuel oils as diesel, has a similar specific gravity and heat of combustion (0.83 and 43.0 MJ/kg, respectively (Ref. 2.2.77, p. A-36) as compared to a typical blend of diesel fuel (0.83 to 0.86) (Ref. 2.2.52, p. 4) and 44.4 MJ/kg (Ref. 2.2.50, p. 3-6), respectively. The JP-5 molecular weight used to represent diesel fuel oil in the estimation is 170 lb/lb-mol (Ref. 2.2.77, p. A-36)	Eq. 22	mw = 170 lb/lb-mol
6.0.5-7	There is sufficient oxygen present in the vapor space to ensure complete combustion of the diesel fuel vapor present. This is conservative and provides for a maximum TNT equivalent value. In reality, imperfect combustion occurs during accidental fires and explosion incidents, mainly due to turbulence, low supply of oxidizer, and other factors that produce free carbon particles (smoke), carbon monoxide, and the like (Ref. 2.2.60, p. 45).	—	—
6.0.5-8	The nominal empirical explosion efficiency, η , is 0.03. Estimating the effects of a diesel fuel vapor explosion inside of a bulk storage tank or tanker truck requires the knowledge of the efficiency of the explosion, as shown in Equation 20. The value of the explosion efficiency depends on the method used to determine the contributing mass of fuel (Ref. 2.2.2, p. 165). A value of 0.03 is adequate when the explosion is based on the quantity of fuel present in the vapor cloud, which is the approach followed. The efficiency of the explosion is dependent on the reactivity of the material, with higher reactivity giving a higher efficiency. Highly reactive materials are assigned higher efficiencies: an efficiency of 10% for diethyl ether, 5% for propane, and 15% for acetylene (Ref. 2.2.2, p. 165). Therefore, a nominal efficiency of 3% and a maximized case of 100% appear adequate.	Eq. 20	0.03 (nominal) 1 (maximum)

NOTE: °F = degree Fahrenheit; ft³ = cubic foot; gal = gallon; lb = pound; lb-mol = pound-mole; LFL = lower flammable limit; MJ/kg = megajoules per kilogram; mw = molecular weight; Pa = Pascal; psi = pounds per square inch; °R = degree Rankine; TNT = trinitrotoluene; UFL = upper flammable limit.

Source: Original

In addition to the parameters identified in Table 6.0-3, the inputs shown in Table 6.0-4 are used to estimate the pressure pulse generated by the combustion of diesel fuel.

Table 6.0-4. Additional Inputs Used for Quantitative Evaluation of a Fuel Tank Explosion

Input	Numerical Value/ Characteristic	Applicable Equation No(s).	Comment
Gas constant	10.73 ft ³ psi °R ⁻¹ lb-mol ⁻¹	Eq. 21	This value is used to calculate the number of moles of fuel vapor contained in the tank, using the ideal gas law, which is an appropriate approximation of the behavior of gases for the quantitative evaluation provided. (Ref. 2.2.88)
Heat of combustion of TNT	1,943 BTU/lb	Eq. 20	This value is the lower bound of a range of TNT heat combustions given in AIChE (Ref. 2.2.2, p. 160). By taking the lower value of the range, the vapor cloud in the storage tank has a calculated equivalent TNT mass greater than if a higher value from the range was used, based on the use of this value in Equation 20. The use of this value is conservative.
Heat of combustion of diesel fuel	44.4 MJ/kg (equivalent to 19,089 BTU/lb)	Eq. 20	This value varies depending on the grade of diesel; however, it is typical of those reported in literature. (Ref. 2.2.50, p. 3-6)
Design criteria for transportation cask	20 psi	N/A (used to evaluate stand-off distances)	Transportation casks are designed for the effects of increased external pressure equal to 20 psi (Ref. 2.2.67, Section 2.5.5.4) and (Ref. 2.3.3, Section 71.71, (c)(4)).
Waste handling facility structure design	1 psi	N/A (used to evaluate stand-off distances)	Waste handling facilities are evaluated for distance based on an increased external pressure of 1 psi (Ref. 2.2.74).

NOTE: ¹ J = 9.4782E-4 BTU and 1 lb = 0.4536 kg.
 BTU = British Thermal Unit; ft³ = cubic foot; kg = kilogram; lb = pound; lb-mol = pound-mole;
 MJ = megajoule; N/A = not applicable; psi = pound per square inch; °R = degree Rankine;
 TNT = trinitrotoluene.

Source: Original

The term *explosion*, in its most widely accepted sense, means a bursting associated with a loud, sharp noise and an expanding pressure front, varying from a supersonic shock wave to a relatively mild wind (Ref. 2.2.33, p. 4-17). A combustible vapor explodes under a very specific set of conditions. There are two explosive mechanisms that need to be considered when evaluating combustible vapor incidents: detonations and deflagrations. A detonation is a shock reaction where flames travel at supersonic speeds (i.e., faster than sound). Flames travel at subsonic speeds in a deflagration. It is generally recognized that vapor cloud explosions have flames that travel at subsonic speeds and are, therefore, technically classified as deflagrations but are still commonly referred to as explosions (Ref. 2.2.60, p. 48). Therefore, the postulated events in this analysis involve a vapor cloud explosion (deflagration) in Area 70A and in the diesel fuel tanker truck. The following three elements must exist simultaneously in order for a deflagration to occur:

1. A flammable mixture consisting of fuel and oxygen, usually from air, or other oxidant.
2. A means of ignition.
3. An enclosure.

The scenario analyzed includes the ignition of vapors in a tank, regardless of the cause or source of ignition (Table 6.0-3, Parameter 6.0.5-1). There is sufficient oxygen in the air present in the vapor mixture to act as an oxidizer and completely combust the diesel fuel present such that a bounding trinitrotoluene (TNT)-equivalent value is calculated for the deflagration (Table 6.0-3, Parameter 6.0.5-7).

With proper safety precautions and operating procedures, the occurrence of explosions in the vapor space of fixed-roof storage tanks or tanker trucks are rare events. Explosive mixtures may exist in the vapor space of a tank unless precautions are taken. Any vapor will seek an ignition source, so prevention of ignition cannot be guaranteed (Ref. 2.2.60, pp. 155-156).

The methods applied are based upon *Guidelines for Chemical Process Quantitative Risk Analysis* (Ref. 2.2.2), used to calculate TNT equivalencies and *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44), used to determine the increased external pressure at a given distance. Damages to structures and process equipment of a facility are dependent on the pressure generated by the explosion (Ref. 2.2.2, Tables 2.18a and 2.18b). To calculate the increased external pressure, TNT-equivalency is used. This postulates an equivalency between the flammable material and TNT, factored by an explosion efficiency term. This method is appropriate for this assessment because refined values of the damages caused by the explosion are not required, but rather reasonable estimates.

The following formula (Equation 20) is used to determine the TNT-equivalent values for the 120,000-gal tank (Area 70A) and the 10,000-gal tanker truck (Ref. 2.2.2, pp. 159 and 160):

$$W = \frac{\eta M E_c}{E_{TNT}} \quad (\text{Eq. 20})$$

where

- W = equivalent mass of TNT, in lb
- η = empirical explosion efficiency, unitless
- M = mass of hydrocarbon, in lb
- E_c = heat of combustion of flammable gas, in BTU/lb
- E_{TNT} = heat of combustion of TNT, in BTU/lb.

Hydrocarbon materials must first be in a vapor condition before combustion processes can occur. Consequently, the mass, M , of hydrocarbon is the mass of the diesel fuel in the diesel fuel–air vapor mixture in the storage tank and can be calculated using Equation 22, below. It is conservative to calculate the diesel fuel–air vapor mixture as if it occupies a volume equal to the entire tank capacity, which is 16,044 ft³ for Area 70A, and 1,337 ft³ for the tanker truck (Table 6.0-3, Parameter 6.0.5-5). In reality, each tank will always have a quantity of liquid diesel fuel present, with the diesel fuel–air vapor occupying the volume above the liquid, including the tank freeboard volume. However, considering the entire capacity to be available provides for a maximum value of the TNT-equivalent for the deflagration. The quantity, M , is calculated as a product of the total mass of the vapor mixture, the molecular weight, and the percent concentration.

To obtain the total mass of the diesel fuel–air vapor mixture (in lb-mol), Equation 21 is used. The pressure in the vapor space is evaluated as equivalent to atmospheric pressure, 14.70 psi, because such tanks are typically vented (Table 6.0-3, Parameter 6.0.5-2). The temperature in the vapor space is equivalent to a typical flash point of diesel fuel, 600°R (Table 6.0-3, Parameter 6.0.5-3). Using the stated volume for each container and the ideal gas law (Ref. 2.2.88, p. F-249), the mass of the diesel fuel–air vapor mixture, n_{tot} is calculated for Area 70A and for the tanker truck as:

$$n_{tot} = \frac{PV}{RT} \quad (\text{Eq. 21})$$

where

- n_{tot} = total mass of the diesel fuel–air vapor mixture, in lb-mole
- P = pressure of diesel fuel–air vapor cloud, in psi
- V = volume of diesel fuel–air vapor cloud, in cubic feet
- R = universal gas constant, in ft³•psi/lb-mole•R°
- T = temperature of diesel fuel–air vapor cloud, in R°

Therefore, for Area 70A,

$$n_{tot} = \frac{(14.70 \text{ psi})(16,044 \text{ ft}^3)}{(10.73 \text{ ft}^3 \cdot \text{psi}/^\circ\text{R} \cdot \text{lb} - \text{mole})(600^\circ\text{R})}$$

$$n_{tot} = 36.6 \text{ lb – mole}$$

and for the tanker truck,

$$n_{tot} = \frac{(14.70 \text{ psi})(1,337 \text{ ft}^3)}{(10.73 \text{ ft}^3 \cdot \text{psi}/^\circ\text{R} \cdot \text{lb – mole})(600^\circ\text{R})}$$

$$n_{tot} = 3.1 \text{ lb – mole}$$

As described in Parameter 6.0.5-4 (Table 6.0-3), the diesel fuel concentration, c , is equal to the UFL for diesel fuel, which is typically 7.0%. If the concentration of diesel fuel were in the intermediate range between the LFL and UFL, the ignition would be more intense and violent than if the mixture were closer to either the upper or lower limits; however, to maximize the TNT-equivalent values, the upper limit is chosen. The molecular weight of the diesel fuel is approximated to be equivalent to that for JP-5, that is, 170 lb/lb-mol (Table 6.0-3, Parameter 6.0.5-6). Using the mass of the diesel fuel–air vapor mixture (n_{tot}) calculated for each tank size, the mass of hydrocarbon, M , can be calculated using Equation. 22, as follows:

$$M = c n_{tot} mw \quad (\text{Eq. 22})$$

where

- M = mass of diesel fuel in the vapor, in lb
- c = diesel fuel concentration percentage, unitless
- n_{tot} = total mass of the diesel fuel–air vapor mixture, in lb-mole
- mw = molecular weight of the diesel fuel, in lb/lb-mole

Therefore, for Area 70A,

$$M = (0.07)(36.6 \text{ lb – mole})(170 \text{ lb/lb – mole})$$

$$M = 435.5 \text{ lb}$$

and for the tanker truck,

$$M = (0.07)(3.1 \text{ lb – mole})(170 \text{ lb/lb – mole})$$

$$M = 36.9 \text{ lb}$$

Equation 20 can now be used to calculate the TNT-equivalent of a deflagration involving 435.5 lb of diesel fuel in the vapor mixture for Area 70A and a deflagration of 36.9 lb for the tanker truck. The values of the heat of combustion for TNT and diesel fuel are $E_{TNT} = 1,943 \text{ BTU/lb}$ and $E_c = 19,089 \text{ BTU/lb}$, respectively (Table 6.0-4). The value of the explosion efficiency, η , is described in Table 6.0-3, parameter 6.0.5-8, with a nominal value of 3% (0.03) and maximized case of 100% (1.0).

Applying Equation 20 for the nominal case for Area 70A:

$$W = \frac{\eta M E_c}{E_{TNT}}$$

$$W = \frac{(0.03)(435.5 \text{ lb})(19,089 \text{ BTU/lb})}{1,943 \text{ BTU/lb}}$$

$$W = 128.4 \text{ lb}$$

Therefore, for the nominal case ($\eta = 0.03$), the equivalent mass of TNT, W , is calculated to be 128.4 lb for Area 70A. For the maximized case ($\eta = 1.0$), the value is 4278.6 lb.

Applying Equation 20 for the nominal case for the tanker truck:

$$W = \frac{\eta M E_c}{E_{TNT}}$$

$$W = \frac{(0.03)(36.9 \text{ lb})(19,089 \text{ BTU/lb})}{1,943 \text{ BTU/lb}}$$

$$W = 10.9 \text{ lb}$$

Therefore, for the nominal case ($\eta = 0.03$), the equivalent mass of TNT, W , is calculated to be 10.9 lb for the tanker truck. For the maximized case ($\eta = 1.0$), the value is 362.5 lb.

The safe distance in regards to the increased external pressure from a postulated explosion is evaluated based on 10 CFR Part 71, Subpart F (Ref. 2.3.3), and Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants* (Ref. 2.2.74), NUREG-1617 (Ref. 2.2.67), and *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44, p. 45). For the waste handling facilities and Area 70A, the safe distance is based on a level of peak positive incident overpressure below which no significant damage would be expected. Based on Regulatory Guide 1.91 (Ref. 2.2.74) a pressure level of 1 psi is used to determine a safe distance for the waste handling facilities. For the transportation casks outside of a facility, 20 psi is used to assess the safe distance, based on NUREG-1617 (Ref. 2.2.67) and 10 CFR Part 71 (Ref. 2.3.3).

To calculate the distance in feet from the explosion to a point at which the increased external pressure measures 20 psi and 1 psi for each of the explosion scenarios, the following equation (Equation 23) was used *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44). The equation is valid for an explosion at ground level at 20°C, ignoring any redirection of the overpressure by structures and terrain. If the explosion occurred up in the air (unconfined in all directions), the distance X would be reduced by a factor of 1.26.

$$X = W^{1/3} \exp[3.5031 - 0.7241 (\ln(P)) + 0.0398 (\ln(P))^2] \quad (\text{Eq. 23})$$

where

- X = distance to a given external pressure, P, in ft
- W = TNT equivalent mass, in lbs
- P = increased external pressure, in psi

Given the increased overpressures of 1 psi and 20 psi, the stand-off distance can be determined. The solver function in Excel was also used with Equation 23 to confirm the distances for each calculated TNT equivalent value. The spreadsheet is included electronically (Attachment H, *Shock wave dissipationR1.xls*). Table 6.0-5 presents the results.

Table 6.0-5. Estimated Stand-Off Distances for Area 70A and a Tanker Resupply Truck

Item Evaluated	Amount of Diesel Fuel Oil	TNT equivalent mass	Distance at which increased external pressure equals 20 psi ^a	Distance at which increased external pressure equals 1 psi ^a
Area 70A tanks	120,000 gal	$W_{\text{nominal}} = 128.4 \text{ lb}$	27 ft	168 ft
		$W_{\text{maximized}} = 4278.6 \text{ lb}$	88 ft	539 ft
Typical tanker truck	10,000 gal	$W_{\text{nominal}} = 10.9 \text{ lb}$	12 ft	74 ft
		$W_{\text{maximized}} = 362.5 \text{ lb}$	39 ft	237 ft

NOTE: ^a Rounded to nearest integer.
ft = foot; gal = gallon; lb = pound; psi = pound per square inch.

Source: Original

For the waste handling facilities, the nominal Area 70A stand-off distance is 168 ft for 1 psi, and maximized (i.e., calculated $\eta=1.0$), the stand-off distance is 539 ft. The nominal tanker truck stand-off distance is 74 ft for 1 psi, and maximized, the stand-off distance is 237 ft. The current site layout allows considerably more distance between Area 70A and the nearest waste handling facility than the nominal stand-off distance, and at least 200 ft more than the maximized distance (Ref. 2.2.28). Similarly, the roadways that the tanker trucks use to access Area 70A are located well beyond either the nominal or maximized distances to a waste handling facility (Ref. 2.2.28).

The site transportation routes used to move loaded transportation casks in the GROA are the closest to the BOP areas and roadways outside of the security fencing; therefore, transportation casks are at the highest risk for this initiating event. Transportation casks are designed to withstand an increased external pressure of 20 psi, so the nominal stand-off distance for Area 70A is 27 ft, and maximized, the stand-off distance is 88 ft. The nominal tanker truck stand-off distance is 12 ft for 20 psi, and maximized, the stand-off distance is 39 ft. The site transportation routes closest to Area 70A or to the roadways used by tanker trucks to access Area 70A are more than 150 ft inside a security fence and, therefore, well beyond the greatest distance of 88 ft (Ref. 2.2.28).

Therefore, no event sequence involving the waste handling facilities would be expected from a diesel fuel vapor explosion associated with either the 120,000-gal storage tank or a 10,000-gal tanker truck. Explosion of the diesel fuel oil storage tank (Area 70A) or of a tanker resupply truck is not analyzed further for categorization.

6.0.6 Conservatism in PEFA Values for Truck Trailer Collision Followed by Rollover/Drop

As summarized in Section 6.3.2.2 and detailed in Attachment D, Section D1, analysis of loaded transportation casks resulted in a passive equipment failure probability of 1E-08 for drops, which did not include or credit the impact limiters. The PSCA incorporated additional conservatism, electing to use 1E-05 for analyzing drops (termed “LLNL, adjusted”). In the waste handling facilities, many activities involving the transportation casks are performed without the impact limiters installed, so this conservatism is reasonable to allow for uncertainty in future cask and canister designs and epistemic uncertainty. However, site transportation activities involving transportation casks that are moved by the SPM always occur with impact limiters and buffer cars; therefore, a failure probability of 1E-05 for dropping a transportation cask is overly conservative. Thus, the actual calculated failure probability of 1E-08 can be applied appropriately for analyzing drops during site transportation activities that involve a transportation cask with impact limiters installed, while still maintaining conservatism.

6.0.7 Probability of Moderator Intrusion for Uncanistered Commercial SNF in Sealed Transportation Casks

For fires that occur in locations that contain uncanistered commercial SNF sealed within bolted transportation casks, the fire location is floor level. The analysis is performed without the salutary effects of fire suppression (for Intra-Site Operations this means response of firefighters) in order to demonstrate large margins of safety during fire event sequences. Should fire suppression be available, then cask failure would not occur (i.e., it would be orders of magnitude lower in probability). Therefore, if fire suppression water or a flood has occurred before or during the fire, there would be no breach of containment for entry into the cask. (Note that cask seal failure takes approximately one hour during a severe fire to occur and, thus, the breach analysis that ignores fire suppression is quite conservative.) The cask failure mode is from overpressurization and degradation of the seals between the lid and the shell; therefore, the area of the seal provides a small target for fire suppression entry. If the fire brigade responds or other unborated water becomes available after the cask has failed, then as long as the cask is internally pressurized, water cannot enter. Due to the heat source provided by the SNF, in addition to heat generated by the fire, there will always be a higher pressure on the inside of the cask than the atmosphere on the outside of the cask. Moreover, the small area associated with seal failure resists entry of significant amounts of water. There are no water sources other than those used by the fire brigade available during Intra-Site Operations activities.

6.0.8 Screening of Release Due to Rupture of Bare Fuel in Transportation Cask Exposed to Fire

If a transportation cask containing uncanistered commercial SNF is exposed to fire, the contents (fuel rods) could be heated to the point of degradation, allowing release of radionuclides within

the sealed transportation cask. In addition, if the fire reaches the top of the transportation cask and causes failure of the lid seals, the radionuclides could be released to the surroundings.

An assessment of the temperature at which SNF rods would fail is summarized in NUREG/CR-6672 (Ref. 2.2.82, Section 7.2.5.2). A critical review of accident conditions indicates that rod rupture is expected to occur at temperatures near 725°C to 750°C. After correcting for differences in burn-up and internal pressure, data in NUREG/CR-6672 (Ref. 2.2.82, Section 7.2.5.2) suggest that SNF rods may fail due to creep rupture at temperatures as low as 700°C or require temperatures as high as 850°C. Because the release of cesium vapors will be greater when rods fail at higher temperatures than lower temperatures, the middle of the range, about 750°C, is taken as the temperature at which rods fail by thermal rupture.

The probability of fuel rod failure at 750°C is 2.7E-04 given exposure to fire (Attachment D, Table D2.1-11). The probability of exposure of a transportation cask containing bare fuel to fire in the Truck or Rail Buffer Areas is 0.3 (Attachment F, Section F5.2.2). The overall probability that a transportation cask is exposed to a fire sufficient to cause rupture of the fuel rods contained within and release of radionuclides to the surroundings is $0.3 \times 2.7E-04$, that is, about 8E-05 for Intra-Site Operations.

The analysis includes some extreme conservatisms:

- A view factor of one was used to determine the probability that the fuel rods would heat up to the failure temperature, given exposure of the transportation cask to fire. Not all fires to which a transportation cask could be exposed would be positioned such that complete exposure to thermal radiation would be possible. For example, some severe fires would be expected to occur at ground level owing to diesel fuel pooling. Transportation casks are elevated on trucks.
- The lid seals are at the top of the transportation cask, which is approximately 15 feet tall. Only a limited fraction of the fires to which a transportation cask could be exposed would be large enough to cause failure of the lid seals even if the lower portion of the cask became hot enough to allow rupture of the fuel rods.

Thus, this event is considered to be beyond Category 2 and is screened from further analysis.

6.0.9 Loss of Electrical Power as an Initiating Event for Intra-Site Operations

Because activities associated with Intra-Site Operations generally occur outside of surface nuclear facilities, the loss of offsite power does not impact Intra-Site Operations with the exception of movers (i.e., site transporter and SPM) that are connected to AC power for operations within the surface nuclear facility. The AC power connection is made (and disconnected) outside of the facility. Intra-Site Operations include transit of the movers between the surface nuclear facility and outside. Therefore, the loss of power to the affected movers (including from a loss of offsite power) was treated as a contributing failure in the analysis as a potential site transporter or SPM collision initiating event.

6.1 EVENT TREE ANALYSIS

The event trees that are quantified in this analysis were developed from ESDs in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29, Attachment F (ESDs) and Attachment G (event trees)). This section describes the modeling of event sequences. The related event trees are discussed and presented in Attachment A.

6.1.1 Event Tree Analysis Methods

6.1.1.1 Linked Event Trees and Fault Trees

As described in Section 4, the PCSA uses event trees and fault trees to calculate the frequency of occurrence of event sequences. The event tree quantification is supported by FTA (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), active component reliability data (Section 6.3.1 and Attachment C), and PEFA (Section 6.3.2 and Attachment D). The SAPHIRE computer program is used as needed for the fault tree quantification process, and the event sequences generated from the event trees are quantified using a Microsoft Excel spreadsheet (discussions in Section 4.2 and Section 4.3.1 provide more information).

The YMP preclosure handling uses four types of buildings, as summarized below:

1. The RF accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.
2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program for placement in waste packages destined for emplacement in the repository emplacement drifts.
3. The WHF accepts DPCs and transportation casks containing uncanistered commercial SNF, transfers the SNF to TAD canisters which are destined for the CRCF or the aging pads.
4. The Initial Handling Facility (IHF) accepts SNF canisters from the Naval Nuclear Propulsion Program and some canisters containing HLW for placement in waste packages destined for emplacement in the repository emplacement drifts.

Preclosure waste handling as modeled in the PCSA also includes Subsurface Operations and Intra-Site Operations. Subsurface Operations involve the TEV, which accepts a waste package in the CRCF or IHF and, by means of rail, transports it and deposits it into the designated location in the emplacement drifts. All other waste form transportation in the GROA, BOP facilities, and the LLWF is evaluated as part of Intra-Site Operations.

Event sequences are developed for each of the four building types, Subsurface Operations, and Intra-Site Operations. Because each type of waste container transported has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container, included and described in the *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29). Event sequences are also developed separately for

each major group of waste handling processes during Intra-Site Operations. Therefore, event sequences also distinguish among the various steps in waste handling.

As described in Section 4.3, event sequences result in one of the following end states:

1. “OK”
2. Direct Exposure, Degraded Shielding
3. Direct Exposure, LOS
4. Radionuclide Release, Filtered (HVAC) (not applicable to Intra-Site Operations)
5. Radionuclide Release, Unfiltered (HVAC system is not operating)
6. Radionuclide Release, Filtered, Also Important to Criticality (not applicable to Intra-Site Operations)
7. Radionuclide Release, Unfiltered, Also Important to Criticality
8. Important to Criticality (not applicable to the CRCF).

Radionuclide release describes a condition where radioactive material has been released from the container creating a potential inhalation or ingestion hazard, accompanied by the potential for immersion in a radioactive plume and direct exposure.

Since the reliability model for Intra-Site Operations is less complex than those of the surface processing facilities, event sequences are not modeled completely in SAPHIRE. Instead, the event sequence logic depicted by the event trees is entered into an Excel spreadsheet, with the following data input:

- Event tree logic structure.
- Waste form throughputs and the number of opportunities for initiating the event sequence.
- Initiating event frequencies — In some cases, initiating events are modeled as fault trees, and in those instances, SAPHIRE is used to quantify the initiating event frequencies and uncertainties, with the results input into the spreadsheet.
- Basic event data that provides failure rates for active and passive equipment and for HFEs—The basic event data also includes a probability distribution of uncertainty associated with each basic event. The fault tree models are linked to the basic event library.

Each basic event in the fault tree is characterized by a probability distribution. SAPHIRE’s Monte Carlo sampling method is employed to propagate the uncertainties to obtain system failure probability or initiating event frequency mean values and parameters of the underlying

probability distribution such as standard deviation. As described in Section 4.3.6, categorization is done on aggregated event sequences, and the resultant probability distributions are also calculated in the Excel spreadsheet. For applicable fault tree models, SAPHIRE accounts for the correlation between analogous basic events sharing the same reliability information, ensuring that the spread of the probability distribution is not underestimated for the event sequences in which these basic events intervene.

6.1.1.2 Initiator, System-Response, and Self-Contained Event Trees

Event sequences are described and graphically depicted using one or two event trees, depending on whether the ESD considered has a single initiating event or multiple initiating events (represented on the ESD as one or more small circles):

1. **Self-contained event trees.** Self-contained event trees are used when only one initiating event appears in the corresponding ESD (Ref. 2.2.29, Attachment F). An example of a self-contained event tree is ISO-ESD05-LLWDAW, shown in Figure 6.1-1. The feed on the left side of the event tree is the event that represents the frequency of challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of low-level waste containers that are handled over the preclosure period. The initiating event is presented next, followed by the pivotal events. By convention, the description of each branching event is stated as a success. The branching under each event heading represents success by an upward branch and failure by a downward branch. If a given pivotal event cannot occur in a given sequence due to a prior pivotal event or is irrelevant to the sequence, it does not appear in the event sequence. Each pathway through a self-contained event tree terminates in an end state. End states that are labeled “OK” mean that the sequence of events does not result in one of the specifically identified undesired outcomes. “OK” may mean that normal operation can continue.

Containers containing DAW	Impact to single container at LLWF	Containment boundary of LLW container remains intact	#	END-STATE-NAMES
LLWDAW	INIT-EVENT	LLW-CONTAINER		
			1	OK
			2	OK
			3	RR-UNFILTERED

ISO-ESD05-LLWDAW - Single Container DAW LLW Operations in the LLWF 2008/01/28 Sheet 17

NOTE: DAW = dry active waste; ESD = event sequence diagram; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility.

Source: Original

Figure 6.1-1. Example of a Self-Contained Event Tree

- Separate initiator and SRETs.** Separate event trees for initiating events and system responses are used when more than one initiating event appears in the corresponding ESD. The IET decomposes a group of initiating events into the specific failure events that comprise the group. For example, an IET, ISO-ESD-01, and the corresponding SRET, RESPONSE-TCASK, are shown in Figures 6.1-2 and 6.1-3. In the IET, the feed on the left side is an event that represents the frequency of challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of transportation casks containing DPCs that are handled over the preclosure period. Unlike the self-contained event tree that has only one defined initiating event, separate initiator and system response event trees contain multiple initiating events. The initiating events for the example (Figure 6.1-2) are railcar derailment, railcar collision, truck trailer collision, and drop of an object on the transportation cask. Since these initiating events have different responses, the IET does not end at end states, but transfers to an SRET. The right side (branches) of the IET represent the initiating event values which, for the Intra-Site Operations, are the parameters of the distribution extracted from independent

SAPHIRE fault trees or basic event data and entered into the Excel spreadsheet. If multiple movements need to be accounted for, they are included in the Excel spreadsheet to calculate separately, however, in SAPHIRE models for a surface facility, these movements would be built into an initiating event fault tree.

Figure 6.1-3 provides an example SRET, RESPONSE-TCASK. System response event trees contain only pivotal events. Because the conditional probability of each pivotal event may be specific to the initiating event for each event sequence, the same SRET is quantified as many times as there are initiating events in the IET, using multiple lines in the Excel spreadsheet.

Transportation cask containing DPC	Identify initiating events		
DPC	INIT-EVENT	#	XFER-TO-RESP-TREE
	Railcar derailment	1	OK
	Railcar collision	2	T => 2
	Truck trailer collision	3	T => 2
	Drop of object	4	T => 2
		5	T => 2

ISO-ESD01-DPC - Movement of Transportation Cask Containing DPC on Railcar 2008/01/28 Sheet 1

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; RESP = response; TCASK = transportation cask; XFER = transfer.

Source: Original

Figure 6.1-2. Example of an Initiator Event Tree

INIT-EVENT	TRANSCASK	CANISTER	SHIELDING	MODERATOR	#	END-STATE-NAMES
					1	OK
					2	DE-SHIELD-DEGRADE
					3	DE-SHIELD-LOSS
					4	RR-UNFILTERED
					5	RR-UNFILTERED-ITC

RESPONSE-TCASK - Transportation Cask System Response 2008/01/28 Sheet 2

NOTE: DE = direct exposure; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure 6.1-3. Example of a System Response Event Tree

6.1.1.3 Summary of the Major Pivotal Events

A self-contained event tree or an SRET may include pivotal events concerning the success or failure of the cask, canister, shielding properties, and moderator intrusion susceptibility. The pivotal events are summarized in Attachment A, Section A3.

The pivotal events applicable to the analysis of Intra-Site Operations do not have associated fault trees because they are used in Excel as point values from the summary of passive event failure probabilities table in Section 6.3. Sections 6.2 and 6.3 provide details about the reliability information developed for this analysis.

6.1.2 Waste Form Throughputs

Each IET and self-contained event tree begins with the container throughputs, if applicable, that is, the numbers of casks, aging overpacks, or low-level radioactive waste (LLW) containers to be handled over the preclosure period. The number of containers transported during Intra-Site Operations activities is shown in Table 6.1-1. This number is drawn into the descriptions of

specific event trees as needed. With the number of containers as a multiplier in the event tree and the initiating events specified as a probability per container, the value passed to the system response is the number of occurrences of the initiating event expected over the period of operation. In event sequences for which the given frequency for an initiator is the frequency of occurrence over the preclosure period, such as fire events, the number of waste forms is not included separately.

Table 6.1-1. Waste Form Throughputs over the Preclosure Period

Waste Form Unit	ISO Throughput	Comment
Transportation casks containing a TAD canister	6,978	One canister per cask
Transportation casks containing a dual-purpose canister	346	One canister per cask
Transportation casks containing HLW canisters	2,360	1,860 rail-based transportation casks containing 5 HLW canisters and 500 truck-based transportation casks containing 1 HLW canister
Transportation casks containing DOE standardized canisters	385	5 to 9 canisters per transportation cask
Transportation casks containing MCOs	113	4 canisters per transportation cask
Transportation casks or horizontal shielded transfer casks containing a horizontal DPC	346	These DPCs are sent directly to or come from aging.
Transportation casks containing a naval canister	400	One canister per cask
Transportation cask containing uncanistered CSNF assemblies	3,775	9 BWR or 4 PWR SNF assemblies per cask
Aging overpack containing a TAD canister	8,143	One canister per aging overpack
Aging overpack containing a vertical DPC	346	One canister per aging overpack

NOTE: BWR = boiling water reactor; CSNF = commercial spent nuclear fuel; DOE = U.S. Department of Energy; DPC = dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; MCO = multiccanister overpack; PWR = pressurized water reactor; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Ref. 2.2.23, Table 4

6.1.3 Guide to Event Trees

Event tree figures are located in Attachment A. Table 6.1-2 contains the crosswalk from each ESD developed in the event sequence development analysis (Ref. 2.2.29, Attachment F) to the associated IET and SRET figure location in Attachment A, Table A5-1.

Table 6.1-2. Figure Locations for Initiator Event Trees and System Response Event Trees

ESD#	ESD Title	Initiator Event Tree Name	Initiator Event Tree Location	System Response Event Tree Name	System Response Event Tree Location
ISO-ESD-01	Event Sequences for Activities Associated with Movement of Transportation Cask during Site Transportation	ISO-ESD01-DPC ISO-ESD01-DSTD ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-MCO ISO-ESD01-NAV ISO-ESD01-TAD ISO-ESD01-UCSNF	Figure A5-2 Figure A5-4 Figure A5-5 Figure A5-6 Figure A5-7 Figure A5-8 Figure A5-9 Figure A5-10	RESPONSE-TCASK	Figure A5-3
ISO-ESD-02	Event Sequences for Activities Associated with Aging Overpack Transit, Placement, and Retrieval	ISO-ESD02-DPC ISO-ESD02-TAD	Figure A5-11 Figure A5-13	RESPONSE-AO	Figure A5-12
ISO-ESD-03	Event Sequences for Activities Associated with the Transporting and Positioning of an HTC or an HSTC	ISO-ESD03-HDPC	Figure A5-14	RESPONSE-HTC	Figure A5-15
ISO-ESD-04	Event Sequences Associated with Impacts during Canister Operations at a Horizontal Aging Module	ISO-ESD04-HDPC	Figure A5-16	RESPONSE-HAM	Figure A5-17
ISO-ESD-05	Event Sequences for Activities Associated with a Single Low-Level Radioactive Waste Container at the Low-Level Waste Facility	ISO-ESD05-LLWDAW ISO-ESD05-LLWLIQ ISO-ESD05-LLWWETnr	Figure A5-18 Figure A5-19 Figure A5-20	N/A	N/A
ISO-ESD-06	Event Sequences Associated with Nonfire Events Involving all Low-Level Radioactive Waste Containers at the Low-Level Waste Facility	ISO-ESD06-LLW	Figure A5-21	N/A	N/A

Table 6.1-2. Figure Locations for Initiator Event Trees and System Response Event Trees (Continued)

ESD#	ESD Title	Initiator Event Tree Name	Initiator Event Tree Location	System Response Event Tree Name	System Response Event Tree Location
ISO-ESD-07	Event Sequences Associated with Fire Events for All Combustible Low-Level Radioactive Waste at the Low-Level Waste Facility	ISO-ESD07-LLW	Figure A5-22	N/A	N/A
ISO-ESD-08	Event Sequences for Activities Associated with Waste Transfers to the Low-Level Waste Facility	ISO-ESD08-LLWDAW ISO-ESD08-LLWLIQ ISO-ESD08-LLWWETnr ISO-ESD08-LLWWETr	Figure A5-23 Figure A5-25 Figure A5-26 Figure A5-27	RESPONSE-LLW	Figure A5-24
ISO-ESD-09	Event Sequences for Fire Occurring during Site Transportation Activities or at the Aging Facility	ISO-ESD09-DPC ISO-ESD09-DSTD ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-MCO ISO-ESD09-NAV ISO-ESD09-TAD ISO-ESD09-UCSNF	Figure A5-28 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34 Figure A5-35 Figure A5-36	RESPONSE-FIRE	Figure A5-29

NOTE: AO = aging overpack; DAW = dry active low-level radioactive waste; DPC = dual-purpose canister; DOE = U.S. Department of Energy; DSTD = DOE standardized canister; ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations; LLW = low-level radioactive waste; MCO = multiccanister overpack; NAV = naval; nr = nonresin; r = resin; TAD = transportation, aging and disposal (canister); TCASK = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

INTENTIONALLY LEFT BLANK

6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS

6.2.1 Approach to Analysis of Initiating and Pivotal Events for Linking to Event Sequence Quantification

Section 4.3.2 provides a brief introduction to the application of FTA for initiating and pivotal events, including an example fault tree. Many of the initiating events involve faults in complex machinery for which no historical data exists at the system level; however, an exception to this lack of information is the historical data on load drops from cranes. Therefore, FTA is employed to map elements of equipment, design, and operational features to various failure modes of components down to a level of assembly, termed “basic events” for which historical data is available. Attachment B presents the fault tree logic and stand-alone quantifications.

Much of the equipment used in the Intra-Site Operations is also used in the surface facilities. Furthermore, a given system, such as the site transporter, may affect the event sequences for several operational nodes of the same facility or several kinds of waste forms, as it does for Intra-Site Operations. Therefore, the logic of the fault trees described in this section and Attachment B are linked to event trees where appropriate, via an intermediate top event name that is unique to the event sequence per the waste form involved and operational node. In this way, the logic structure of the system fault tree may be used over and over.

The fault trees are linked to the event trees via an Excel spreadsheet. Other data inputs to the event tree are either input directly into the spreadsheet representation or are updated through the application of the statistical capabilities of SAPHIRE to generate the required distribution parameters (mean, median, and standard deviation) used to describe the uncertainty associated with the quantified event sequences. The data quantification is usually simple, one or two basic event fault trees, usually having a single top event, an OR gate or AND gate that has the basic events as inputs.

Attachment B, Sections B1 through B3, present all of the system fault trees. These sections describe the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B4 presents the additional fault trees (simple data quantification trees) used in the Intra-Site Operations analysis. These fault trees are self-explanatory, and they are quantified only to develop the appropriate distribution parameters used in the Excel spreadsheet quantification of the event sequences.

A top event occurs when one of the ITS success criteria for a given SSC fails to be achieved. At least one success criterion is defined for each system. Multiple success criteria are defined for systems that perform multiple safety functions in the Intra-Site Operations.

Each of the top events for the initiating event fault trees represent the conditional probability that the top event will occur when the system is put into service. That is, the results of the FTA answer a question such as “what is the probability for each canister movement that the site transporter drops the canister?” The expected number of canister drop initiating events during the preclosure period is the product of the number of times a canister is moved by the site transporter during the preclosure operations and the conditional probability of the top event. Such values for the expected number of canister drops are not developed directly, however.

Instead, the IET representation in the Excel spreadsheet links the various fault tree logic models to the canister, or other waste form, and the throughput values to generate the quantified event sequence.

In general, each of the FTAs in Attachment B is developed to include both HFEs, and mechanical failures that result in the occurrence of the top event. The HFEs include postulated unintended operator actions that could potentially occur during the facility activity and, as applicable, hardware failures for those SSCs whose function is to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (electrical, mechanical, etc.) and failures from the loss of a supporting system (e.g., loss of power).

For quantification of the probability of the top event, failure probabilities are developed for each basic event (hardware or HFE) and are used to compute the probability of each cut set. For component failure data that is expressed as “failures per hour,” a “mission time” must be defined. In many instances in the FTA quantification, a mission time of one hour is used if this value is conservative. Where mission time is critical, appropriate times are justified and incorporated into the event sequence quantification. Hardware failure probabilities are taken from the reliability analysis data discussed in Sections 6.3. HFE probabilities are taken from the HFE analysis discussed in Section 6.4.

Uncertainties in the probabilities of basic events are included in the inputs to the SAPHIRE FTA. The uncertainties are propagated through the FTA to yield the uncertainty distribution of the top event.

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

- Basic event data
- Common-cause and common-mode failures such as failures induced by common training, maintenance practices, fabrication, common electrical supplies, etc.
- Support systems and subsystems such as HVAC and electrical, etc.
- System interactions
- HFEs
- Control logic malfunctions.

The following subsections provide summaries of the analyses detailed in Attachment B. For each fault tree, the following information is provided:

- Physical description
- Operation
- Control system
- System/pivotal event success criteria

- Mission time
- Fault tree results.

6.2.2 Summary of Fault Tree Analysis

6.2.2.1 SPM FTA

The FTA is detailed in Attachment B, Section B1. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

6.2.2.1.1 Physical Description

The SPM is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs for both the Intra-Site and within the site facilities. Movement of the SPM with railcars or SPM with truck trailers within the site facilities is limited to the entrance vestibule and the Cask Preparation Room.

Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations. The driving and braking power comes directly from the road tires, as they are in contact with the rails. A diesel engine provides the energy to operate the SPM outside the facilities. Inside, the SPM is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

6.2.2.1.2 Operations

SPM activities for Intra-Site Operations begin once the railcar or truck trailer carrying a transportation cask arrive onsite at the receipt area. Receipt activities include the placement of temporary protective shielding around the railcar or truck trailer, inspection of the transportation cask, and connection of the railcar or truck trailer to the SPM. Once all receipt activities are completed the SPM with the railcar or truck trailer proceeds to the appropriate facility (CRCF, IHF, RF, or WHF) or, if the facility is not immediately available to receive the cask, to the appropriate buffer area.

In the event of loss of power, the SPM is designed to stop, retain control of the railcar or truck trailer, and enter a locked mode where it remains until operator action is taken, to return to normal operations.

6.2.2.1.3 Control System

A simplified schematic of the functional components on the Site Prime Mover Railcar/Truck Trailer (SPMRC/SPMTT) is shown in Attachment B, Section B1.

The control system provides features for preventing initiating events:

- The SPM is designed to stop whenever commanded to stop or when there is a loss of power.
- The operator can stop the SPM by either commanding a “stop” from the start/stop button or by releasing the palm switch which initiates an emergency stop.
- At anytime there is a loss of power detected, the SPM will immediately stop all movement and enter into “lock mode” safe state. The SPM will remain in this locked mode until power is returned and the operator restarts the SPM.

6.2.2.1.4 System/Pivotal Event Success Criteria

Success criteria for the SPM are the following:

- Prevent collisions which includes:
 - Prevent a runaway situation
 - Respond correctly to operator commands.

Various design features are provided to achieve this success criterion.

6.2.2.1.5 Mission Time

A nominal one-hour mission time is used to calculate the failure probability for components having a time-based failure rate. Otherwise, failure-on-demand probabilities are used.

For railcar derailment, the probability is based on the distance traveled from the receipt area to any facility; 2.0 miles is used for the distance to all facilities, an industry data derailment rate of $1.18E-5$ per mile traveled (Attachment C, Table C4-1, DER-FOM).

6.2.2.1.6 Fault Tree Results

The detailed description in Attachment B, Section B1 documents the application of basic event data, CCFs, and HRA (refer also to Attachment E).

The SPMRC or SPMTT has two credible failure scenarios:

- Collision with site structures, including doors
- SPMRC derailment.

These failure modes may occur with various waste forms that are received in the transportation casks. The site transporter collision with the facility door fault tree model was used to model the collision of the facility door with the SPM.

Results of the analysis are summarized in Table 6.2-1.

Table 6.2-1. Summary of Top Event Quantification for the SPM

Top Event	Mean Probability	Standard Deviation
SPMRC collides with facility structures	4.5E-03	1.3E-02
SPMRC derailment	2.4E-05	2.6E-06
SPMTT collides with facility structures	4.4E-03	1.5E-02

NOTE: SPM = site prime mover; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.

Source: Attachment B, Figures B1.4-1, B1.4-6, B4-2, and Table B4-3

6.2.2.2 Site Transporter FTA

The FTA for the site transporter is detailed in Attachment B, Section B2. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

6.2.2.2.1 Physical Description

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a concrete and steel ventilated aging overpack from a facility vestibule to the aging pads.

The site transporter is a track driven vehicle with four synchronized tracks (two on each side). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not ITS. An integrated diesel powered electric generator provides the energy to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

A rear fork assembly and a pair of support arms are used to lift and lower the cask. The rear forks are inserted in two rectangular slots near the base of aging overpack. Casks are carried in a vertical orientation with the lid at the top. Access to the top of the casks is unobstructed.

A passive restraint system provides stabilization during cask movement. These restraints come into contact with the cask after it has been raised to the desire height. A pin is inserted into each of the three restraint arms to keep the restraint in place, should there be a failure of the electromechanical assembly. The pins also serve as an interlock that prevents movement of a loaded site transporter without the restraints being properly installed.

6.2.2.2.2 Control System

There are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter. All safety interlocks and controls of the site transporter are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No programmable logic controller (PLC) or computer is used to control the machine.

6.2.2.2.3 Normal Operations

Once the aging overpack is securely positioned on the site transporter, movement of the loaded site transporter can begin.

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. At the facility, the operator stops the site transporter outside the facility's entrance vestibule and turns off the diesel generator, and an electric power cable is attached.

Once inside the building, the operator positions the site transporter in the Cask Preparation Room and in the Cask Unloading Rooms.

6.2.2.2.4 System/Pivotal Event Success Criteria

Success criteria for the site transporter are the following:

- Prevent a collision of the site transporter with objects, structures, or shield doors which includes
 - Prevent runaway situations
 - Prevent site transporter movements in the wrong direction.

Various design features are provided to achieve these success criteria. The failure to achieve this success criterion defines the top event for a fault tree for the site transporter.

6.2.2.2.5 Mission Time

For quantification of the site transporter fault trees in Attachment B, Section B2, a mission time of one hour per cask transfer is used.

6.2.2.2.6 Fault Tree Results

There are two basic site transporter fault trees developed for the Intra-Site Operations. The scenarios represented and the variations by these fault trees are the following:

1. Site transporter collides with site structures (including facility doors) or other vehicles:
 - A. Importing aging overpack from aging pads to Cask Preparation Room.
 - B. Export aging overpack from Cask Preparation Room to aging pad.
2. Site transporter drops an aging overpack.

The results of the analysis are summarized in Table 6.2-2 for the fault trees.

Table 6.2-2. Summary of Top Event Quantification for the Site Transporter

Top Event	Mean Probability	Standard Deviation
Collision	4.8E-03	1.6E-02
Drop	4.0E-08	1.2E-07

Source: Attachment B, Figures B2.4-1, B2.4-6

6.2.2.3 Cask Tractor and Cask Transfer Trailer FTA

The FTA for the cask tractor/cask transfer trailer is detailed in Attachment B, Section B3. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

6.2.2.3.1 Physical Description

The cask tractor is a large, four-wheel drive, diesel tractor designed specifically for pulling the cask transfer trailer. The cask tractor has redundant brakes in addition to having a fail-safe emergency brake. The cask transfer trailer has independently mounted non-driven hydraulic pendular axles with a minimum of four tires per axles that will ensure the cask remains level during transportation across uneven terrain. In addition to the pendular axles, the cask transfer trailer has three other hydraulic systems: (1) stabilizing jacks, (2) cask support skid and positioning system, and (3) hydraulic ram.

6.2.2.3.2 Control System

Operators manually control every operation on the cask tractor/cask transfer trailer. All safety interlocks and controls of the cask tractor and cask transfer trailer are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No PLC or computer is used to control the machine.

6.2.2.3.3 Normal Operations

For normal operations the horizontal cask tractor and trailer are used to transport horizontal casks from facilities to the aging pads. At the aging pads the cask tractor and cask transfer trailer have self-contained rams to insert the horizontal cask into the HAM.

6.2.2.3.4 System/Pivotal Event Success Criteria

Success criterion for the cask tractor and cask transfer trailer is the following:

- Prevent a collision of the cask transfer trailer with objects, or structure doors which include:
 - Prevent runaway situations
 - Prevent site transporter movements in the wrong direction
 - Prevent a load drop during lift/lower or transport operations.

Various design features are provided to achieve the success criteria. The failure to achieve this success criterion defines the top event for a fault tree for the cask tractor and cask transfer trailer.

6.2.2.3.5 Mission Time

For quantification of the cask transfer trailer fault trees in Attachment B, Section B3, a mission time of two hours per cask transfer is used, except for the failures associated with the facility door closing on the cask transfer trailer for which a mission time of one hour was used.

6.2.2.3.6 Fault Tree Results

There is one basic cask tractor and cask transfer trailer fault tree developed for Intra-Site Operations. The scenarios represented and the variations by these fault trees are the following: Cask tractor and cask transfer trailer collision with site structures, vehicles, or facility doors:

- A. Importing horizontal transfer casks from aging pads to Cask Preparation Room.
- B. Export horizontal transfer casks from Cask Preparation Room to aging pads.

The results of the analysis are summarized in Table 6.2-3 for the fault tree.

Table 6.2-3. Summary of Top Event Quantification for the Cask Tractor and Cask Transfer Trailer

Top Event	Mean Probability	Standard Deviation
Collision	4.8E-3	2.9E-2

Source: Attachment B, Figure B3.4-1

6.2.2.4 Additional Fault Trees

Eleven additional fault trees were developed to address events that could impact Intra-Site Operations and are detailed in Attachment B, Section B4. These fault trees are identified in Table 6.2-4. All of these trees are top level trees. The results of quantifying these trees were input directly into the Excel spreadsheet used to quantify Intra-Site event sequences as initiating events. Some provide the link between the top level events in the event trees and the system fault trees described in Attachment B, Sections B1 through B3. This relationship is identified in Table 6.2-4.

Table 6.2-4. Top Level and Linking Fault Trees

Fault Tree	Description	Events considered	System Fault Trees Used as Input
INTRASITE-PMRC-COLLIDE	SPMRC collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMRC-COLLISION (B1.4.1)
INTRASITE-DERAIL	SPMRC derails during transit from receipt area to facility	SPMRC derailment	None
INTRASITE-PMTT-COLLIDE	SPMTT collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMTT-COLLISION (B1.4.2)
INTRASITE-JIB-CRANE	Drop of heavy load onto TC during receipt processing and transit to facility	Crane drops onto TC	None
INTRASITE-ST-COLLIDE	ST collisions in transport of aging overpack from facility to Aging Facility	Collisions during transit or with facility door	INT-2-ST-COLLISION (B2.4)
INTRASITE-HCTT-COLLISION	HCTT collisions in transport of horizontal casks from facility to Aging Facility	HCTT collision during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HCTT-DROP	HCTT drops in transport of horizontal casks from facility to Aging Facility	HCTT drops during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HAM-INSERT	Canister damaged during insertion into HAM	Operator or equipment failure during canister insertion into HAM	None
INTRASITE-HAM-AUX-EQUIPMENT	HAM damaged during canister loading/unloading operations	Impacts from crane operation	None
INTRASITE-HEPA-TRANSFER	Damage to LLW container during transit from WHF to LLWF or offsite	Vehicle collisions during transit	None
INTRASITE-COLL-TRANSFER	Damage to LLW container during transit from WHF to LLWF	Forklift or vehicle collisions during transit	None

NOTE: HAM = horizontal aging module; HCTT = cask tractor/cask transfer trailer (used only for SAPHIRE fault tree codes); LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; ST = site transporter; TC = transportation cask; WHF = Wet Handling Facility.

Source: Original

INTENTIONALLY LEFT BLANK

6.3 DATA UTILIZATION

6.3.1 Active Component Reliability Data

The fault tree models described in Section 6.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. The active component reliability estimates are developed by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represent the range of the industry-wide information.

6.3.1.1 Industry-Wide Reliability Data for Active Components

While data from the facility being studied are the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP is a one-of-a-kind facility, it is necessary to develop the required data from industry-wide data experience of other industries. Industry-wide data sources are documents containing industrial or military experience on component performance. Usually data sources are previous safety/risk analyses and reliability studies performed nationally or internationally, but the data source can also be standards or published handbooks. For the YMP PCSA, an industry-wide database is constructed using a library of industry-wide data sources of reliability data from nuclear power plants, as well as equipment used by the military, chemical processing plants, and other facilities. The sources used are listed in Attachment C, Section C1.2.

The data source scope must be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might be used for electronics data versus mechanical data, so long as the detail and the applicability of the information provided justify its use. In addition, the quality of the data source is considered to be a measure of the source's credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort is made in this analysis to use the highest quality data source available for each active component type and failure mode (TYP-FM).

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the generic source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, is to evaluate the similarity between the YMP operating environment and that represented in each data source to ensure data appropriateness. This evaluation process is described in Attachment C, Section C1.2.

Given the fact that the YMP is a relatively unique facility (although portions are similar to the SNF handling and storage areas of commercial nuclear plants), the data development perspective is to collect as much relevant failure estimate information as possible to cover the spectrum of equipment operational experience. It is reasonable to expect that the YMP equipment would fall

within this spectrum (Section 3.2.1). The scope of the sources selected for this data set is therefore deliberately broad to take advantage of the combined experience of many facilities, not a single plant. It is then intended to provide a combined estimate that reflects as best as possible the uncertainty ranges of the individual estimates. This ensures that the data are not skewed towards the possibly atypical behavior of one particular plant, industry or operating environment. The combinatorial process, utilizing Bayes' theorem, is discussed in the following subsection.

Among the active components whose reliability is quantified with industry-wide data are the 200-ton cranes, jib cranes, waste package maneuvering cranes, and the SNF transfer machine (SFTM). Cranes other than mobile/portable (jib) cranes and the SFTM are not used in Intra-Site operations; however they are being discussed in this section for completeness. The rationale for using such data for these estimates is that a significant amount of crane experience exists within the commercial nuclear power industry and other applications, and this experience can be used to bound the anticipated crane performance at YMP. Furthermore, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants. Crane and SFTM handling incidents that result in a drop are included in the drop probability regardless of cause; they may be caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

Every attempt was made to find more than one data source for each TYP-FM, although multiple sources are not always available for a specific piece of equipment. When data was extracted from several sources in many cases, then combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs were quantified with one data source, 8% with two data sources, 8% with three data sources and 31% with four or more data sources.

6.3.1.2 Application of Bayes' Theorem to PCSA Database

The application of industry-wide data sources introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes' theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in NUREG/CR-6823 (Ref. 2.2.8, Section 8). For the PCSA, the method known as "parametric empirical Bayes" is primarily used. This permits a variety of different sources to be statistically combined and compared, whether the inputs are expressed as the number of failures and exposure time or demands, or as means and lognormal error factors.

A typical application of Bayes' theorem is illustrated as follows. A failure rate for a given component is needed for a fault tree (e.g., a fan motor in the HVAC system). There is no absolute value for the failure rate, but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data to the YMP introduces uncertainty in the analysis of the reliability of the

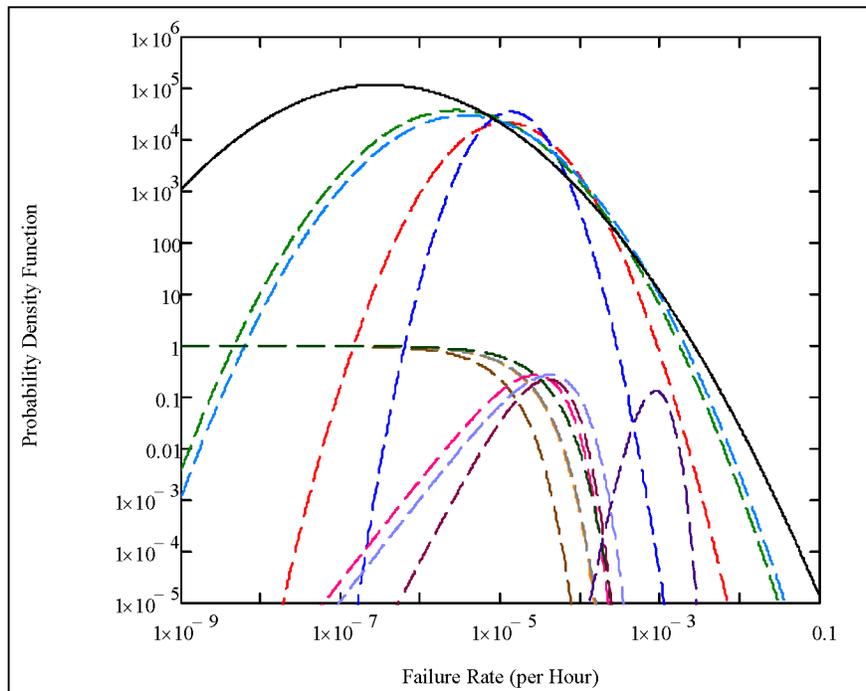
HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying available data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trials if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur over a certain exposure, operational, or test duration.
3. Update the probability distribution for the failure rate based on the new body of evidence.

The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The mathematical expression for applying Bayes' theorem to data analysis is described in Attachment C, Section C2.

For the analysis presented herein, MathCAD is used to calculate the population-variability (prior) distributions of active components. As described in Attachment C, Section C2.1, the method of "The Combined Use of Data and Expert Estimates in Population Variability Analysis" (Ref. 2.2.54, pp. 311–321) is used as the basis example for the combinations performed. In this method, the population-variability distribution of the failure rate is approximated by a lognormal distribution whose unknown parameters, ν and τ , respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating ν and τ involves calculating the likelihood function associated with the reliability information in each data source. For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate x , and characterized by its median value and associated error factor. For a data source providing exposure data (given in the form of a number n of recorded failures over an exposure time t), the likelihood function is a Poisson distribution, expressing the probability that n failures are observed when the expected number of failures is x times t .

The maximum likelihood method is used to calculate ν and τ . This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source because the data sources are independent from each other. It is equivalent and computationally convenient to find the maximum likelihood estimators for ν and τ by using the sum of the log-likelihood (logarithm of the likelihood) of each data source. As a result, the likelihood functions from the individual data sources and a population-variability PDF for the combination are produced and plotted for comparison, as in the example shown as Figure 6.3-1.



Source: Attachment C, Figure C2.1-1

Figure 6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

If only a single data source is considered applicable to a given TYP-FM combination and 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. However, 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 (i.e., gamma for time-related failure modes, and beta for demand-based failure modes).

Example implementations of the methods used for these cases are provided in Attachment C, Section C2.2.

6.3.1.3 Common-Cause Failure Data

Dependent failures are modeled in event tree and fault tree logic models. When possible, potential dependent failures are modeled explicitly via the logic models. For example, failure of the HVAC system is explicitly dependent upon failure in the electrical supply system that is modeled in the fault trees. Similarly, the effects of erroneous calibration or other HFEs can be explicitly included in the system fault tree models and the basic event probabilities considered during the HRA. Otherwise, potential dependencies known as CCFs are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate CCF probabilities.

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. 2.2.46), the Multiple Greek Letter method *Analytical Background and Techniques*. Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780 (Ref. 2.2.58), and the Alpha Factor method (Ref. 2.2.59). In a parametric model, the probability of two or more components failing by a CCF is estimated by use of the equations provided in Section 4.3.3.3.

For the PCSA, CCF rates or probabilities are estimated using the *Alpha Factor Method* (Ref. 2.2.59) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in NUREG/CR-5485 (Ref. 2.2.59) consisted of:

1. Identifying the number of redundant components in each subsystem being reported, (e.g., two, three, or four (termed the CCF group size)).
2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, (i.e., one component at a time, two components at a time, and so on up to failure of all components in a given CCF group).
3. Calculating the alpha factor for a given component type to provide a basis for estimating the probability of CCFs involving two, three, etc., or all components (the equation in Attachment C, Section C3 provides more information).
4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produces prior distributions for the alpha factors. The results are the mean alpha factors and uncertainty bounds, reported in NUREG/CR-5485 (Ref. 2.2.59, Table 5-11) and reproduced in Attachment C, Table C3-1.

These alpha-factor values are used for failure-on-demand events (e.g., pump fails to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run). For example, for a two-out-of-two failure on demand event, the mean alpha factor of 0.047 (shown in the far right column of Table C3-1 associated with α_2) was used in conjunction with the mean failure probability for the appropriate component type and failure mode (from Table C4-1) as inputs to a compound event to yield the common-cause failure probability.

Similarly, for the two-out-of-two operational failure, the mean alpha factor identified above is divided by 2 (0.0235) and is used in conjunction with the mean failure probability for the appropriate component type and operational failure mode. In addition, the parameter b associated with the beta distribution function for the alpha factor (Table C3-1) is modified to reflect the change in the alpha factor mean value while preserving the coefficient of variation from the distribution described by the parameters presented in Table C3-1. To preserve the coefficient of variation, the variance associated with the distribution is reduced by a factor of 4

(the square of the reduction of the mean). (See Attachment C, Section C3 for the derivation of the value for the parameter b.) The parameter b for the operational α_2 is 21.03.

6.3.1.4 Input to SAPHIRE Models

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data has to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

- .BEA – attributes to assign information to the proper SAPHIRE fields
- .BED – descriptions of the component type name and failure mode
- .BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement to ensure that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the PCSA case was the TYP-FM coding). Examples of descriptions used for the PCSA template data were: clutch failed to operate, relay spurious operation, position sensor fails on demand, and wire rope breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the lognormal error factor, or the shape parameter of the beta or gamma distributions.

Geometric means of the input parameters from the data sources are initially used as screening values for each TYP-FM and are entered into the .BEI file, along with a default error factor of 10. Once the Bayesian combination process is completed for all of the TYP-FM combinations, mean and uncertainty parameter information are entered into the .BEI files, and tested in SAPHIRE before being distributed to the systems analysts.

The template data is used by the fault tree models. The data is imported into SAPHIRE using the MAR-D portion of the SAPHIRE code, then the modify event feature links the template data to each basic event in the fault tree. This permits each active component of the same TYP-FM to mode to utilize the same failure estimate and uncertainty information, based on the results of the industry-wide data investigation and Bayesian combination process.

Attachment C, Section C4, presents a more thorough discussion of the active component reliability data development process, as well as a table of the template data that is imported into SAPHIRE.

6.3.1.5 Summary of Active Component Reliability Data in Intra-Site Operations Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the Intra-Site models. Development of this table is discussed in detail in Attachment C, Section C4.

Table 6.3-1.Active Component Reliability Data Summary

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-CRWT-ATB1001-AT--FOH	Screw Actuator Mechanism on Lift Boom #1 Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATB1011-AT--FOH	Screw Actuator Mechanism on Lift Boom #1 Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATB2002-AT--FOH	Screw Actuator Mechanism on Lift Boom #2 Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATB222-AT--FOH	Screw Actuator Mechanism on Lift Boom #2 Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATD0002-AT--FOH	ST D-Axis Electrical Actuator #2 Fails Lift/Lower	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATD001-AT--FOH	ST D-Axis Electrical Actuator #1 Fails Lift/Lower	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATD03-AT--FOH	ST D Axis Electrical Actuator #1 Movement Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATD04-AT--FOH	ST D-Axis Electrical Actuator #2 Movement Fails	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATP002-AT--FOH	ST P-Axis Electrical Failure During Movement	3	7.54E-05	7.54E-05	1
ISO-CRWT-ATR10002-AT-FOH	ST R-Axis Electrical Actuator #1 Fails Movement	3	7.54E-05	7.54E-05	1
ISO-CRWT-BEA#1-BEA-BRK	Boom#1 Fails During Cask Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEA22-BEA-BRK	Boom#2 Fails During Cask Lift	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEAB202-BEA-BRK	Boom#2 Fails During Cask Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEAD003-BEA-BRK	ST D-Axis Actuator Structural Arm #2 Failure Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEAD006-BEA-BRK	ST D-Axis Actuator Structural Arm #1 Failure Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEAP02-BEA-BRK	ST P-Axis Mechanical Failure During Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BEAR103-BEA-BRK	ST R-Axis Actuator Structural Arm #1 Failure Movement	3	2.40E-08	2.40E-08	1

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-CRWT-BEAR204-BEA-BRK	ST R-Axis Actuator Structural Arm #2 Failure Movement	3	2.40E-08	2.40E-08	1
ISO-CRWT-BRK001--BRK-FOD	Tractor Brake A Fails	1	1.46E-06	—	—
ISO-CRWT-BRK002--BRK-FOD	Tractor Brake B Fails	1	1.46E-06	—	—
ISO-CRWT-BRK003--BRK-FOD	Trailer Brakes Fail	1	1.46E-06	—	—
ISO-CRWT-BRKCCF--BRK-FOD	CCF of Both Tractor Brakes	C	6.86E-08	—	1
ISO-CRWT-CBP0000-CBP-OPC	Electrical Power Dist Cable Failure on ST	3	9.13E-08	9.13E-08	1
ISO-CRWT-CON0000-CON-FOH	Electrical Power Dist Connectors Fail on ST	3	7.14E-05	7.14E-05	1
ISO-CRWT-CTSHC000-CT-SPO	Spurious Command to Raise/Lower AO or STC	3	2.27E-05	2.27E-05	1
ISO-CRWT-DROP11-BEA-BRK	Boom#1 Fails During Cask Lift	3	2.40E-08	2.40E-08	1
ISO-CRWT-EATR2004-AT-FOH	ST R-Axis electrical Actuator #2 Fails Movement	3	7.54E-05	7.54E-05	1
ISO-CRWT-ECP0000-ECP-FOH	ST Restraint Arms Position Selector Fails	3	1.79E-06	1.79E-06	1
ISO-CRWT-ELEC-MOE-FOD	ST Electric Motor Failure	1	6.00E-05	—	1
ISO-CRWT-IEL0001-IEL-FOD	Restraint System Interlock Failure	1	2.75E-05	—	—
ISO-CRWT-LM000011-LC-FOD	ST Lift/Lower Selector Lever Fails	1	6.25E-04	—	—
ISO-CRWT-LPATH--ATH--CCF	CCF of Pendular Axle Hydraulics During Load/Unload	C	8.74E-05	—	—
ISO-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	3	1.78E-03	8.91E-04	2

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	3	1.78E-03	8.91E-04	2
ISO-CRWT-LSJATH1-ATH-FOH	Stabilizing Jack 1 Failure	3	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH2-ATH-FOH	Stabilizing Jack 2 Failure	3	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH3-ATH-FOH	Actuator (Hydraulic) Failure	3	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH4-ATH-FOH	Stabilizing Jack 4 Failure	3	8.91E-04	8.91E-04	1
ISO-CRWT-LVRD01-LVR-FOH	ST D-Axis Actuator Structural Arm #1 Failure	3	2.10E-06	2.10E-06	1
ISO-CRWT-LVRD02-LVR-FOH	ST D-Axis Actuator Structural Arm #2 Failure	3	2.10E-06	2.10E-06	1
ISO-CRWT-PIND004-PIN-BRK	ST D-Axis Actuator Pin #2 Failure Movement	3	2.12E-09	2.12E-09	1
ISO-CRWT-PIND005-PIN-BRK	ST D-Axis Actuator Pin #1 Failure Movement	3	2.12E-09	2.12E-09	1
ISO-CRWT-PINP04-PIN-BRK	ST P-Axis Pin failure During Movement	3	2.12E-09	2.12E-09	1
ISO-CRWT-PINR103-PIN-BRK	ST R-Axis Mechanical Pin #1 Failure During Movement	3	2.12E-09	2.12E-09	1
ISO-CRWT-PINR202-PIN-BRK	ST R-Axis Mechanical Pin #2 Failure During Movement	3	2.12E-09	2.12E-09	1
ISO-CRWT-SJKB011-SJK-FOH	Screw Lift on Boom #1 Fails	3	8.14E-06	8.14E-06	1
ISO-CRWT-SJKB101-SJK-FOH	Screw Lift on Boom #1 Fails	3	8.14E-06	8.14E-06	1
ISO-CRWT-SJKB202-SJK-FOH	Screw Lift on Boom #2 Fails	3	8.14E-06	8.14E-06	1
ISO-CRWT-SJKB22-SJK-FOH	Screw Lift on Boom #2 Fails	3	8.14E-06	8.14E-06	1
ISO-CRWT-ZSD00005-ZS-FOD	ST D-Axis Position Switch Failure Movement	1	2.93E-04	—	—
ISO-CRWT-ZSD00006-ZS-FOD	ST D-Axis Position Switch Failure Lift/Lower	1	2.93E-04	—	—
ISO-CRWT-TRCT-ST-STR-FOH	Tractor Steering System Failure	3	1.85E-05	1.85E-05	1

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-CRWT-TRLR-ST-STR-FOH	Trailer Steering System Failure	3	1.85E-05	1.85E-05	1
ISO-CRWT-ZSP00003-ZS-FOD	ST P-Axis Position Switch Failure During Movement	1	2.93E-04	—	—
ISO-CRWT-ZSR00005-ZS-FOD	ST R-Axis Position Switch Failure Movement	1	2.93E-04	—	—
ISO-HAM-RAM-INSERT	Motor (Hydraulic) Failure	3	2.50E-04	2.50E-04	1
ISO-HTTCOLLIDE--G65-FOH	Sped Limiter Fails	3	1.16E-05	1.16E-05	1
ISO-SPMRC-BRP000-BRP-FOD	SPMRC Brake 000 Failure on Demand	1	5.02E-05	—	—
ISO-SPMRC-BRP001-BRP-FOD	SPMRC Fails to Stop on Loss of Power	1	5.02E-05	—	—
ISO-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	3	9.13E-08	9.13E-08	1
ISO-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable - Short Circuit	3	1.88E-08	1.88E-08	1
ISO-SPMRC-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	3	1.91E-06	1.91E-06	1
ISO-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	1	4.00E-06	—	—
ISO-SPMRC--CT001-CT--FOD	On-Board Controller Fails to Respond	1	4.00E-06	—	—
ISO-SPMRC--CT003-CT--SPO	On-Board Controller Initiates Spurious Signal	3	2.27E-05	2.27E-05	1
ISO-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	3	1.16E-05	1.16E-05	1
ISO-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1	1.74E-03	—	—
ISO-SPMRC-MOE000-MOE-FSO	SPMRC Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
ISO-SPMRC-SC021--SC--FOH	Speed Controller on SPMRC Pendant Fails	3	1.28E-04	1.28E-04	1
ISO-SPMRC-SEL021-SEL-FOH	Speed Selector on SPMRC Pendant Fails	3	4.16E-06	4.16E-06	1
ISO-SPMTT-BRK000-BRP-FOD	Pneumatic Brakes on SPMTT Fail on Demand	1	5.02E-05	—	—

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-SPMTT-BRK001-BRP-FOD	SPMTT Pneumatic Brakes Fail	1	5.02E-05	—	—
ISO-SPMTT-CBP002-CBP-OPC	SPMTT Power Cable - Open Circuit	3	9.13E-08	9.13E-08	1
ISO-SPMTT-CBP003-CBP-SHC	Cables (Electrical Power) Short Circuit	3	1.88E-08	1.88E-08	1
ISO-SPMTT-CPL000-CPL-FOH	Truck Trailer Automatic Coupler System Fails	3	1.91E-06	1.91E-06	1
ISO-SPMTT-CT000--CT--FOD	Controller Mechanical Jamming	1	4.00E-06	—	—
ISO-SPMTT--CT001-CT--FOD	On-Board Controller Fails to Respond	1	4.00E-06	—	—
ISO-SPMTT--CT001-CT--SPO	On-Board Controller Spurious Operation	3	2.27E-05	2.27E-05	1
ISO-SPMTT-CT002--CT-FOH	Controller Failure	3	6.88E-05	6.88E-05	1
ISO-SPMTT-G65000-G65-FOH	SPMTT Speed Control (Governor) Fails	3	1.16E-05	1.16E-05	1
ISO-SPMTT-HC001-HC--FOD	Remote Control Transmits Wrong Signal	1	1.74E-03	—	—
ISO-SPMTT-HC002--HC--SPO	Spurious Signal from Pendant Controller	3	5.23E-07	5.23E-07	1
ISO-SPMTT-MOE000-MOE-FSO	SPMTT Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
ISO-SPMTT-SC021--SC--FOH	Speed Controller on SPMTT Pendant Fails	3	1.28E-04	1.28E-04	1
ISO-SPMTT-SEL021-SEL-FOH	Speed Selector on SPMTT Pendant Fails	3	4.16E-06	4.16E-06	1
ISO-SPMTT-STU001-STU-FOH	SPMTT End Stops Fail	3	2.11E-04	4.81E-08	4.38E+03
ISO-ST--BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1	1.46E-06	—	—
ISO-ST--CBP004-CBP--OPC	ST Power Cable - Open Circuit	3	9.13E-08	9.13E-08	1
ISO-ST--CBP004-CBP--SHC	ST Power Cable Short Circuit	3	1.88E-08	1.88E-08	1
ISO-ST--CT000--CT--FOD	ST Primary Stop Switch Fails	1	4.00E-06	—	—
ISO-ST--CT002--CT--FOH	Direction Controller Fails	3	6.88E-05	6.88E-05	1

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Calculation Type ^a	Basic Event Mean Probability ^b	Mean Failure Rate ^b	Mission Time (Hours)
ISO-ST--HC001--HC--FOD	Remote Control Transmits Wrong Signal	1	1.74E-03	—	—
ISO-ST--HC002--HC--SPO	Spurious Command to Lift/Lower AO or STC	3	5.23E-07	5.23E-07	1
ISO-ST-MOE0001-MOE-FSO	ST Lock Mode State Fails on Loss of Power	3	1.35E-08	1.35E-08	1
ISO-ST--MOE000--MOE-FSO	ST Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
ISO-ST--MOE021--MOE-FSO	Drive System on Primary Propulsion Fails	3	1.35E-08	1.35E-08	1
ISO-ST--SC021--SC--FOH	Speed Controller on ST Pendant Fails	3	1.28E-04	1.28E-04	1
ISO-ST--SC021--SC--SPO	On-Board Controller Initiates Spurious Signal	3	3.20E-05	3.20E-05	1
ISO-ST--SEL021--SEL-FOH	Speed Selector on ST Pendant Fails	3	4.16E-06	4.16E-06	1

NOTE: ^aThe relevant SAPHIRE calculation types are as follows: (1) For failure on demand, the value specified is used directly as the basic event mean failure probability. (3) For failure an operating component without repair in nondemand failure mode, the basic event mean failure probability is calculated as $P = 1 - \exp(-L \times t_m)$, where L is the hourly failure rate and t_m is the mission time in hours. A calculation of type "C", i.e., "compound event" is used to evaluate CCFs. For this type of calculation, SAPHIRE uses 1) information on the failure rate or failure probability of the underlying components and 2) information on the probability distribution of the alpha factors involved in the CCF to internally evaluate the probability distribution of the resulting basic event (see Attachment C, Section C3). The number shown in the "Basic event mean probability" column is actually a point estimate which approximates the mean.

^bAlthough the values in this table are shown to a precision of three significant figures, the values are not known to that level of precision. The values in Attachment C may show fewer significant figures. Such differences are not meaningful in the context of this analysis because the corresponding uncertainties (which are accounted for in the analysis) are much greater than differences due to rounding.

AO = aging overpack; CCF = common-cause failure; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; ST = site transporter.

Source: Attachment C, Section C4

6.3.2 Passive Equipment Failure Analysis

Many event sequences described in Section 6.1 include pivotal events that arise from loss of integrity of a passive component, namely one of the aging overpacks, casks or canisters that contain a radioactive waste form. Such pivotal events involve (1) loss of containment of radioactive material that prevents airborne releases, or (2) LOS effectiveness. Both types of pivotal events may be caused by failure modes caused by either physical impact to the container or by thermal energy transferred to the container. This section summarizes the results of the passive failure analyses detailed in Attachment D that yield the conditional probability of loss of containment or LOS.

6.3.2.1 Probability of Loss of Containment

An overview of the methodology for calculating the probability of failure of passive equipment from drops and impact loads is presented in Section 4.3.2.2. Consistent with *Interim* HLWRS-ISG-02 (Ref. 2.2.70), the methodology essentially consists of comparing the demand upon the equipment to a capacity curve. The probability of failure is the value of the cumulative distribution function for the capacity curve, evaluated at the demand upon the container. More detailed discussion is presented in Attachment D, Section D1. The methodology is applicable to the waste forms associated with Intra-Site activities, including transportation casks, aging overpacks, and canisters. (Note that this does not include LLW containers, because when analyzed for each initiating event, these containers were modeled as if they would always fail.) As described in Section 4.3.2.2, the condition at which a passive component is said to fail depends on the success criteria defined for the component in the operation. Passive components are designed and manufactured to ensure that the success criteria are met in normal operating conditions and with margin, to ensure that the success criteria are also met when subjected to abnormal loads, including those expected during event sequences. The design margins, and in some cases materials, may be dictated by the code and standards applied to a given type of container as characterized by tensile elongation data for impact loads and by strength at temperature data for thermal loads.

As described in Section 4.3.2.2, the probability of a passive failure is often based on consideration of variability (uncertainty) in the applied load, and the variability in the strength (resistance) of the component. The variability in the physical and thermal loading are derived from the systems analysis that defines the probabilities of physical or thermal loads of a given magnitude in a given event sequence. Such conditions arise from the event sequence analysis described in Section 6.1. For the analysis of the effects of fires on waste containers, probability distributions were developed for both the load and the response. For drops and impacts, however, an event sequence analysis is used to define conservative conditions for the load rather than deal with possible ranges of such parameters. Therefore, the calculation of the probability of passive failures is based on the response or resistance characteristics of the container, given the conservative point value for the drop or impact load defined for a given event sequence.

6.3.2.2 Probability of Loss of Containment for Drops and Impacts

Calculation of the probability of failure of the various containers is based on the variability in the strength (resistance) of the container as derived from tests and structural analysis, including

FEA, detailed in Attachment D, Section D1. Loss of containment probability analysis has been evaluated for various containers in the studies listed below:

- *Seismic and Structural Container Analysis for the PCSA* (Ref. 2.2.32)
- *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations* (Ref. 2.2.80) and *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository* (Ref. 2.2.81)
- *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert* (Ref. 2.2.21).

All analyses have applied essentially the same methods that include FEA to determine the structural response of the various canisters and casks to drop and impact loads, developing a fragility function for the material used in the respective container, and using the calculated responses (strains) with the fragility function to derive the probability of container breach.

Failure probabilities for drops are summarized in Table 6.3-2. Conservative representations of drop height are defined for operations with each type of container. Sometimes more than one conservative drop height is specified, for example, for normal height crane lifts and two-block height crane lifts. Lawrence Livermore National Laboratory (LLNL), in *Seismic and Structural Container Analysis for the PCSA* (Ref. 2.2.32, Section 7) predicts failure probabilities of less than 1.0E-08 for most of the events. If a probability for the event sequence is less than 1E-08, additional conservatism is incorporated into the PCSA by using a failure probability of 1E-05, termed "LLNL, adjusted." This additional conservatism is added to account for (a) future evolutions of cask and canister designs; and (b) uncertainties such as undetected material defects, undetected manufacturing deviations, and undetected damage associated with handling before the container reaches the repository, which are not included in the tensile elongation data.

LLNL calculates strains by modeling representative casks, aging overpacks and canisters that encompass TAD canisters, naval SNF canisters, and a variety of DPCs with the dynamic finite element code, LS-DYNA (Ref. 2.2.32). For these canisters, only flat-bottom drops are considered to model transfers by a canister transfer machine (CTM). This is justified because these canisters fit sufficiently tightly within the CTM and potential dropped canisters are guided by the canister guide sleeve of the CTM to remain in a vertical position.

Probability of failure is conservatively calculated by comparing the peak strain to the cumulative distribution function derived from tensile strain to failure test data. BSC FEA analysis used LS-DYNA to model waste packages. Alloy 22 is not stainless steel, but a nickel based alloy, and the most appropriate metric for probability of failure is a cumulative distribution function over extended toughness fraction (Attachment D, Section D1.4). The probability of failure is calculated using the peak toughness index over the waste package, which is a measure of the alloy's energy absorbing capability.