

Table 6.0-2. Bases for Screening Internal Initiating Events

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
RF-ESD03-DPC (#2) (Figure A5-7) RF-ESD03-TAD (#2) (Figure A5-8)	Operator drops cask during cask preparation activities	<p>The 20-ton auxiliary crane, rather than the 200-ton crane, is used in the lid-removal operation. Because the cask is not intentionally lifted in this step, dropping the cask would require a series of extraordinary human failures.</p> <p>For DPCs, a cask drop would require a series of human failures as follows:</p> <p>During lid removal, the crew must fail to remove some fraction of the lid bolts, fail to properly use the check list to verify bolt removal, and use the wrong crane (the 20-ton crane would be incapable of lifting the cask). The crane operator and at least two other crewmembers will be standing on the platform in direct view of the cask during lid removal and they all would have to fail to notice that the entire cask is being lifted before the bolts break. Therefore, event sequences associated with this initiating event are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.</p> <p>For casks other than DPCs, the lid is not removed from the cask at this point. Therefore, no configuration that could result in a crane lifting the cask occurs for such casks. This initiating event, as it relates to casks other than DPC casks, is considered to be unrealizable.</p>
RF-ESD04-DPC (#2) (Figure A5-9) RF-ESD04-TAD (#2) (Figure A5-11)	Structural damage to transportation cask due to impact from the crane hook or rigging while under the cask preparation platform	In this operation, the lid is unbolted and the lid lift fixture is attached. The cask is flush or recessed with respect to the cask preparation platform, and therefore cannot be impacted. Therefore, event sequences associated with these initiating events are considered to be physically unrealizable.
No applicable event trees	Conveyance carrying a waste form collides with a shield door, causing the door to dislodge from its supports and fall onto the waste form	The shield doors are designed to withstand collision of the conveyance into the door without dislodging from their supports such that the stress of all support mechanisms of the door stay below yield. Therefore, this initiating event is considered physically unrealizable.
RF-ESD06-DPC (#7) (Figure A5-14) RF-ESD06-TAD (#7) (Figure A5-16)	Canister dropped inside the shield bell (with CTM slide gate closed)	Drops within the shield bell have been subsumed within event sequences for drops from the operational lift height and are not separately addressed. This is conservative because the drop height within the shield bell is less than the operational lift height.
RF-ESD06-DPC (#5) (Figure A5-14) RF-ESD06-TAD (#5) (Figure A5-16)	Side impact from a slide gate	Slide gate impacts during CTM transfer are included in the CTM fault tree as a cause of canister drop, rather than as an independent initiating event. In addition, the motors on the slide gates have insufficient power to significantly damage a canister. Branch #5 of the listed event trees covers side impact with the CTM shield bell due to CTM collision.
RF-ESD06-DPC (#2) (Figure A5-14)	Canister impact during lid removal by the CTM	This initiating event is not applicable to the event tree listed because the DPC lid is not removed by the CTM. Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
RF-ESD09 (#2) Figure A5-22	Rollover of horizontal cask transfer trailer carrying a transportation cask in the Transportation Cask Vestibule or Cask Preparation Room	For a truck trailer to roll over, its center of mass has to move laterally beyond the wheel base of the trailer. This could occur upon traversing a significantly uneven surface, running over a very large object, turning sharply at high speed, or by jackknifing the trailer while backing up. There are no uneven surfaces in the Transportation Cask Vestibule/Annex or Cask Preparation Room. The area in question has a flat concrete surface. There are no objects that could be run over that could significantly shift the trailer's center of mass. Turning sharply at high speed or jackknifing the trailer is not possible inside the building because the rooms are too narrow and the truck comes to a complete stop outside the closed entrance door prior to the door opening and the truck entering. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened from further analysis in Section 6.0.4.
No applicable event trees	Canister dropped into the Loading Room with no aging overpack present	Dropping a canister through the port without a staged aging overpack below would require a series of human failures and mechanical failures that makes the initiating event unlikely. The design incorporates an interlock to prevent the opening of the port slide gate when the aging overpack is not present (Ref. 2.2.30). The combination of (a) failure to stage the aging overpack, (b) failure of more than one operator to notice that it is not staged, (c) failure of the hardwired interlock, and (d) drop of the canister are required for such an initiating event to occur. Considering the combination of unlikely events that must occur to cause this initiating event, event sequences involving this combination of failures are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.
No applicable event trees	Tipover of CTT	The CTT is designed to prevent tipover (Ref. 2.2.21, Section 3.2). The size, weight, low center of gravity, and low speed of the CTT ensure that no tipover can occur. During cask preparation activities, the CTT is normally set on the floor inside the cask preparation platform. As such, tipover is not physically realizable during preparation activities. During transit, the CTT glides slowly on a cushion of air, an inch or less above the floor. If air pressure is lost, the CTT, with its load, settles to the floor. While the CTT is in transit, or after settling to the floor, any applied force from facility operations is incapable of tipping over the CTT. Due to the slow travel of the CTT, a loss of air pressure or a collision with other equipment or a facility structure will not result in tipover. Therefore, tipover of the CTT is considered physically unrealizable for internal events. CTT tipover, however, is analyzed in the seismic event sequence and categorization analysis.
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.

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. 2.2.86, Section 2.1.3); (Ref. 2.2.87); and (Ref. 2.2.88)). Therefore, further consideration of this initiating event is not required.

NOTE: Initiator event trees are provided in Attachment A in the figures cited. The branch numbers are shown in each figure under the column labeled "#." The branch numbers are shown in each figure under the column labeled "#."  
 CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HDPC = horizontal dual-purpose canister; HSTC = horizontal site transfer cask; HTC = a transportation cask that is never upended; SPM = site prime mover.

Source: Original

### 6.0.4 Screening of Internal Flooding as an Initiating Event

By the definition of an event sequence, a flood inside a facility would be an initiating event if it led to a sequence of events that would either breach waste containers, causing a release, or if it caused elevated radiological exposure without a release (i.e., direct exposure of personnel). Internal floods, whether caused by random failure or earthquakes, emerge from two sources. The first is inadvertent actuation of the fire-suppression system. The second is failure of water-carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems. Drains, channels and curbs are situated to remove water from these sources. However, the following discussion does not rely on these.

Transportation casks and canisters are not physically susceptible to breaches associated with water in the short-term. With extremely long exposure to water, corrosion may be a factor, but intervention to drain water from the buildings would prevent such exposure. Short-term breaches do not occur owing to exposure to water. Canisters are surrounded by transportation casks or aging overpacks. Transportation casks are elevated at all times at least five feet above the floor by railcar or CTT. A lifted canister or/and cask is higher than these minimum elevations. Therefore, water from fire suppression and other water systems is unlikely to attain a depth that would contact transportation casks or canisters. Of greater significance, however, is that the fuel is contained in canisters within an overpack nearly all the time, and these containers do not fail from short-term exposure to flood water. In this context, short-term is a time period that is at least 30 days but less than the length of time in which significant corrosion may occur.

Water impingement on electrical equipment (e.g., motor control centers, motors, and switchgear cabinets) would ordinarily trigger circuit protection features that would open the circuit and cause a loss of electrical power (which is covered in Section 6.0.2.2). If a short circuit occurred as a result of water impingement, normal circuit protection features or overheating of the wires would subsequently open the affected circuit. In an extreme situation, an electrical fire might be started. Fires from all causes are covered in Section 6.5.

The possibility of inadvertent direct exposure of workers due to internal flooding is considered next. Direct exposure to workers during a flood would occur if shielding were disabled as a result of the flooding. Canisters are always shielded during facility operations by transportation casks, cask preparation platforms, concrete floors and walls, the CTM shield bell or shield skirt, or the unloading or loading room shield doors. Loss of electrical power to any of these simply stops operation, if any, without affecting the shielding. Flooding might also cause hot shorts in control boxes. However, hardwired interlocks between the CTM slide gate, shield bell skirt, and shield doors prevents such inadvertent motion. Therefore, internal flooding cannot initiate an event sequence that causes increased levels of radiological exposure to workers.

Moderator intrusion into canisters resulting from event sequences that might breach a waste container is treated quantitatively as described in the pivotal event descriptions of Section 6.2.

## 6.1 EVENT TREE ANALYSIS

The event trees that are quantified in this analysis were developed from ESDs in the *Receipt Facility Event Sequence Development Analysis* (Ref. 2.2.34, Attachments F and G). This section describes the use of SAPHIRE (Section 4.2) to model event sequences. The 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 linked event trees with linked fault trees to calculate the frequency of occurrence of event sequences. The SAPHIRE computer program (Section 4.2) is used for this purpose. The event tree quantification is supported by FTA (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), and PEFA (Section 6.3 and Attachment D). The YMP preclosure handling is performed using four kinds 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 (NNPP) for placement in waste packages destined for emplacement in the repository emplacement drifts. Three CRCFs are currently considered.
3. The WHF accepts DPCs and transportation casks containing uncanistered commercial SNF and transfers the SNF to TAD canisters, which are destined for the CRCF or the aging pads.
4. The Initial Handling Facility (IHF) accepts canisters from the NNPP and some canisters containing high-level radioactive waste for placement in waste packages destined for emplacement in the repository emplacement drifts.

Preclosure waste handling as modeled in the PCSA also includes TEV and Subsurface Operations. The TEV accepts waste packages from the CRCF and IHF and, by means of rail, transports and deposits them into their designated location in the emplacement drifts. All other extra-building transportation, low-level waste handling, and balance of plant is called Intra-Site Operations.

Event sequences are developed for each of the four building types, TEV and Subsurface Operations, and Intra-Site Operations. Because each type of waste container in the RF has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container. As described in the *Receipt Facility Event Sequence Development Analysis* (Ref. 2.2.34), event sequences are also developed separately for each major group of waste handling processes by location within the building. 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, Loss of Shielding
4. Radionuclide Release, Filtered (HVAC)
5. Radionuclide Release, Unfiltered (HVAC system is not operating)
6. Radionuclide Release, Filtered, Also Important to Criticality
7. Radionuclide Release, Unfiltered, Also Important to Criticality
8. Important to Criticality (not applicable to the RF).

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.

The SAPHIRE computer program has advanced features that permit the analyst to control the inputs and conditions for quantifying linked event trees and fault trees. One feature is the use of “basic rules” by which the analyst tells the program how and when to link certain variations of fault trees and basic event data that describe a given initiating and pivotal event. This allows path dependent development of sequence minimal cut sets and probabilities.

The primary inputs to the program are the following:

- Event tree logic models
- Fault tree logic models for initiating and pivotal events
- Initiating event frequencies derived from waste-form throughputs and numbers of opportunities for initiating an event sequence
- 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 event tree and fault tree logic models are linked to the basic event library.

Each basic event is characterized by a probability distribution. SAPHIRE’s Monte Carlo sampling method is employed to propagate the uncertainties to obtain event sequence mean values and parameters of the underlying probability distribution such as variance. As described in Section 4.3.6, categorization is done on aggregated event sequences, whose resultant probability distributions are also obtained by Monte Carlo simulation. SAPHIRE accounts for the correlation between analogous basic events sharing the same reliability information, which ensures the spread of the probability distribution of the event sequences in which these basic events intervene is not underestimated.

### 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 one or more initiating events:

1. **Self-contained event trees.** Self-contained event trees are used when only one initiating event appears in the corresponding ESD (Ref. 2.2.34, Attachment F). An example is RF-ESD05-DPC, which is shown in Figure A5-12 in Attachment A. The feed on the left side of the event tree is an event that represents the frequency of the 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. 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 as illustrated in the corresponding ESD and no branching occurs in the event tree. 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” often means that normal operation can continue. The undesired end states represent a release of airborne radioactivity, a direct exposure to radiation, or a potential criticality condition.
2. **Separate initiator and system-response event trees.** Separate event trees for initiating events and the system response are used when more than one initiating event appears in the corresponding ESD (Ref. 2.2.34, Attachment F). The initiator event tree decomposes a group of initiating events into the specific failure events that comprise the group. For example, an initiator event tree, RF-ESD01-DPC, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, RESPONSE-TCASK1, is shown in Figure A5-3. The feed to the left side of the initiator event tree 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 received during the preclosure period. Initiator event trees do not end at end states but transfer to a system response event tree. The models to be used for the initiating events associated with each initiator event tree are specified in SAPHIRE “basic rules,” which are attached to the initiator event tree.

System response event trees contain only pivotal events. In accordance with the basic rules that are written for a given initiator event tree, the SAPHIRE program links specific fault tree model or basic event to a given pivotal event. For example, the system response tree in Attachment A, Figure A5-3 shows the system response event tree RESPONSE-TCASK1. Because the conditional probability of each pivotal event may be specific to the initiating event for each event sequence, the same system response event tree is quantified by SAPHIRE as many times as there are initiating events in the initiator event tree. The models to be used for the pivotal events

associated with each initiating event and system response event tree are specified in SAPHIRE basic rules, which are attached to the associated initiator event tree.

### **6.1.1.3 Summary of the Major Pivotal Events**

A self-contained event tree or a system response event tree may include pivotal events concerning the success or failure of the transportation cask, canister, shielding properties, HEPA filtration availability, and moderator intrusion susceptibility. The pivotal events are summarized in Attachment A, Section A3.

Each of the specific failure events included in a self-contained or system-response event tree may be linked to a basic event or to the top event of a fault tree. Two kinds of fault trees are developed and represented in Attachment B. The first type represents equipment fault trees including HFEs that contribute directly to the specific pivotal or initiating event. The second type links initiating and pivotal events to these equipment fault trees (via transfer gates) and miscellaneous events. This second type is called linking or connector fault trees. The equipment fault tree models are, in turn, linked to basic event reliability information separately entered into SAPHIRE. Some of the pivotal events do not have associated fault trees because they are linked directly to probabilities in the reliability database entered into SAPHIRE. Section 6.2 provides more information about the reliability information developed for this analysis.

### **6.1.2 Waste Form Throughputs**

Each initiator event tree and self-contained event tree begins with the container throughputs, that is, the numbers of waste form units (such as casks or canisters) to be handled over the life of the RF. The throughputs are identified in Table 6.1-1 and are drawn into the descriptions of specific event trees as needed. With the number of waste form units as a multiplier in the event tree and the initiating events specified as a probability per waste form unit, the value passed to the system response is the number of occurrences of the initiating event expected over the life of the facility.

Table 6.1-1. Waste Form Throughputs for the RF Over the Preclosure Period

Waste Form Unit	RF Throughput Over Preclosure Period	Comment
Transportation casks containing a TAD canister	6,978	One canister per cask
Transportation casks containing a DPC	346	One canister per cask
TAD canisters (44 BWR or 21 PWR SNF assemblies per canister)	6,978	Same as number of TAD canister casks
DPCs (64 BWR or 25 PWR SNF assemblies per canister)	346	Same as number of DPC casks
Aging overpack containing a TAD canister	6,978	One canister per aging overpack
Aging overpack containing a DPC	346	One canister per aging overpack
Transportation casks containing a TAD canister	6,978	One canister per cask

NOTE: BWR = boiling water reactor; DPC = dual-purpose canister; PWR = pressurized water reactor; RF = Receipt Facility; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Ref. 2.2.27, Table 4

### 6.1.3 Guide to Event Trees

Event trees are located in Attachment A. Table 6.1-2 contains the crosswalk from the ESD (Ref. 2.2.34, Attachment F) to the initiating event tree and response tree figure location in Attachment A.

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

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
RF-ESD-01	Event Sequences for Activities Associated with Receipt of Transportation Cask into Cask Preparation Room	RF-ESD01-DPC RF-ESD01-TAD	Figure A5-2 Figure A5-4	RESPONSE -TCASK1	Figure A5-3
RF-ESD-02	Event Sequences for Activities Associated with Removal of Impact Limiters, Cask Upending, and Transfer to CTT or Cask Transfer Trailer	RF-ESD02-DPC RF-ESD02-TAD	Figure A5-5 Figure A5-6	RESPONSE -TCASK1	Figure A5-3
RF-ESD-03	Event Sequences Associated with Unbolting and Lid Adapter Installation	RF-ESD03-DPC RF-ESD03-TAD	Figure A5-7 Figure A5-8	RESPONSE -TCASK1	Figure A5-3
RF-ESD-04	Event Sequences Associated with Transfer of a Cask on CTT from Cask Preparation Area to Cask Unloading Room	RF-ESD04-DPC RF-ESD04-TAD	Figure A5-9 Figure A5-11	RESPONSE -TCASK2	Figure A5-10
RF-ESD-05	Event Sequences Associated with a Transportation Cask on a CTT or Site Transporter Colliding with Lid Bolting Room or Cask Unloading Room Shield Doors	RF-ESD05-DPC RF-ESD05-TAD	Figure A5-12 Figure A5-13	N/A	N/A
RF-ESD-06	Event Sequences for Activities Associated with the Transfer of a Canister from Transportation Cask, to Aging Overpack with CTM	RF-ESD06-DPC RF-ESD06-TAD	Figure A5-14 Figure A5-16	RESPONSE - CANISTER1	Figure A5-15
RF-ESD-07	Event Sequences for Activities Associated with Assembly and Closure of an Aging Overpack	RF-ESD07-DPC RF-ESD07-TAD	Figure A5-17 Figure A5-19	RESPONSE -AO1	Figure A5-18
RF-ESD-08	Event Sequences for Activities Associated with the Exporting of an Aging Overpack from the RF	RF-ESD08-DPC RF-ESD08-TAD	Figure A5-20 Figure A5-21	RESPONSE -AO1	Figure A5-18
RF-ESD-09	Event Sequences for Activities Associated with Export of Horizontal Cask on Cask Transfer Trailer	RF-ESD09	Figure A5-22	RESPONSE -TCASK1	Figure A5-3
RF-ESD-10	Event Sequences for Activities Associated with Direct Exposure During DPC Handling Activities	RF-ESD10	Figure A5-23	N/A	N/A
RF-ESD-11	Event Sequences for Activities Associated with Direct Exposure During CTM Activities	RF-ESD11	Figure A5-24	N/A	N/A
RF-ESD-12	Event Sequences for a Fire Occurring in Receipt Facility	RF-ESD12-DPC RF-ESD12-TAD	Figure A5-25 Figure A5-27	RESPONSE -FIRE	Figure A5-26

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; N/A = not applicable.

Source: Attachment A, Table A5-1

## 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, an exception being 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 RF is also used in other surface facilities and the Intra-Site Operations. 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 the RF. 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 but, by virtue of the rules feature of SAPHIRE, the inputs to each fault tree can be tailored to fit the event sequence.

The fault trees are linked to the event trees via the initiating event tree rules file and the application of linking fault trees. The rules file specifies the names of the linking fault trees for initiating event and pivotal event fault trees to be substituted into the event tree top events during quantification. The rules file also specifies the use of particular values for basic events and other probabilistic factors that affect the event sequence quantification. The linking fault trees have unique names for the facility and the operational nodes for each event tree. The linking fault trees are very simple, usually having a single top event that is an OR gate that connects to one of the system fault trees. This allows for application of unique top event probabilities to the different initiating events modeled in the initiating event tree.

Attachment B, Sections B1 to B8, presents the system fault trees. These sections describe the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B9, presents the linking fault trees used in the RF analysis. The linking fault trees are self-explanatory. No quantification is performed for the linking trees alone.

A top event occurs when one of the ITS success criterion 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 RF.

Each of the top events for the initiating event fault trees represents 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 lift that the CTM drops the canister, given a lift? The expected number of canister drop initiating events during the preclosure period is the product of the number of times a canister is lifted 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 initiating event tree in SAPHIRE links the various fault tree logic models to the canister, or other waste form, and the throughput values to generate the initial portions of event sequence cut sets that are subsequently processed as part of the solution of the complete event sequence that includes pivotal events.

By contrast, the top event for the confinement function of the HVAC represents the conditional probability that the confinement feature is not achieved for the required duration following an airborne release of radioactive material inside the RF. The quantification of the top event, as summarized in Section 6.2.2.7 and detailed in Attachment B, Section B7, is expressed as unavailability. The results provide insight into the reliability of the HVAC and its contribution to event sequence quantification. Again, the quantified top event is not used directly in the event sequence quantification. Instead, the fault tree logic for the HVAC is linked to event sequence analysis via SAPHIRE.

In general, each of the FTAs in Attachment B are developed to include both (1) HFEs, and (2) 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 functions are to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (e.g., electrical and mechanical) 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 analysis. 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, and common electrical supplies
- Support systems and subsystems such as filtering (HVAC HEPA filters) and electrical
- 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 Site Prime Mover Fault Tree Analysis**

The FTA for the site prime mover (SPM) 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. See Attachment B, Section B1, for sources of information on the physical and operational characteristics of the SPM.

#### **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 Operations and within the RF. A speed limiter is used on the SPM to ensure the maximum speed does not exceed 9 mph. Movement of the SPM with railcars (termed SPMRC) within the RF is limited to the Transportation Cask 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 from the facility main electrical supply.

#### **6.2.2.1.2 Operations**

In-facility SPM operations begin after the SPM has positioned the railcar outside the RF. The SPM diesel engine is shut down and the outer door is opened. Facility power is connected to the SPM for all operations inside the facility. The operator connects the pendant controller or uses a remote (wireless) controller to move the SPM to push the railcar into the vestibule. The Transportation Cask Vestibule serves as an air lock for the facility, providing an environmental separation between the Cask Preparation Room and the outside environment. To maintain negative pressure within the facility, the vestibule has interlocked inner and outer access doors. Only one door can open at a time when moving equipment in or out.

In the event of loss of power, the SPM is designed to stop, retain control of the railcar, 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 block diagram of the functional components on the SPM is shown in Attachment B, Section B1, Figure B1.2-1.

The control system provides features for preventing initiating events:

- The SPM is designed to stop whenever (1) commanded to stop or (2) 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 SPM collisions
- Prevent SPM derailment.

Various design features are provided to achieve each success criterion. The failure to achieve each success criterion defines the top event of a fault tree for the SPM.

#### **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. One hour is conservative because it does not require more than one hour to disconnect the SPM from the railcar and move it from the facility. Otherwise, failure-on-demand probabilities are used.

For railcar derailment, the probability is based on the distance traveled inside the RF, 0.04 miles, and industry data derailment rate of  $1.18E-5$  per mile traveled (Attachment C, Table C4-1, Item 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.

The SPM has two credible failure scenarios:

- SPM collides with RF structures
- SPM derailment.

Each failure mode may occur with various waste forms that are received in the transportation casks.

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
SPM collides with RF structures (DPC on RC)	4.3E-03	1.1E-2
SPM derailment (DPC on RC)	4.7E-7	8.8E-14

NOTE: DPC = dual-purpose canister; RC = railcar; RF = Receipt Facility; SPM = site prime mover.

Source: Attachment B, Section B1, Figures B1.4-1 and B1.4-6

### 6.2.2.2 Cask Transfer Trolley Fault Tree Analysis

The FTA for the CTT 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. See Attachment B, Section B2 for sources of information on the physical and operational characteristics of the CTT.

#### 6.2.2.2.1 Physical Description

The CTT is an air-powered machine that is used to transport various vertically oriented transportation casks from the Cask Preparation Room to the Cask Unloading Room. The CTT consists of a platform, a cask support assembly, a pedestal assembly, a seismic restraint system, and an air system.

The CTT will handle a number of different casks so several different pedestals are used to properly position the cask height. Each pedestal subcomponent is designed for its respective cask to be set down in a “cavity.” In addition, the cask is restrained in the longitudinal and transverse directions by the cavity walls and restrained in the vertical down direction by the pedestal itself. This design also ensures the cask is positioned correctly. The CTT is positioned within a set tolerance under the cask port in the Cask Unloading Room using bumpers and stops that are bolted to the floor of the Cask Unloading Room and which are designed with bolts that would break to allow the CTT to slide during a seismic event.

In addition, the cask is restrained by two electric powered linkage systems that prevent side motions during a seismic event. Different cask diameters are handled by bolting unique interface clamps on the seismic restraints. When the restraint system is properly positioned next to the cask, two locking pins are pneumatically actuated to secure the position of the system. If the locking pins are not secured, the CTT will not be able to power up and move/levitate.

The facility compressed air supply inflates air casters beneath the trolley platform, which allow the CTT to rise above the steel floor. The platform mounted hose reel has an air-powered return, a ball valve shutoff, quick disconnect fittings, and a safety air fuse. A main “off/on” control valve and separate flow control/monitoring valves for each air bearing allow adjustment and verification of pressure/flow for each individual bearing. Interlocks for the air are provided to verify the main incoming pressure is not too high and to verify that all bearings have sufficient air pressure.

End mounted turtle-style drive units that are 360-degrees steerable are used to steer the CTT. Traction is produced by down-pressure on the wheels provided by a small air bag on each drive unit.

The CTT is evaluated for a collision with another object while carrying the cask. The speed of the drives, 10 ft/min, has been set so that the forces the cask experiences during a 10 ft/min collision is less than the forces the cask would experience during a seismic event. The speed is controlled in two ways. First, the electrical control system is designed to only give a proportional signal to the air valve that produces a speed of 0 to 10 ft/min. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, allows a maximum amount of air through at any time to prevent a “runaway” condition.

#### **6.2.2.2.2 Operation**

Initially, the CTT is located in the Cask Preparation Room with the battery fully charged, the seismic restraints retracted, and with no air or electrical power connected. Based on the next planned cask to be loaded onto the trolley, the corresponding pedestal components are installed into the base, and bumpers are bolted onto the seismic restraints and supports. The air hose is then connected to the CTT.

The overhead crane moves a cask onto the pedestal. With the cask still attached to the crane, the operator remotely operates the seismic restraints and secures the cask to the CTT. When the restraints are in place, the locking pins are remotely inserted pneumatically. With the cask secured to the CTT, the overhead crane is disengaged from the cask.

When the locking pins are inserted properly, an interlock allows the air bearings and drive motors to be operated. Once all preparations of the cask are complete, the CTT can be raised and moved to the Cask Unloading Room. Guides bolted to the floor ensure that the CTT can only move forward and back, and will position the CTT so that the cask is directly below the transfer port. Once in position, the air pressure to the bearings is stopped and the CTT rests in position. The shield doors that separate the Cask Preparation Room from the Cask Unloading Room are then closed.

#### **6.2.2.2.3 Control System**

The control system is relay based and includes a pendant station as its operator interface.

No programmable logic controller (PLC) is used – all interlocks are hard wired. The pendant is a standard crane pendant that has all of the controls for the unit including:

- Deadman handle – operator must depress both handles to allow air to flow to the system so the CTT can levitate or move horizontally.
- Emergency-stop button on the pendant control and on the CTT.
- Clockwise/counterclockwise momentary switch to turn the drive units for horizontal movement. This rotational characteristic is used to move the CTT to storage or maintenance location after it leaves the Cask Preparation Room.
- Forward/reverse switch to determine direction of the drive units.
- Drive speed – variable speed control switch.
- Cask restraint – selector switch that actuates the motor to close the restraints and automatically engage the locking pin.

During normal operations, the controls operate off a battery system contained on the CTT. Only one operator is needed to drive the CTT since it only travels in one direction when it is carrying a cask.

The main air supply valve is a pilot operated solenoid valve that is fail-safe (i.e., it is a spring valve that closes upon loss of electrical power or loss of air pressure). The air supply valve opens when the locking pins actuate the limit switches and the pendant deadman switches are actuated.

#### **6.2.2.2.4 System/Pivotal Event Success Criteria**

Success criteria for the CTT are the following:

- Ensure the CTT remains stationary with no spurious movement during transportation cask placement onto the CTT, transportation cask preparation, or during unloading.
- Prevent collisions while moving the CTT with cask from the Cask Preparation Room to the Cask Unloading Room.

Various design features are provided to achieve each success criterion. The failure to achieve each success criterion defines the top event of a fault tree for the CTT.

#### **6.2.2.2.5 Mission Time**

In all cases a conservative mission time of one hour per cask transfer is used for each fault tree.

#### **6.2.2.2.6 Fault Tree Results**

The detailed analysis is presented in Attachment B, Section B2.

There are four fault trees associated with the CTT:

1. Spurious movement of the CTT in the Cask Preparation Room while loading a cask onto the CTT.
2. Spurious movement of the CTT in the Cask Preparation Room during unbolting and lid adapter installation.
3. Collision with an object or structure while moving a cask from the Cask Preparation Room to the Cask Unloading Room.
4. Spurious movement of the CTT in the Cask Unloading Room while unloading canisters from the CTT.

The results of the analysis are summarized in Table 6.2-2. Four fault trees were developed where the top events correspond to one of the scenarios listed above.

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

Top Event	Mean Probability	Standard Deviation
Spurious movement of the CTT during cask loading	1.8E-9	5.8E-9
Spurious movement of the CTT during cask preparation	1.2E-4	1.2E-4
CTT collision into structure	1.0E-3	1.2E-3
Spurious movement during canister transfer	3.0E-14	1.7E-13

NOTE: CTT = cask transfer trolley.

Source: Attachment B, Section B2, Figures B2.4-1, B2.4-5, B2.4-8, B2.4-12

### 6.2.2.3 Shield Door and Slide Gate Fault Tree Analysis

The RF Cask Unloading Room and Loading Room each have a slide gate providing access to the Canister Transfer Room and a shield door providing access to either the Cask Preparation Room or the Lid Bolting Room. The shield doors and slide gates provide shielding during canister unloading and loading.

The FTA 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 Unloading Room shield door is opened to allow cask-carrying equipment, such as the CTT, to enter the room. Once equipment is positioned properly in a Cask Unloading Room, the shield door may be shut in preparation for removing canisters from the cask. Once the shield door is shut, the slide gate may be opened to allow the CTM to perform cask unloading operations. Similarly, the Loading Room shield door is opened to allow canister-carrying equipment, such as the site transporter, to enter the room. Once the site transporter is in place under the slide gate in the Loading Room, the shield door may be shut in preparation for loading

the canister into an aging overpack. Once the shield door is shut, the slide gate may be opened, to allow the CTM to perform canister loading operations.

The shield doors consist of a pair of large heavy doors that close together. The doors are operated by individual motors that have over-torque sensors to prevent crushing of an object. Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand lever that must be enabled by an enable/disable switch. An emergency open switch exists, enabling the doors to be opened in case of an emergency situation.

Similar to the shield doors, the slide gates that separate the Cask Unloading and Loading Rooms from the CTM (located in the Canister Transfer Room above these rooms) consist of two gates that close together between the Cask Unloading and Loading Rooms and the Canister Transfer Room. The gates are operated by individual motors that also have over-torque sensors. Each gate has limit switches to indicate open or closed gates. A CTM skirt-in-place switch is interlocked to the slide gate to prevent the gates from opening without the CTM in place, and a CTM in-place bypass hand switch exists for maintenance activities. Slide gate operation is controlled by a hand switch coupled with an enable/disable switch, and shield door interlocks prevent the slide gate from opening when the shield door is open. Open/closed and CTM in-place indicators exist to assist operators in their activities.

#### **6.2.2.3.2 Operation**

The Cask Unloading Room shield door is opened to allow cask-carrying equipment, such as the CTT, to enter the room. Once equipment is positioned properly in the Cask Unloading Room, shield doors are shut in preparation for removing canisters from the cask. Once the shield doors are shut, the slide gate may be opened to allow the CTM to perform cask unloading operations. Loading of the aging overpack in the Loading Room is analogous to cask unloading operations. The slide gate may be opened to allow aging overpack loading access if the shield doors are closed. Once loading is complete and the slide gate is closed, the shield doors are opened to allow aging overpack removal.

#### **6.2.2.3.3 Control System**

The control systems have hard-wired interlocks for the following functions:

- Redundant hardwire interlocks prevent the shield door from opening while the slide gate is open.
- The shield door system will not have any test, maintenance, or other modes/settings that will allow bypass of interlocks.
- A single interlock prevents the slide gate from opening when the CTM skirt is not in place.

- An obstruction sensor is provided to detect objects between the shield doors and prevent door closure initiation.
- Motor over-torque sensors are provided to prevent shield doors from causing damage to casks in the event of closure on a conveyance.
- Shield doors and slide gates are equipped with redundant hardwire interlocks to prevent one another from opening when the other is open.

#### **6.2.2.3.4 System/Pivotal Event Success Criteria**

Success criteria for the shield door and slide gate are the following:

- Prevent inadvertent opening of shield door
- Prevent inadvertent opening of the slide gate
- Prevent concurrent opening of the shield door and slide gate when waste is present
- Prevent shield door closing on conveyance.

Various design features are provided to achieve each success criterion. The failure to achieve each success criterion defines the top event for the slide gate/shield door fault trees presented in Attachment B.

#### **6.2.2.3.5 Mission Time**

Most of the basic events in the fault tree models are “failure on demand” for equipment failures and “failure per operation” for HFEs. A mission time of one hour is used to calculate the probability of a spurious signal being sent due to PLC failure.

#### **6.2.2.3.6 Fault Tree Results**

The detailed analysis is presented in Attachment B, Section B3.

The slide gate and shield door system has three credible failure scenarios:

1. Inadvertent opening of the shield door
2. Inadvertent opening of the slide gate
3. Shield door closes on conveyance.

The results of the analysis are summarized in Table 6.2-3. Three fault trees were developed where the top events correspond to one of the scenarios listed above.

#### **6.2.2.4 Canister Transfer Machine Fault Tree Analysis**

The FTA for the CTM is detailed in Attachment B, Section B4. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B4, for sources of information on the physical and operational characteristics of the CTM.

Table 6.2-3. Summary of Top Event Quantification for the Shield Doors and Slide Gate

Top Event	Mean Probability	Standard Deviation
Inadvertent Opening of the Shield Door	1.3E-7	4.6E-7
Inadvertent Opening of the Slide Gate	3.6E-9	9.8E-9
Shield Door Closes on Conveyance	3.3E-6	5.9E-6

Source: Attachment B, Section B3, Figures B3.4-1, B3.4-4, B3.4-7

#### 6.2.2.4.1 Physical Description and Functions

The CTM operates in the Canister Transfer Room of the RF. The function is to transfer waste canisters from a cask on a CTT to an aging overpack on a site transporter. The ports in the floor of the Canister Transfer Room provide access to the Cask Unloading Room and Loading Room and access to the canister staging areas.

The CTM is an overhead crane bridge with two trolleys. The first is a canister hoist trolley with a grapple attachment and hoisting capacity of 70 tons. The second is a shield bell trolley that supports the shield bell. The bottom end of the shield bell is attached to a larger chamber to accommodate cask lids. The CTM bottom plate assembly supports a thick motorized slide gate. The slide gate, when closed, provides bottom shielding of the canister once the canister is inside the shield bell. Around the perimeter of the bottom plate, a thick shield skirt is provided that can be raised and lowered to prevent lateral radiation shine during a canister transfer operation.

#### 6.2.2.4.2 Operations

A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to an aging overpack. For this operation, a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. The cask lid is in place but unbolted. Similarly, an empty aging overpack secured by the site transporter is positioned under the adjacent transfer port in the Loading Room.

The CTM is moved to a position over the center of the port above the loaded cask. The shield skirt is lowered to rest on the floor, and the port slide gate is opened. The CTM slide gate is opened and the canister grapple is lowered through the shield bell to engage and lift the cask lid. The port slide gate is closed and the shield skirt is raised so the CTM can be moved to a cask lid staging area to set down the lid.

Once the lid is staged the CTM is moved back over the port above the loaded cask to align the canister grapple. The shield skirt is lowered, the port slide gate is opened, and the grapple is lowered to engage the canister lifting feature. The canister is raised into the shield bell. The CTM slide gate and the port slide gate are closed and the shield skirt is raised so the CTM can be moved to the port above the empty aging overpack. The aging overpack loading operations are essentially the reverse of the cask unloading.

The CTM canister grapple is used for handling large diameter canisters such as TAD canisters and DPCs. These grapples are attached to the CTM canister grapple by positioning the CTM

over a slide gate located in the Canister Transfer Room floor and lowering the CTM hoist until the CTM grapple is accessible in the room below.

The CTM is normally controlled from the facility operations room, but a local control station is also provided.

Generally, under off-normal conditions the CTM is not in operation. Following a LOSP, all power to the CTM motors (e.g., hoist, bridge, trolley, and bell trolley) is lost. If a transfer is underway when power is lost, all of the CTM motors stop and the hoist holding brake engages. Operations would be suspended until power is restored and the load can be safely moved. Under other off-normal conditions, transfer operations would be suspended and the CTM would remain idle.

#### **6.2.2.4.3 Control System**

Hard-wired interlocks are provided to:

- Prevent bridge and trolley movement when the shield bell skirt is lowered
- Prevent raising the shield bell skirt when the slide gate is open
- Prevent hoist movement unless the grapple is fully engaged or disengaged
- Stop the hoist and erase the lift command when a canister clears the shield bell slide gate
- Stop a lift before upper lift heights are reached (two interlocks are provided for this function)
- Prevent opening of the port gate unless the shield bell skirt is lowered and in position
- Prevent hoist movement unless the shield bell skirt is lowered
- Prevent lifting of a load beyond the operational limit of the CTM (load cells).

Some of these interlocks can be bypassed during maintenance. The most significant of these interlocks that can be bypassed is the interlock between the shield skirt position and the position of the slide gate. (The shield skirt cannot be raised unless the slide gate is closed or the maintenance bypass is engaged.) The design of the grapple interlock ensures that the bypass is voided when a canister is grappled.

Much of the operational controls are provided by non-ITS PLCs. Spurious or failed operation of the PLCs is in the FTA when such operation may contribute to a drop or collision event.

#### 6.2.2.4.4 System/Pivotal Event Success Criteria

Success criteria for the CTM are the following:

- Prevent a canister drop from a height below the design basis height for canister damage from any cause during the lifting, lateral movement, and lowering portions of the canister transfer.
- Prevent a canister drop from above the canister design limit drop height from any cause during the lifting, lateral movement, and lowering portions of the canister transfer.
- Prevent a drop of any object onto the canister from any cause during the lifting, lateral movement, and lowering portions of the canister transfer.
- Prevent a collision between the canister and the shield bell or Canister Transfer Room floor from any cause during the lifting, lateral movement, and lowering portions of the canister transfer.
- Prevent CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the RF.

The failure to achieve each success criterion defines the top event for a fault tree for the CTM.

#### 6.2.2.4.5 Mission Time

The mission time for the ITS CTM is set to 1 hour.

#### 6.2.2.4.6 Fault Tree Results

The analysis is detailed in Attachment B, Section B4.

There are four scenarios associated with the CTM that represent potential initiating events:

1. The CTM drops a canister from a height below the design basis height for canister damage (this includes canister drops within the shield bell once the bell slide gate has been closed and drops through the Canister Transfer Room ports to the loading/unloading areas that can occur before the bell slide gate is closed).
2. The CTM drops a canister from a height above the design basis height for canister damage.
3. The CTM drops an object onto a canister.
4. The CTM, while carrying a canister, moves in such a manner (spurious movements, exceeding bridge or trolley end of travel limits) as to cause an impact of the canister with the shield bell.

The results of the analysis are summarized in Table 6.2-4. Five fault trees were developed. The top events correspond to the four potential initiating events defined above.

The results of the analysis are summarized in Table 6.2-4. Five fault trees were developed. The top events correspond to the four potential initiating events defined above.

Table 6.2-4. Summary of Top Event Quantification for the CTM

Top Event	Mean Probability	Standard Deviation
CTM drop all heights	1.4E-5	1.4E-5
CTM high drops from two blocking events	2.8E-8	1.6E-7
Drop of object onto cask	1.4E-5	1.3E-5
CTM collision	3.9E-6	2.7E-7
CTM shear	4.9E-9	9.6E-9

NOTE: CTM = canister transfer machine.

Source: Attachment B, Section B4, Figures B4.4-1, B4.4-16, B4.4-21, B4.4-35, and B4.4-41

### 6.2.2.5 CASK TRACTOR AND CASK TRANSFER TRAILER FAULT TREE ANALYSIS

The FTA for the cask tractor and cask transfer trailer (HCTT) is detailed in Attachment B, Section B5. For the purposes of this analysis, the cask tractor and the cask transfer trailer are collectively called the HCTT. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B5, for sources of information on the physical and operational characteristics of the HCTT.

#### 6.2.2.5.1 Physical Description and Functions

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

#### 6.2.2.5.2 Operation

The casks involved in these operations are kept horizontal from unloading off the SPMRC to a cask stand and then to the HCTT for export to the Aging Facility. After the impact limiters have been removed from the transportation cask, the cask is lifted off the SPMRC using the sling lift and placed on the cask stand. Trunnions are installed on the cask. The cask is then lifted off of the cask stand using yoke fixtures on the crane. The cask is then placed on the HCTT and secured. The HCTT is then driven out of the RF.

### 6.2.2.5.3 Control System

Once the HCTT is properly positioned in the RF, the brakes on both the tractor and trailer are engaged. The brakes are spring applied with hydraulic release calipers. There is a backup system on the tractor consisting of a split master cylinder.

Stabilizing jacks provide vertical support during the loading and unloading of the cask on the HCTT.

### 6.2.2.5.4 System/Pivotal Event Success Criteria

Success criteria for the HCTT is the prevention of a collision with other vehicles, facility structures, or equipment.

Various design features are provided to achieve each success criterion. These include redundant braking systems in the tractor and parking brakes that fail safe. The failure to achieve each success criterion defines the top event for a fault tree for the HCTT.

### 6.2.2.5.5 Mission Times

A conservative mission time of one hour is used to account for the time it takes the HCTT, loaded with a transportation cask, to move from the Cask Preparation Room through the vestibule doors to outside the RF. Once outside, movement of the HCTT is addressed in the Intra-Site Operations analysis.

### 6.2.2.5.6 Fault Tree Results

The HCTT fault tree analysis is detailed in Attachment B, Section B5.

There is one fault tree associated with the HCTT that represents a potential initiating event: HCTT collision with other vehicles, RF facility structures, or equipment when loaded with a transportation cask.

The results of the analysis are summarized in Table 6.2-5.

Table 6.2-5. Summary of Top Event Quantification for the HCTT

Top Event	Mean Probability	Standard Deviation
HCTT Collision	4.4E-3	2.3E-2

NOTE: HCTT = cask tractor and cask transfer trailer.

Source: Attachment B, Section B5, Figure B5.4-1

### 6.2.2.6 Site Transporter Fault Tree Analysis

The FTA for the site transporter is detailed in Attachment B, Section B6. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B6, for sources of information on the physical and operational characteristics of the site transporter.

### 6.2.2.6.1 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. The transport occurs both within the Intra-Site and within the RF. The analysis described herein is limited to movement of the site transporter within the RF, which is limited to the Loading Room and the Lid Bolting Room.

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 electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable 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 the 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 are brought 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.

### 6.2.2.6.2 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 PLC or computer is used to control the machine.

### 6.2.2.6.3 Normal Operations

The site transporter operator lines up the front opening of the site transporter to envelop the aging overpack and positions the rear fork down and in-line with the rectangular lifting slots near the bottom of the aging overpack and moves the site transporter forward until the aging overpack is centered in the interior of the site transporter.

The rear forks are raised to contact the bottom of the lift slots but do not attempt to lift the cask at this time. The operator and interlocks (torque and/or position) are incorporated to prevent lifting with the rear forms only.

The operator initiates the lift support arm's interface sequence with the rear forks and cask to prepare for lifting. After the operator and machine's switches have confirmed that the rear forks and lift support are properly aligned with one another, the lift sequence is initiated. The control system will sequence the lift motors so all screws operate together.

When the lift has been completed, the operator performs the final positioning of the upper restraint arms and inserts a pin in each arm. When the pins are properly installed, the site transporter can move.

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 Site Transporter Vestibule, turns off the diesel generator, and attaches an electric power cable.

Once inside the building, the operator positions the site transporter in the Loading Room. During the various movements inside the RF, the operator disengages the restraint arms for lower and lift operations at the various stations. Each time, the operator removes or replaces the pins from the restraint arms, as appropriate. The movement interlock is engaged when the pins are removed. For example, once inside the Loading Room, the pins will be inserted, the restraints will be engaged, the aging overpack raised from the floor, and the umbilical cord attached. At the completion of the loading, the site transporter is moved out of the Loading Room into the Lid Bolting Room for completing the lid bolting.

#### **6.2.2.6.4 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
- Prevent runaway situations
- Prevent site transporter movements in the wrong direction
- Prevent a rollover of the site transporter
- Prevent spurious site transporter movements
- Prevent a load drop during lift/lower or transport operations.

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

#### **6.2.2.6.5 Mission Time**

For quantification of the site transporter fault trees in Attachment B, Section B6, a mission time of one hour per cask transfer is used.

#### **6.2.2.6.6 Fault Tree Results**

There are four basic site transporter fault trees developed for the RF. The scenarios represented and the variations by these fault trees are the following:

1. Site transporter collides with RF structures:
  - A. Importing aging overpack to Loading Room
  - B. Transfer from Loading Room to Lid Bolting Room
  - C. Exporting aging overpack from Lid Bolting Room.

2. Site transporter load drop during lift/lower
3. Site transporter tipover
4. Site transporter spurious movement.

The results of the analysis are summarized in Table 6.2-6 for the seven fault trees.

Table 6.2-6. Summary of Top Event Quantification for the Site Transporter

Top Event	Mean Probability	Standard Deviation
ST collision in RF	4.6E-3	1.4E-2
ST load drop during lift/lower	3.8E-8	8.9E-8
ST rollover	2.3E-6	1.9E-6
ST spurious movement	2.0E-13	7.3E-13

NOTE: RF = Receipt Facility; ST = site transporter.

Source: Attachment B, Section B6, Figure B6.4-1, B6.4-6, B6.4-20, B6.4-23

### 6.2.2.7 HVAC FAULT TREE ANALYSIS

The FTA for the HVAC is detailed in Attachment B, Section B7. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B7, for sources of information on the physical and operational characteristics of the HVAC system.

#### 6.2.2.7.1 HVAC Description and Function

The ITS HVAC is a two train system of identical components. One train is always operational and one train is in standby mode. This system is not configured to run both trains at the same time without bypassing control circuitry. This off-normal situation is not addressed in this analysis.

In the RF, the Train A HVAC equipment is located on the opposite end of the building from Train B HVAC equipment. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. Although these trains are interconnected through interior duct work, the trains are independent. A back-draft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

This HVAC system is composed of four subsystems:

1. A series of dampers are used to control pressure and flow as well as flow direction in the system.
2. Three HEPA filters, each consisting of one medium efficiency roughing filter (60–90% efficiency), two high-efficiency filters for particulate removal in air (99.97% efficiency), and a mister/demister for maintaining proper humidity levels.

3. One exhaust fan with a rated capacity of 40,500 cfm and an exhaust fan motor rated at 200 hp.
4. Control circuitry with logic contained in an erasable programmable read-only memory located in the adjustable speed drive (ASD) controller used for controlling the speed of the operating fan and on fault detection, and for off-nominal conditions, shutting down the operating train and transmitting signals to the standby system to start.

#### **6.2.2.7.2 Success Criteria**

One success criterion is defined for the each of independent Trains, A and B, for providing the HVAC confinement function: maintain negative differential pressure in the RF for the specified mission time.

The respective trains of the ITS portions of the HVAC are identical. Various design features are provided to achieve each success criterion for the respective trains and for the combined system.

The FTA for the HVAC includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the HVAC.

#### **6.2.2.7.3 Mission Time**

The mission time for the HVAC system is 720 hours (Attachment B, Section B7). However, the mission time for the backup system has been taken as half of the active system (i.e., 360 hours). This is to account for the difference in failure rates between active and passive systems.

#### **6.2.2.7.4 Fault Tree Results**

The top event in this fault tree is “Delta pressure not maintained in RF.” This is defined as the inability of the ITS HVAC system to maintain proper delta pressure within the facility. The system failure probability and standard deviation, including failure of electrical power are as follows:

- The mean HVAC system probability of failure, including loss of electrical power, is 3.4E-02.
- The standard deviation is 9.3E-02.

These results are presented in Attachment B, Section B7, Figure B7.4-1.

#### **6.2.2.8 AC Power Fault Tree Analysis**

The FTA for the AC power system is detailed in Attachment B, Section B8. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B8, for sources of information on the physical and operational characteristics of the AC power system.

### 6.2.2.8.1 System Description

The ITS AC power system supplies power to the ITS systems (for example, the HVAC systems). The ITS power system consists of two elements; those used during normal operations and those used during off-normal conditions. During normal operations AC power is supplied from one of two offsite 138 kV power lines through the 138 kV to 13.8 kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site. Off-normal conditions for the distribution of AC power occur during a LOSP.

A LOSP may be the result of problems on the power grid, or may be the result of failures within the plant AC power systems. Under these conditions, the AC power source for the RF ITS equipment is two onsite ITS diesel generators. Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each ITS diesel generator supplies power to one Train (A or B) of ITS systems. Each diesel generator, its associate support systems, and the power distribution system are independent and electrically isolated from the other ITS diesel generator, its support systems, and power distribution system.

The ITS loads within the RF are powered via two ITS 480 V load centers and two ITS 480 V motor control centers (MCC) located within separate areas of the RF. Each division of the AC power supply from the diesel generator switchgears to the RF passes through a 13.8 kV to 480 V transformer.

The ITS onsite power portion of the ITS power supply system is intended to provide backup power to selected buildings and operations in the event of a main transmission power loss (a LOSP). The primary components in each division include an ITS diesel generator, support systems for the diesel generator, and a load sequencer. Both ITS diesel generators are located in the Emergency Diesel Generator Facility (EDGF). Each is sized to provide sufficient 13.8 kV power to support all ITS loads of one division in six facilities (i.e., three CRCFs, the WHF, the RF, and the EDGF).

The ITS diesel generator starts upon detection of an undervoltage condition via an undervoltage relay of the 13.8 kV ITS switchgear. Each ITS diesel generator is equipped with a complete independent set of support systems including HVAC systems, uninterruptible and DC power systems, a fuel oil system, diesel generator start subsystem, diesel generator cooling subsystem, and lube oil subsystem.

The load sequencer controls sequence of events that occur after a LOSP and the ITS diesel generator start. Upon a LOSP the load sequencer opens the RF ITS load center feed breaker. After the diesel generator starts and reaches rated capacity, the load sequence connects the ITS diesel generator to the 13.8 kV ITS switchgear and then reconnects the RF loads.

### 6.2.2.8.2 Operations

Under normal operating conditions, AC power is supplied from two 138 kV offsite power lines. Power is passed through the 138 kV to 13.8 kV switchyard to the two independent 13.8 kV ITS switchgear. From here, power is transmitted via separate lines to a 13.8 kV to 480 V transformer supporting Trains A and B of the RF. Power to individual ITS components within each facility

is provided via 480 V load centers and MCCs (one of each for Train A and one of each for Train B in each facility) powered through these transformers.

During a LOSP, both ITS diesel generators are required to start and accept loads in a timely manner. Upon a LOSP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8 kV ITS switchgear and the switchyard 13.8 kV switchgear in each train automatically opens. Both ITS diesel generators start automatically and are connected to the 13.8 kV ITS switchgear when the connecting breaker is closed by the load sequencer. The load sequencer then reconnects the RF loads to the 13.8 kV ITS switchgear. Both diesel generators continue to supply AC power until normal power is restored.

Environmental systems are provided to maintain the temperature in the various EDGF rooms and RF ITS electrical rooms within acceptable levels.

#### **6.2.2.8.3 Control System**

The ITS diesel generator starts upon detection of an undervoltage condition via an undervoltage relay of the 13.8 kV ITS switchgear. The 13.8 kV ITS switchgears are isolated from the main switchyard upon a loss of power in the switchyard. The loads in the RF are shed upon a loss of power indication.

A load sequencer controls the loading of the ITS diesel generator onto the 13.8 kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the RF loads onto the AC power system.

#### **6.2.2.8.4 System/Pivotal Event Success Criteria**

Success criterion for the AC power system is defined in terms of its support function for the ITS HVAC confinement function. The AC power system must operate in support of the HVAC system for as long as necessary to successfully provide confinement after the potential release of radioactive material inside the RF. There are two independent trains of HVAC and each of these must be supported by an independent AC power system. Therefore, the following success criteria apply to the respective AC power supply trains:

- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG A) to the HVAC train powered through RF ITS Load Center A and ITS MCC A1 for the mission time of 720 hours.
- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG B) to the HVAC train powered through RF ITS Load Center B and ITS MCC B1 for the mission time of 720 hours.

The respective trains of the ITS portions of the AC power system are essentially identical. Various design features are provided to achieve each success criterion for the respective trains.

The FTA for the AC power system includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the AC power system.

#### **6.2.2.8.5 Mission Time**

The mission time for the ITS AC power system is the same as for the HVAC system, 720 hours.

#### **6.2.2.8.6 Fault Tree Results**

Two fault trees are developed for the AC power system, one for Train A and one for Train B. The respective top events are:

- “Loss of AC power at ITS Load Center A for the RF,” defined as a failure of the normal and ITS on-site power supplies to provide power to ITS load center A1.
- “Loss of AC power at ITS Load Center B for the RF,” defined as a failure of the normal and ITS on-site power supplies to provide power to ITS load center B.

The results are essentially the same for either train:

- The mean probability of failure or either train value is 3.1E-02
- The standard deviation is 7.6E-02.

These results are presented in Attachment B, Section B8, Figures B8.4-1 and B8.4-3.

#### **6.2.2.9 Potential Moderator Sources**

##### **6.2.2.9.1 Internal Floods**

Internal floods are potential sources of moderator addition into a canister associated with pivotal events in the event sequences included in Section 6.1. Moderator addition into a canister can occur following a breach of the canister and a subsequent internal flood. The internal flooding analysis considers all waste handling facilities.

During most of its handling at the repository, a canister is surrounded by at least one other barrier to water intrusion: a transportation cask, a transportation cask within a CTT, an aging overpack, a waste package, a waste package within a WPTT, or a waste package within a TEV.

Each facility is equipped with a normally dry, double-preaction sprinkler system in areas where waste forms are handled ((Ref. 2.2.16), (Ref. 2.2.29), (Ref. 2.2.23), and (Ref. 2.2.36)). Such systems, which require both actuation of smoke and flame detectors to allow the preaction valve to open and to allow heat actuation of a fusible link sprinkler head to initiate suppression, have a very low frequency of spurious operation. A 30-day period from the occurrence of the canister breach to the time definitive action can be taken to prevent introduction of water into the canister is reasonable and is the same as the period used to assess dose for a radiological release. The spurious actuation frequency over a 30-day mission time after a breach is calculated below.

An estimate of the probability of spurious actuation is developed using a simplified screening model that addressed the following cut sets that result in actuation:

- Spurious preaction valve opens before canister breach  $\times$  failure of a sprinkler head during post-breach mission time (30 days).
- Failure of a sprinkler head during building evacuation  $\times$  water left in dry piping after last test (first quarter following annual test).

The frequency of sprinkler failure is estimated using an individual sprinkler head failure frequency of  $1.6\text{E-}6/\text{yr}$  (Ref. 2.2.13, Table 1), the estimated number of sprinklers (1 per  $130\text{ ft}^2$  based on NFPA 13-2007 (Ref. 2.2.59, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2.20). For example, the area of CRCF Waste Package Loadout Room (Room 1015) is listed as  $7,470\text{ ft}^2$  (Ref. 2.2.20). At  $130\text{ ft}^2/\text{sprinkler}$ , 58 sprinklers are estimated. The failure of any sprinkler in the room is then estimated to be  $58 \times 1.6\text{E-}6/\text{yr} \times 1/8,760\text{ hrs/yr}$ , or  $1.1\text{E-}8/\text{hr}$ .

The frequency of preaction valve spurious open is estimated using the solenoid valve spurious open data in Section 6.3 of  $8.1\text{E-}07/\text{hr}$ . This is reasonable because a solenoid valve must open to relieve the air pressure from the diaphragm which keeps the valve closed.

The value of the first cut set is  $(1.6\text{E-}6/\text{yr} \times 1/8760\text{ hr/yr} \times 720\text{ h}) \times (8.1\text{E-}7/\text{hr} \times 720\text{ h}) = 8\text{E-}11/\text{sprinkler head}$ . The second cut set is more significant:  $0.025$  (human error screening value)  $\times (1.6\text{E-}6/\text{yr} \times 1/8760\text{ hr/yr} \times 720\text{ h}) = 3\text{E-}9/\text{sprinkler head}$ .

Applying the sum of these values,  $3\text{E-}9/\text{sprinkler head}$ , to the number of sprinklers calculated for the waste handling areas of the four facilities results in the following estimates of the probability of spurious sprinkler actuation found in Table 6.2-7.

Piping carrying water is present in the waste form handling areas of the CRCF, IHF, and WHF. Piping lengths in these areas of the CRCF and WHF are below 100 feet per facility. For the IHF, approximately 6,800 feet of piping runs no closer than 60 feet of the cask unbolting area (Ref. 2.2.83). Even the length of piping in the IHF has little impact post-breach, as the probability of a pipe crack or rupture in a 30-day period following a potential breach is less than  $2.0\text{E-}3$ . There is no wet piping in the waste form handling areas of the RF (Ref. 2.2.83).

Table 6.2-7. Probability of Spurious Sprinkler Actuation

Facility	Waste Handling Area (ft <sup>2</sup> ) <sup>a</sup>	Number of Sprinkler Heads	Probability of Spurious Actuation in 30-day Period in Waste Handling Areas
CRCF(ea)	42,000	330	1E-6
IHF	30,000	240	9E-7
RF	19,000	150	5E-7
WHF	28,000	215	6E-7

NOTE: <sup>a</sup>CRCF area based on room numbers 1005E, 1016-1026, 2004,2007, 2007A, and 2007B;  
 IHF area based on room numbers 1001-1003, 1006-1008, 1011,1012, 1026, and 2004;  
 RF area based on room numbers 1013, 1015, 1016, 1017, 1017A, and 2007;  
 WHF area based on room numbers 1007-1010, 1016, 2004, 2006, and 2008.  
 CRCF = Canister Receipt and Closure Facility, IHF = Initial Handling Facility, RF = Receipt Facility,  
 WHF = Wet Handling Facility.

Source: Original

The probability of a pipe crack in a 30-day period was estimated using the pipe leak data from NUREG/CR-6928 (Ref. 2.2.43, Table 5-1). Piping leaks and large break rates applicable to nonservice water applications are used in the analysis. These values are considered appropriate for repository systems because of the conditioning applied to the fluids in the systems will be that typical of the commercial nuclear power plant:

External leak small (1 to 50 gpm): Leak rate =  $2.5E-10 \text{ hr}^{-1}\text{ft}^{-1}$

External leak large (> 50 gpm): Leak rate =  $2.5E-11 \text{ hr}^{-1}\text{ft}^{-1}$

Multiplying the sum of the small and large crack frequencies ( $2.8E-10 \text{ hr}^{-1}\text{ft}^{-1}$ ) by the length of piping in the waste handling areas of each facility, and the number of hours in a 30-day period (720 hr), a conditional probability of water leakage in all waste handling areas given a breach is approximated as follows:

$$\text{CRCF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 100 \text{ ft} \times 720 \text{ h} = 2.0E-05$$

$$\text{IHF} < 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 6,800 \text{ ft} \times 720 \text{ h} = 1.4E-03$$

$$\text{WHF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 75 \text{ ft} \times 720 \text{ h} = 1.5E-05$$

$$\text{RF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 0 \text{ ft} \times 720 \text{ h} = 0.$$

It is appropriate to use the waste handling area piping lengths because they are separated by concrete walls from the nonwaste handling areas of buildings.

The above applies to event sequences that do not involve fires as an initiating event. During fire initiating event sequences, fire suppression would actuate in the locations sufficiently heated by the fire. The fire initiating event analysis is described in Section 6.5, and the conditional probability of canister failure owing to fires is described in Section 6.3. The analysis is performed without the salutary effects of fire suppression in order to demonstrate large margins of safety during fire event sequences. Furthermore, the location of each fire is analyzed as around the outer shell of the overpack that surrounds the canister, which neither accounts for the CTT or WPTT enclosures that surround the overpack nor the elevated position of the canisters with respect to a fire on the floor. The frequency of containment breach due to fire is significantly overestimated because of this conservative approach.

For fires that occur in locations that contain canisters sealed within bolted transportation casks, the fire location will be floor level and the transportation casks rise as much as 20 feet above the floor. Casks are relatively thick walled compared to canisters and sustain a relatively small internal pressurization when compared to canisters. Therefore, if a fire is large enough, it will fail the internal canister first, as indicated in Attachment D. This will cause the bolted and sealed cask to bear the overpressure that is inside the canister. The cask bolts might act as elastic springs allowing the top to break the seal and relieve the internal pressure. This would be a mechanism that prevents cask breach. However, a hot fire may result in sufficient loss of strength of the bottom portion of the stainless steel cask such that it breaches. If failure occurs because of bolt stretching the cask lid remains on top of the cask preventing fire suppression water from entering. Commercial DPCs and TAD canisters will require at least 100 liters of water to enter the canister if optimally distributed among the fuel rods (Ref. 2.2.33). Casks are raised above the floor. They lay on top of railcars, are lifted from there by cranes, sit inside a CTT, or lay sideways on a pallet. They are at least 5 feet from the floor. If the bottom portion of the canister breaches, there is no physical mechanism for this much water to enter the cask and then the canister, remain as water (not boil off), and optimally mix with the fuel rods.

This latter situation also applies to canisters sealed within a welded waste package. The waste package sits inside a WPTT or is inside a TEV. In the former case it is more than 3 feet from the floor (Ref. 2.2.17) and in the latter case about 1 foot from the floor (Ref. 2.2.18). In the latter case, however, the TEV offers an additional layer of protection against fires. In addition, it is physically unrealistic for a sufficient amount of available fire suppression water to cause 100 liters to leak into a breached canister, but not extinguish the fire or at least reduce the severity of the fire such that a breach would not occur.

For a canister inside of an open transportation cask or waste package, the orientation of these is always vertical, and the cask and waste package are always elevated above the floor where the fire occurs. The occurrence of a fire of sufficient severity will fail the canister first as described above. An open transportation cask or waste package might allow fire suppression water to spray in from the top. The building configuration, however, precludes this occurrence. The cask lids are removed while in the upload cell below the CTM. The cask and waste package ports are above the casks and waste package. There is no fire suppression piping spanning the ports because the ports must be kept clear in order to perform lift and load operations. In the Waste Package Positioning Room and welding area, the lid is on the waste package and fire suppression piping cannot be above an open waste package because of the welding machine. In the cutting cell in which a cask is open (WHF only), there can be no fire suppression piping above an open cask because of the cutting equipment.

Upon failure of the canister inside the cask, the cask will not be susceptible to pressurization failures as above. Instead, water can only enter in a cask (or waste package) if the cask body melts through. Fires capable of melting stainless steel or Alloy 22, however, have an occurrence frequency within the waste handling facilities of less than  $1E-05$  over the preclosure period (Attachment D). Thus, breach of the cask or waste package in a manner that would allow water to enter the canister is essentially not physically realizable.

When a canister is being lifted, transferred inside the shield bell, and lowered, it is not inside an outer cask. However, fires cannot be severe enough to breach a canister while being moved, as

described in more detail in Attachment D. Water intrusion, therefore, is not physically realizable for this situation.

It is concluded that moderator entry into breached canisters during fire event sequences is not physically realizable because of a combination of physical mechanisms, building and equipment configuration, and overpack material properties. Furthermore, the existence of water from fire suppression is inconsistent with the fire analyses performed to obtain the probability of containment failure owing to fire. If fire suppression were indeed available, the probabilities of canister breach would be far lower. However, in order to complete an event sequence quantification, the conditional probability of moderator entry into a canister after canister breach during a fire initiating event sequence is assessed as *extremely unlikely* and assigned a lognormal distribution with a median of 0.001 and an error factor of 10. This yields a mean value of 3E-03. The large error factor is assigned because of the potential of human error to defeat some of the reasons that water will not enter the cask or waste package (e.g., neglecting to place a lid on the waste package just before a severe fire). These assignments are consistent with the methodology on the use of judgment provided in Section 4.3.10.

#### 6.2.2.9.2 Lubricating Fluid

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a welded gear box with a leak pan below it capable of capturing the entire gearbox fluid inventory. An estimate of the leakage rate through the gear box and drip pan is found by multiplying the gear case motor failure frequency (all modes) of 0.88E-06 per hour (Ref. 2.2.38, p. 2-104 and Section 6.3) over the 50 years by the conditional probability of oil pan failure. A loss of lubrication would fail the crane operation and also be detected by oil pressure indicators. The conditional probability of oil pan failure may be estimated by analogy to receiver tank leakage during the interval between gearbox failure and detection. The interval is conservatively estimated to be 30 days (720 hr). The all modes failure rate of a receiver tank is 0.34 E-06 per hour (Ref. 2.2.38, p. 2-213). Using an exposure interval of 50 years (which represents the operating life of the surface facilities), the conditional probability of lubricating fluid entering a breached canister would be less than:

$$0.88\text{E-}06/\text{hr} \times 50 \text{ yr} \times 8,760 \text{ hr/yr} \times 0.34\text{E-}06/\text{hr} \times 720 \text{ hr} = 9\text{E-}05$$

over the preclosure period.

This probability is overstated because (1) it does not account for inspections during the operating period of the facility, and (2) it does not account for the conditional probability that lubricating fluid can find its way into a breached canister. Therefore, lubricating fluid is eliminated as a potential moderator.

## 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 represented 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-kind facility and has no operating history, it is necessary to develop the required data from the experience of other nuclear and non-nuclear equipment operations. Industry-wide data sources are documents containing industrial or military experience on component performance. These sources are from previous safety/risk analyses and reliability studies performed nationally or internationally and also standards or published handbooks. For the YMP PCSA, a database is constructed using a library of industry-wide data sources of reliability data from nuclear power plants, 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 has to 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, as long as the detail and the applicability of the information provided justify its use. Lastly, 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.

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the industry-wide 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 Section C1.2.

Given the fact that the YMP is a relatively unique facility (although portions are similar to the spent fuel 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, canister maneuvering cranes, and the spent fuel transfer machine (SFTM). The SFTM is not used in the RF; however, it is 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 that 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 component type and failure mode combination (TYP-FM), although multiple sources are not always available for a specific piece of equipment. When data was extracted from several sources, it was 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. 2.2.11). 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

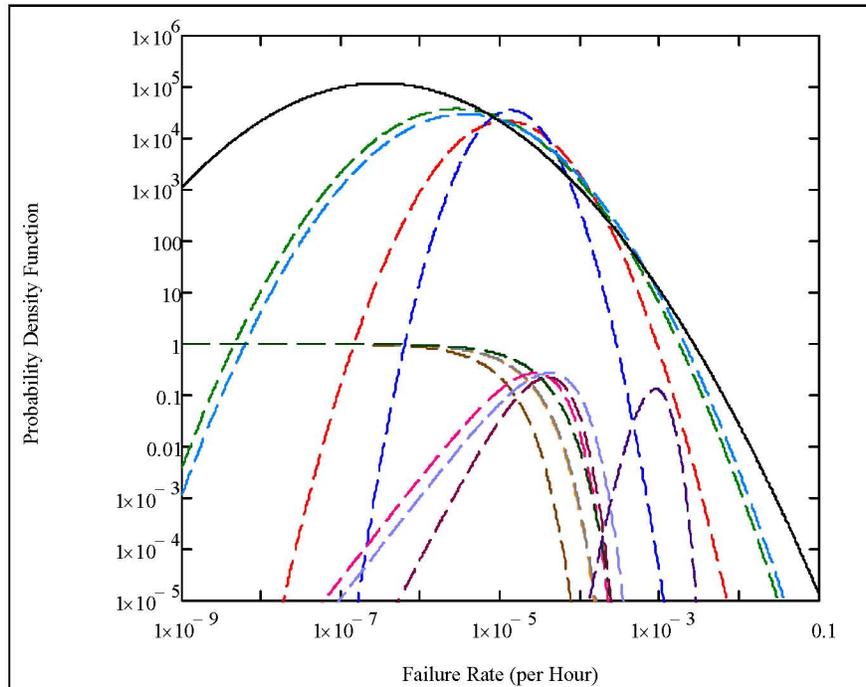
the available data to the YMP introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying available data sources using the following steps:

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. 2.2.53, 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,  $\nu$  and  $\tau$ , respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating  $\nu$  and  $\tau$  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  $\nu$  and  $\tau$ . 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  $\nu$  and  $\tau$  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 probability density function 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 Jeffrey's 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.

### 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 human failure events 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 common-cause failure 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. 2.2.48), the Multiple Greek Letter method (Ref. 2.2.57), and the Alpha Factor method (Ref. 2.2.58). 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, common-cause failure rates or probabilities are estimated using the Alpha Factor method (Ref. 2.2.58) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in NUREG/CR-5485 (Ref. 2.2.58) 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 (see equation in Attachment C, Section C3).
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. 2.2.58, Table 5-11) and reproduced in Attachment C, Table C3-1.

These alpha-factors values are used for failure-on-demand events (e.g., pump failure 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  $\alpha_2$ ) 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  $\alpha_2$  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 such 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 utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the SAPHIRE code, then by using the modify event feature to link the template data to each basic event in the fault tree. This permits each active component of the same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the 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 RF Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the RF models. Development of this table is discussed in detail in Attachment C, Section C4. Mission times are discussed in Section 6.2.

Table 6.3-1. Active Component Reliability Data Summary

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-#EEE-LDCNTRA-BUA-FOH	RF ITS Load Center A fails	3	4.39E-04	6.10E-07	720
200-#EEE-LDCNTRA-C52-FOD	ITS Load Center A feed breaker fails to reclose	1	2.24E-03	—	—
200-#EEE-LDCNTRA-C52-SPO	Load Center A feed circuit breaker spurious operation	3	3.82E-03	5.31E-06	720
200-#EEE-LDCNTRB-BUA-FOH	RF ITS Load Center B fails	3	4.39E-04	6.10E-07	720
200-#EEE-LDCNTRB-C52-FOD	13.8 kV ITS SWGR to RF LC B circuit breaker fails on demand	1	2.24E-03	—	—
200-#EEE-LDCNTRB-C52-SPO	RF load center circuit breaker (AC) spurious operation	3	3.82E-03	5.31E-06	720
200-#EEE-LDCNTRS-C52-CCF	Common-cause failure of the ITS load center feed breakers to reclose	C	1.05E-04	—	—
200-#EEE-MCC0001-C52-SPO	RF ITS MCC 0001 feed breaker spurious operation	3	3.82E-03	5.31E-06	720
200-#EEE-MCC0001-MCC-FOH	RF ITS MCC 00001 fails	3	5.38E-03	7.49E-06	720
200-#EEE-MCC0002-C52-SPO	RF MCC-00002 feed breaker spurious operation	3	3.82E-03	5.31E-06	720
200-#EEE-MCC0002-MCC-FOH	RF ITS MCC00002 failure	3	5.38E-03	7.49E-06	720
200-#EEE-RFITS-A-XMR-CCF	RF ITS transformer Train A CCF	C	4.92E-06	—	—
200-#EEE-RFITS-A-XMR-FOH	RF ITS transformer Train B failure	3	2.10E-04	2.91E-07	720
200-#EEE-RFITS-B-XMR-FOH	RF ITS transformer Train B failure	3	2.10E-04	2.91E-07	720
200-DRUM001-DM-FOD	CTM drum failure on demand	1	4.00E-08	—	—
200-CR--IEL001--IEL-FOD	Interlock A from slide gate fails	1	2.75E-05	—	—
200-CR--IEL001-IEL-FOD	Skirt interlock failure	1	2.75E-05	—	—
200-CR--IEL002--IEL-FOD	Interlock B from slide gate fails	1	2.75E-05	—	—
200-CR--IELCCF--IEL-CCF	Common-cause failure of interlocks from slide gate	C	1.29E-06	—	—
200-CR--IEL001--IEL-FOD	Interlock A from slide gate fails	1	2.75E-05	—	—
200-CR--IEL002--IEL-FOD	Interlock B from slide gate fails	1	2.75E-05	—	—
200-CR--IELCCF-IEL-CCF	Common-cause failure of interlocks from slide gate	C	1.29E-06	—	—
200-CR--PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3	3.65E-07	3.65E-07	1
200-CR-PLC001-PLC-SPO	Inadvertent signal sent due to PLC failure	3	3.65E-07	3.65E-07	1
200-CRN-HSTTRLMO-MOE-FSO	Crane hoist motor (electric) fails to shut off	3	1.35E-08	1.35E-08	1
200-CRN-PLC0101--PLC-SPO	Crane bridge motor PLC spurious operation	3	3.65E-07	3.65E-07	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CRN2-2-BLOCK-CRN-TBK	200-ton crane two-block drop	1	4.41E-07	—	—
200-CRN2-2BLKDON-CRN-TBK	200-ton crane two-block drop	1	4.41E-07	—	—
200-CRN2-DROPDPC-CRN-DRP	200-ton crane drop	1	3.20E-05	—	—
200-CRN2-DROPDPC-CRS-DRP	200-ton crane sling drop	1	1.17E-04	—	—
200-CRN2-DROPON--CRN-DRP	200-ton crane drop	1	3.20E-05	—	—
200-CRN2-DROPTAD-CRN-DRP	200-ton crane drop	1	3.20E-05	—	—
200-CRNBRIDGMTR-MOE-FSO	Crane bridge motor (electric) fails to shut off	3	1.35E-08	1.35E-08	1
200-CRNDRPONDPC-CRN-DRP	200-ton crane drop	1	3.20E-05	—	—
200-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on Lift Boom #1 fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on Lift Boom #1 fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on Lift Boom #2 fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATB222-AT--FOH	Screw actuator mechanism on Lift Boom #2 fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATD0002-AT-FOH	ST D-axis Electrical Actuator #2 fails lift/lower	3	7.54E-05	7.54E-05	1
200-CRWT-ATD001-AT-FOH	ST D-axis Electrical Actuator #1 fails lift/lower	3	7.54E-05	7.54E-05	1
200-CRWT-ATD03-AT-FOH	ST D-axis Electrical Actuator #1 movement fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATD04-AT-FOH	ST D-axis Electrical Actuator #2 movement fails	3	7.54E-05	7.54E-05	1
200-CRWT-ATP002-AT-FOH	ST P-axis electrical failure during movement	3	7.54E-05	7.54E-05	1
200-CRWT-ATR10002-AT-FOH	ST R-axis Electrical Actuator #1 fails movement	3	7.54E-05	7.54E-05	1
200-CRWT-ATR2004-AT-FOH	ST R-axis Electrical Actuator #2 fails movement	3	7.54E-05	7.54E-05	1
200-CRWT-BEA#1-BEA-BRK	Boom#1 fails during cask movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	3	2.40E-08	2.40E-08	1
200-CRWT-BEAB202-BEA-BRK	Boom#2 fails during cask movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEAD003-BEA-BRK	ST D-axis Actuator Structural Arm #2 failure movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEAD006-BEA-BRK	ST D-axis Actuator Structural Arm #1 failure movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEAP02-BEA-BRK	ST P-axis mechanical failure during movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEAR103-BEA-BRK	ST R-axis Actuator Structural Arm #1 failure movement	3	2.40E-08	2.40E-08	1
200-CRWT-BEAR204-BEA-BRK	ST R-axis actuator structural arm #2 failure movement	3	2.40E-08	2.40E-08	1
200-CRWT-BRK001--BRK-FOD	Tractor Brake A fails	1	1.46E-06	—	—
200-CRWT-BRK002--BRK-FOD	Tractor Brake B fails	1	1.46E-06	—	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CRWT-BRK003--BRK-FOD	Trailer brakes fail	1	1.46E-06	—	—
200-CRWT-BRKCCF--BRK-CCF	CCF of both tractor brakes	C	6.86E-08	—	—
200-CRWT-CBP0000-CBP-OPC	Electrical power dist cable failure on ST	3	9.13E-08	9.13E-08	1
200-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	3	7.14E-05	7.14E-05	1
200-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	3	2.27E-05	2.27E-05	1
200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	3	2.40E-08	2.40E-08	1
200-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	3	1.79E-06	1.79E-06	1
200-CRWT-ELEC-MOE-FOD	ST electric motor failure	1	6.00E-05	—	—
200-CRWT-IEL0001-IEL-FOH	Restraint system interlock failure	1	3.43E-05	—	—
200-CRWT-LC000011-LC-FOD	ST lift/lower selector level fails	1	6.25E-04	—	—
200-CRWT-LPATH--ATH--CCF	CCF of pendular axle hydraulics during load/unload	C	8.74E-05	—	—
200-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LSJATH1-ATH-FOH	Stabilizing Jack 1 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LSJATH2-ATH-FOH	Stabilizing Jack 2 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LSJATH3-ATH-FOH	Stabilizing Jack 3 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LSJATH4-ATH-FOH	Stabilizing Jack 4 failure	3	1.78E-03	8.91E-04	2
200-CRWT-LVRD01-LVR-FOH	ST D-axis Actuator Structural Arm #1 failure	3	2.10E-06	2.10E-06	1
200-CRWT-LVRD02-LVR-FOH	ST D-axis Actuator Structural Arm #2 failure	3	2.10E-06	2.10E-06	1
200-CRWT-PIND004-PIN-BRK	ST D-axis Actuator Pin #2 failure movement	3	2.12E-09	2.12E-09	1
200-CRWT-PIND005-PIN-BRK	ST D-axis Actuator Pin #1 failure movement	3	2.12E-09	2.12E-09	1
200-CRWT-PINP04-PIN-BRK	ST P-axis pin failure during movement	3	2.12E-09	2.12E-09	1
200-CRWT-PINR103-PIN-BRK	ST R-axis Mechanical Pin #1 failure during movement	3	2.12E-09	2.12E-09	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CRWT-PINR202-PIN-BRK	ST R-axis Mechanical Pin #2 failure during movement	3	2.12E-09	2.12E-09	1
200-CRWT-SJKB011-SJK-FOH	Screw lift on Boom #1 fails	3	8.14E-06	8.14E-06	1
200-CRWT-SJKB101-SJK-FOH	Screw lift on Boom #1 fails	3	8.14E-06	8.14E-06	1
200-CRWT-SJKB202-SJK-FOH	Screw lift on Boom #2 fails	3	8.14E-06	8.14E-06	1
200-CRWT-SJKB22-SJK-FOH	Screw lift on Boom #2 fails	3	8.14E-06	8.14E-06	1
200-CRWT-TRCT-ST-STR-FOH	Tractor steering system failure	3	1.84E-05	1.84E-05	1
200-CRWT-TRD0001-TRD-FOH	Front portside track failure	3	5.89E-07	5.89E-07	1
200-CRWT-TRD0002-TRD-FOH	Rear portside track failure	3	5.89E-07	5.89E-07	1
200-CRWT-TRD0003-TRD-FOH	Front starboard track failure	3	5.89E-07	5.89E-07	1
200-CRWT-TRD0004-TRD-FOH	Rear starboard track failure	3	5.89E-07	5.89E-07	1
200-CRWT-TRLR-ST-STR-FOH	Trailer steering system failure	3	1.84E-05	1.84E-05	1
200-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	1	2.93E-04	—	—
200-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	1	2.93E-04	—	—
200-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	1	2.93E-04	—	—
200-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	1	2.93E-04	—	—
200-CTM-#ZSH0112-1ZS-FOD	CTM shield skirt position switch 0112 fails	1	2.93E-04	—	—
200-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	C	1.38E-05	—	—
200-CTM--330121--ZS--FOD	CTM hoist first upper limit switch 0121 failure on demand	1	2.93E-04	—	—
200-CTM--330122--ZS--FOD	CTM final hoist upper limit switch 0122 failure on demand	1	2.93E-04	—	—
200-CTM--CBL0001-CBL-FOD	CTM hoist wire rope breaks	1	2.00E-06	—	—
200-CTM--CBL0002-CBL-FOD	CTM hoist wire rope breaks	1	2.00E-06	—	—
200-CTM--CBL0102-CBL-CCF	CCF CTM hoist wire ropes	C	9.40E-08	—	—
200-CTM--EQL-SHV-BLK-FOD	CTM sheaves failure on demand	1	1.15E-06	—	—
200-CTM--GRAPPLE-GPL-FOD	CTM grapple failure on demand	1	1.15E-06	—	—
200-CTM--HOISTMT-MOE-FTR	CTM hoist motor (electric) fails to run	3	6.50E-06	6.50E-06	1
200-CTM--HOLDBRK-BRK-FOD	Brake failure on demand	1	1.46E-06	—	—
200-CTM--HOLDBRK-BRK-FOH	CTM holding brake (electric) failure to hold	3	3.52E-05	4.40E-06	8
200-CTM--IMEC125-IEL-FOD	CTM hoist motor control interlock failure on demand	1	2.75E-05	—	—
200-CTM--IMEC125-ZS-FOD	CTM load cell limit switch failure on demand	1	2.93E-04	—	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CTM--LOWERBL-BLK-FOD	CTM lower sheaves failure on demand	1	1.15E-06	—	—
200-CTM--MISSPOOL-DM-MSP	CTM misspool events pool event	3	6.86E-07	6.86E-07	1
200-CTM--OVERSP--ZS--FOD	CTM hoist motor speed limit switch failure on demand	1	2.93E-04	—	—
200-CTM--PORTGT1-MOE-SPO	Spurious Port Gate 1 motor operation	3	6.74E-07	6.74E-07	1
200-CTM--PORTGT1-PLC-SPO	Port gage PCL spurious operation	3	3.65E-07	3.65E-07	1
200-CTM--PORTGT2-MOE-SPO	Port gate motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM--PORTGT2-PLC-SPO	Port gage PCL spurious operation	3	3.65E-07	3.65E-07	1
200-CTM--SLIDEGT-MOE-SPO	CTM slide gate motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM--SLIDEGT-PLC-SPO	CTM slide gate PLC spurious operation	3	3.65E-07	3.65E-07	1
200-CTM--SLIDGT2-IEL-FOD	CTM slide gate interlock failure	1	2.75E-05	—	—
200-CTM--TROLLY-MOE-SPO	CTM trolley motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM--UPPERBL-BLK-FOD	CTM upper sheaves failure	1	1.15E-06	—	—
200-CTM--WT0125--SRP-FOD	CTM load cell pressure sensor fails on demand	1	3.99E-03	—	—
200-CTM--WTSW125-IEL-FOD	CTM hoist motor control interlock failure on demand	1	2.75E-05	—	—
200-CTM--WTSW125-ZS--FOD	CTM load cell limit switch failure on demand	1	2.93E-04	—	—
200-CTM--YS01129-ZS--FOD	CTM drum brake control circuit limit switch 1129 failure	1	2.93E-04	—	—
200-CTM--ZSH0111-ZS--SPO	CTM grapple engaged limit switch spurious operation	3	1.28E-06	1.28E-06	1
200-CTM--ASD0122#-CTL-FOD	CTM hoist ASD controller fails	1	2.03E-03	—	—
200-CTM--BIDGMTR-#TL-FOH	CTM bridge motor torque limiter failure	3	2.86E-02	8.05E-05	360
200-CTM--BRDGEMTR-MOE-SPO	CTM bridge motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM--BREDGMTR-#CT-FOD	CTM hand held radio remote controller fails	1	4.00E-06	—	—
200-CTM--BRIDGETR-#PR-FOH	CTM bridge passive restraint (end stops) failure	3	1.95E-06	4.45E-10	4380
200-CTM--BRIDGETR-MOE-FSO	CTM bridge motor fails to stop	3	1.35E-08	1.35E-08	1
200-CTM--BRIDGMTR-IEL-FOD	CTM shield skirt-bridge motor interlock failure	1	2.75E-05	—	—
200-CTM--BRIDGMTS-MOE-SPO	CTM bridge motor (electric) spurious operation -shear	3	3.37E-08	6.74E-07	.05
200-CTM--DRTM-CT-FOD	CTM drive train protection and fail det. controller failure	1	4.00E-06	—	—
200-CTM--DRUMBRK-BRP-FOH	CTM drum brake (pneumatic) failure to hold	3	6.70E-05	8.38E-06	8
200-CTM--HOISTMTR-MOE-FSO	CTM hoist motor (electric) fails to shut off	3	1.35E-08	1.35E-08	1
200-CTM--HSTTRLLS-MOE-SPO	CTM hoist trolley motor (electric) spurious operation m- shear	3	3.37E-08	6.74E-07	.05

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CTM-HSTTRLLY-#TL-FOH	CTM hoist motor torque limiter failure	3	2.86E-02	8.05E-05	360
200-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt hoist trolley motor interlock failure	1	2.75E-05	—	—
200-CTM-HSTTRLLY-MOE-SPO	Motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.70E-06	4.70E-06	1
200-CTM-PLC0101S-PLC-SPO	CTM bridge motor PLC spurious operation - shear	3	3.65E-07	3.65E-07	1
200-CTM-PLC0102S-PLC-SPO	CTM shield bell trolley PLC spurious operation -shear	3	3.65E-07	3.65E-07	1
200-CTM-PLC0103S-PLC-SPO	CTM hoist trolley PLC spurious operation -shear	3	3.65E-07	3.65E-07	1
200-CTM-SBELTRLS-MOE-SPO	Motor (electric) spurious operation	3	6.74E-08	6.74E-07	0.1
200-CTM-SBELTRLY-#TL-FOH	CTM shield bell motor torque limiter failure	3	2.86E-02	8.05E-05	360
200-CTM-SBELTRLY-IEL-FOD	CTM shield bell trolley interlock failure	1	2.75E-05	—	—
200-CTM-SBELTRLY-MOE-SPO	Motor (electric) spurious operation	3	6.74E-07	6.74E-07	1
200-CTM-SKRTCTCT-SRP-FOD	CTM skirt floor contact sensors fail	1	3.99E-03	—	—
200-CTM-SLIDGT2-SRX-FOD	CTM slide gate position sensor fails on demand	1	1.10E-03	—	—
200-CTM-TROLLEYT-MOE-FSO	CTM trolley motor fails to stop	3	1.35E-08	1.35E-08	1
200-CTM-TROLLYTR-#PR-FOH	CTM trolley end run stops failure	3	1.95E-06	4.45E-10	4380
200-CTM-TROLYCNT-#HC-FOD	CTM trolley motor hand controller fails	1	1.74E-03	—	—
200-CTM-ZSL0111-ZS--SPO	CTM grapple engaged limit switch spurious operation	3	1.28E-06	1.28E-06	1
200-CTT--CT001--CT--SPO	On-board controller initiates spurious signal	3	2.27E-05	2.27E-05	1
200-CTT--DSW000--ESC-CCF	Common-cause failure of deadman switches	C	1.18E-05	—	—
200-CTT--DSW001--ESC-FOD	Deadman Switch #1 fails closed	1	2.50E-04	—	—
200-CTT--DSW002--ESC-FOD	Deadman Switch #2 fails closed	1	2.50E-04	—	—
200-CTT--HC001--HC--SPO	Hand held controller initiates spurious signal	3	5.23E-07	5.23E-07	1
200-CTT-SV301-SV-SPO	Air supply solenoid valve spurious operation	3	4.09E-07	4.09E-07	1
200-CTT--ZS301--ZS--FOD	Pin Limit Switch #1 fails	1	2.93E-04	—	—
200-CTT--ZS302--ZS--FOD	Pin Limit Switch #2 fails	1	2.93E-04	—	—
200-CTT-FWDREVM1-SV-FOH	Failure of SV providing fwd/rev to Motor 1	3	4.87E-05	4.87E-05	1
200-CTT-FWDREVM2-SV-FOH	Failure of SV providing fwd/rev to Motor 2	3	4.87E-05	4.87E-05	1
200-CTT-SV301-SV-SPO	Air supply solenoid valve spurious operation	3	4.09E-07	4.09E-07	1
200-CTT-SV401-SV-FOH	Failure of air supply solenoid valve for air bags	3	4.87E-05	4.87E-05	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-CTT-SVROTM1-SV-FOH	Failure of SV providing rotation to Motor 1	3	4.87E-05	4.87E-05	1
200-CTT-SVROTM2-SV-FOH	Failure of SV providing rotation to Motor 2	3	4.87E-05	4.87E-05	1
200-CTT-ZS301-SW-CCF	Common-cause failure of limit switches	C	1.38E-05	—	—
200-DRUMBRK-BRP-FOH	CTM drum brake (pneumatic) failure on demand	3	8.38E-06	8.38E-06	1
200-FL---SC001---SC--FOH	Forklift speed control fails	3	1.28E-04	1.28E-04	1
200-FL---SC006---SC--FOH	Forklift speed control fails	3	1.28E-04	1.28E-04	1
200-HTC--HC021---HC--FOD	Remote stop control transmits wrong instruction	1	1.74E-03	—	—
200-HTC--SV601---SV--FOD	Main air supply valve fails on demand	1	6.28E-04	—	—
200-HTC--SV602---SV--FOD	Solenoid valve fails to close	1	6.28E-04	—	—
200-HTTCOLLIDE--G65-FOH	Speed limiter fails	3	1.16E-05	1.16E-05	1
200-PORTSLIDEGTE-IEL-FOD	Port slide gate interlock fails	1	2.75E-05	—	—
200-SD--PLC001-PLC-SPO	Spurious signal from PLC closes door	3	3.65E-07	3.65E-07	1
200-SD--SRU001--SRU-FOH	Ultrasonic obstruction sensor fails	7	2.16E-03	9.62E-05	45
200-SD--TL000---TL--CCF	Common cause failure of over torque sensors	C	6.68E-04	—	—
200-SD--TL001---TL--FOH	Motor #1 over-torque sensor fails	7	2.84E-02	8.05E-05	720
200-SD--TL002---TL--FOH	Motor #2 over-torque sensor fails	7	2.84E-02	8.05E-05	720
200-SLDGATE-IEL-FOD	Slide gate interlock fails	1	2.75E-05	—	—
200-SPMRC-BRP000-BRP-FOD	Brake (pneumatic) failure on demand SPMRC fails to stop on loss of power	1	5.02E-05	—	—
200-SPMRC-BRP001-BRP-FOD	SPMRC brake (pneumatic) failure on demand	1	5.02E-05	—	—
200-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	3	9.13E-08	9.13E-08	1
200-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	3	1.88E-08	1.88E-08	1
200-SPMRC-CPL00-CPL-FOH	Railcar automatic coupler system fails	3	1.91E-06	1.91E-06	1
200-SPMRC-CT000--CT--FOD	SPMRC primary stop switch fails	1	4.00E-06	—	—
200-SPMRC-CT0001-CT-FOD	On-board controller fails to respond	1	4.00E-06	—	—
200-SPMRC-CT002--CT--FOH	Pendant direction controller fails	3	6.88E-05	6.88E-05	1
200-SPMRC-CT003-CT-SPO	On-board controller initiates spurious signal	3	2.27E-05	2.27E-05	1
200-SPMRC-DERIL-PER-MILE	Derailment of a railcar per mile	3	1.18E-05	1.18E-05	1
200-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	3	1.16E-05	1.16E-05	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type <sup>a</sup>	Basic Event Mean Probability <sup>b</sup>	Mean Failure Rate <sup>b</sup>	Mission Time (Hours)
200-SPMRC-HC001--HC--SPO	Spurious command from pendant controller	3	5.23E-07	5.23E-07	1
200-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1	1.74E-03	—	—
200-SPMRC-IEL011-IEL-FOD	Failure of mobile platform anti-coll interlock	1	2.75E-05	—	—
200-SPMRC-MOE000-MOE-FSO	SPMRC lock mode state fails on loss of power	3	1.35E-08	1.35E-08	1
200-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	3	1.28E-04	1.28E-04	1
200-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	3	4.16E-06	4.16E-06	1
200-SPMRC-STU001-STU-FOH	SPMRC end stops fail	3	2.11E-04	4.81E-08	4380
200-ST--BRK001--BRK-FOD	ST fails to stop on loss of power	1	1.46E-06	—	—
200-ST--CBP004-CBP--OPC	ST power cable - open circuit	3	9.13E-08	9.13E-08	1
200-ST--CBP004-CBP--SHC	ST power cable short circuit	3	1.88E-08	1.88E-08	1
200-ST--CT000--CT--FOD	ST primary stop switch fails	1	4.00E-06	—	—
200-ST--CT002--CT--FOH	Direction controller fails	3	6.88E-05	6.88E-05	1
200-ST--HC000--HC--SPO	Spurious commands from remote control	3	5.23E-07	5.23E-07	1
200-ST--HC001--HC--FOD	Remote control transmits wrong signal	1	1.74E-03	—	—
200-ST--HC002--HC--SPO	Spurious command to lift/lower AO	3	5.23E-07	5.23E-07	1
200-ST--MOE000--MOE-FSO	ST lock mode state fails on loss of power	3	1.35E-08	1.35E-08	1
200-ST--MOE021--MOE-FSO	Drive system on primary propulsion fails	3	1.35E-08	1.35E-08	1
200-ST--SC002--SC--FOH	Speed control on ST pendant control fails	3	1.28E-04	1.28E-04	1
200-ST--SC021--SC--FOH	Speed controller on ST pendant fails	3	1.28E-04	1.28E-04	1
200-ST--SC021--SC--SPO	On-board controller initiates spurious signal	3	3.20E-05	3.20E-05	1
200-ST--SEL021--SEL-FOH	Speed selector on ST pendant fails	3	4.16E-06	4.16E-06	1
200-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	3	1.35E-08	1.35E-08	1
200-ST-SC021-SC-SPO	On board controller initiates spurious signals	3	3.20E-05	3.20E-05	1
200-TILTFRAME-CSC-FOH	Cask tilting frame fails	3	4.81E-08	4.81E-08	1
200-VCOO-SFAN001-FAN-FTR	Supply fan #1 for RF fails	3	5.06E-02	7.21E-05	720
200-VCOO-SFAN002-FAN-FTR	Supply fan #2 for CRCF fails	3	5.06E-02	7.21E-05	720
200-VCT0-AHU0001-AHU-FTR	RF ITS elec AHU 00001 fails to run	3	2.73E-03	3.80E-06	720
200-VCT0-AHU0001-CTL-FOD	RF ITS elec AHU 00001 controller fails	1	2.03E-03	—	—
200-VCT0-AHU0002-AHU-FTR	RF ITS elec AHU 00002 fails to run	3	2.73E-03	3.80E-06	720