ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

INTENTIONALLY LEFT BLANK

CONTENTS

Page

CONTENTS (Continued)

Page

FIGURES

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

TABLES

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

Acronyms

AAR	Association of American Railroads
AHU	air handling unit
ASD	adjustable speed drive
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
CTM	canister transfer machine
CTT	cask transfer trolley
DCMIS	digital control and management information system
DPC	dual-purpose canister
EDGF	Emergency Diesel Generator Facility
ESD	event sequence diagram
FRA	Federal Railroad Administration
HAM	horizontal aging module
HCTT	horizontal cask tractor and trailer
HEP	human error probability
HEPA	high-efficiency particulate air
HFE	human failure event
HVAC	heating, ventilation, and air-conditioning
IHF	Initial Handling Facility
ITS	important to safety
LOSP	loss of offsite power
MCC	motor control center
OOS	out of service
PCSA	preclosure safety analysis
PLC	programmable logic controller
RF	Receipt Facility
SPM	site prime mover
SPMRC	site prime mover railcar
TAD	transportation, aging, and disposal

ACRONYMS AND ABBREVIATIONS (Continued)

UPS	uninterruptible power system
WHF	Wet Handling Facility

Abbreviations

AC	alternating current
cfm	cubic foot per minute
DC	direct current
ft/min	foot per minute
hp	horsepower
Hz	Hertz
in.	inch
kV	kilovolt
kW	kilowatt
mph	mile per hour
psi	pound per square inch
rpm	revolution per minute
scfm	standard cubic foot per minute
V	volt

ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

This attachment presents system and pivotal event fault trees that are used in the event trees described in Attachment A. The system fault trees are presented and described in Sections B1 through B8, on a system basis. The pivotal event fault trees are presented in Section B9. For the most part, the pivotal events link to a basic event and these are presented in tables. In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the generic fault tree or basic event level. These supplemental fault trees are presented and described.

B1 SITE PRIME MOVER ANALYSIS – FAULT TREES

B1.1 REFERENCES

Design Input

The preclosure safety analysis (PCSA) is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B1.1.1 *AAR S-2043. 2003. *Performance Specification for Trains Used to Carry High-Level Radioactive Material*. Washington, D.C.: Association of American Railroads. TIC: 257585.

B1.2 SITE PRIME MOVER DESCRIPTION

B1.2.1 Overview

The site prime mover (SPM) is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs both in the Intra-Site Operations and within the Canister Receipt and Closure Facility (CRCF), the Wet Handling Facility (WHF), the Initial Handling Facility (IHF), and the Receipt Facility (RF).

Only the site prime mover railcar (SPMRC) enters the RF. Movement of SPMRC within the RF is limited to the Transportation Cask Vestibule (1021A), Transportation Cask Vestibule Annex (1021), the Cask Preparation Room Annex (1017A), and the Cask Preparation Room (1017).

Transportation casks arriving at the RF can contain:

- Dual-purpose canisters (DPCs)
- Transportation, aging, and disposal (TAD) canisters.

B1.2.2 System Description

B1.2.2.1 Site Prime Mover

The SPM is a commercially available vehicle that has the capability of moving both railcars and truck trailers loaded with transportation casks. 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. Weight sharing between the flanged rail and regular road wheels is automatically varied to achieve the required power transmission needs. More weight can be distributed on the rail wheels when moving, or more on the road wheels when braking, accelerating, and negotiating inclines. The SPM has speed limiters that set the maximum speed of the vehicle to less than 9.0 mph.

During Intra-Site Operation activities, the diesel engine drives the generator, which provides the required 480 V, 3-phase, 60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480 V, 3-phase, 60 Hz power is supplied to the generator. The diesel engine is not used to move the railcar inside the facility.

The SPM is equipped with an automatic wagon coupling system for railcars. In addition, the SPM is equipped with high-performance compressors, a priority filling system, an electronic regulating valve with filling speed adjustments, and a 99 gallon diesel fuel tank.

B1.2.2.2 Railcars

Railcars used for movement of transportation casks are designed in accordance with Federal Railroad Administration (FRA) requirements under authority delegated by the Secretary of Transportation. The FRA administers a safety program that oversees the movement of nuclear shipments throughout the national rail transportation system. Performance standards are addressed in the Association of American Railroads (AAR) Standard S-2043 (Ref. B1.1.1).

B1.2.2.3 Subsystems

The SPM system is composed of four subsystems:

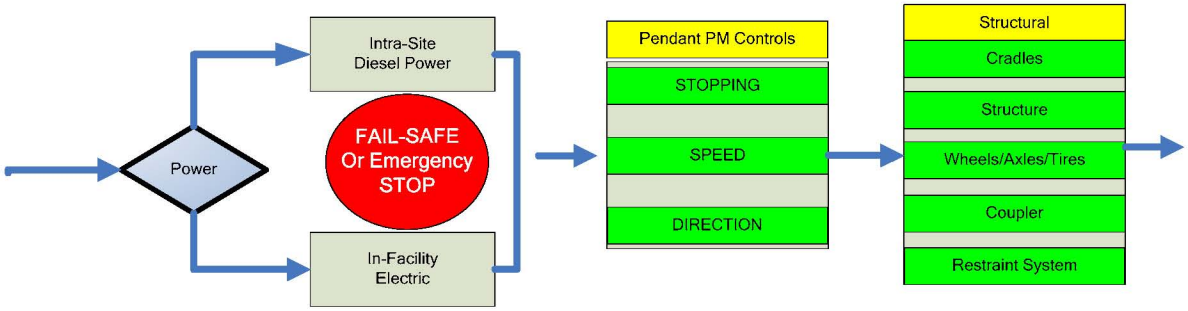
- Power plant–a diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all Intra-Site Operations. For operations conducted inside facilities, the SPM is connected to facility 480 V, 3-phase, 60 Hz power.

- Vehicle controls–during Intra-Site Operations, the operator controls the SPM at the operator's console inside the SPM. For all operations inside of facilities, the operator controls the SPM with either a remote (wireless) controller or through a pendant connected to the vehicle.

- Structural controls–these subsystems include restraints for securing the transportation casks to the railcar/truck trailer; automatic coupler hardware; cradles for supporting the transportation cask; and wheels/tires and axles.

- Brakes–for the railcar, brakes comply with FRA requirements.

A simplified block diagram of the functional components on the SPM is shown in Figure B1.2-1.



Source: Original

Figure B1.2-1. Site Prime Mover Simplified Block Diagram Intra-Site and In-Facility

B1.2.3 Operations

B1.2.3.1 Normal Operations

In-facility SPM operations begin when the SPM has positioned the railcar outside the Transportation Cask Vestibule at the facility such that the railcar is pushed into the facility. The SPM diesel engine is shut down and the outer and inner vestibule doors are opened. Facility 480 V, 3-phase, 60 Hz power is connected to the SPM for all operations inside the facility. The SPM is never operated inside a facility using the diesel engine.

The operator connects the pendant controller or uses a remote (wireless) controller to move the railcar into the Transportation Cask Vestibule and Transportation Cask Vestibule Annex. Once inside, the outer vestibule door is closed. The Cask Preparation Room Annex door is then opened and the SPM moves the railcar into position in the Cask Preparation Room. Once in position, the SPM is disconnected from the railcar and returns to the Transportation Cask Vestibule. The Cask Preparation Room Annex door is then closed. The outer vestibule door can then be opened and the SPM exits the facility. Once outside, the SPM is shut down and the facility power is removed and the inner and outer vestibule doors are closed.

B1.2.3.2 Site Prime Mover Off-Normal Operations

In the event of loss of power, the SPM is designed to stop, retain control of the railcar, and enter a locked mode. Upon the restoration of power the SPM remains in the locked mode until operator action is taken to return to normal operations.

B1.2.3.3 Site Prime Mover Testing and Maintenance

Testing and maintenance of the SPM is done on a periodic basis and does not affect the normal operations of the SPM. Testing and/or maintenance are not performed on a SPM when it is coupled with a railcar. A SPM that has malfunctioned or has a warning light lit on the SPM is deemed unserviceable and turned in for maintenance. Unserviceable vehicles are not used.

If an unserviceable state is identified during movement, the operator puts the SPM into a safe state (as quickly as possible) and recovery actions for the SPM are invoked.

B1.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with system, structures, and components. The five areas considered are addressed in Table B1.3-1 with the following dependencies:

1. Functional dependence
2. Environmental dependence
3. Spatial dependence
4. Human dependence
5. Failures based on external events.

Table B1.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Structural	Material failure Coupler Wheels/tires/axle	—	—	—	—
Brakes	Material failure	—	—	Failure to engage (set)	—
Power plant	Governor fails Safe state on	—	—	Failure to stop	—
Remote control	Spurious commands	—	—	Improper command	Collide end stops

Source: Original

B1.4 SITE PRIME MOVER RELATED FAILURE SCENARIOS

There are two top events for the SPMRC operating inside the RF:

1. SPMRC collides with RF structures
2. SPMRC derailment.

Table B1.4-1 provides a cross reference between the event sequence diagram (ESD) and the SPM fault trees that support them. Potential fire scenarios associated with the SPM are discussed in Section 6.5 and Attachment F.

Table B1.4-1. ESD Cross Reference with SPMRC Fault Trees

RF ESD Number	SPMRC Collision	SPMRC Derailment
ESD01-DPC	X	X
ESD01-TAD	X	X

NOTE: ESD = event sequence diagram, RF = Receipt Facility; SPMRC = site prime mover railcar.

Source: Original

B1.4.1 SPMRC Collides with RF Structures

B1.4.1.1 Description

The two fault trees for SPMRC collision within the RF are identical for each type of transportation cask. Collision can occur as a result of human error or mechanical failures. Mechanical failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

B1.4.1.2 Success Criteria

The success criteria for preventing a collision includes safety design features incorporated in the SPM for mechanical failures and the SPM operator maintaining situational awareness and proper control of the movement of the SPM. To avoid collisions, the SPM must stop when commanded, be prevented from entering a runaway situation, or respond correctly to a SPM movement command.

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

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a speed limiter on the diesel engine for outside facility movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. Simultaneous operation of the railroad wheels and the road tires is prevented by design of the SPM.

B1.4.1.3 Design Requirements and Features

Requirements

Since the dominant contributor to a SPMRC collision in the facility is human error, no priority is given to either the remote or the pendant controllers. The SPM is operated on electrical power when inside the building. The SPM is disconnected from the railcar in the Cask Preparation Room and moved out of the building before cask preparation activities begin.

Design Features

The SPM has two off-equipment control devices that have complete control over the SPMRC. The drive system limits the maximum speed of the SPM to 9.0 mph.

System Configuration and Operating Conditions

Requirements

Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a "deadman switch." On the loss of AC power derived from the facility, the SPM immediately enters the lock mode state. The lock mode state is not reversible without specific operator action.

Design Features and Inputs

Stopping the SPM is accomplished by pushing the "stop" button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source, immediately responds by removing power from the propulsion system on the SPM.

Testing and Maintenance

Requirements

No maintenance or testing is permitted on a SPM loaded with a transportation cask.

Design Feature

None.

B1.4.1.4 Fault Tree Model

The fault tree model for "SPMRC Collision in the RF" accounts for both human error and/or SPMRC mechanical problems that could result in a collision. There is only one movement within the RF. Once the SPMRC has been properly positioned within the Cask Preparation Room, the SPM is decoupled from the railcar and is moved out of the facility.

The top event is a collision of the SPMRC in the RF and is shown in Figure B1.4-3. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system, including failure to stop (Figure B1.4-4) or exceeding a safe speed (Figure B1.4-5). Failure to stop may occur due to mechanical failure of brakes or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

This fault tree model for "SPMRC Collision in the RF" is identical for both DPC and TAD canister movements.

B1.4.1.5 Basic Event Data

Table B1.4-2 contains a list of basic events used in the "SPMRC Collides with RF Structures" fault trees. The mission time has been set at one hour. This is a conservative estimate since it does not require one hour to move the railcar into the facility, disconnect the SPM from the railcar, and move the SPM back outside the facility.

Table B1.4-2. Basic Event Probability for SPMRC Collides with RF Structures

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-OPRCCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000
200-OPRCINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
200-OPRCINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
200-PWR-LOSS	1	4.100E-006	4.100E-006	0.000E+000	0.000E+000
200-SPMRC-BRP000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
200-SPMRC-BRP001-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
200-SPMRC-CBP001-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
200-SPMRC-CBP001-CBP-SHC	3	1.880E-008	0.000E+000	1.880E-008	1.000E+000
200-SPMRC-CPL00-CPL-FOH	3	1.910E-006	0.000E+000	1.910E-006	1.000E+000
200-SPMRC-CT000--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
200-SPMRC-CT0001-CT-FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
200-SPMRC-CT002--CT--FOH	3	6.880E-005	0.000E+000	6.880E-005	1.000E+000
200-SPMRC-CT003-CT-SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
200-SPMRC-G65000-G65-FOH	3	1.160E-005	0.000E+000	1.160E-005	1.000E+000
200-SPMRC-HC001--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
200-SPMRC-HC001-HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
200-SPMRC-IEL011-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
200-SPMRC-MOE000-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
200-SPMRC-SC021--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
200-SPMRC-SEL021-SEL-FOH	3	4.160E-006	0.000E+000	4.160E-006	1.000E+000
200-SPMRC-STU001-STU-FOH	3	2.107E-004	0.000E+000	4.810E-008	4.380E+003

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B1.4.1.5.1 Human Failure Events

Three human errors have been identified for this fault tree. Section 6.4 and Attachment E contain a detailed analysis on the derivation of the failure data.

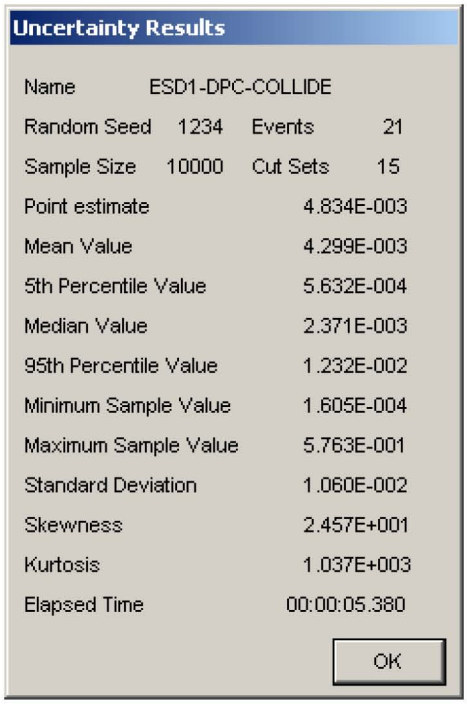
1. Operator causes collision (200-OPRCCOLLIDE1-HFI-NOD)
2. Operator initiates runaway (200-OPRCINTCOL01-HFI-NOD)
3. Operator causes SPMRC collision with mobile platform (200-OPRCINTCOL02-HFI-NOD).

B1.4.1.5.2 Common-Cause Failures

There are no common-cause failures.

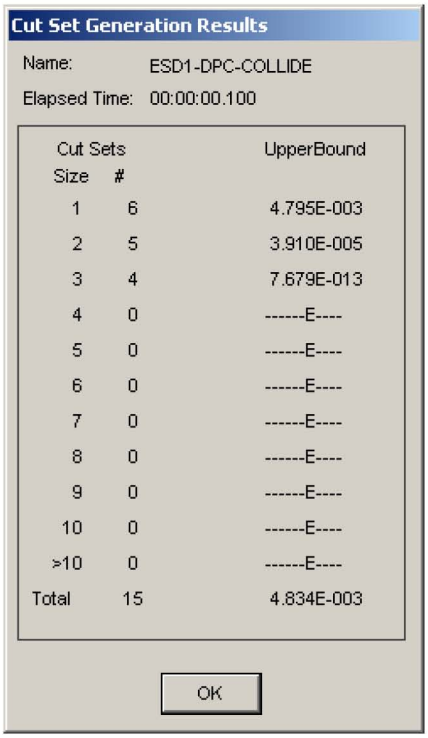
B1.4.1.6 Uncertainty and Cut Set Generation Results

Figure B1.4-1 contains the uncertainty results obtained from running the fault tree for the "SPMRC Collides with RF Structures" fault tree. Figure B1.4-2 provides the cut set generation results for the "SPMRC Collides with RF Structures" fault tree, calculated using a 1E-15 cutoff.



Source: Original

Figure B1.4-1. Uncertainty Results of the SPMRC Collides with RF Structures Fault Tree



Source: Original

Figure B1.4-2. Cut Set Generation Results for the SPMRC Collides with RF Structures Fault Tree

B1.4.1.7 Cut Sets

Table B1.4-3 contains the cut sets for "SPMRC Collides with RF Structures". The probability of failure is 4.834E-3.

Table B1.4-3. Cut Sets for SPMRC Collides with RF Structures

Fault Tree	Cut set %	Prob./Freq.	Basic Event	Description	Probability
ESD1-DPC-COLLIDE	62.07	3.000E-003	200-OPRCCOLLIDE1-HFI-NOD	Operator causes collision	3.0E-003
	36.00	1.740E-003	200-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1.7E-003
	1.04	5.020E-005	200-SPMRC-BRP000-BRP-FOD	Brake (pneumatic) failure on demand brake (pneumatic) failure on demand SPMRC fails to stop on loss of power	5.0E-005
	0.57	2.750E-005	200-OPRCINTCOL02-HFI-NOD	Operator causes collision with mobile platform	1.0E+000
			200-SPMRC-IEL011-IEL-FOD	Failure of mobile platform anti-coll interlock	2.8E-005

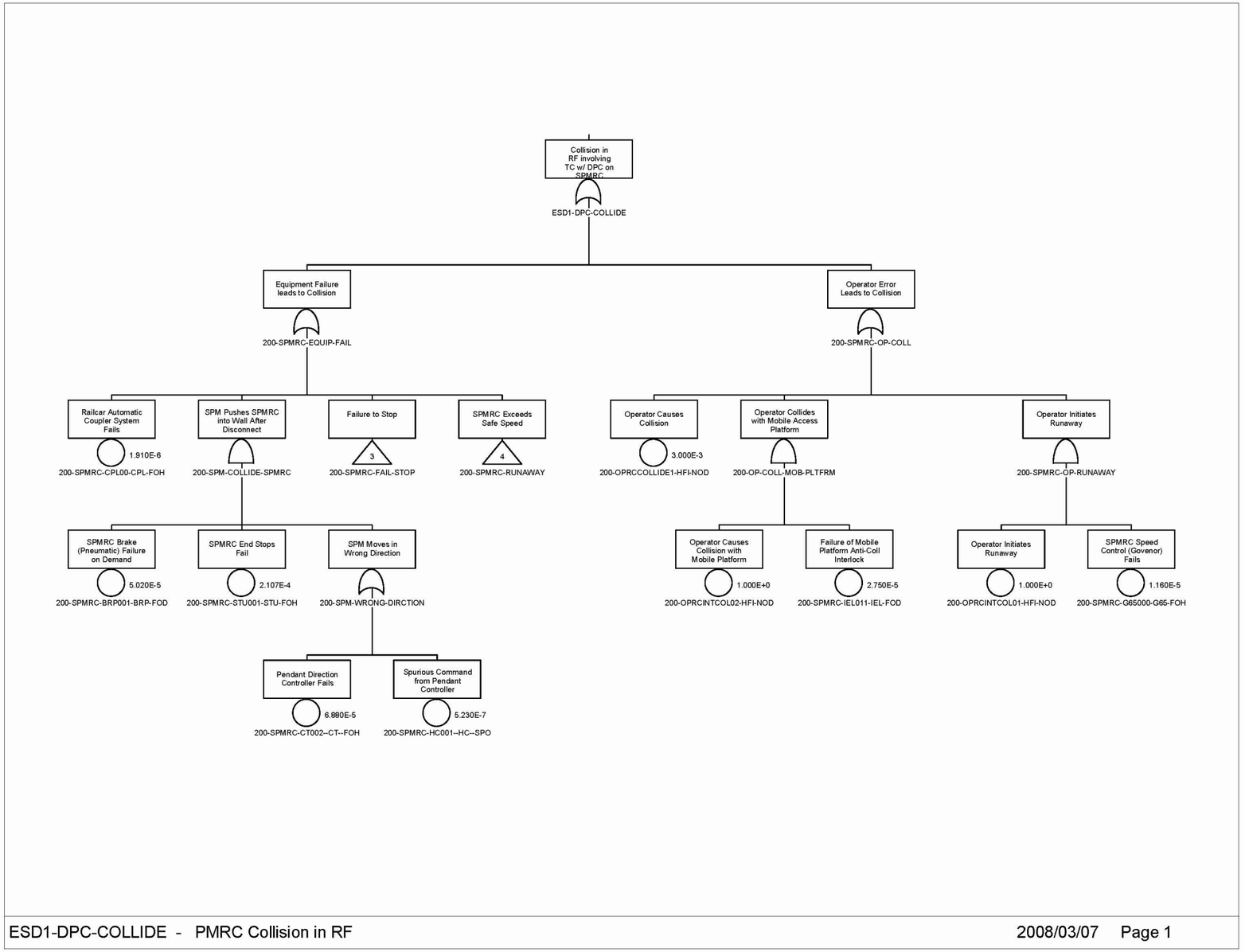
Table B1.4-3. Cut Sets for SPMRC Collides with RF Structures (Continued)

Fault Tree	Cut set %	Prob./Freq.	Basic Event	Description	Probability
ESD1-DPC-COLLIDE (continued)	0.24	1.160E-005	200-OPRCINTCOL01-HFI-NOD	Operator initiates runaway	1.0E+000
			200-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.2E-005
	0.08	4.000E-006	200-SPMRC-CT000--CT--FOD	SPMRC primary stop switch fails	4.0E-006
	0.08	4.000E-006	200-SPMRC-CT0001-CT-FOD	On-board controller fails to respond	4.0E-006
	0.04	1.910E-006	200-SPMRC-CPL00-CPL-FOH	Railcar automatic coupler system fails	1.9E-006
		7.275E-013	200-SPMRC-BRP001-BRP-FOD	SPMRC brake (pneumatic) failure on demand	5.0E-005
	0.00		200-SPMRC-CT002--CT--FOH	Pendant direction controller fails	6.9E-005
			200-SPMRC-STU001-STU-FOH	SPMRC end stops fail	2.1E-004
		5.535E-014	200-PWR-LOSS	Loss of site power	4.1E-006
	0.00		200-SPMRC-MOE000-MOE-FSO	SPMRC lock mode state fails on loss of power	1.4E-008
		3.370E-014	200-SPMRC-CT003-CT-SPO	On-board controller initiates spurious signal	2.3E-005
	0.00		200-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.2E-005
			200-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	1.3E-004
		5.531E-015	200-SPMRC-BRP001-BRP-FOD	SPMRC brake (pneumatic) failure on demand	5.0E-005
	0.00		200-SPMRC-HC001--HC--SPO	Spurious command from pendant controller	5.2E-007
			200-SPMRC-STU001-STU-FOH	SPMRC end stops fail	2.1E-004
	0.00	1.233E-015	200-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	9.1E-008
			200-SPMRC-MOE000-MOE-FSO	SPMRC lock mode state fails on loss of power	1.4E-008
		1.095E-015	200-SPMRC-CT003-CT-SPO	On-board controller initiates spurious signal	2.3E-005
	0.00		200-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.2E-005
			200-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	4.2E-006
	0.00	2.538E-016	200-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	1.9E-008
			200-SPMRC-MOE000-MOE-FSO	SPMRC lock mode state fails on loss of power	1.4E-008
	4.834E-003		= Total		

NOTE: Freq. = frequency; Prob. = probability; SPMRC = site prime mover railcar.

Source: Original

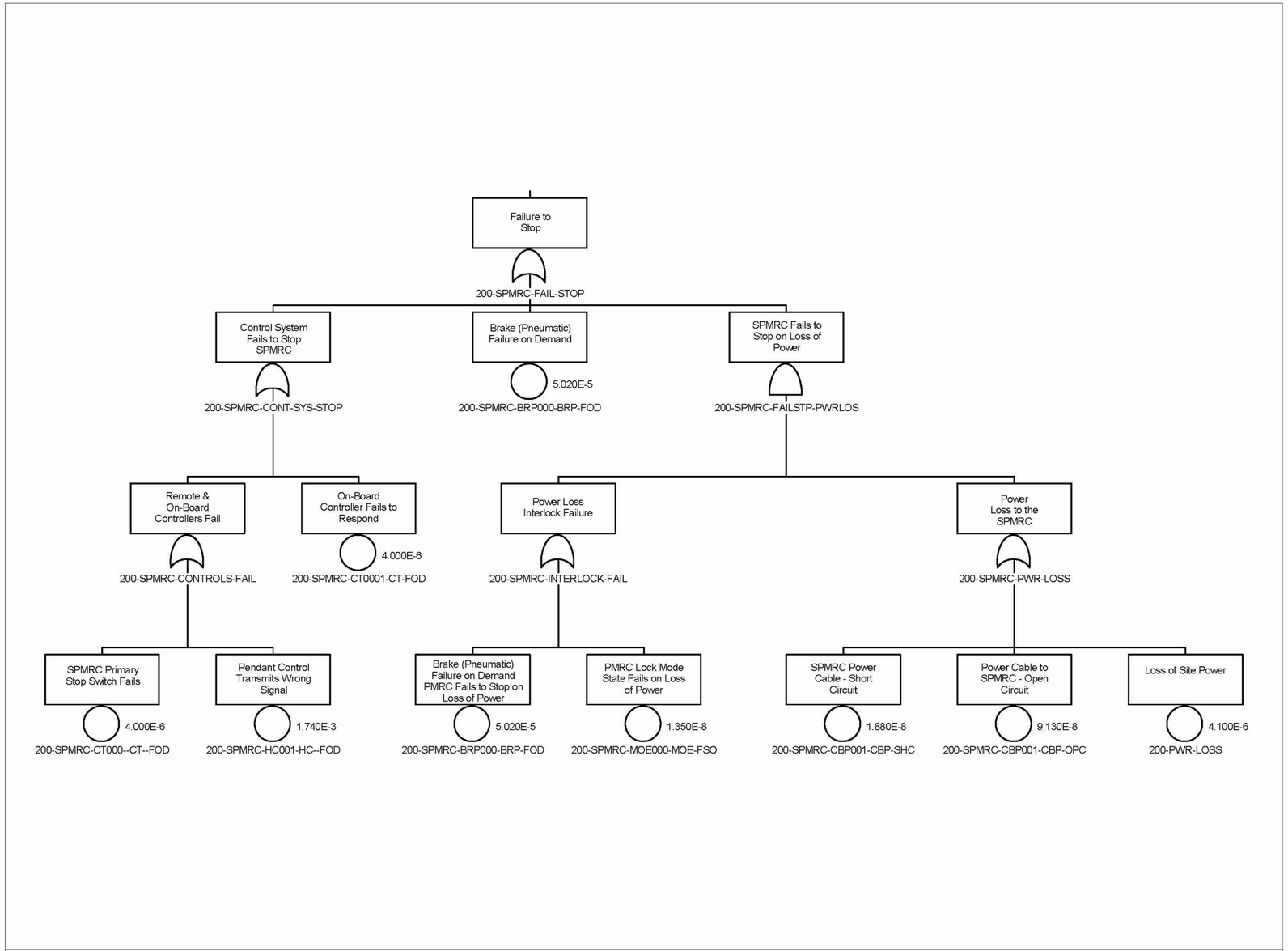
B1.4.1.8 Fault Trees



Source: Original

Figure B1.4-3. SPMRC Collision in RF

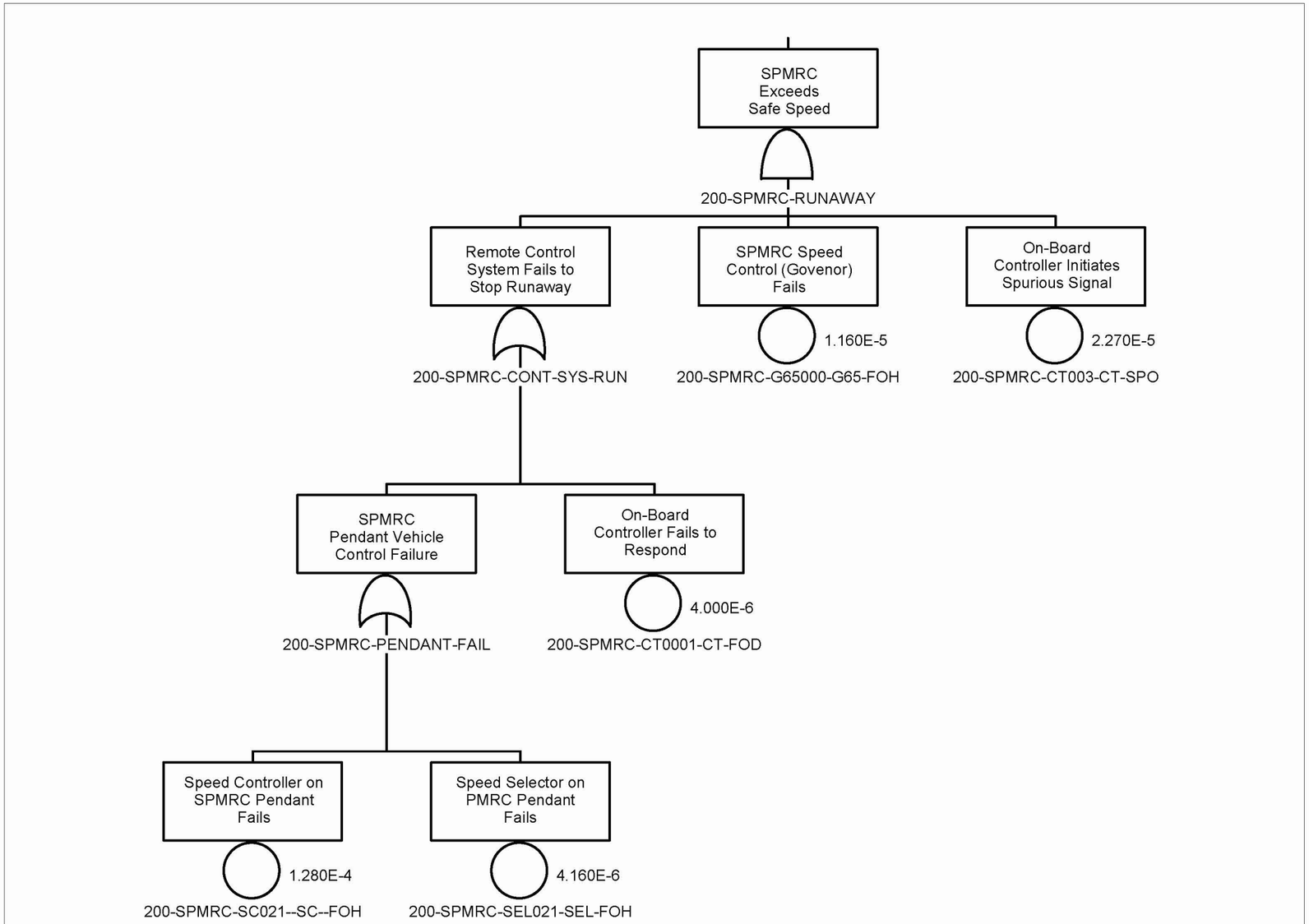
INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-4. SPMRC Fail to Stop

INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-5. SPMRC Exceeds Safe Speed

INTENTIONALLY LEFT BLANK

B1.4.2 SPMRC Derailment

B1.4.2.1 Description

The two fault trees for SPMRC derailment within the RF are identical for each type of transportation cask. Derailment is characterized by a basic event that accounts for the probability of a railcar derailment per mile of travel with in the RF.

This fault tree considers the potential for the SPM to derail during movement of the railcar to the preparation area. The top event is "SPMRC Derails Causing Impact to Transportation Cask." This fault tree is shown in Figure B1.4-8.

The probability of derailment is based on historical data for train derailment at low speeds. The probability of derailment per mile is multiplied by the number of miles the SPM travels from the vestibule to the preparation area (approximately 4E-02 miles). Detailed analysis for this basic event is contained in Attachment C.

B1.4.2.2 Success Criteria

The success criterion for this fault tree is that the SPMRC does not derail during the transport process.

B1.4.2.3 Design Requirements and Features

Requirements

The railcar design requirements comply with AAR Standard S-2043 *Performance Specification for Trains Used to Carry High-Level Radioactive Material* (Ref. B1.1.1).

Design Feature

The design features of the railcar are in compliance with AAR Standard S-2043 (Ref. B1.1.1).

Testing and Maintenance

Requirements

No maintenance or testing is permitted on a railcar loaded with a transportation cask.

Design Feature

None.

B1.4.2.4 Fault Tree Model

The fault tree model for "SPMRC Derailment Causing a Transportation Cask Impact" consists of the probability for a railcar derailment per mile of travel times the number of occurrences for each type of transportation cask.

B1.4.2.5 Basic Event Data

Table B1.4-4 contains a list of basic events used in the "SPMRC Derailment" fault trees.

Table B1.4-4. Basic Event Probability for SPMRC Derailment

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-SPMRC- DERIL-PER-MILE	3	1.180E-005	0.000E+000	1.180E-005	1.000E+000
200-SPMRC-MILES-IN- RF	V	4.000E-002	4.000E-002	0.000E+000	0.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B1.4.2.5.1 Human Failure Events

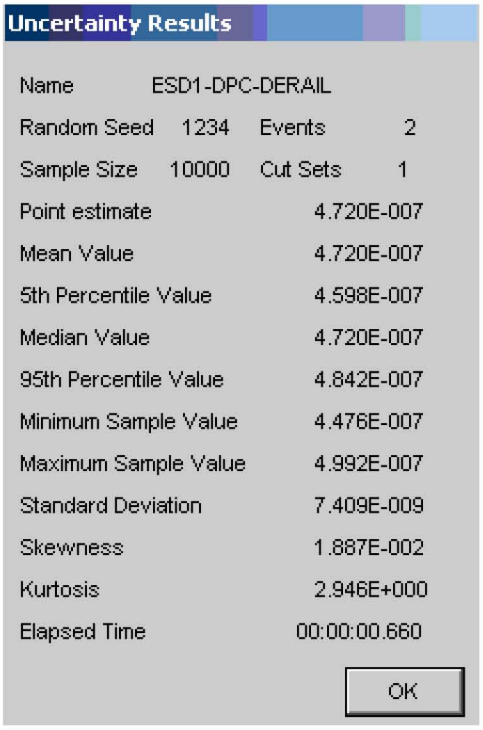
There are no human errors identified for this fault tree.

B1.4.2.5.2 Common-Cause Failures

There are no common-cause failures (CCFs) identified for this fault tree.

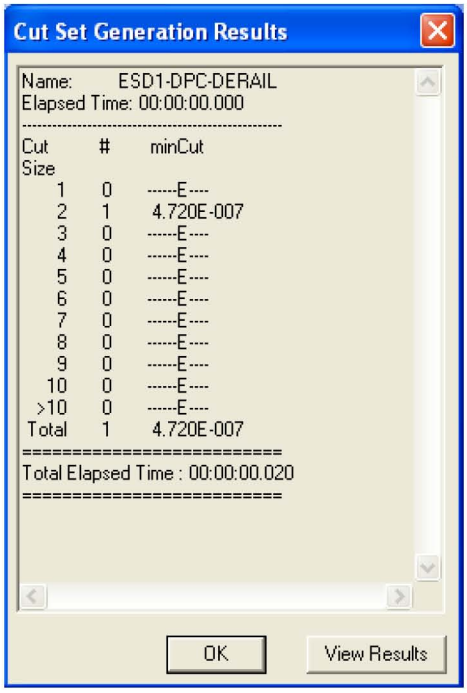
B1.4.2.6 Uncertainty and Cut Set Generation Results

Figure B1.4-6 contains the uncertainty results obtained from running the fault tree for "SPMRC derailment". Figure B1.4-7 provides the cut set generation results for the "SPMRC derailment" fault tree, calculated using a 1E-15 cutoff.



Source: Original

Figure B1.4-6. Uncertainty Results of the SPMRC Derailment Fault Tree



Source: Original

Figure B1.4-7. Cut Set Generation Results for the SPMRC Derailment Fault Tree

B1.4.2.7 Cut Sets

Table B1.4-5 contains the cut sets for the "SPMRC Derailment" fault tree. The probability of derailment per cask is 4.720E-007.

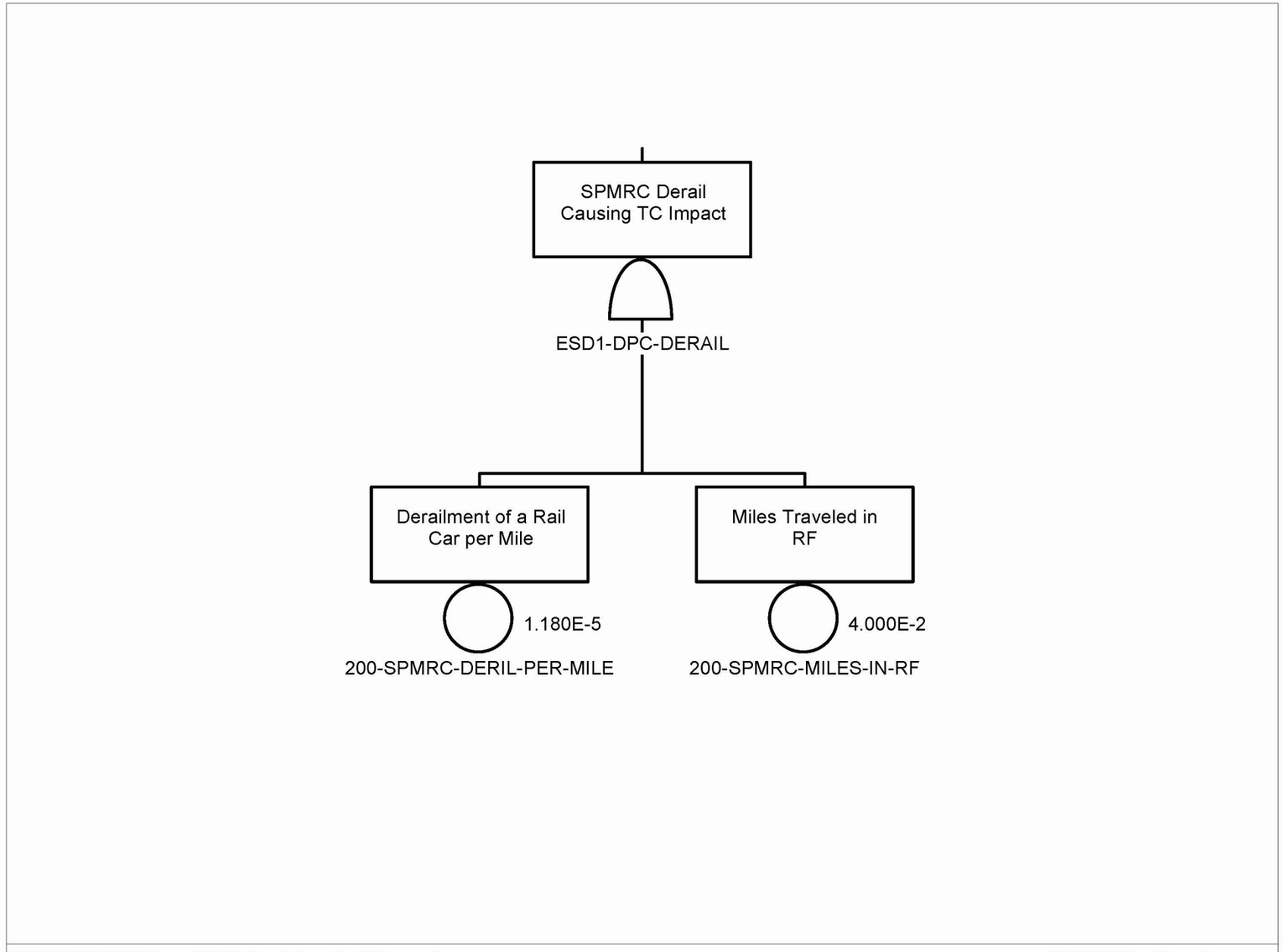
Table B1.4-5. Cut Sets for SPMRC Derailment

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD1-DPC-DERAIL	100.00	4.720E-007	200-SPMRC-DERIL-PER-MILE	Derailment of a railcar per mile	1.2E-005
			200-SPMRC-MILES-IN-RF	Miles traveled in RF	4.0E-002
		4.720E-007	= Total		

NOTE: Freq. = frequency; Prob. = probability; RF = Receipt Facility.

Source: Original

B1.4.2.8 Fault Trees



Source: Original

Figure B1.4-8. SPMRC Derailment in RF

INTENTIONALLY LEFT BLANK

B2 CASK TRANSFER TROLLEY – FAULT TREES ANALYSIS

B2.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of this document. There are no superseded or cancelled documents associated with the modifications that led to the issuance of this revision. Cancelled or superseded documents associated with the portions of this document for which the snapshot has not yet been updated are designated herein with a dagger (†).

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B2.1.1 †BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report for Cask Transfer Trolley*. 000-30R-HM00-00200-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071219.0001.

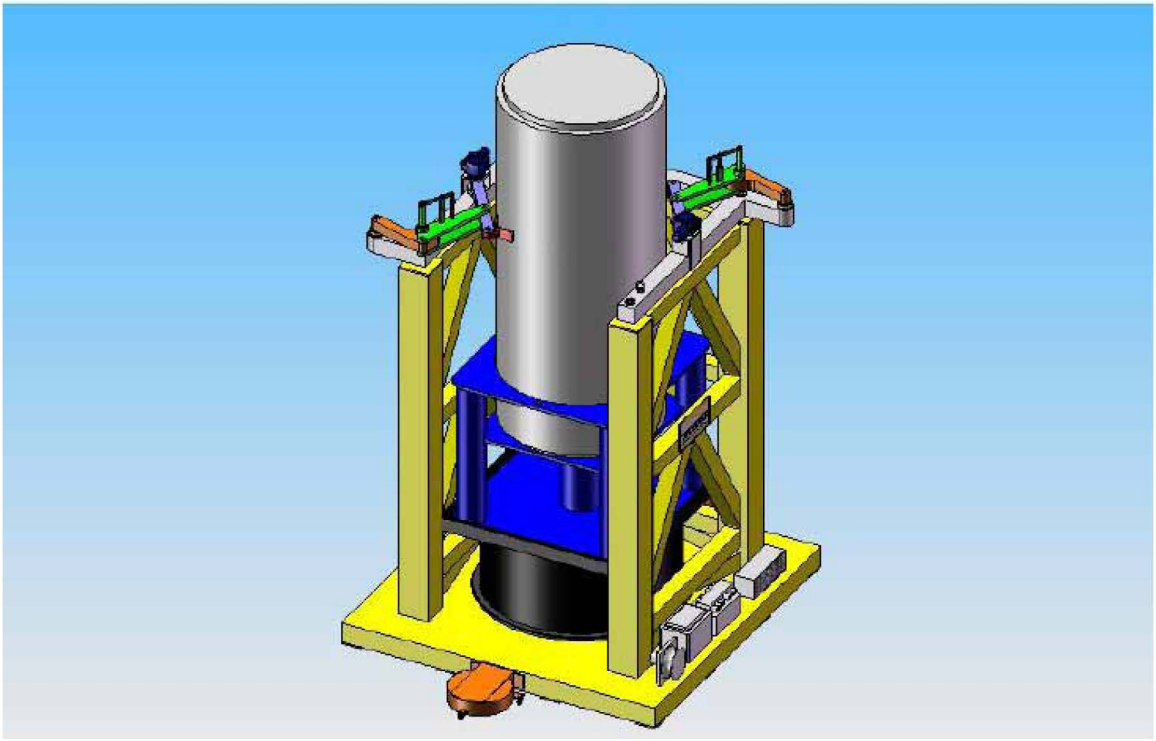
B2.1.2 *BSC 2007. *Preliminary Throughput Study for the Receipt Facility*. 200-30R-RF00-00300-000-002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071227.0021.

B2.1.3 *Morris Material Handling 2007. *P&ID – Cask Transfer Trolley*. V0-CY05-QHC4-00459-00029-001 Rev. 005. Oak Creek, Wisconsin: Morris Material Handling. ACC: ENG.20071019.0003.

B2.2 CASK TRANSFER TROLLEY DESCRIPTION

B2.2.1 Physical Description

The cask transfer trolley (CTT) is an air powered machine that is used to transport vertically oriented transportation casks from the Cask Preparation Room to the Cask Unloading Room. The trolley consists of a platform, a cask support assembly, a pedestal assembly, a seismic restraint system, and an air system as illustrated in Figure B2.2-1.



Source: Modified from Ref. B2.1.1

Figure B2.2-1. Cask Transfer Trolley

The platform, or main deck, is the main support structure for the trolley. The structure is designed to hold the air bearings under the deck and simultaneously support the cask support assembly and cask. The cask support assembly is the truss work that is welded to the platform and cradles three sides of the cask. The cask support assembly provides the structural support for the seismic restraint system and pedestal assembly to hold the cask during an earthquake or collision event.

The CTT must handle a number of different types of casks; consequently, different pedestals are used to position the top of the cask at the appropriate height above the floor. Each pedestal sub-component is designed for its respective cask to sit down in a "cavity." The depth of the cavity is a minimum of 6 in. which is sufficient to prevent the cask from exiting from the pedestal due to uplift during the worst case seismic event. 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 in the correct position in the trolley. The trolley is positioned within a set tolerance under the cask transfer port in the transfer area using bumpers and stops that are bolted to the floor with bolts that shear to allow the CTT to slide during a significant seismic event.

In addition to the cask being restrained at the bottom by the pedestal assembly, the upper section of the cask is restrained to prevent side motions during a seismic event. The system is made up of two linkage systems that are mounted on opposite corners of the cask support assembly. An

electric motor extends and retracts the restraint brackets to predetermined positions. Different cask diameters are handled by bolting unique interface clamps onto the seismic restraints.

When the restraint system is properly positioned next to the cask, a locking pin is air-actuated to secure the system. This solid high-strength alloy locking pin can withstand the shear stresses that would be experienced during a seismic event. Both locking pins are monitored by proximity switches (or limit switches) that are hard-wired to the control system to verify the pins are in place. If the locking pins are not secured properly, the CTT is not able to power up and move/levitate.

The facility compressed air supply inflates nine 54-in. diameter air casters beneath the trolley platform. Each air caster consists of a urethane torus-shaped bag with a chamber inside the torus. The air film is produced when air is distributed to each air caster causing the air bags to inflate. The inflated bags create a seal against the floor surface and confine the air within the chambers of the bags until the air pressure is sufficient to offset the weight of the loaded trolley. The air bearings allow the CTT to rise above the steel floor approximately 1/2 in. to 7/8 in. The air bearings are supplied with facility air (between 75-100 psi optimal) and consume from 500 to 700 scfm. A hose reel for the 1-1/2-in. diameter air hose is mounted on the platform. The reel is equipped with an air-powered return, a ball valve shut-off, quick-disconnect fittings, and a safety air fuse.

A main "off/on" control valve and separate flow control/monitoring valve for each air bearing allows adjustment and verification of pressure/flow for each individual bearing. There are two interlocks for the air; one pressure monitor verifies the main incoming pressure is not too high, and a second set of monitors verifies that all bearings have sufficient air pressure. This air monitoring system for the air bearings is not important to safety and therefore has not been analyzed.

End mounted turtle-style drive units that are 360-degree 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. Air is supplied from facility air to a high-speed pneumatic motor in combination with a reducer to limit the wheel speed of the turtle drives. The maximum speed of the system is less than or equal to 10 ft/min at the maximum air pressure available from the facility compressed air supply.

The CTT speed is controlled in two ways. First, the electrical control system is designed to provide a control signal to the air valve that produces a speed range of 0-10 ft/min. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, restricts the air flow to prevent a "run-away" condition.

B2.2.2 Control System

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

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

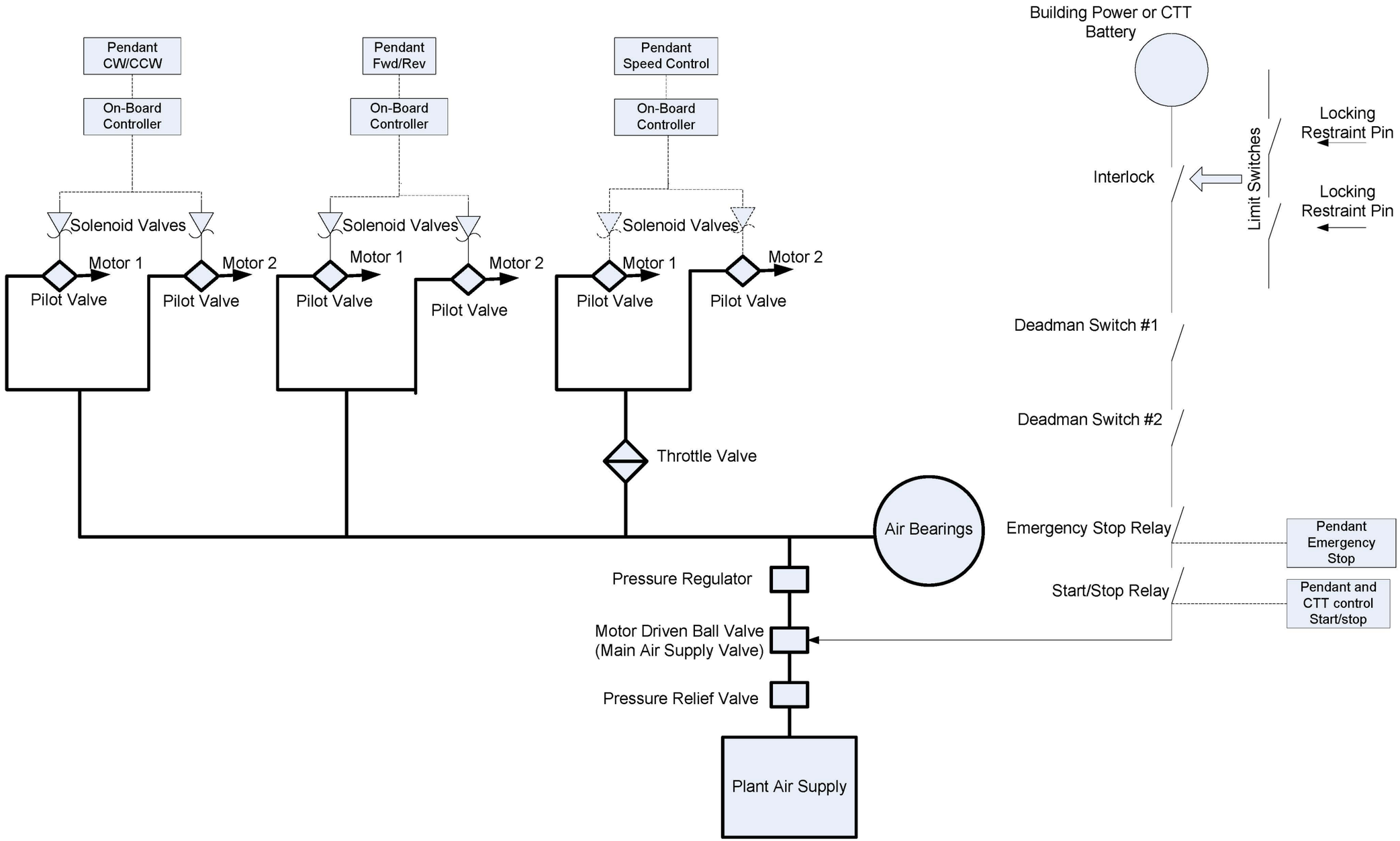
- Deadman handle–The operator presses both handles to allow air to flow to the CTT to levitate and move it horizontally.
- Emergency-stop button–The operator presses the emergency stop button on the pendant control or on the CTT to stop the CTT.
- Clockwise/counterclockwise momentary switch– The operator turns this switch to turn the drive units for horizontal movement. This rotational characteristic is used to move the CTT to the storage or maintenance location after it leaves the Cask Preparation Room.
- Forward/reverse switch–The operator uses the forward/reverse switch to determine the direction of the drive units.
- Variable speed control switch–The operator uses the variable speed control switch to adjust the CTT drive speed.
- Cask restraint– The operator uses the selector switch to actuate 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 move the CTT since it only travels in one direction when it is carrying a cask. The CTT moves forward and reverse between the Cask Preparation Room and the Cask Unloading Room and is restrained from side to side by removable barriers that are mounted to the building floor.

A schematic of the control system is shown in Figure B2.2-2.

The main air supply valve is a solenoid operated pilot 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 restraint pins actuate the limit switches and the pendant deadman switches are actuated.

The controls on the pendant are clockwise/counterclockwise, forward/reverse, and drive speed to control the valves for the motor drives. These valves are also fail safe solenoid operated pilot valves.



Source: Modified from Ref. B2.1.3

Figure B2.2-2. Schematic of the CTT Control System

INTENTIONALLY LEFT BLANK

Releasing the deadman switches or pressing the emergency-stop or start/stop buttons on the pendant control or the emergency-stop button on the CTT opens a relay to interrupt power to the main air supply valve, causing it to close. Upon closing the main supply valve the air pressure levitating the CTT and driving the motors is reduced and the CTT lowers to the floor.

B2.2.3 Operation

B2.2.3.1 Initial Conditions

The CTT is initially located in the Cask Preparation Room with the battery fully charged, the seismic restraints retracted, and with no air 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 by extending the electric motor driven actuators. When the restraints are in place, the locking pins are pneumatically inserted. With the cask secured to the trolley, the overhead crane is disengaged from the cask.

When the locking pins are inserted properly (thus locking the seismic restraints in place), a pair of proximity switches (limit switches) de-activates the interlock and the main air supply valve can be opened to allow the air bearings and drive motors can be operated. Once all preparations of the cask are complete, the trolley can be moved to the Cask Unloading Room using the pendant controls.

B2.2.3.2 Cask Movement

When all steps are properly completed, air is introduced to the CTT. The operator actuates the air bearings, levitating the CTT with the load. The system continuously and automatically checks the flow and pressure to each air bearing; if a problem is detected, the air supply to all bearings is stopped and the system lowers to the ground.

Once the trolley is raised, the operator drives the CTT into the Cask Unloading Room. By moving forward and reverse, the CTT is driven through the door way. Guides bolted to the floor ensures the CTT can only move forward and back, and in addition, will ensure the CTT is properly positioned directly below the transfer port. Once in position, the air flow to the bearings is stopped and the CTT lowers to the ground and rests in position. The operator disconnects the quick-disconnect air hose and rewinds the hose onto the trolley. The shield doors that separate the Cask Preparation Room from the Cask Unloading Room are then closed.

B2.2.3.3 System/Pivotal Event Success Criteria

Success criteria for loading a cask onto the CTT in the Cask Preparation Room, and unloading the canisters from the cask in the Cask Unloading Room require the CTT remain stationary during these operations with no spurious movement. Success criteria for moving the CTT with a

cask from the Cask Preparation Room to the Cask Unloading Room requires the CTT to travel at an allowable speed, and the operator is able to control the CTT movement.

During cask loading at the Cask Preparation Room, compressed air must be available to the CTT to remotely insert the locking pins into the restraint system. Both pin interlocks must function before the main air supply valve can be opened thereby preventing movement of the CTT until the cask has been loaded and restrained. Once the locking pins are in place the crane is removed from the cask. During the time the crane is being removed from the cask, the air supply valve is closed and the valves that control the air to the air bags and motors are closed. Movement is not initiated until both deadman switches on the remote pendant control are pressed to allow air to the air bags to levitate the CTT.

Upon the CTT reaching the Cask Unloading Room, procedures require that the air supply hose to be disconnected and removed from the CTT to prevent any movement while unloading the canisters from the cask. This is accomplished by locating the air supply outside the Cask Unloading Room. An interlock prevents the transfer port slide gate from opening until the shield door to the Cask Unloading Room is closed. Thus, because the air supply is external to the Cask Unloading Room, the air hose must be removed from the CTT before the shield door can be closed, and the shield door must be closed before the port slide gate can be opened, allowing canister transfer from the cask. Therefore, the location of the air supply and the shield door interlock requires removal of the air supply from the CTT before canister transfer can begin.

When moving the cask between the Cask Preparation Room and the Cask Unloading Room, movement in the wrong direction is prevented by the guide rails bolted to the floor along the path of the CTT. This forces the CTT to move only in a straight line forward and back between the two areas. Runaway of the CTT is prevented by the throttle valve which is set at the factory such that the maximum speed is 10 ft/min at the maximum facility air pressure.

The CTT is stopped to prevent a collision into a closed shield door or the end stops in the Cask Unloading Room by the operator speed controls on the pendant, by the deadman switches on the pendant, or by the emergency stop buttons on the pendant and on the CTT. The speed controls slow down and stop the CTT by controlling the air flow through the drive speed valve, and the deadman switches and emergency stop buttons remove power to the main air supply valve causing it to close. Because the emergency stop function is a recovery action performed by the operator and requires operator intervention, these functions were not modeled in the analysis.

On loss of electrical power from the battery, the air valves all fail closed, and no air will pass through to the air bearings or drive units and the CTT settles to the floor. If the air pressure and flow is lost, the unit can not levitate or move horizontally and the CTT lowers to the floor and no other action occurs. A separate sustained signal is needed to actuate the air valves to raise the load (positive operator action). Thus, although a spurious signal may cause air to flow momentarily, additional operator controls are needed to cause the unit to levitate or move horizontally.

B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B2.3-1 with the following dependencies:

1. Functional dependence
2. Environmental dependence
3. Spatial dependence
4. Human dependence
5. Failures based on external events.

Table B2.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Air supply	Provides levitation and motive force	—	—	Fail to disconnect air hose	—
Locking pin limit switches	Prevents spurious movement	—	—	—	—
Guide rails	Prevents movement in wrong direction	—	—	—	Shear during seismic event allows CTT to slide
Pendant control	Controls direction and speed and initiates movement	—	—	Wrong instructions	—
Deadman switch	Allows operation	—	—	Fail to release	—
Emergency stop	Stops CTT	—	—	Fail to energize	—
Throttle valve	Limits maximum speed	—	—	—	—
Structure	Constrains and supports cask	—	—	—	Seismic causes impact
Shield door	Opens for CTT to pass through	—	—	Close door inadvertently	Closes on CTT

NOTE: CTT = cask transfer trolley

Source: Original

B2.4 CTT-RELATED FAILURE SCENARIOS

There are four fault trees associated with the CTT:

1. Spurious movement of the CTT in the Cask Preparation Room during cask loading.
2. Spurious movement of the CTT in the Cask Preparation Room during cask preparation.
3. Collision of the CTT during cask transfer.
4. Spurious movement of the CTT in the Cask Unloading Room.

An additional fault tree involving the CTT is closing of the shield door on the CTT as the CTT moves a cask from the Cask Preparation Room to the Cask Unloading Room. This fault tree is described in a separate section involving inadvertent shield door closure that satisfies ESD-06, pivotal event "Collision with Cask Unloading Room Shield Door."

In all cases a conservative mission time of one hour per cask transfer was used for each fault tree. The time required to move a cask to the trolley and disconnect the crane is approximately 55 minutes, while the time required moving the trolley from the Cask Preparation Room to the Cask Unloading Room is approximately 15 minutes. The time required to extract the canister from the cask is approximately 20 minutes (Ref. B2.1.2). Therefore, a one-hour mission time is considered a conservative value.

B2.4.1 Spurious Movement of the CTT in the Cask Preparation Room during Cask Loading

B2.4.1.1 Description

This fault tree describes spurious movement of the CTT during cask loading to satisfy ESD-02, pivotal event "Unplanned Conveyance Movement Causes Drop." The top event is "Spurious Movement of the CTT during Cask Loading" which is defined as unplanned movement of the CTT while the cask is being loaded onto the CTT. This fault tree is shown in Figures B2.4-3 and B2.4-4.

Spurious movement can be caused by equipment failures or by a combination of equipment failure and operator error. For equipment failures to cause spurious movement the main air supply valve must open to supply air to the air bags to levitate the CTT. This can occur if the main air supply valve fails open or the locking pin limit switches and control system fail causing the valve to open. For the operator to initiate spurious movement, the locking pin limit switches must fail allowing the operator to open the main air supply valve.

B2.4.1.2 Success Criteria

The success criterion is that the CTT remains motionless during loading of the transportation cask. Movement of the CTT during this operation could cause impact and damage to the transportation cask.

B2.4.1.3 Design Requirements and Features

Requirements

There are no additional design requirements.

Features

The design feature is the two locking restraint pins that prevent power to the main air supply valve until the pins are in place and the limit switches are activated to allow power to the air supply valve.