

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

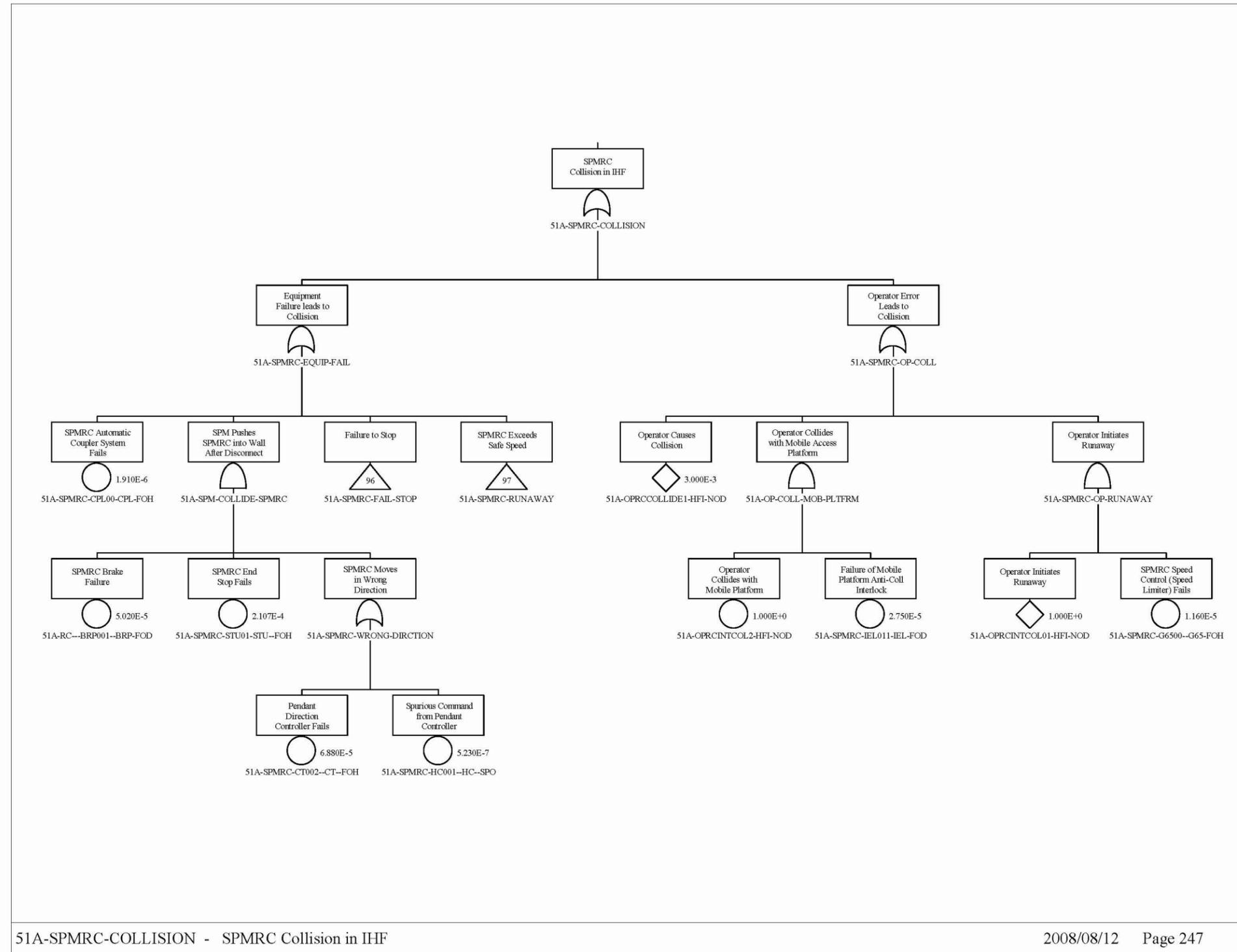
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMRC-COLLISION	62.07	3.000E-003	51A-OPRCCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	51A-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	51A-SPMRC-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand Brake (Pneumatic) Failure on Demand PMRC Fails to Stop on Loss of Power	5.0E-005
	0.57	2.750E-005	51A-OPRCINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000
			51A-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.8E-005
	0.24	1.160E-005	51A-OPRCINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			51A-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	51A-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	51A-SPMRC-CT001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	51A-SPMRC-CPL00-CPL-FOH	Railcar Automatic Coupler System Fails	1.9E-006
		4.834E-003 = Total			
		4.83E-03 = Total			

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

Source: Original

B1.4.1.8 Fault Trees

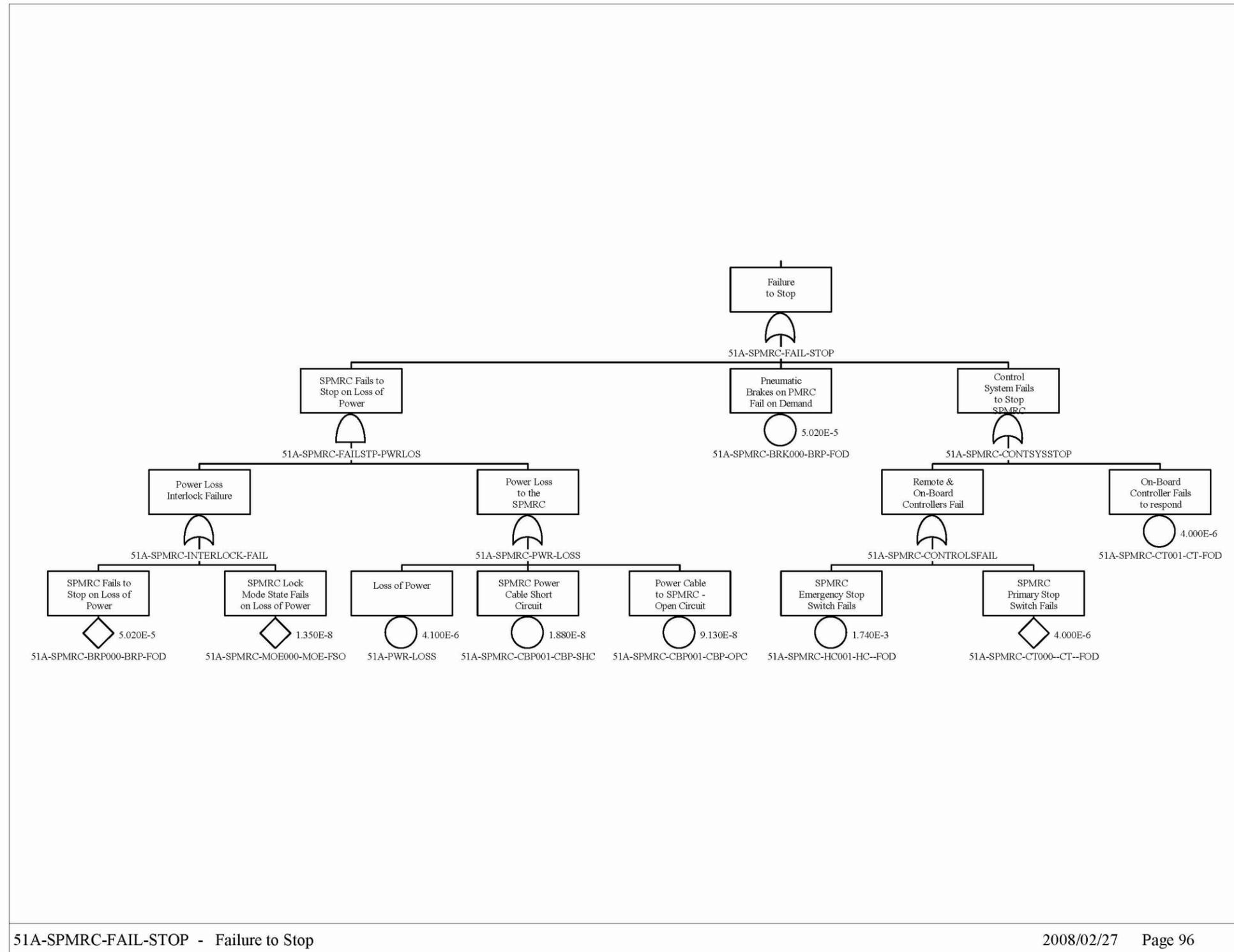
INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-3. SPMRC Collides with IHF Structures

INTENTIONALLY LEFT BLANK



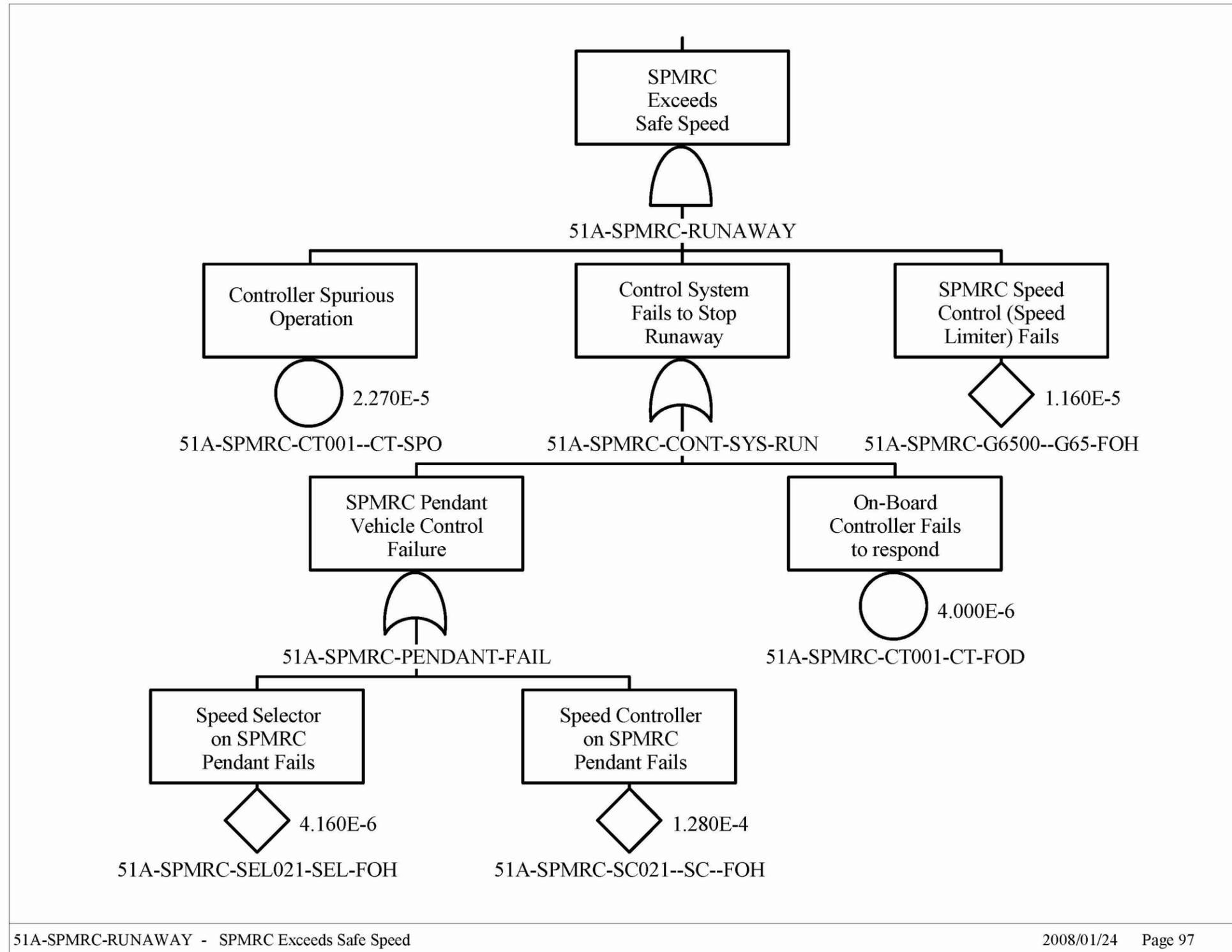
51A-SPMRC-FAIL-STOP - Failure to Stop

2008/02/27 Page 96

Source: Original

Figure B1.4-4. SPMRC Fails to Stop

INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-5. SPMRC Exceeds Safe Speed

INTENTIONALLY LEFT BLANK

B1.4.2 SPMTT Collides with IHF Structures

B1.4.2.1 Description

The two fault trees for SPMTT collision within the IHF are identical with the exception of the number of transportation casks that are processed at the IHF for each configuration. 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 with commanded, the SPM exceeding a safe speed or the SPM moving in a wrong direction.

B1.4.2.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the SPM for mechanical failures and the SPM operator maintains 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 performs a controlled stop. Once stopped, the SPM stops all movement and enters into “lock mode” safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM. The SPM remains in this fail safe mode until power is returned and restarted by the operator.

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 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 miles per hour. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

B1.4.2.3 Requirements and Design Features

Requirements

Since the dominant contributor to SPMTT 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 truck trailer at the preparation area 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 SPMTT. The drive system contains both a speed limiter and a transmission constraint which limits the maximum speed of the SPM to 9.0 miles per hour.

Common-Cause Failures

There are no CCFs identified for this fault tree.

B1.4.2.4 System Configuration and Operating Conditions

Requirements

Two means of stopping the SPM is 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.

Testing and Maintenance

Requirements

There is no maintenance or testing permitted on a SPMTT loaded with a transportation cask.

Design Feature

None.

B1.4.2.5 Fault Tree Model

The fault tree model for “SPMTT Collides with IHF Structures” accounts for both human error and for SPMTT hardware problems that could result in collision. There is only one movement within the IHF. Once the SPMTT has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the truck trailer and it is moved out of the facility.

The fault trees for SPMRC and SPMTT are identical and a split fraction is used to account for the number/type of transportation casks that arrive at the IHF on either the railcar or truck trailer.

The top event is a collision of the SPMTT in the IHF and is shown in Figure B1.4-8. 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 (Figure B1.4-9) including failure to stop (Figure B1.4-10) or exceeding a safe speed (Figure B1.4-11). 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.

B1.4.2.6 Basic Event Data

Table B1.4-4 contains a list of basic events used in the “SPMTT Collides with IHF Structures” fault trees. The mission time has been set at one hour which is conservative because it does not require more than one hour to disconnect the SPM from the rail car and remove it from the facility.

Table B1.4-4. Basic Event Probabilities for SPMTT Collides with IHF Structures

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹)	Miss. Time (hr) ^a
51A-OPTTCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	—	—
51A-OPTTINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	—	—
51A-OPTTINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	—	—
51A-PWR-LOSS	1	4.100E-006	4.100E-006	—	—
51A-SPMTT-BRK000-BRP-FOD	1	5.020E-005	5.020E-005	—	—
51A-SPMTT-BRP001-BRP-FOD	1	5.020E-005	5.020E-005	—	—
51A-SPMTT-CBP002-CBP-OPC	3	9.130E-008	—	9.130E-008	1
51A-SPMTT-CBP003-CBP-SHC	3	1.880E-008	—	1.880E-008	1
51A-SPMTT-CPL00-CPL-FOH	3	1.910E-006	—	1.910E-006	1
51A-SPMTT-CT000--CT--FOD	1	4.000E-006	4.000E-006	—	—
51A-SPMTT-CT001--CT--FOD	1	4.000E-006	4.000E-006	—	—
51A-SPMTT-CT002--CT--FOH	3	6.880E-005	—	6.880E-005	1
51A-SPMTT-G65000-G65-FOH	3	1.160E-005	—	1.160E-005	1
51A-SPMTT-HC001-HC-FOD	1	1.740E-003	1.740E-003	—	—
51A-SPMTT-HC002--HC--SPO	3	5.230E-007	—	5.230E-007	1
51A-SPMTT-IEL102-IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-SPMTT-MOE000-MOE-FSO	3	1.350E-008	—	1.350E-008	1
51A-SPMTT-SC001--CT--SPO	1	2.270E-005	2.270E-005	—	—
51A-SPMTT-SC021--SC--FOH	3	1.280E-004	—	1.280E-004	1
51A-SPMTT-SEL021-SEL-FOH	3	2.840E-006	—	2.840E-006	1
51A-SPMTT-STU001-STU-FOH	3	2.107E-004	—	4.810E-008	4380

NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B1.4.2.6.1 Human Failure Events

Three human errors have been identified for this fault tree. Both “operator initiates a runaway” and “operator causes a collision with mobile platform” are assigned a screening failure probability of 1.00E+00. A detailed analysis of “operator causes collision” is addressed in Section 6.4 and Attachment E.

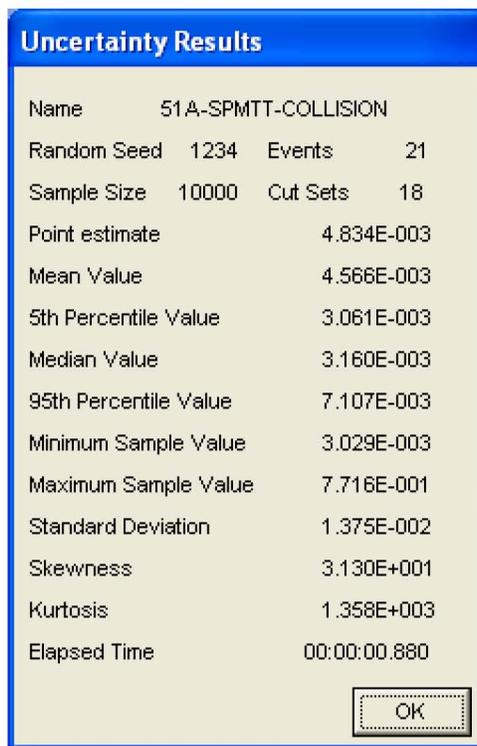
1. Operator causes collision (51A-OPTTCOLLIDE1-HFI-NOD).
2. Operator initiates runaway (51A-OPTTINTCOL01-HFI-NOD).
3. Operator causes a collision with mobile platform (51A-OPTTINTCOL02-HFI-NOD).

B1.4.2.6.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

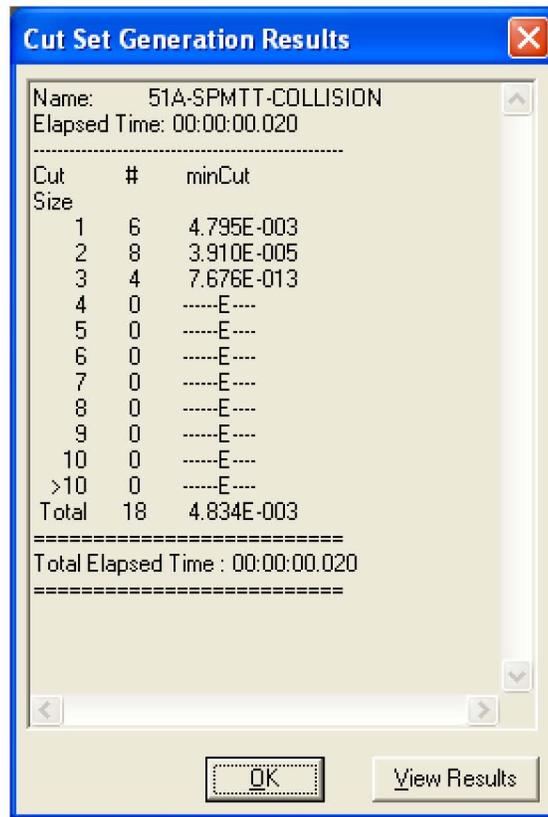
B1.4.2.7 Uncertainty and Cut Set Generation Results

Figure B1.4-6 contains the uncertainty results obtained from running the fault tree for “SPMTT Collides with IHF Structures.” Figure B1.4-7 provides the cut set generation results for the “SPMTT Collides with IHF Structures” fault tree.



Source: Original

Figure B1.4-6. Uncertainty Results of the SPMTT Collides with IHF Structures Fault Tree



Source: Original

Figure B1.4-7. Cut Set Generation Results for the SPMTT Collides with IHF Structures Fault Tree

B1.4.2.8 Cut Sets

Table B1.4-5 contains the cut sets for “SPMTT Collides with IHF Structures”. The probability of failure is 4.83E-03

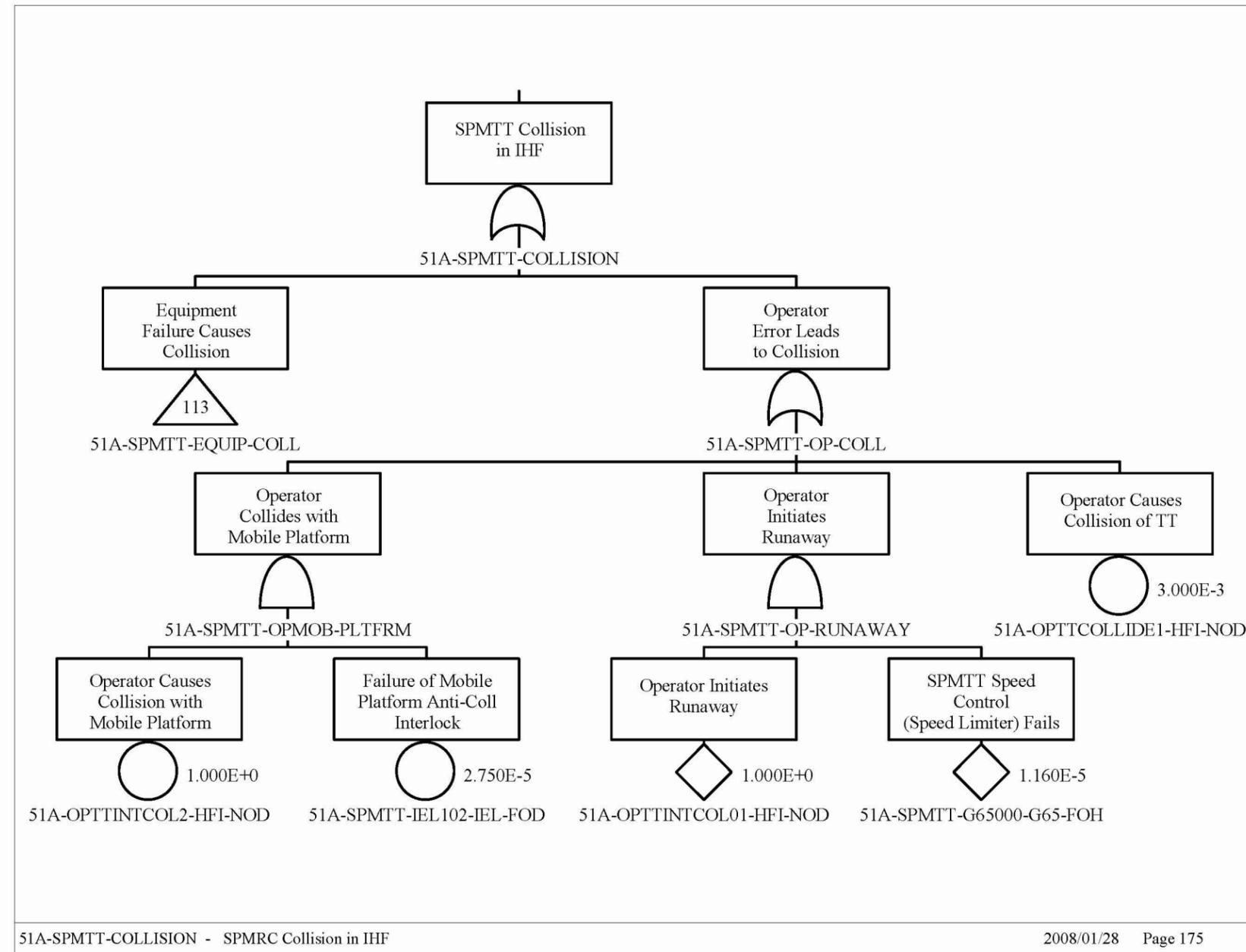
Table B1.4-5. Cut Sets for SPMTT Collides with IHF Structures

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMTT-COLLISION	62.07	3.000E-003	51A-OPRCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	51A-SPMTT-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	51A-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand Brake (Pneumatic) Failure on Demand PMRC Fails to Stop on Loss of Power	5.0E-005
51A-SPMTT-COLLISION (continued)	0.57	2.750E-005	51A-OPRCINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000
			51A-SPMTT-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.8E-005
	0.24	1.160E-005	51A-OPRCINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			51A-SPMTT-G65000-G65-FOH	SPMTT Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	51A-SPMTT-CT000--CT--FOD	SPMTT Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	51A-SPMTT-CT0001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	51A-SPMTT-CPL00-CPL-FOH	Automatic Coupler System Fails	1.9E-006
	4.834E-003 = Total				

NOTE: Freq. = frequency; Prob. = probability; SPMTT = site prime mover truck trailer; TT = truck trailer.

Source: Original

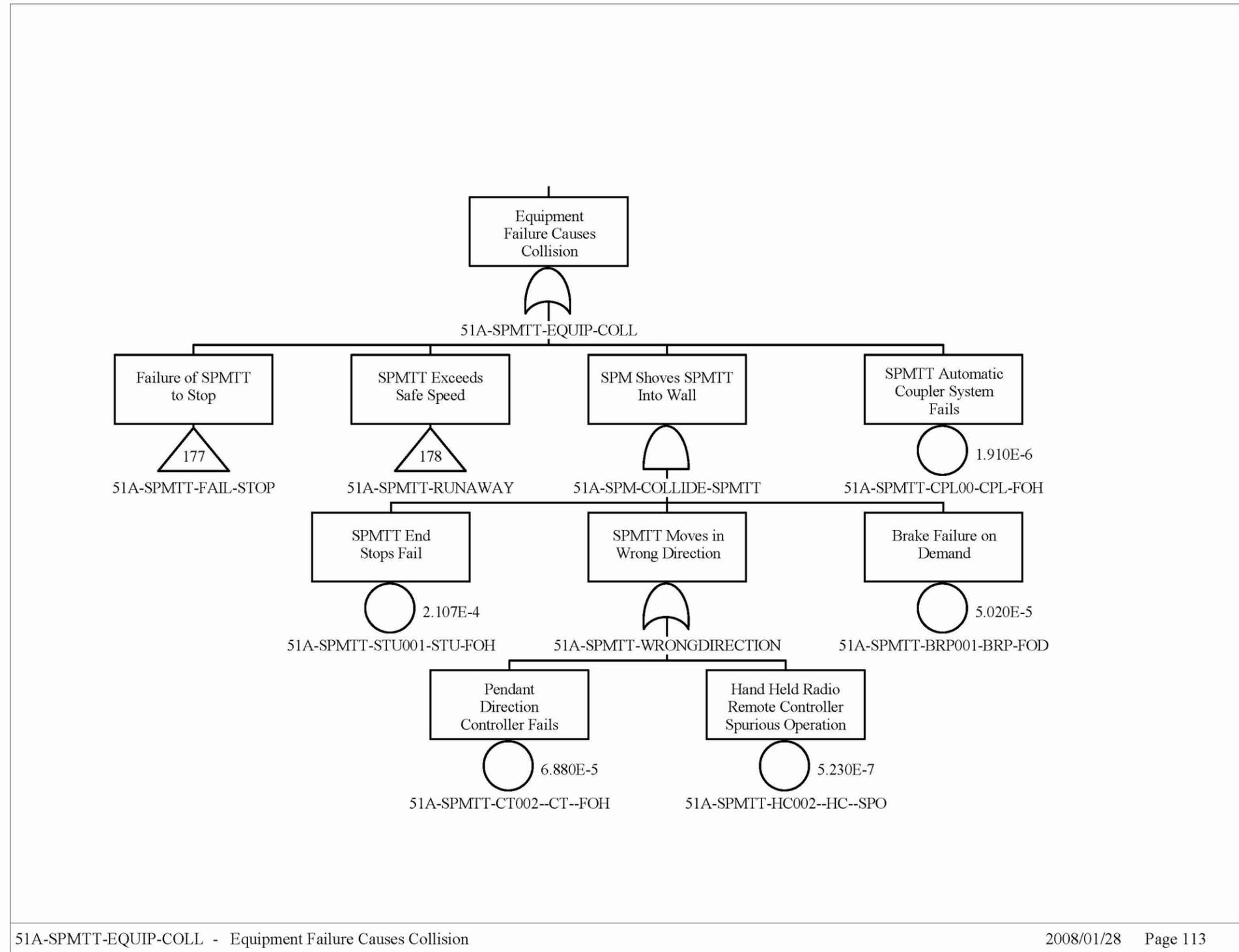
B1.4.2.9 Fault Trees



Source: Original

Figure B1.4-8. SPMTT Collision in IHF

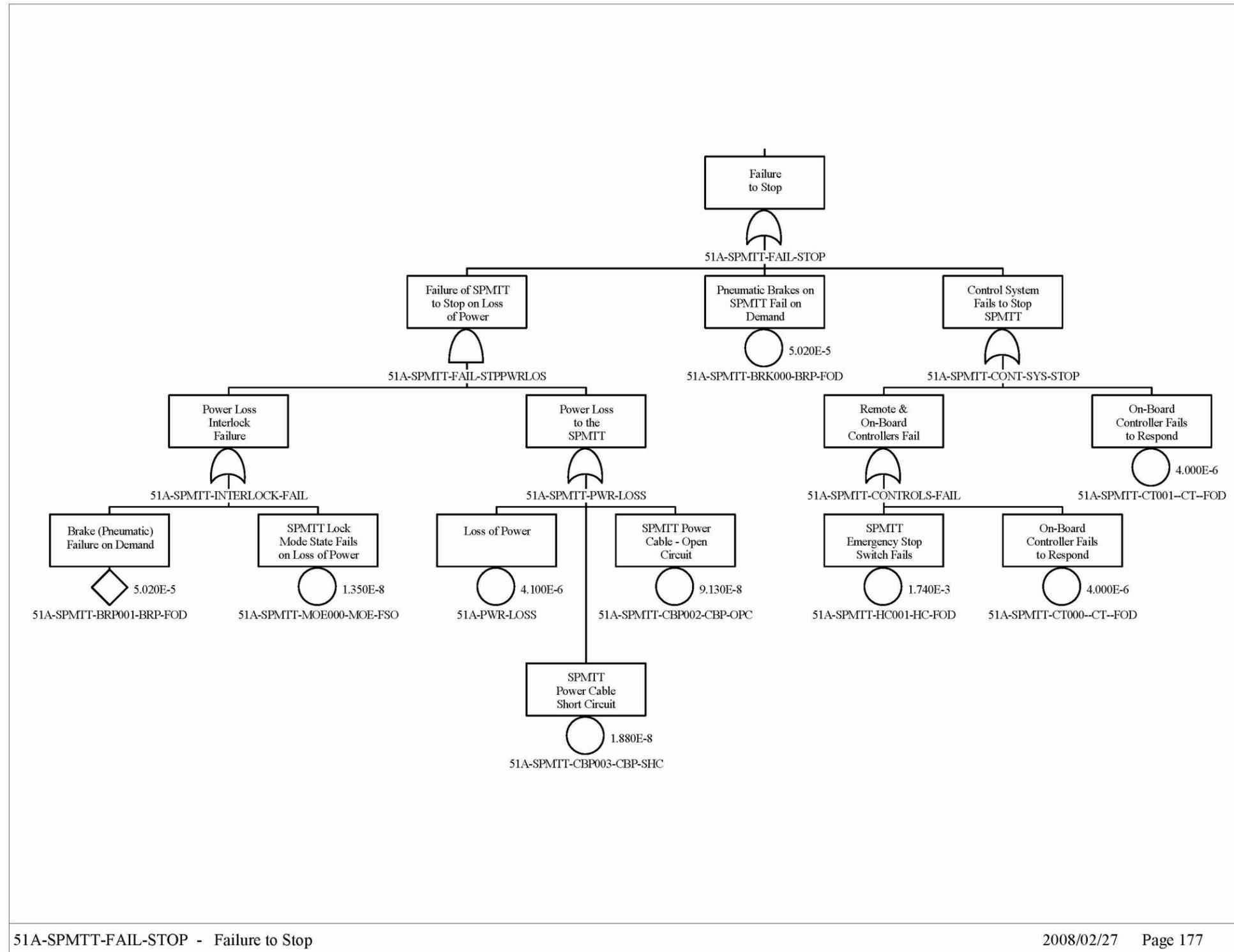
INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-9. Equipment Failure Causes Collision

INTENTIONALLY LEFT BLANK



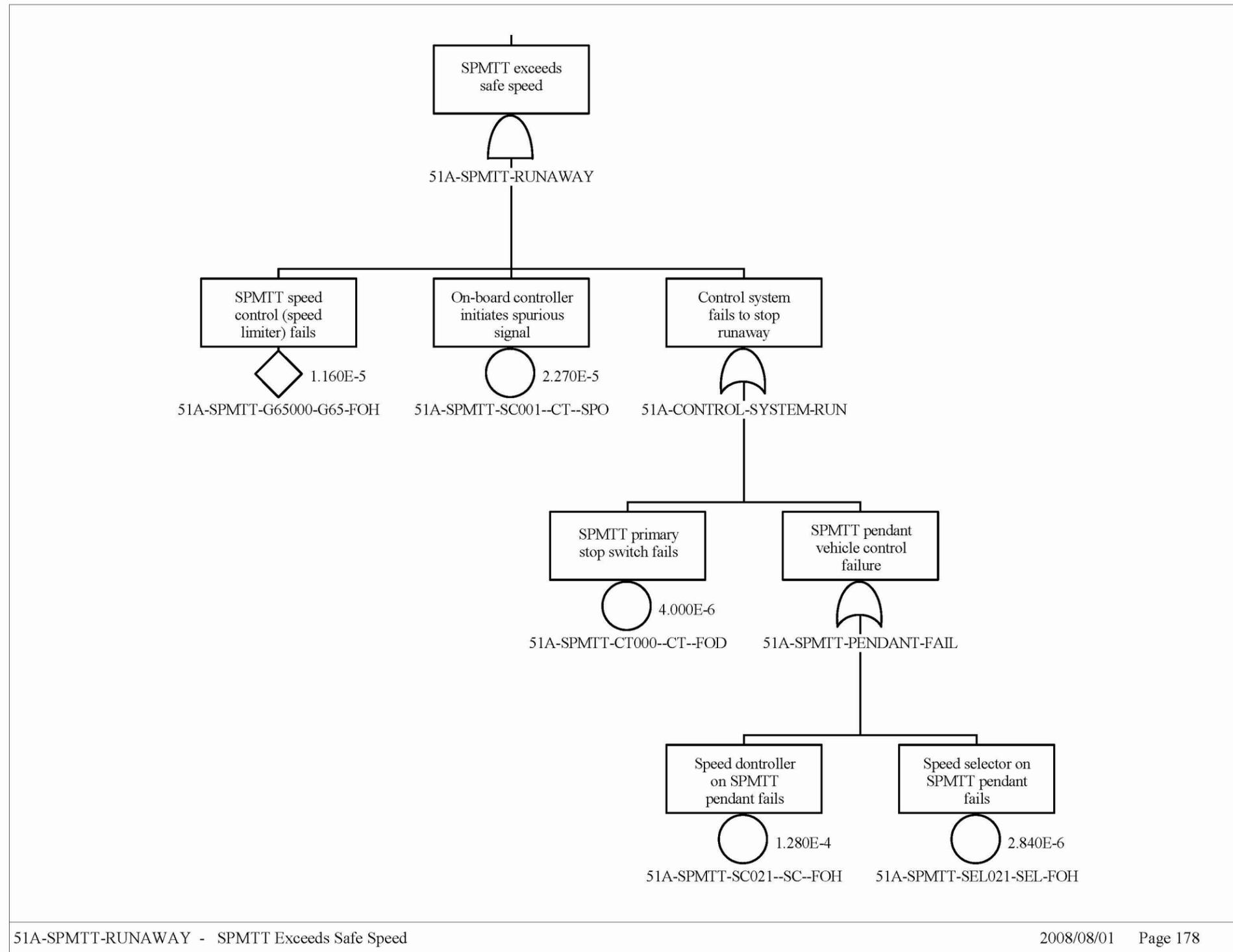
51A-SPMTT-FAIL-STOP - Failure to Stop

2008/02/27 Page 177

Source: Original

Figure B1.4-10. SPMITT Failure to Stop

INTENTIONALLY LEFT BLANK



Source: Original

Figure B1.4-11. SPMTT Exceeds Safe Speed

INTENTIONALLY LEFT BLANK

B1.4.3 SPMRC Derailment

B1.4.3.1 Description

The two fault trees for SPMRC derailment within the IHF are identical with the exception of the number of transportation casks that are processed at the IHF for each configuration. Derailment is characterized by a basic event that accounts for the probability of a railcar derailment per mile of travel within the IHF.

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 B1.4-14.

The probability of derailment is based on historical data for train derailment at low speeds and is discussed in the section on data development (Attachment C, Section C4). The probability of derailment per mile is multiplied by the number of miles the SPM travels inside the Cask Preparation Area (approximately 4.00E-02 miles).

B1.4.3.2 Success Criteria

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

B1.4.3.3 Requirements and Design Features

System Configuration and Operating Conditions

Requirements

The railcar design requirements must 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 must be in compliance with AAR Standard S-2043 *Performance Specification for Trains Used to Carry High-Level Radioactive Material* (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

B1.4.3.4 Fault Tree Model

The fault tree model for “SPMRC Derailment” consists of the probability for a railcar derailment per mile of travel time multiplied by the number of occurrences for each type of transportation cask.

B1.4.3.5 Basic Event Data

Table B1.4-6 contains a list of basic events used in the SPMRC Derailment fault trees.

Table B1.4-6. Basic Event Probability for SPMRC Derailment

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹)	Miss. Time (hr) ^a
51A-SPMRC-DETRAIL-DETR-FOM	3	1.180E-005	—	1.180E-005	1
51A-SPMRC-MILES-IN-IHF	V	4.000E-002	4.000E-002	—	—

NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. Calculation Type V (for “value”) indicates direct numerical entry, where the number is not necessarily a probability and is therefore allowed to be greater than 1. In this case the value is the number of miles travelled by the SPM in the IHF. See Table 6.3-1 for definitions of other calculation types.

Calc = calculation; Fail. = failure; Miss. = mission; Prob. = probability; V = value.

Source: Original

The calculated probability of a derailment inside the IHF is the probability of a railcar derailing per mile of travel times the distance travelled within the facility.

B1.4.3.5.1 Human Failure Events

There are no human errors identified for this fault tree.

B1.4.3.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

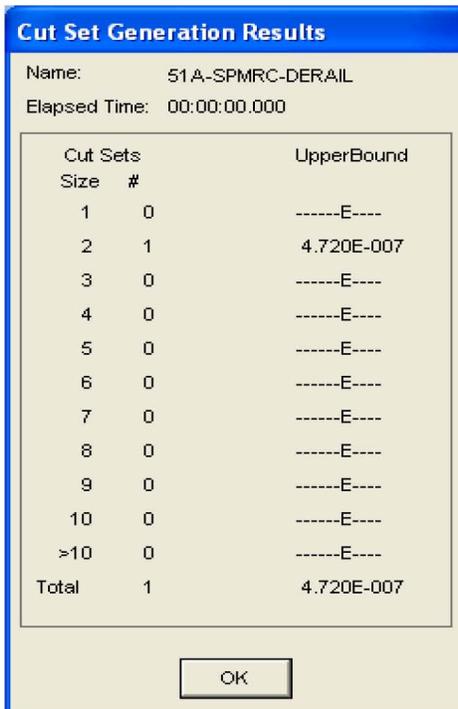
B1.4.3.6 Uncertainty and Cut Set Generation Results

Figure B1.4-12 contains the uncertainty results obtained from running the fault tree for “SPMRC Derailment.” Figure B1.4-13 provides the cut set generation results for the “SPMRC Derailment” fault tree.



Source: Original

Figure B1.4-12. Uncertainty Results of the SPMRC Derailment Fault Tree



Source: Original

Figure B1.4-13. Cut Set Generation Results for SPMRC Derailment*

B1.4.3.7 Cut sets

Tables B1.4-7 contains the cut sets for “SPMRC Derailment”. The probability of derailment per cask is 4.72E-07.

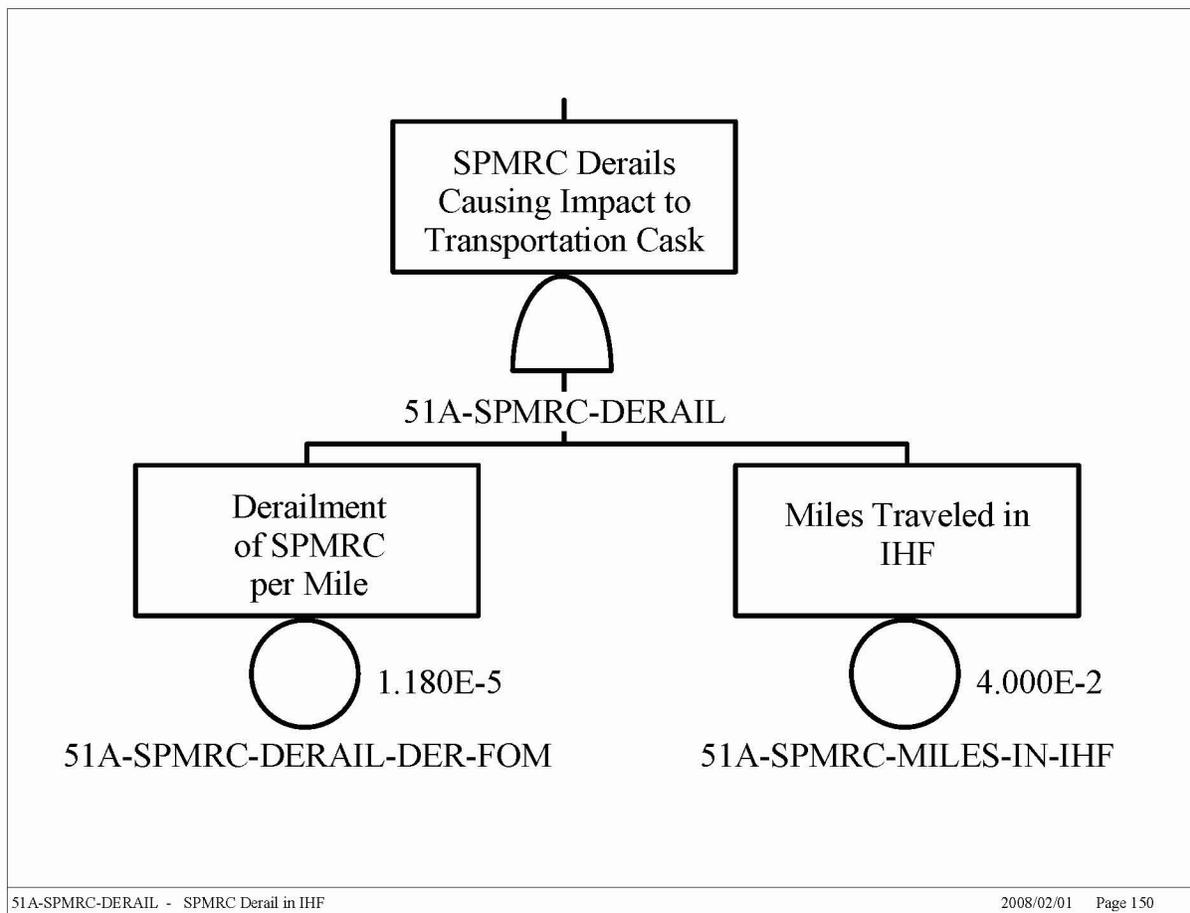
Table B1.4-7. Cut sets for SPMRC Derailment

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMRC- DERAIL	100.00	4.720E-007	51A-SPMRC-DERAIL- DER-FOM	Derailment of a rail car per mile	1.2E-005
			51A-SPMRC-MILES-IN- IHF	Miles traveled in IHF	4.0E-002
4.720E-007 = Total					

NOTE: Freq. = frequency; IHF = Initial Handling Facility; Prob. = probability.

Source: Original

B1.4.3.8 Fault Trees



Source: Original

Figure B1.4-14. SPMRC Derailment in IHF

B1.4.4 SPMTT Rollover in the IHF

B1.4.4.1 Description

The fault trees for “SPMTT Rollover in the IHF” are identical for each type of transportation cask. Rollover is characterized by a human error basic event that accounts for the probability of an operator jackknifing the truck trailer while backing through the IHF Cask Preparation Area.

During movement, a rail track failure, obstacle on the track or a structural failure on the railcar could potentially lead to a rollover. For the truck trailer, an obstacle on the road or a structural failure on the trailer could potentially lead to a rollover. There are no design constraints for these types of failures; to prevent this situation relies on an operator response to initiate an emergency stop command. Since this is a recovery action, no credit is taken for the operator response.

B1.4.4.2 Success Criteria

The design of the SPM prevents the majority of scenarios that could potentially cause a SPM rollover. A low center of gravity and a wide footprint of the railcar/truck trailer results in a stable platform during movements.

The success criterion is that no rollover occurs while transferring the trailer into the IHF with the site prime mover.

B1.4.4.3 Requirements and Design Features

System Configuration and Operating Conditions

Requirements

Trailers used for the movement of transportation casks are designed in accordance with the requirements contained in NHTSA requirements as authorized by Title 49 U.S.C. 30111. Transportation: Federal Motor Vehicle Safety Standards (Ref. B1.1.2). The requirements are delineated in 49 CFR Part 571 (Ref. B1.1.3).

While backing the SPMTT through the Cask Preparation Area, at least one walker-spotter is required to ensure no objects are in the path of the SPMTT and to stop the driver from jackknifing the trailer.

Design Feature

None.

Testing and Maintenance

Requirements

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

Design Feature

None.

B1.4.4.4 Fault Tree Model

The fault tree model for SPMTT rollover (Figure B1.4-15) consists of a single human error associated with the operator jackknifing the truck trailer when positioning it in the IHF.

B1.4.4.5 Basic Event Data

A rollover within the IHF can only occur if the driver of the SPMTT jackknives the truck trailer.

There is only one basic event (51A-OPTTROLLOVER-HFI-NOT) consisting of a human error causing a jackknife of the trailer shown in Figure B1.4-15.

B1.4.4.5.1 Human Failure Events

The human error probability of causing a jackknife of the trailer has been assessed as zero due to the limited space within the Cask Preparation Area and the inability of the trailer to jackknife in such a small space (as discussed in Section 6.0, Table 6.0-2).

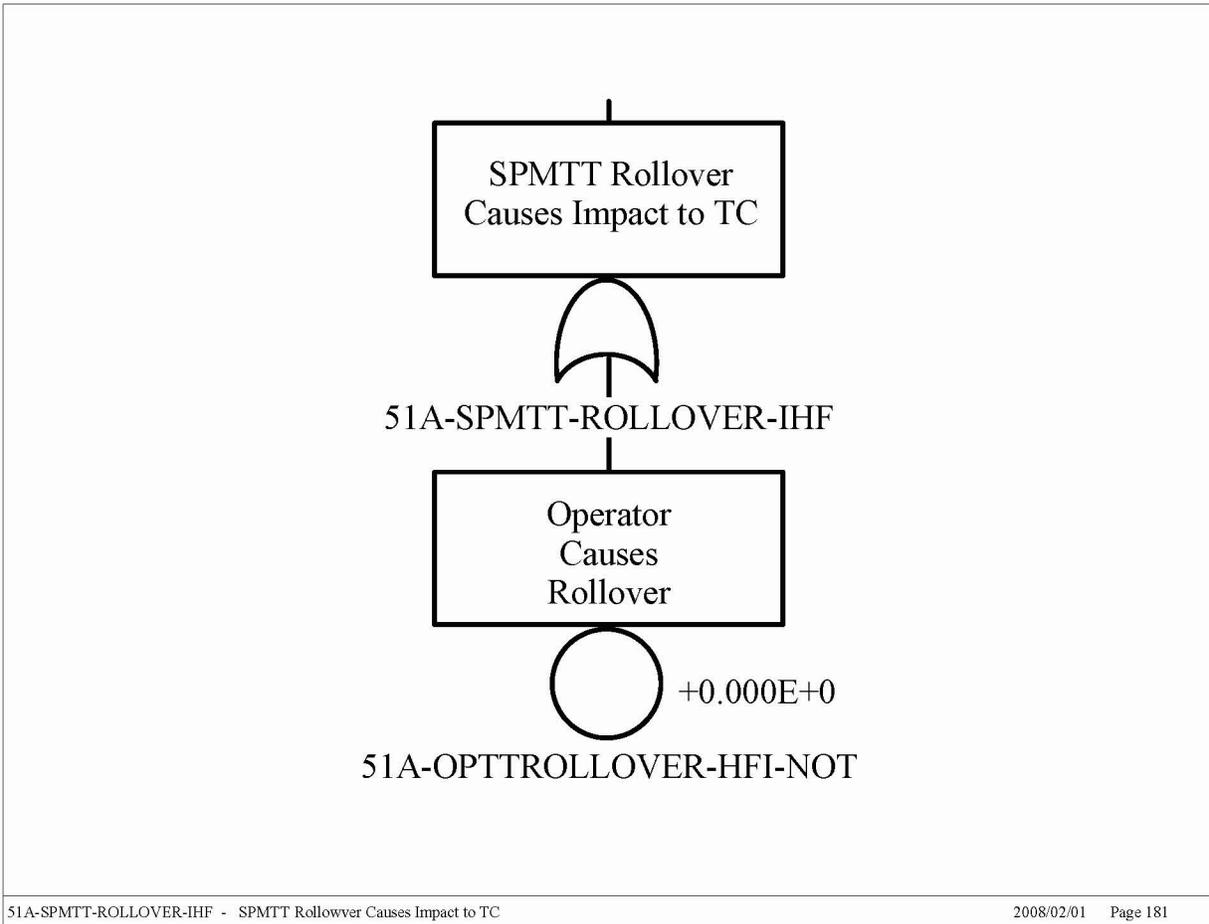
B1.4.4.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

B1.4.4.6 Uncertainty and Cut Set Generation Results

Because there is only a single basic event that is assessed as having zero probability of occurrence, there are no uncertainty values or cut sets to be calculated.

B1.4.4.7 Fault Tree



Source: Original

Figure B1.4-15. SPMTT Rollover in IHF

INTENTIONALLY LEFT BLANK

B2 CASK TRANSFER TROLLEY ANALYSIS – FAULT TREES

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), Sections 3.2.1 and 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.

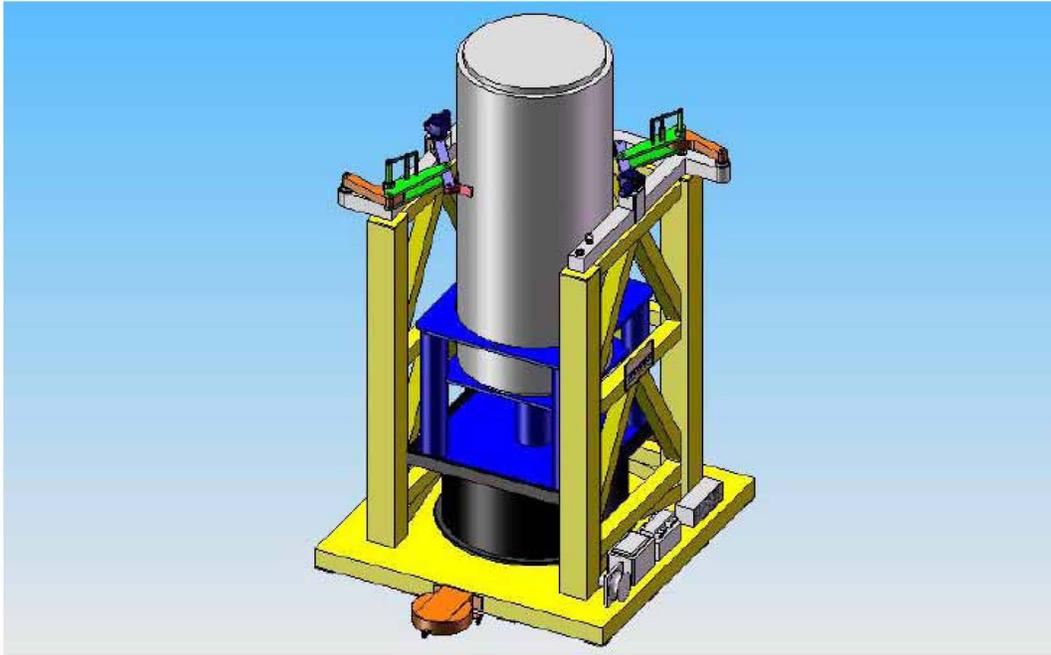
B2.1.2 *BSC (Bechtel SAIC Company) 2007. *Preliminary Throughput Study for the Initial Handling Facility*. 51A-30R-IH00-00100-000-001. Las Vegas, Nevada. Bechtel SAIC Company. ACC: ENG.20071102.0021.

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 Area 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 Canister Transfer Area using bumpers and stops that are bolted to the floor of the Cask Unloading Room 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 does not power up and move/levitate.

The facility compressed air supply inflates nine 54-inch 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 inch to 7/8 inch. The air bearings are supplied with facility air (between 75 to 100 pounds per square inch optimal) and consume from 500 to 700 standard cubic feet per minute. A hose reel for the 1½ inch 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 allow 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-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. 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 feet per minute (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 controllers are 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 Area.
- 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 Unloading Room and the Cask Preparation Area 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.

There 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.

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

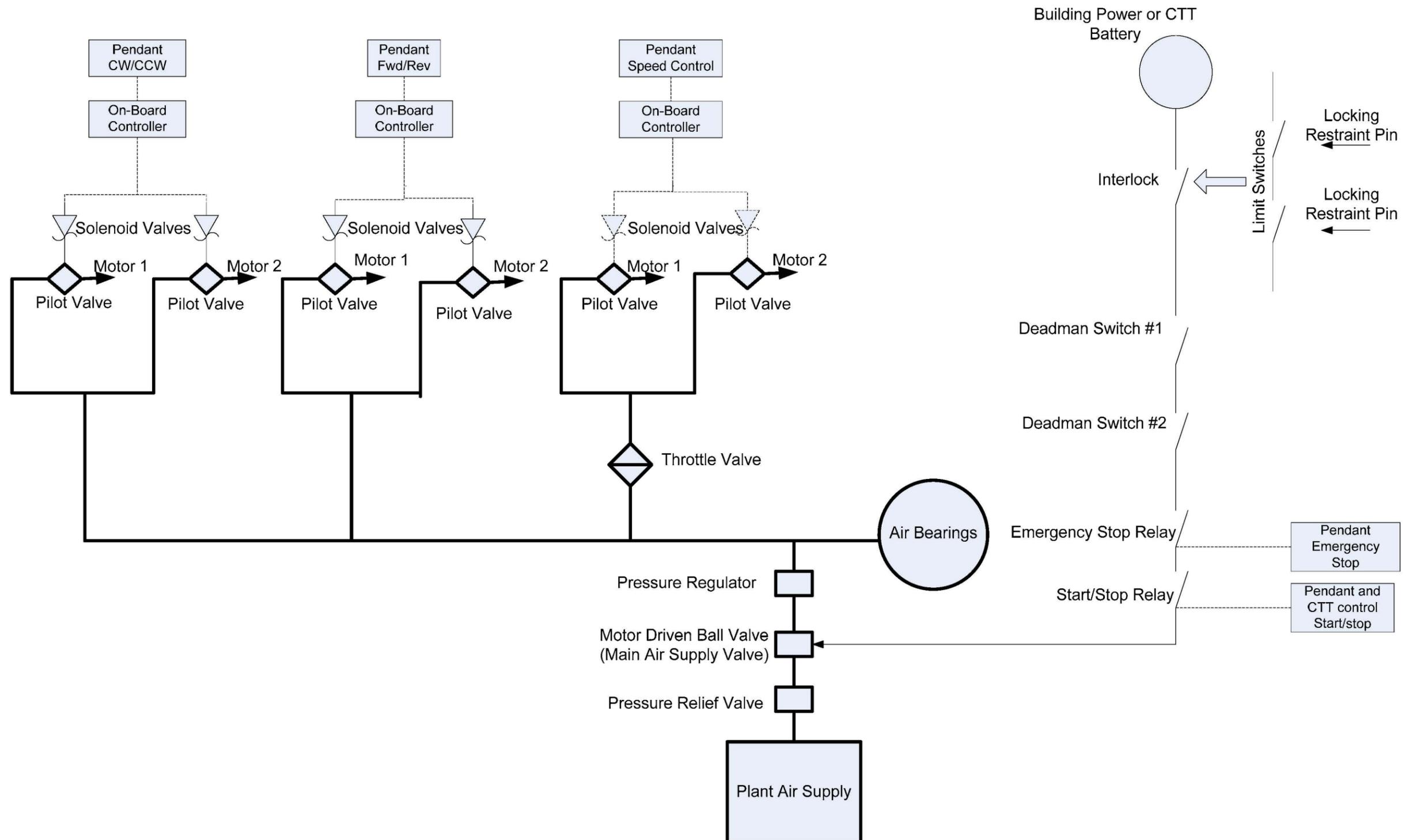
B2.2.3.1 Initial Conditions

The CTT is initially located in the Cask Preparation Area with the battery fully charged, the seismic restraints retracted, and with no air hose 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 to operate. Once all preparations of the cask are complete, the trolley can be moved to the Cask Unloading Room using the pendant controls.

INTENTIONALLY LEFT BLANK



Source: Modified from Ref. B2.1.3

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

INTENTIONALLY LEFT BLANK

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 ensure that the CTT can only move forward and back, and in addition, will ensure that 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 Area 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 at the Cask Preparation Area, and unloading the canisters from the cask in the Cask Unloading Room, require the CTT to remain stationary during these operations with no spurious movement. Success criteria for moving the CTT with cask from the Cask Preparation Area to the Cask Unloading Room require the CTT to travel at an allowable speed, and the operator to be able to control the CTT movement.

During cask loading at the Cask Preparation Area, 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 be disconnected from the CTT to prevent any movement while unloading the canisters from the cask. This is accomplished by locating the air supply unit outside the Cask Unloading Room. An interlock prevents the transfer port slide gate from opening until the shield door to the transfer room is closed. Thus, because the air supply unit is external to the transfer 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 Area 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 again 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 structures, systems or 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	—	—	—	—

Table B2.3-1. Dependencies and Interactions Analysis (Continued)

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
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 Area during cask loading
2. Spurious movement of the CTT in the Cask Preparation Area during cask preparation
3. Collision of 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 Area to the Cask Unloading Room. This fault tree is described in a separate section involving inadvertent shield door closure that satisfies ESD-6, 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 Area 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 Area during Cask Loading

B2.4.1.1 Description

This fault tree describes spurious movement of the CTT during cask loading to satisfy ESD-2, initiating event “Unplanned Carrier Movement Causes Transportation Cask Impact.” 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 (Figure B2.4-3). 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

A success criterion is that the CTT remains motionless during loading of the transportation cask. Movement of the CTT during this operation could cause an impact to occur resulting in 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 locking restraint pin system which prevents power to the main air supply valve until both the pins are in place and the limit switches are activated to allow power to the air supply valve.

B2.4.1.4 Fault Tree Model

The top event is spurious movement of the CTT during cask loading in the Cask Preparation Area (Figure B2.4-3). This can occur if the control system initiates a spurious signal and both of the pin limit switches fail, or the operator initiates a command to move the CTT and both of the pin limit switches fail. A third failure mode is the mechanical failure of the main supply valve in conjunction with a spurious signal from the control system to initiate movement or failures of the control valves or the valve to the air bags.

A conservative mission time for this operation has been set at one hour.

B2.4.1.5 Basic Event Data Inputs

Table B2.4-1 contains a list of basic events used in the fault tree (Figures B2.4-3 and B2.4-4) for “Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading”.

Table B2.4-1. Basic Event Probabilities for Spurious Movement of the CTT during Cask Loading

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹)	Miss. Time (hr) ^a
51A-CTT--CT001---CT--SPO	3	2.270E-005	—	2.270E-005	1
51A-CTT--HC001---HC--SPO	3	5.230E-007	—	5.230E-007	1
51A-CTT--SV301---SV--SPO	3	4.090E-007	—	4.090E-007	1
51A-CTT--ZS301---ZS--FOD	1	2.930E-004	2.930E-004	—	—
51A-CTT--ZS302---ZS--FOD	1	2.930E-004	2.930E-004	—	—
51A-OPSPURMOV01-HFI-NOD	1	1.000E-004	1.000E-004	—	—
51A-CTT-PIN-LIMIT-CCF	C	1.377E-005	—	—	—
51A-CTT--SV401--SV-FOH	3	4.870E-005	—	4.870E-005	1
51A-CTT--FWDREVM1--SV-FOH	3	4.870E-005	—	4.870E-005	1
51A-CTT--FWDREVM2--SV-FOH	3	4.870E-005	—	4.870E-005	1
51A-CTT--SVROT1--SV-FOH	3	4.870E-005	—	4.870E-005	1
51A-CTT--SVROT2--SV-FOH	3	4.870E-005	—	4.870E-005	1

NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B2.4.1.5.1 Human Failure Events

One operator error involves initiation of spurious movement. The operator error is 51A-OPSPURMOVE01-HFI-NOD.

B2.4.1.5.2 Common-Cause Failures

One common-cause failure (CCF) was added to the tree to account for failure of both restraint pin limit switches. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criterion (Section C3). The CCF basic event is 51A-CTT-PIN-LIMIT-CCF.

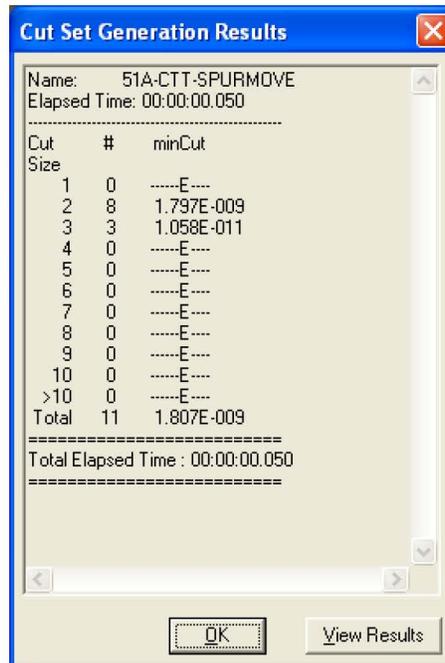
B2.4.1.6 Uncertainty and Cut Set Generation Results

Figure B2.4-1 contains the uncertainty results obtained from running the fault tree for “Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading.” Figure B2.4-2 provides the cut set generation results for “Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading”.



Source: Original

Figure B2.4-1. Uncertainty Results of Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading



Source: Original

Figure B2.4-2. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading

B2.4.1.7 Cut Sets

Table B2.4-2 contains the cut sets for “Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading”. The total probability per cask loading is 1.811E-09.

Table B2.4-2. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-CTT-SPURMOVE	76.21	1.377E-009	51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005
			51A-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement	1.0E-004
	17.30	3.126E-010	51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005
	1.10	1.992E-011	51A-CTT-FWDREVM1-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	1.10	1.992E-011	51A-CTT-FWDREVM2-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SV401-SV-FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.9E-005
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM1-SV-FOH	Failure of SV Providing Rotation to Motor 1	4.9E-005
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM2-SV-FOH	Failure of SV Providing Rotation to Motor 2	4.9E-005
	0.48	8.585E-012	51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004

Table B2.4-2 Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading (Continued)

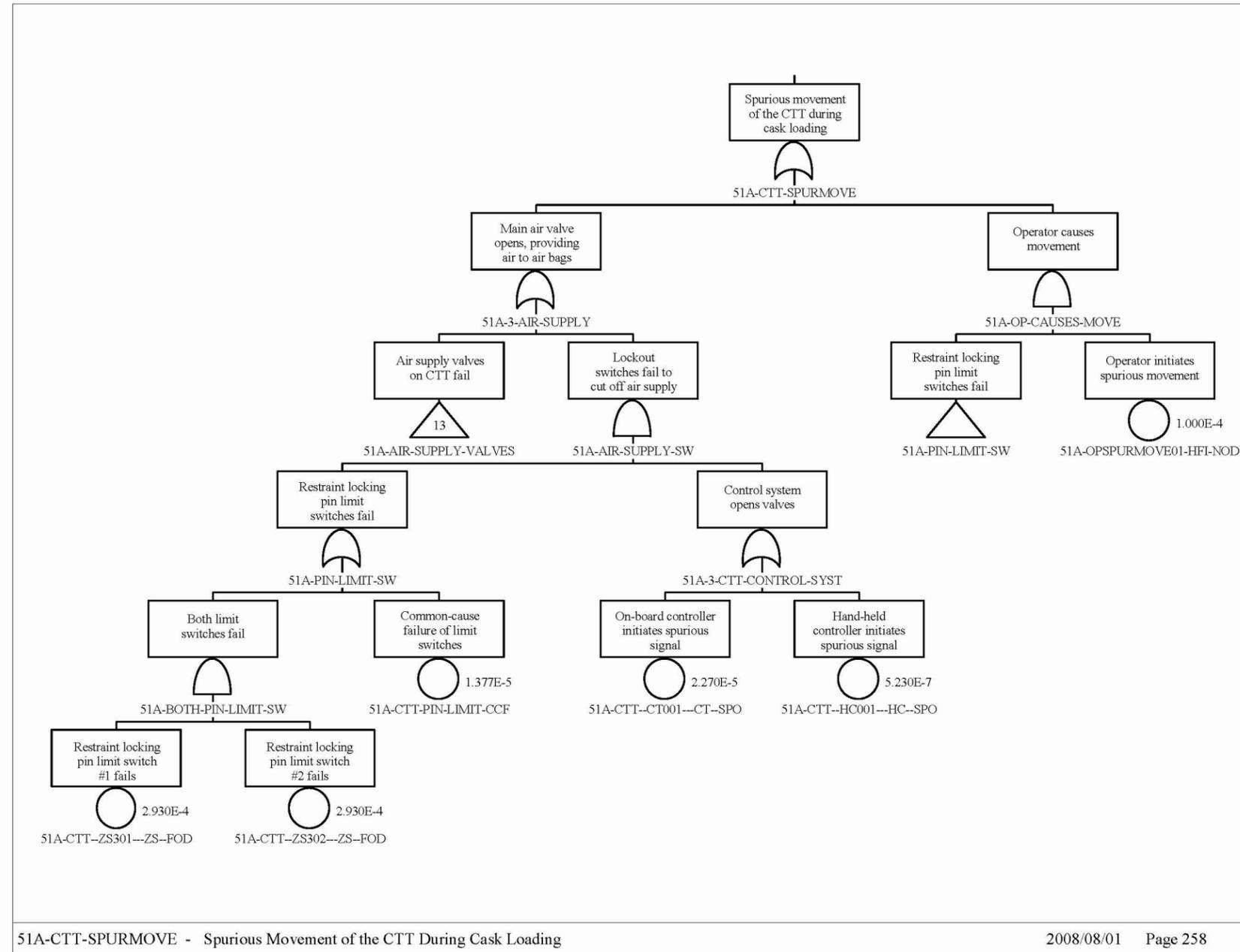
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability	
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004	
			51A-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement	1.0E-004	
	0.40	7.202E-012	51A-CTT--HC001---HC--SPO	Hand Held Controller Initiates Spurious Signal	5.2E-007	
			51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005	
	0.11	1.949E-012	51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005	
			51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004	
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004	
	0.00	4.490E-014	51A-CTT--HC001---HC--SPO	Hand Held Controller Initiates Spurious Signal	5.2E-007	
			51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004	
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004	
	1.807E-009 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B2.4.1.8 Fault Trees

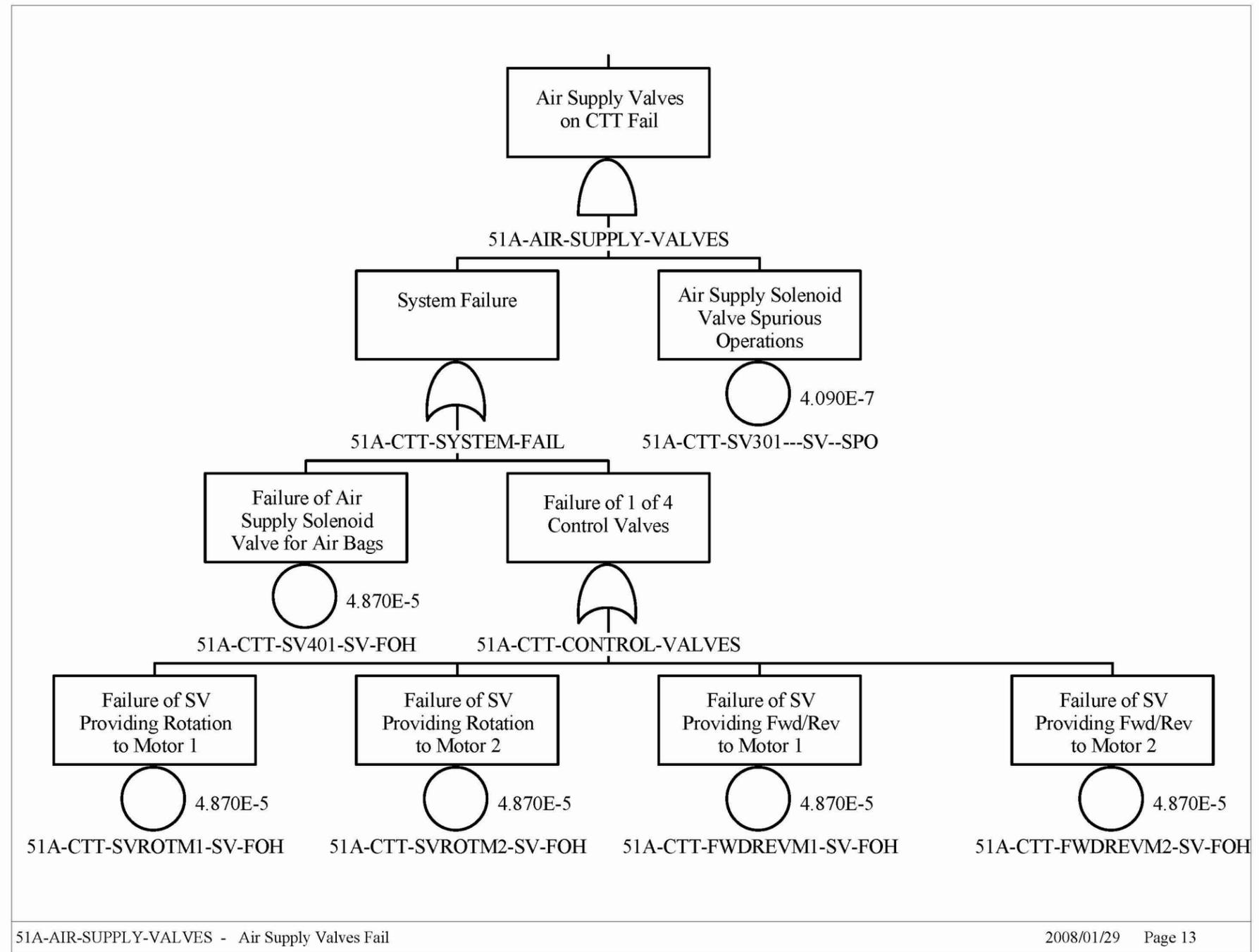
The fault trees for “Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading” are shown in Figures B2.4-3 and B2.4-4.



Source: Original

Figure B2.4-3. Fault Tree for Spurious Movement of the CTT in the Cask Preparation Area During Cask Loading

INTENTIONALLY LEFT BLANK



Source: Original

Figure B2.4-4. Fault Tree for Air Supply Failure

INTENTIONALLY LEFT BLANK