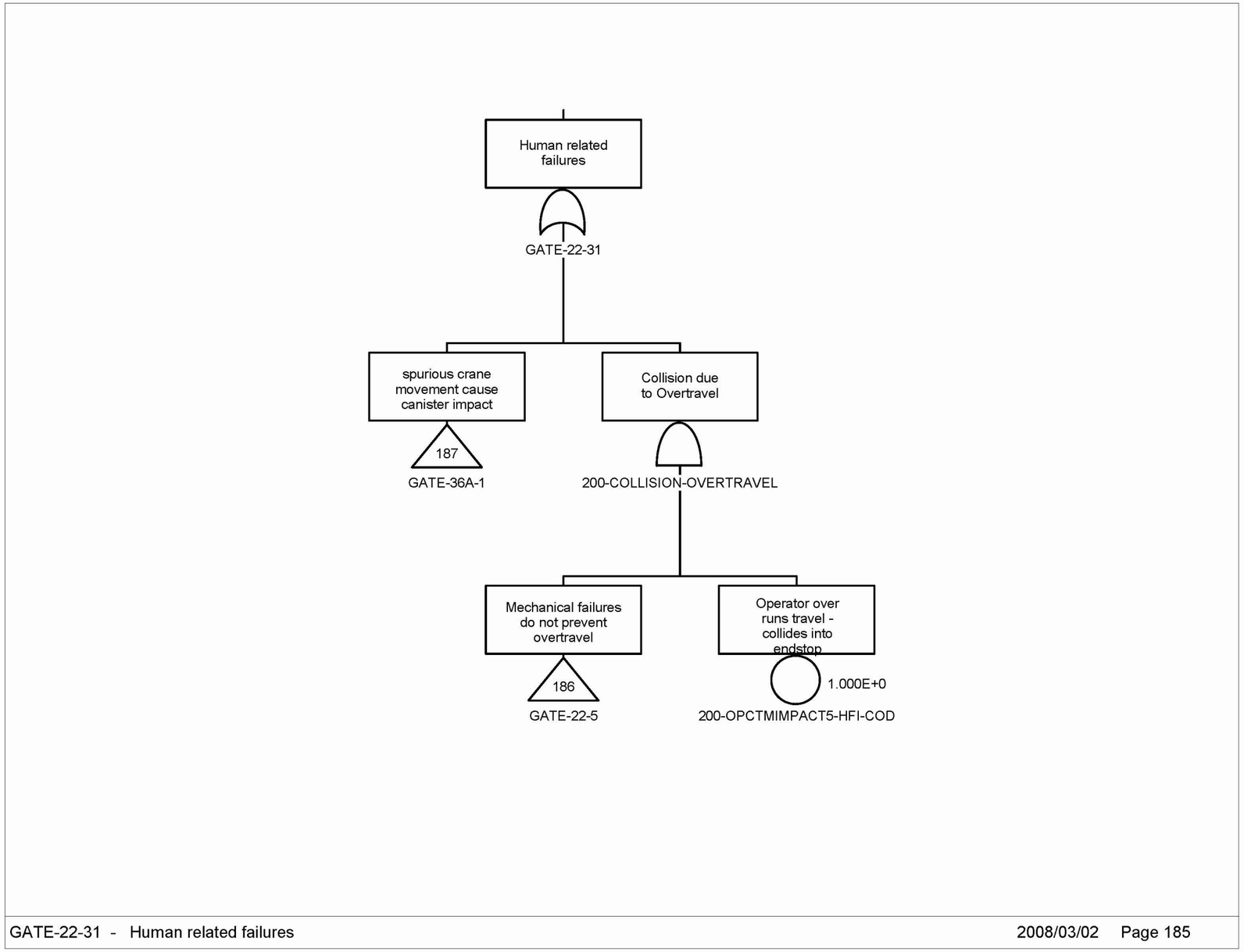
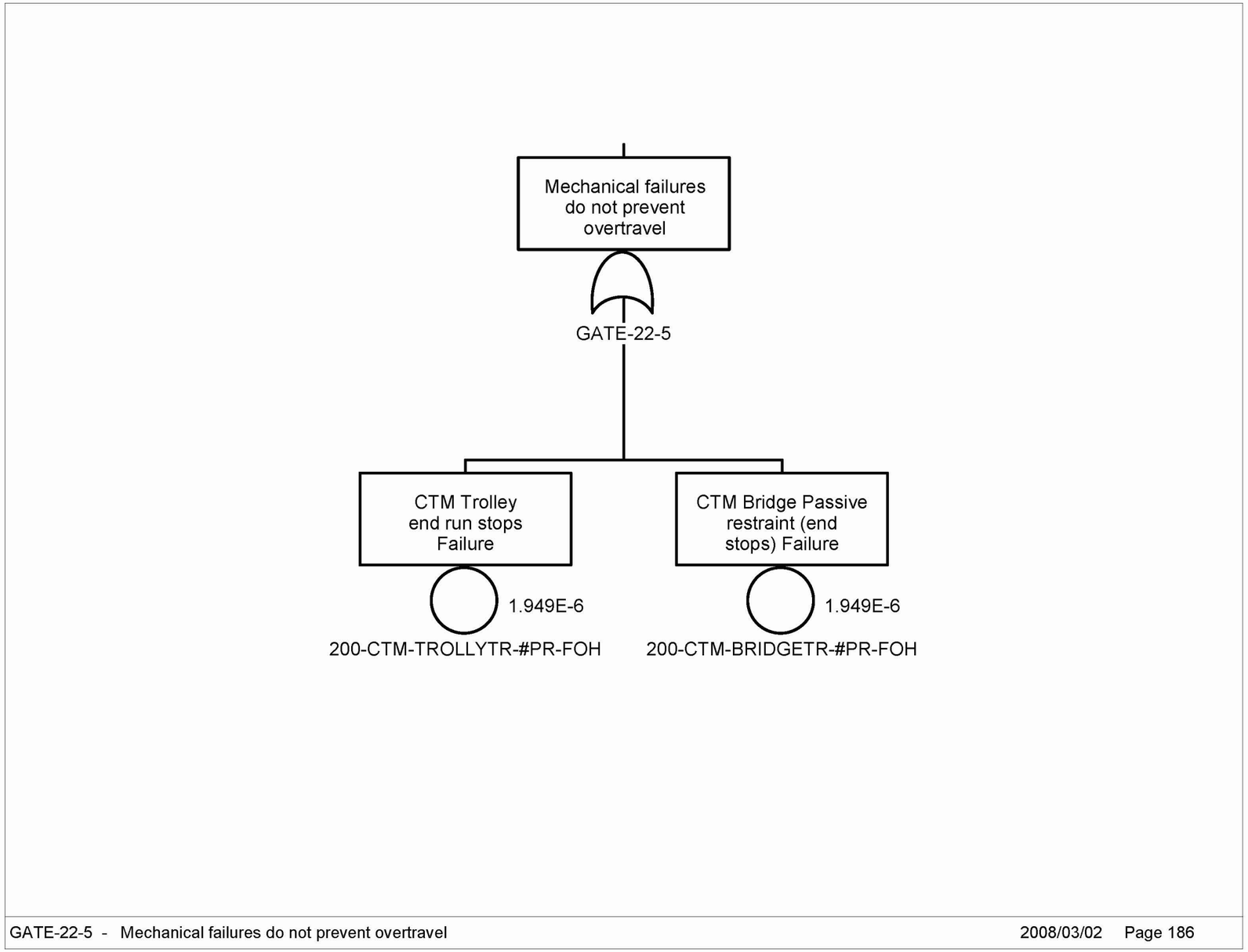


Source: Original

Figure B4.4-39. CTM Collision Sheet 3

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-40. CTM Collision Sheet 4

INTENTIONALLY LEFT BLANK

B4.4.5 CTM Movement Subjects Canister to Shearing Forces

B4.4.5.1 Description

A fault tree was developed to address the potential for movement of the CTM when the canister being transferred is being lifted and is between the RF floors. Movement initiated by the bridge or trolley motors could result in shear forces being applied to the canister should it be lifted when the CTM moves away from the floor port opening.

B4.4.5.2 Success Criteria

Success criteria for the CTM is the prevention of CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the RF during the lift portions of the canister transfer.

B4.4.5.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

An optical sensor at the bottom of the shield bell that, once it is cleared, stops the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.

- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.

- An interlock between the slide gate and shield skirt – the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed to allow the CTM to move with the slide gate open during lid removal.

- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

- The load cells cut off power to the hoist when the crane capacity is exceeded.
- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 ft/min, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard-wired interlocks used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end of travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.5.4 Fault Tree Model

The top event in this fault tree is "CTM Movement Causes Canister Shear." The fault tree includes events (mechanical control failures and human actions, considered in conjunction with the interlocks intended to prevent the erroneous human action) that can initiate a spurious movement of the CTM trolley or bridge while the canister is between the first and second floors of the RF (Figures B4.4-43, B4.4-44 and B4.4-45).

B4.4.5.5 Basic Event Data

Table B4.4-12 contains a list of basic events used in the CTM shear fault tree. Included are the human failure events and the CCF events identified in the following two sections. There are no maintenance-related failures associated with the CTM. The CTM is not in service while undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

Table B4.4-12. Basic Event Probability for the CTM Fault Trees

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-CTM-#ZSH0112-1ZS-FOD	CTM shield skirt position switch 0112 fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
200-CTM-BIDGMTR-#TL-FOH	CTM bridge motor torque limiter failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
200-CTM-BRIDGMTS-MOE-SPO	CTM bridge motor (electric) spurious operation -shear	3	3.370E-08	0.000E+00	6.740E-07	5.000E-02
200-CTM-HSTTRLLS-MOE-SPO	CTM hoist trolley motor (electric) spurious operation m-shear	3	3.370E-08	0.000E+00	6.740E-07	5.000E-02
200-CTM-HSTTRLLY-#TL-FOH	CTM hoist motor torque limiter failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
200-CTM-PLC0101S-PLC-SPO	CTM bridge motor PLC spurious operation - shear	3	3.650E-07	0.000E+00	3.650E-07	0.000E+00
200-CTM-PLC0102S-PLC-SPO	CTM shield bell trolley PLC spurious operation -shear	3	3.650E-07	0.000E+00	3.650E-07	0.000E+00
200-CTM-PLC0103S-PLC-SPO	CTM hoist trolley PLC spurious operation -shear	3	3.650E-07	0.000E+00	3.650E-07	0.000E+00
200-CTM-SBELTRLS-MOE-SPO	Motor (electric) spurious operation	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01
200-CTM-SBELTRLY-#TL-FOH	CTM shield bell motor torque limiter failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
200-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; CTM = canister transfer machine; CTM = canister transfer machine; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

The shear impact probability modeled by the fault tree is evaluated over a mission time of one-tenth of an hour (limited to the time the canister is being lifted and is between the first and second floors). A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are tested. They are consequently evaluated over the interval of time between their tests, and the mission time is assigned a value of the average fault exposure time, half the test interval.

B4.4.5.5.1 Human Failure Events

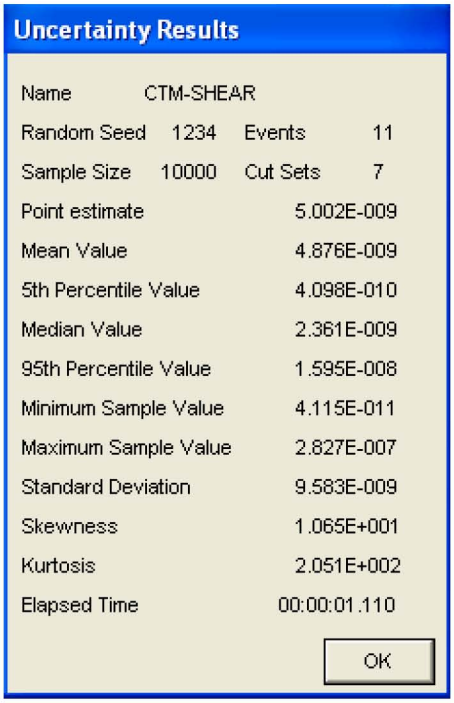
One basic event is associated with human error: 200-OPCTMIMPACT1-HFI-COD (operator moves trolley/crane with canister below floor). This event addresses the possible operator initiated movement of the bridge or trolleys while a canister is being lifted and is between RF floors.

B4.4.5.5.2 Common-Cause Failures

No CCFs apply to this fault tree.

B4.4.5.6 Uncertainty and Cut Set Generation Results

Figure B4.4-41 contains the uncertainty results obtained from running the fault trees for "CTM-SHEAR." Figure B4.4-42 provides the cut set generation results for the "CTM-SHEAR" fault tree, calculated using a 1E-15 cutoff.



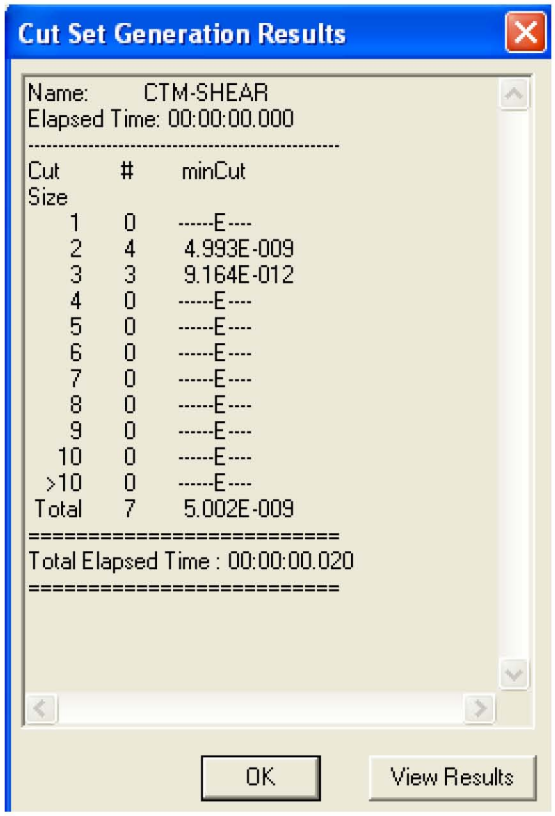
Uncertainty Results

Name	CTM-SHEAR		
Random Seed	1234	Events	11
Sample Size	10000	Cut Sets	7
Point estimate			5.002E-009
Mean Value			4.876E-009
5th Percentile Value			4.098E-010
Median Value			2.361E-009
95th Percentile Value			1.595E-008
Minimum Sample Value			4.115E-011
Maximum Sample Value			2.827E-007
Standard Deviation			9.583E-009
Skewness			1.065E+001
Kurtosis			2.051E+002
Elapsed Time			00:00:01.110

OK

Source: Original

Figure B4.4-41. Uncertainty Results of the CTM Shear Fault Tree



Source: Original

Figure B4.4-42. Cut Set Generation Results for the CTM Shear Fault Tree

B4.4.5.7 Cut Sets

Table B4.4-13 contains the cut sets for the CTM Shear fault tree.

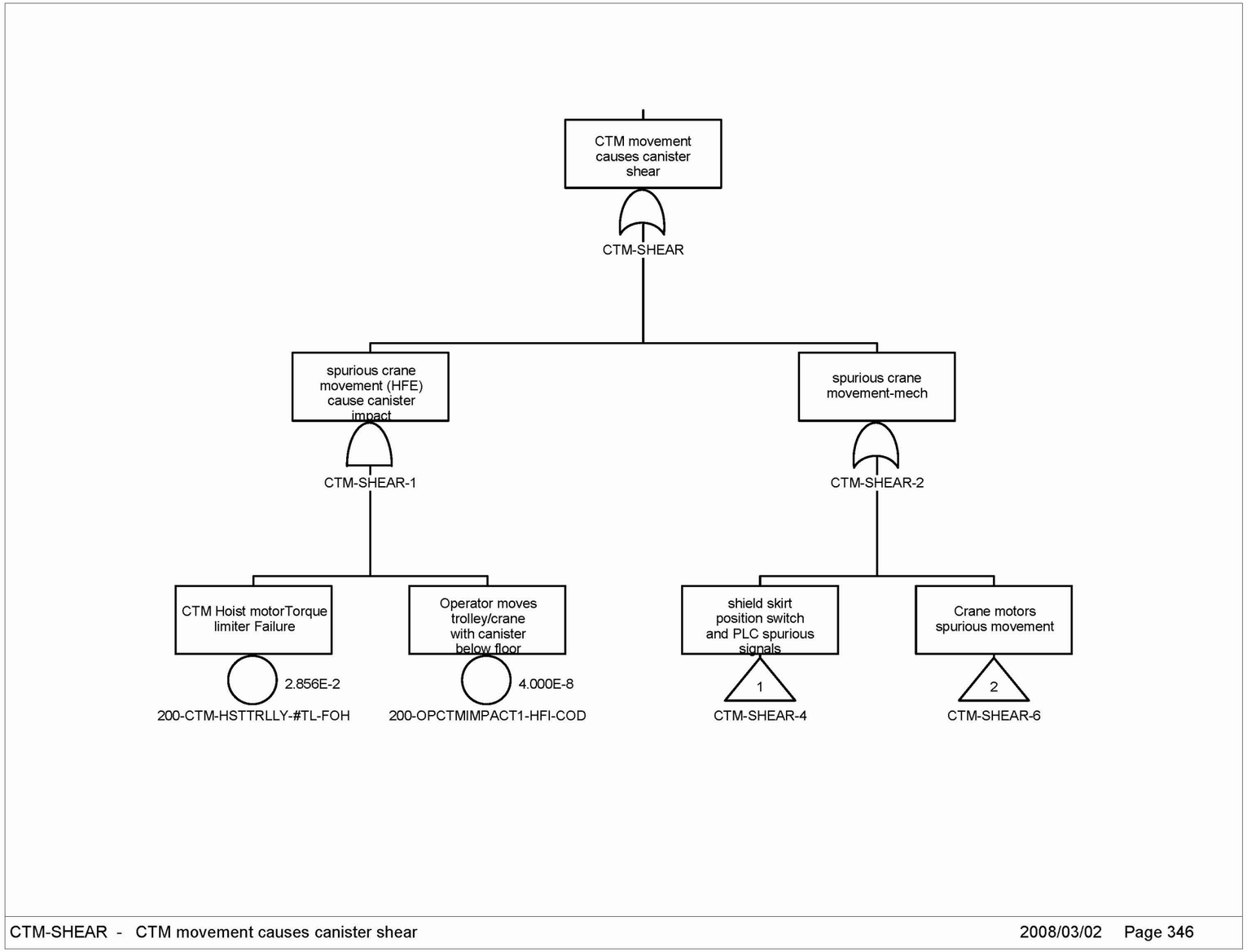
Table B4.4-13. Dominant Cut Sets for the CTM Collision Fault Tree

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
38.49	38.49	1.925E-09	200-CTM-SBELTRLS-MOE-SPO	Motor (electric) spurious operation	6.740E-08
			200-CTM-SBELTRLY-#TL-FOH	CTM shield bell motor torque limiter failure	2.856E-02
61.33	22.84	1.143E-09	200-CTM-HSTTRLLY-#TL-FOH	CTM hoist motor torque limiter failure	2.856E-02
			200-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-08
80.57	19.24	9.626E-10	200-CTM-BIDGMTR-#TL-FOH	CTM bridge motor torque limiter failure	2.856E-02
			200-CTM-BRIDGMTS-MOE-SPO	CTM bridge motor (electric) spurious operation -shear	3.370E-08
99.81	19.24	9.626E-10	200-CTM-HSTTRLLS-MOE-SPO	CTM hoist trolley motor (electric) spurious operation m - shear	3.370E-08
			200-CTM-HSTTRLLY-#TL-FOH	CTM hoist motor torque limiter failure	2.856E-02
99.87	0.06	3.055E-12	200-CTM-#ZSH0112-1ZS-FOD	CTM shield skirt position switch 0112 fails	2.930E-04
			200-CTM-PLC0102S-PLC-SPO	CTM shield bell trolley PLC spurious operation - shear	3.650E-07
			200-CTM-SBELTRLY-#TL-FOH	CTM shield bell motor torque limiter failure	2.856E-02
99.93	0.06	3.055E-12	200-CTM-#ZSH0112-1ZS-FOD	CTM shield skirt position switch 0112 fails	2.930E-04
			200-CTM-BIDGMTR-#TL-FOH	CTM bridge motor torque limiter failure	2.856E-02
			200-CTM-PLC0101S-PLC-SPO	CTM bridge motor plc spurious operation - shear	3.650E-07
99.99	0.06	3.055E-12	200-CTM-#ZSH0112-1ZS-FOD	CTM shield skirt position switch 0112 fails	2.930E-04
			200-CTM-HSTTRLLY-#TL-FOH	CTM hoist motor torque limiter failure	2.856E-02
			200-CTM-PLC0103S-PLC-SPO	CTM hoist trolley PLC spurious operation - shear	3.650E-07

NOTE: CTM = canister transfer machine; PLC = programmable logic controller; Prob. = probability.

Source: Original

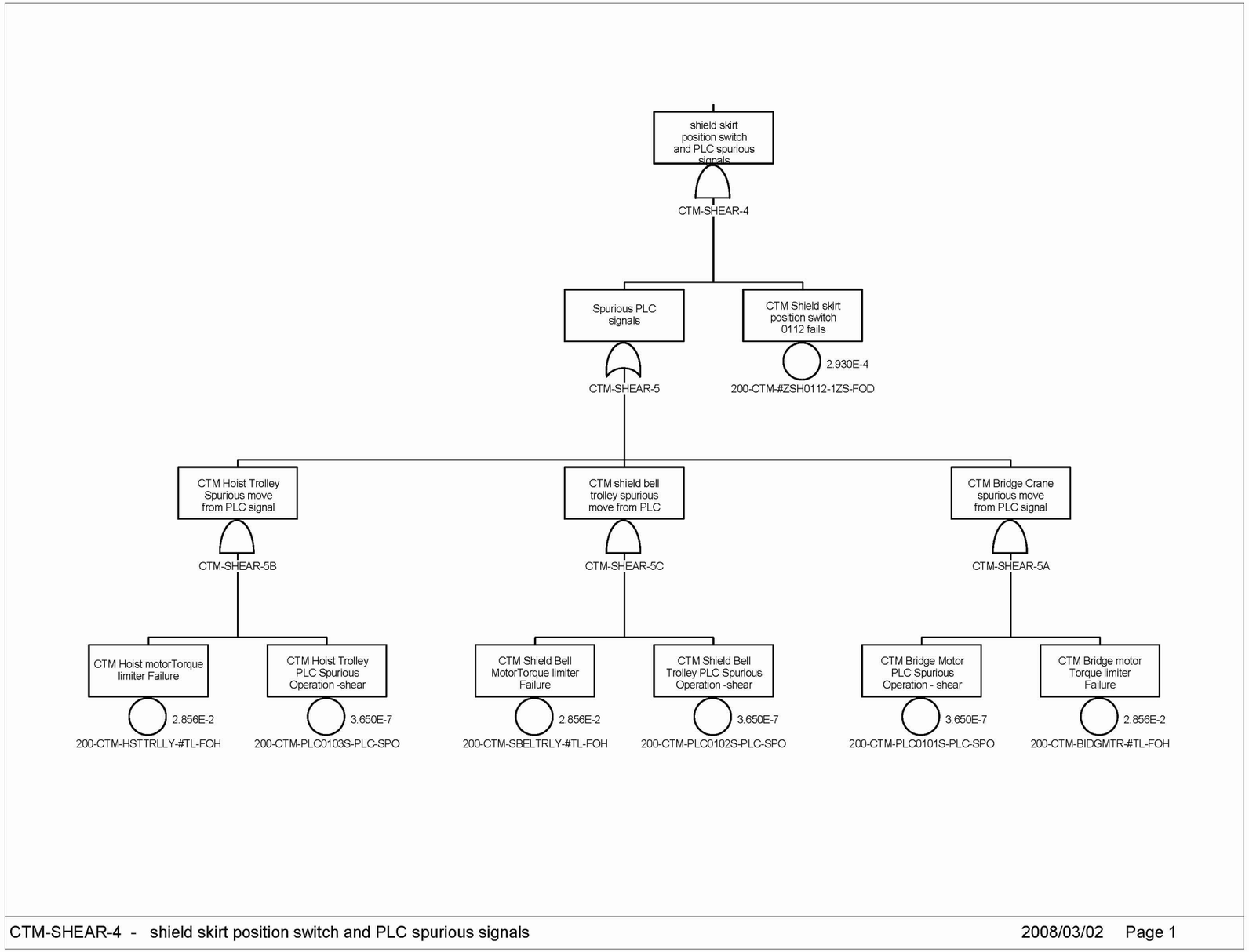
B4.4.5.8 Fault Trees



Source: Original

Figure B4.4-43. CTM Shear Sheet 1

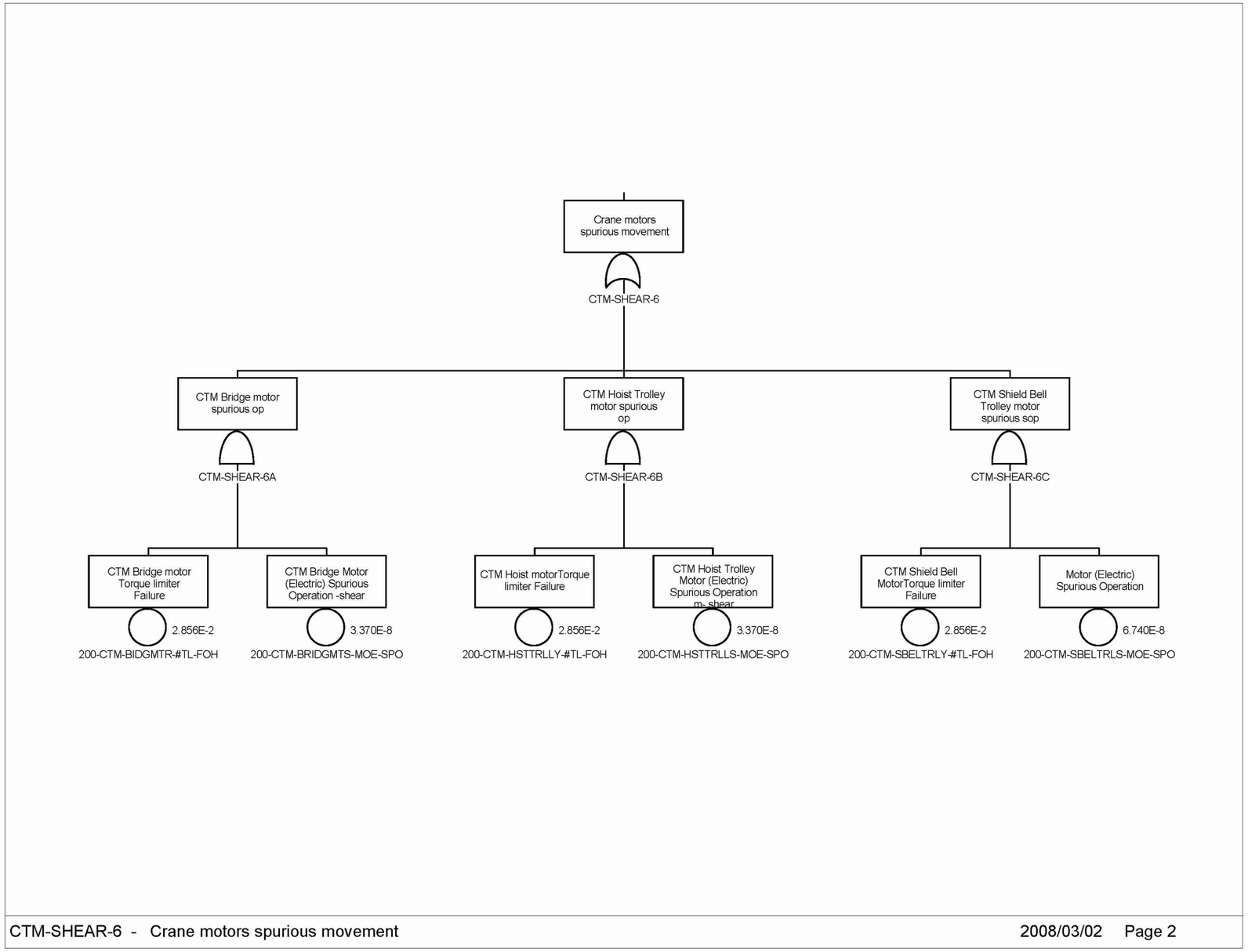
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-44. CTM Shear Sheet 2

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-45. CTM Shear Sheet 3

INTENTIONALLY LEFT BLANK

B5 CASK TRACTOR AND CASK TRANSFER TRAILER FAULT TREE ANALYSIS

B5.1 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 the PCSA.

B5.1.1 BSC (Bechtel SAIC Company) 2007. *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope*. 170-MJ0-HAT0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070518.0002. (DIRS 180896)

B5.1.2 †BSC 2007. *Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailers*. 000-3PS-HAT0-00300-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0004.

B5.2 HORIZONTAL CASK TRACTOR AND TRAILER DESCRIPTION

B5.2.1 Overview

The cask tractor and the cask transfer trailer are collectively called the horizontal cask tractor and trailer (HCTT). This equipment provides the following functions as described in Section 3.1.1 of *Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailers* (Ref. B5.1.2):

The function of the cask tractor coupled with the cask transfer trailer is to:

- Move a transportation cask loaded with a horizontal DPC from the RF to a horizontal aging module (HAM) located on aging pad 17R.
- Retrieve a horizontal DPC from the HAM, place it into the horizontal shielded transfer cask, and transport it to the WHF.

For fault tree models in SAPHIRE, the cask tractor and cask transfer trailer are collectively referred to in the code as an HCTT.

B5.2.2 Physical Description

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

jacks, (2) a cask support skid and positioning system, and (3) a hydraulic ram. The cask tractor and cask transfer trailer are depicted in *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope* (Ref. B5.1.1).

B5.3 DEPENDENCIES AND INTERACTIONS

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 B5.3-1 with the following dependencies:

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

Table B5.3-1. Dependencies and Interactions Analysis

Systems, Structures, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Hydraulic pendular axles	Vertical support and leveling during transport and load/unload	—	—	—	—
Hydraulic stabilizing jacks	Redundant vertical support during load/unload	—	—	—	—
Tractor brakes	Sufficient to stop conveyance with failed trailer brakes	—	—	—	—
Cask transfer trailer brakes	Sufficient to stop conveyance on failed tractor brakes	—	—	—	—
Vehicle steering, control, and speed limiter	Tractor/trailer control	—	—	Collision overspeed	—

Source: Original

B5.4 HORIZONTAL CASK TRACTOR AND TRAILER FAILURE SCENARIOS

A cask tractor and cask transfer trailer collision is the only failure scenario modeled. A rollover scenario was also considered, but is screened-out per Attachment E.

B5.4.1 Horizontal Cask Tractor and Trailer Collision

B5.4.1.1 Description

There are two situations modeled where a cask tractor and cask transfer trailer collision may occur and each has a unique vehicle configuration: (1) during the loading and unloading of the DPCs (the trailer is unhitched from the tractor), and (2) during transport between the facilities and HAMs when the tractor is pulling the trailer.

B5.4.1.2 Success Criteria

A collision is defined as any undesired contact of the cask tractor and cask transfer trailer with another vehicle or facility structure or equipment. Any of the steering, braking, and hydraulic system can cause this to occur, in addition to operator error.

B5.4.1.3 Design Requirements and Features

The tractor brakes are a redundant–brake design and include a backup system with a split master cylinder and an indicator light inside the cabin to warn an operator if one of the systems fails (Ref. B5.1.2, Section 3.9.1.8.b).

- The parking brakes are fail safe – The parking brakes are designed as spring-applied, with hydraulically released calipers mounted on each axle input (Ref. B5.1.2, Section 3.9.1.9.b).
- The tractor and trailer brakes are redundant – either are capable of stopping the conveyance.
- The stabilizing jacks and pendular axles are redundant vertical support systems during loading and unloading operations.
- The trailer has four pendular axles and eight axle hydraulic actuators. The pendular axle hydraulic system can sustain one actuator failure and still function properly.
- There are four stabilizing jacks, failure of any one stabilizing jack results in the failure of the stabilizing jack system.

B5.4.1.4 Fault Tree Model

The top event in this fault tree is "Horizontal Cask Tractor Trailer Collision." This is defined as an undesired contact at any speed between the cask tractor and/or cask transfer trailer with another vehicle, facility structures or equipment. Faults modeled in this tree include axle and stabilizing jack hydraulic failures and vehicle control failures (Figures B5.4-3 thru B5.4-7).

B5.4.1.5 Basic Event Data

A number of basic events are used in this fault tree, including two common-cause failure events and two human failure events as listed in Table B5.4-1.

Table B5.4-1. Basic Event Probabilities for Collision of Cask Tractor and Cask Transfer Trailer

Name	Description	Calc. Type	Calc Prob.	Fail. Prob.	Lambda	Tau	Miss. Time
200-CRWT-BRK001--BRK-FOD	Tractor Brake A fails	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00	0.00E+00
200-CRWT-BRK002--BRK-FOD	Tractor Brake B fails	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00	0.00E+00
200-CRWT-BRK003--BRK-FOD	Trailer brakes fail	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00	0.00E+00
200-CRWT-BRKCCF--BRK-CCF	CCF of both tractor brakes	C	6.86E-08	---	---	---	---
200-CRWT-LPATH--ATH--CCF	CCF of pendular axle hydraulics during load/unload	C	8.74E-05	---	---	---	---
200-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LSJATH1-ATH-FOH	Stabilizing Jack 1 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LSJATH2-ATH-FOH	Stabilizing Jack 2 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LSJATH3-ATH-FOH	Stabilizing Jack 3 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-LSJATH4-ATH-FOH	Stabilizing Jack 4 failure	3	1.78E-03	0.00E+00	8.91E-04	0.00E+00	2.00E+00
200-CRWT-TRCT-ST-STR-FOH	Tractor steering system failure	3	1.84E-05	0.00E+00	1.84E-05	0.00E+00	1.00E+00
200-CRWT-TRLR-ST-STR-FOH	Trailer steering system failure	3	1.84E-05	0.00E+00	1.84E-05	0.00E+00	1.00E+00
200-HTTCOLLIDE---G65-FOH	Speed limiter fails	3	1.16E-05	0.00E+00	1.16E-05	0.00E+00	1.00E+00
200-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HTT while leaving the RF	1	3.00E-03	3.00E-03	0.00E+00	0.00E+00	0.00E+00
200-OPHTINTCOL01-HFI-NOD	Operator causes collision of HTT due to over speed	1	1.00E+00	1.00E+00	0.00E+00	0.00E+00	0.00E+00

NOTE: See Table 6.3-1 for definitions of calculation types.
Calc. = calculation; CCF = common-cause failure; Fail. = failure; HTT = the cask tractor and cask transfer trailer referred to as the HCTT in Section 6.2; Miss. = mission; Prob. = probability; RF = Receipt Facility.

Source: Original

B5.4.1.5.1 Human Failure Events

Two human failure events are modeled in the cask tractor and cask transfer trailer collision failure scenario as follows:

1. Operator causes collision of cask tractor and cask transfer trailer while leaving the RF.
2. Operator causes collision of cask tractor and cask transfer trailer due to overspeed.

Further description of these events can be found in Attachment E.

B5.4.1.5.2 Common-Cause Failures

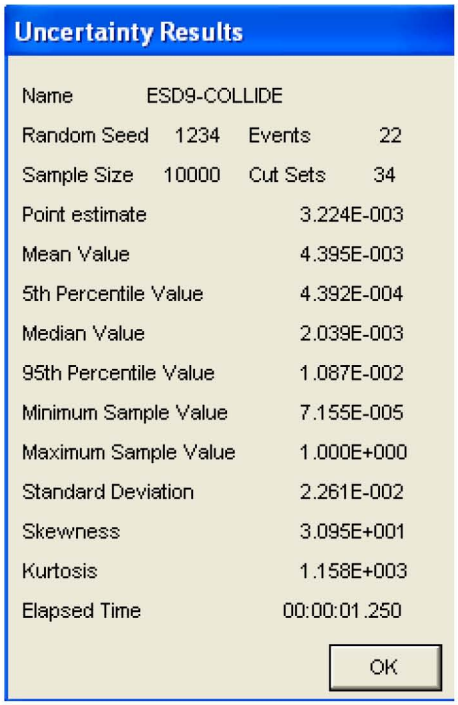
Two common-cause failure events are modeled in the cask tractor and cask transfer trailer collision failure scenario as follows:

1. Common-cause failure of the primary and redundant tractor brakes.
2. Common-cause failure of two or more pendular axle hydraulics.

The methodology used to derive the CCFs for these events is discussed in Section C3.

B5.4.1.6 Uncertainty and Cut Set Generation Results

Figure B5.4-1 contains the uncertainty results obtained from running the fault trees for "Cask Tractor and Cask Transfer Trailer Collision." Figure B5.4-2 provides the cut set generation results for the "Cask Tractor and cask Transfer Trailer Collision" fault tree, calculated using a 1E-15 cutoff.



Uncertainty Results

Name	ESD9-COLLIDE		
Random Seed	1234	Events	22
Sample Size	10000	Cut Sets	34
Point estimate			3.224E-003
Mean Value			4.395E-003
5th Percentile Value			4.392E-004
Median Value			2.039E-003
95th Percentile Value			1.087E-002
Minimum Sample Value			7.155E-005
Maximum Sample Value			1.000E+000
Standard Deviation			2.261E-002
Skewness			3.095E+001
Kurtosis			1.158E+003
Elapsed Time			00:00:01.250

OK

Figure B5.4-1. Uncertainty Results for the Cask Tractor and Cask Transfer Trailer Collision Fault Tree

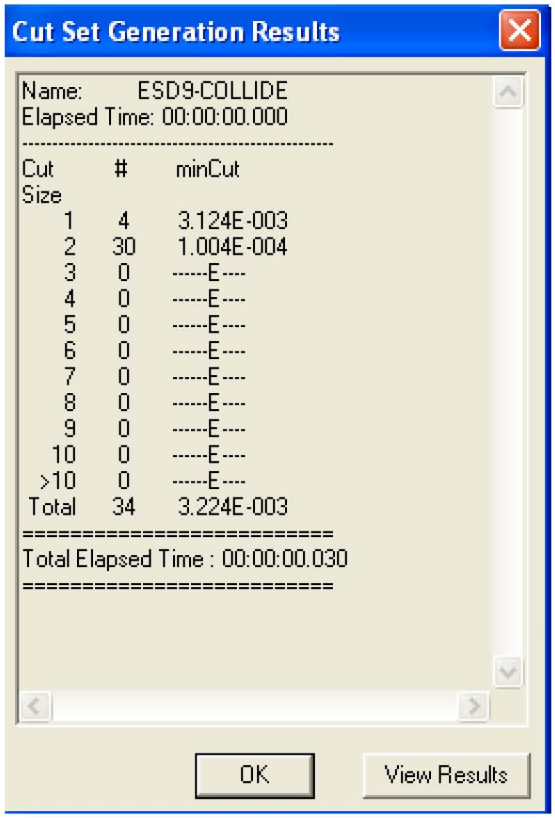


Figure B5.4-2. Cut Set Generation Results

B5.4.1.7 Cut Sets

Table B5.4-2 contains the cut sets for the collision of the cask tractor and cask transfer trailer.

Table B5.4-2. Cut Set for Collision of Cask Tractor and Cask Transfer Trailer

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
200-HCTT-COLLISION	93.06	3.000E-003	200-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HTT while leaving the RF	3.000E-003
	2.71	8.735E-005	200-CRWT-LPATH--ATH--CCF	CCF of pendular axle hydraulics during load/unload	8.735E-005
	0.57	1.840E-005	200-CRWT-TRCT-ST-STR_FOH	Tractor steering system failure	1.840E-005
	0.57	1.840E-005	200-CRWT-TRLR-ST-STR-FOH	Trailer steering system failure	1.840E-005
	0.36	1.160E-005	200-HTTCOLLIDE---G65-FOH	Speed limiter fails	1.160E-005
			200-OPHTINTCOL01-HFI-NOD	Operator causes collision of HTT due to over speed	1.000E+000

Table B5.4-2. Cut Set for Collision of Cask Tractor and Cask Transfer Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
200-HCTT-COLLISION (continued)	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
			200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
			200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
			200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
			200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003

Table B5.4-2. Cut Set for Collision of Cask Tractor and Cask Transfer Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
200-HCTT-COLLISION (continued)	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
			200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
			200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
			200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003

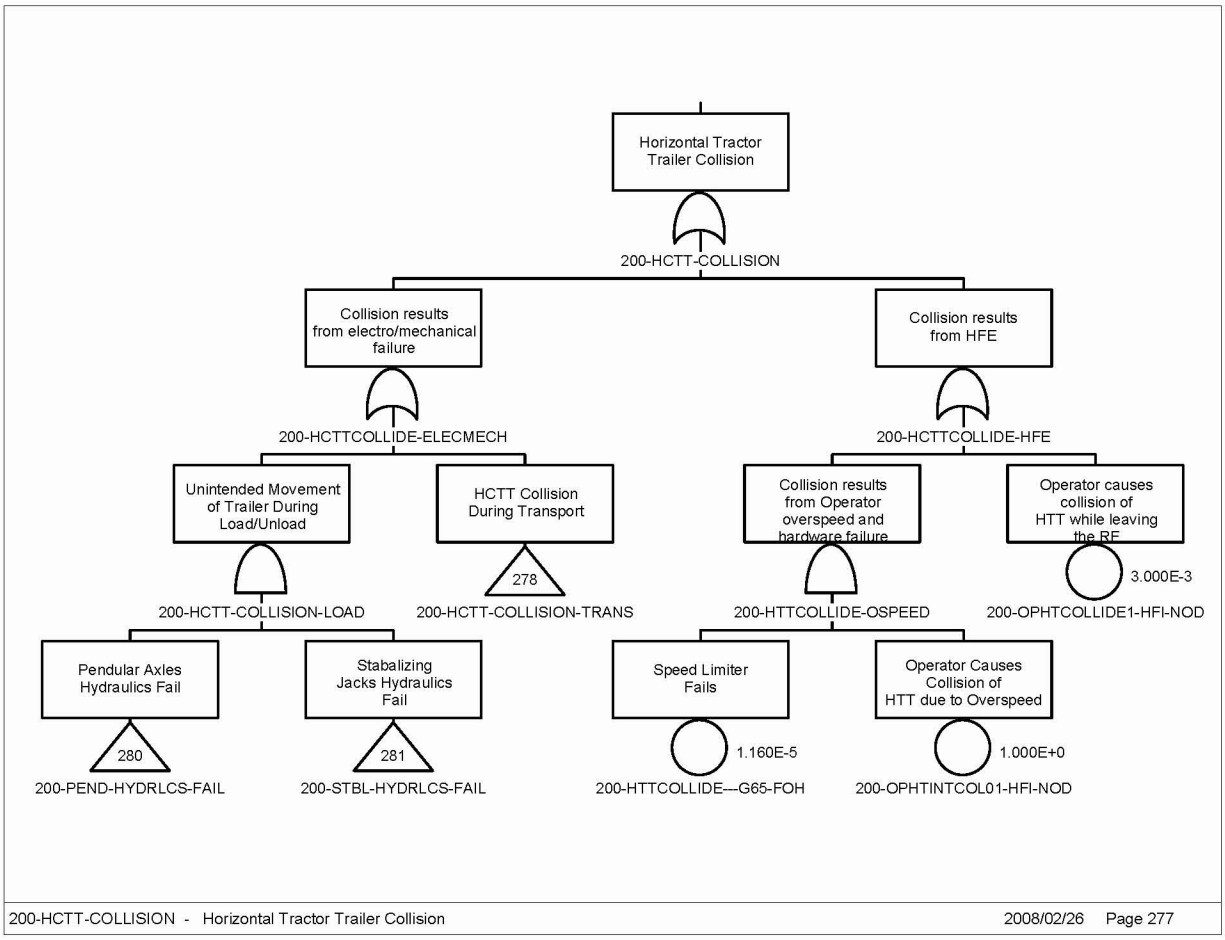
Table B5.4-2. Cut Set for Collision of Cask Tractor and Cask Transfer Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
200-HCTT-COLLISION (continued)	0.10	3.170E-006	200-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.10	3.170E-006	200-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-003
			200-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-003
	0.00	1.002E-013	200-CRWT-BRK003--BRK-FOD	Trailer brakes fail	1.460E-006
			200-CRWT-BRKCCF--BRK-CCF	CCF of both tractor brakes	6.862E-008

NOTE: CCF = common-cause failure; HTT = the cask tractor and cask transfer trailer referred to as the HCTT in Section 6.2; No. = number; Prob. = probability; RF = Receipt Facility.

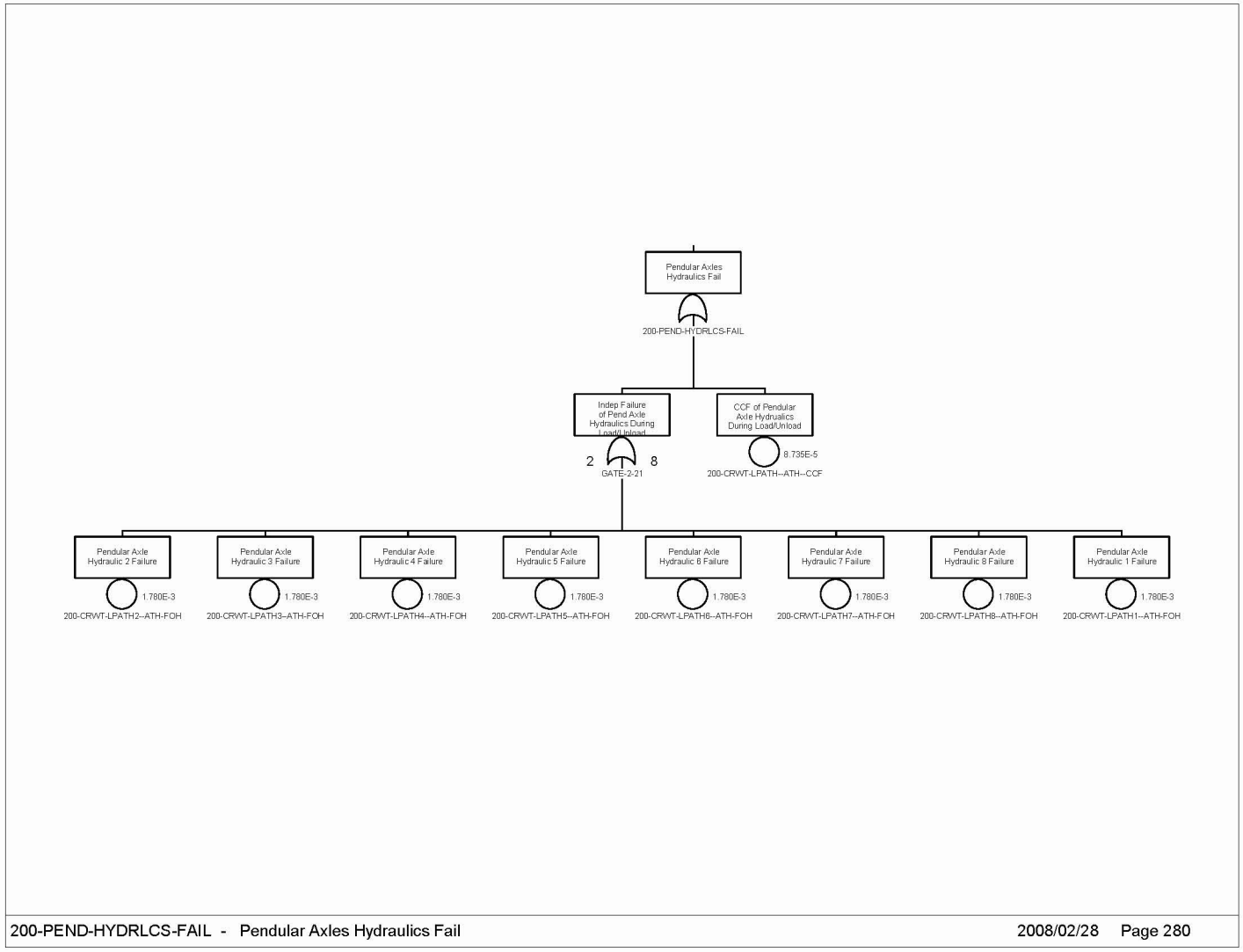
Source: Original

B5.4.1.8 Fault Trees



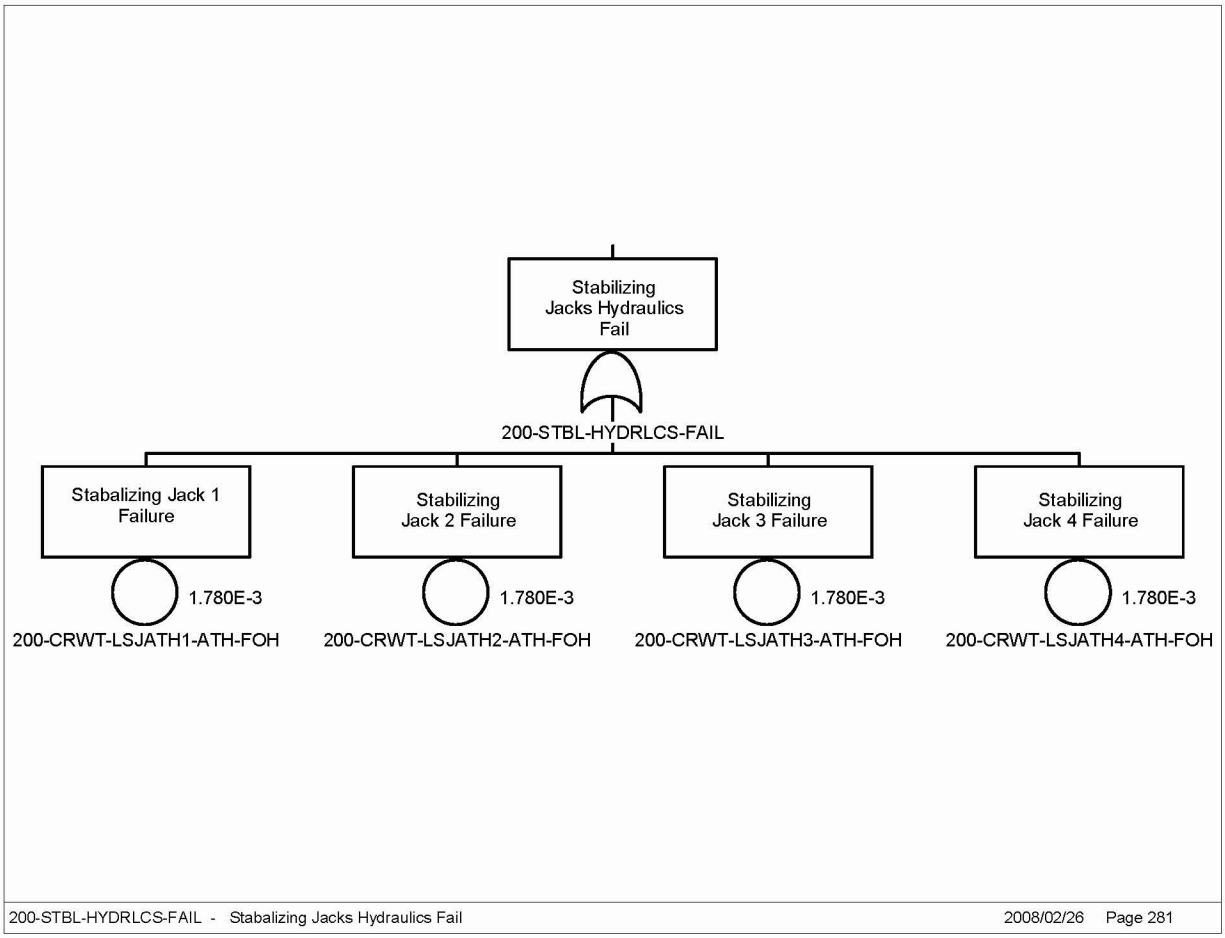
Source: Original

Figure B5.4-3. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision



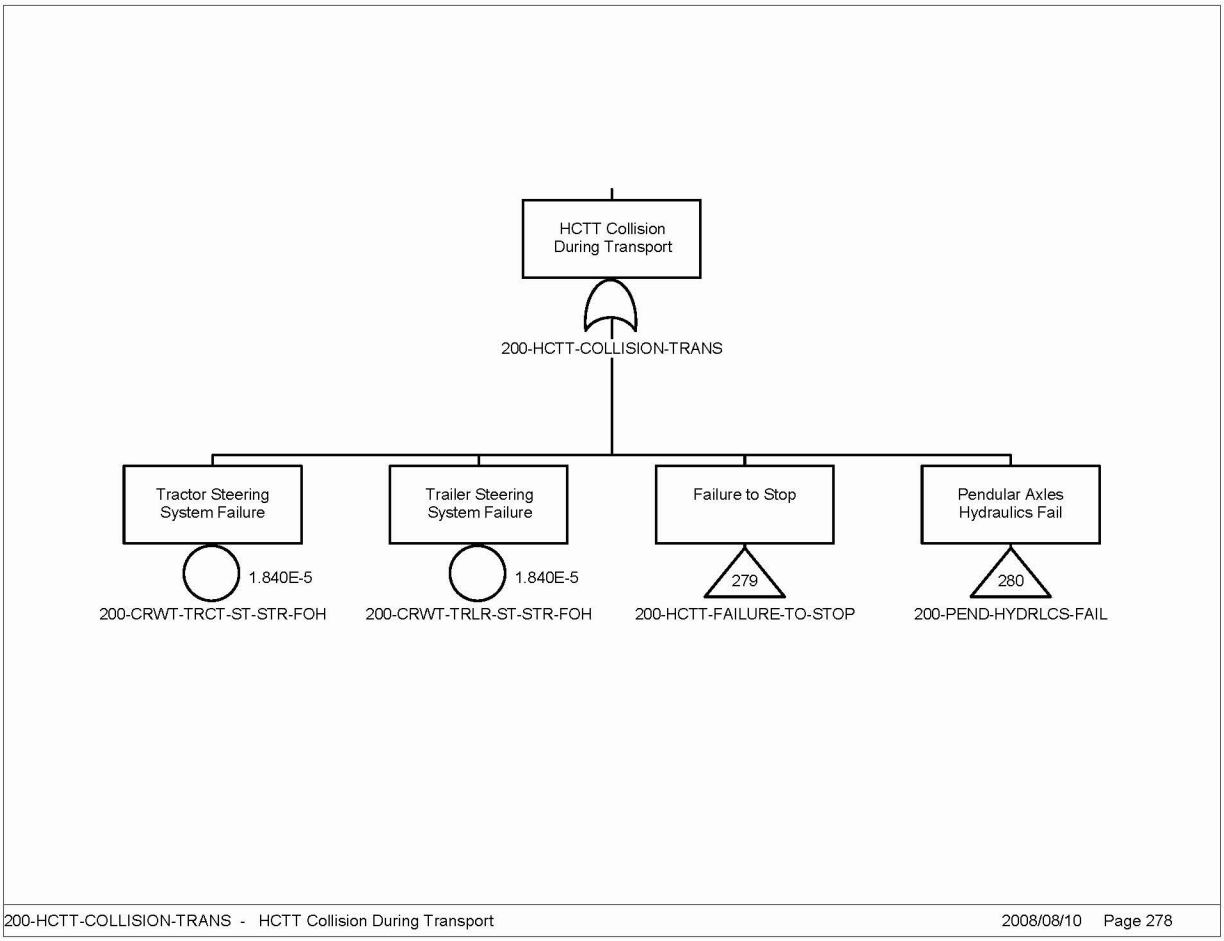
Source: Original

Figure B5.4-4. Fault Tree for Pendular Axles Hydraulics Fail



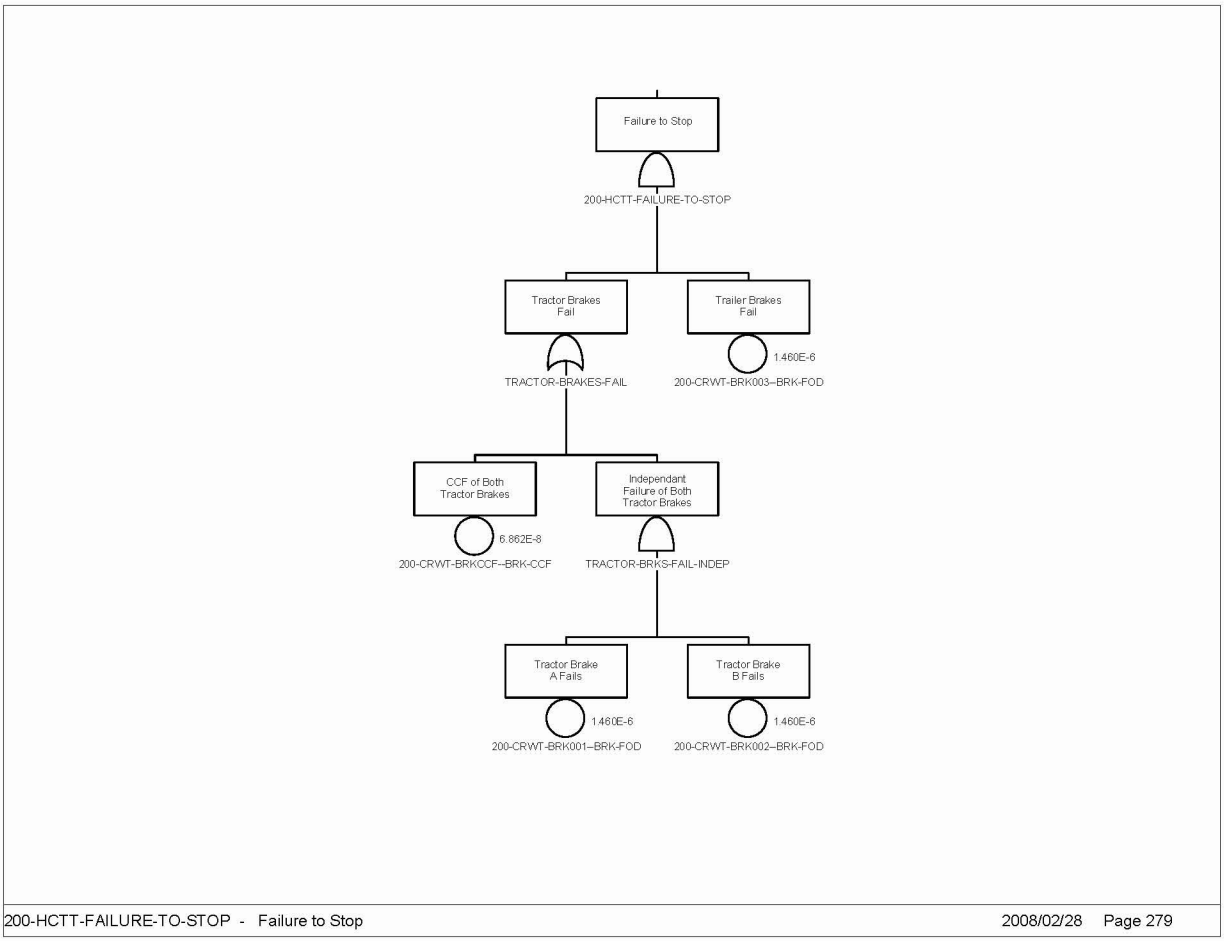
Source: Original

Figure B5.4-5. Fault Tree for Stabilizing Jacks Hydraulics Fail



Source: Original

Figure B5.4-6. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision during Transport



Source: Original

Figure B5.4-7. Fault Tree for Failure to Stop

B6 SITE TRANSPORTER FAULT TREE ANALYSIS

B6.1 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 (†).

B6.1.1 †BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report - Site Transporter*. 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.

B6.1.2 BSE 2007. *Exhibit D, Statement of Work for Mechanical Handling Equipment Design*. 000-3SW-MGR0-00100-000 Rev. 003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070904.0031.

B6.1.3 Morris Material Handling 2007. *P&ID Site Transporter*. V0-CY05-QHC4-00459-00049-001 Rev. 004. Oak Creek, Wisconsin: Morris Material Handling. ACC: ENG.20071022.0012.

B6.2 SITE TRANSPORTER DESCRIPTION

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a cylindrical concrete and steel ventilated aging overpack. The transport occurs both Intra-Site and within the CRCF, the WHF, and the RF[1]. In the RF, the site transporter is only used during the loading of aging overpacks with a DPC or TAD canister, and for removing the loaded aging overpack from the facility.

Movement of the site transporter within the RF is limited to the Loading Room, Lid Bolting Room, and the Site Transporter Vestibule.

B6.2.1 Overview

The interface between the site transporter and the aging overpack is via two parallel rectangular lift slots that pass through the containers near their lower ends. Orientation of the aging overpack is such that the axis of the aging overpack is vertical with lid, at the top. Access to the top of the aging overpack is unobstructed.

[1]Variations in the use of the site transporter for Intra-Site, WHF and CRCF are addressed in their respective volumes.

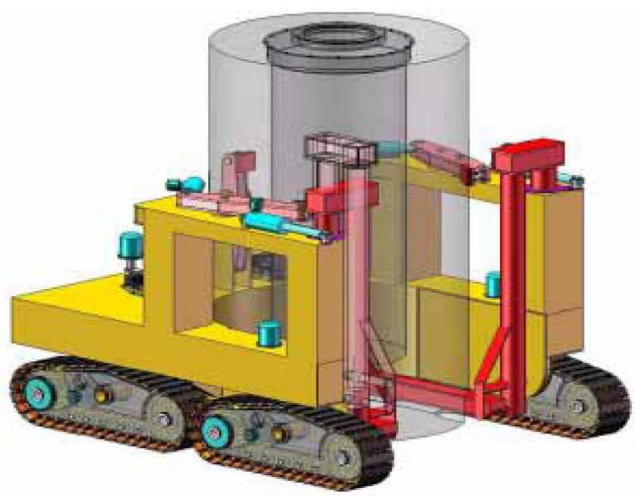
An integrated diesel powered electric generator provides the electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable from the facility main electrical supply (Ref. B6.1.1, Section 2.1).

The site transporter is a track driven vehicle with four synchronized tracks (two on each side of the site transporter). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not ITS.

A rear fork assembly consists of a pair of arms that extend to the front of the site transporter. These forks move up and down for the purpose of raising, lowering, and supporting the aging overpack during movement. A pair of support arms is located at the front of the site transporter which is moved into position around the forks to provide support and assistance during the lifting and lowering of the aging overpack.

A passive restraint system stabilizes the aging overpack during movement. There are two mechanisms that control aging overpack movement on the pitch and roll axis. These restraints are not engaged until the aging overpack has been raised to the desired height. Once engaged, three pins are inserted, one in each restraint arm, that keep the restraints in place should there be a failure of the electromechanical assembly used to position and secure the restraint device. They also serve as an interlock that prevents movement of a loaded site transporter if they are not properly installed.

Control of the site transporter is provided by a wireless remote control or a wired pendant. Although these devices only provide a subset of the controls and indicators that are available on the control console located on the site transporter, they do contain all the necessary controls and indicators to perform and monitor the operation state of the site transporter during normal operations. The site transporter is shown in Figure B6.2-1.



Source: Ref. B6.1.1

Figure B6.2-1. Site Transporter

The site transporter system is composed of six subsystems:

1. Crawler Tracks Subsystem—four crawlers, two on each side of the site transporter, are used to move the vehicle. These crawlers use tracks with chamfered flat steel plates mounted to double grouser shoes on a continuous chain.

2. Power Plant Subsystem—a diesel engine, generator, and diesel fuel tank are enclosed in the back of the site transporter. During Intra-Site Operation activities, the diesel engine will drive 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 operate the vehicle.

3. Rear Lift Fork Subsystem—the site transporter contains a pair of arms that extend forward from the site transporter through slots in the aging overpack. The lift/lower drive system utilizes an ACME type nut that changes the elevation of the fork as the screw lift mechanism turns through the ACME nut. A lift synchronizer controls the lift/lower operation.

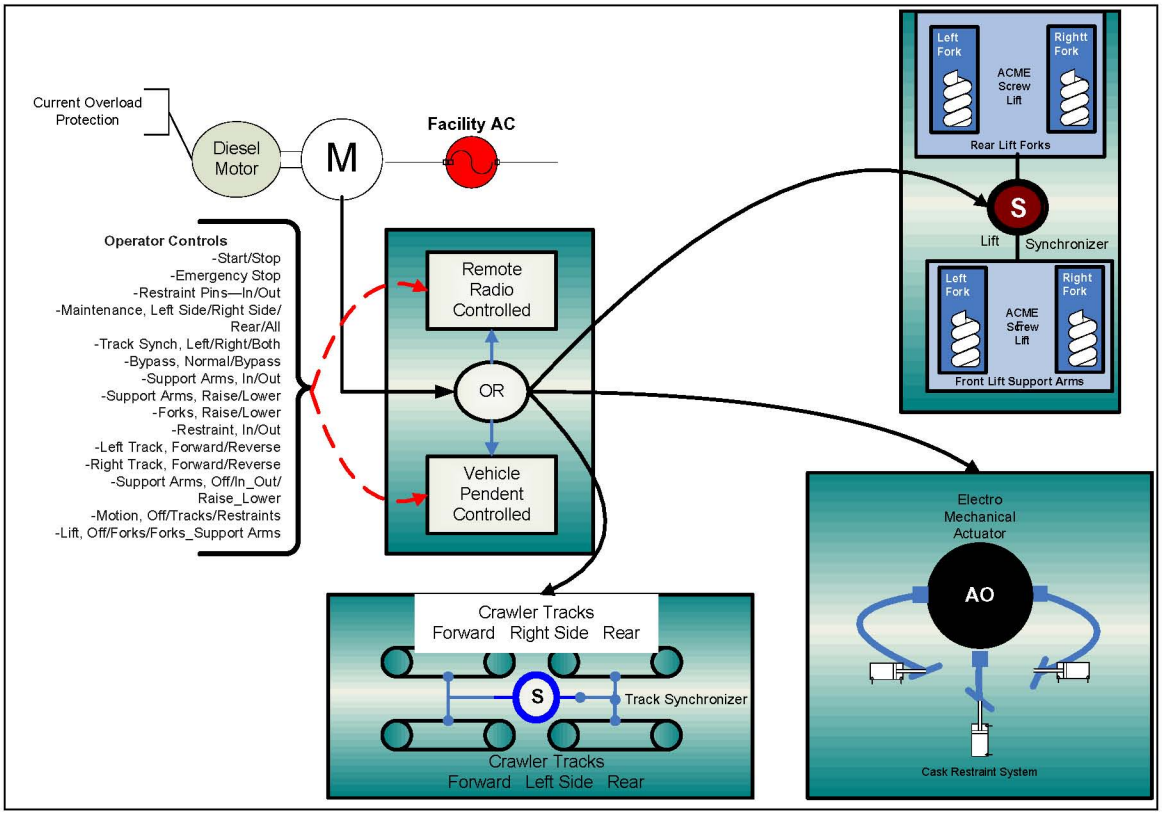
4. Lift Support Arms Subsystem—two support arms with electromechanical actuators are located on the front of the site transporter. These support arms are rotated 90 degrees to provide support and stabilization for the lift forks during lifting/lowering/moving operations. ACME nuts are used on these arms and synchronized with the lift forks during lifting/lowering/moving.

5. Restraint Subsystem—a two axis restraint system is incorporated to stabilize the aging overpack during site transporter movement. The restraints are emplaced/retracted with electromechanical actuators. These restraints, when positioned against the aging overpack will be secured with a locking pin. The three pins serve as an interlock and must be properly installed before the site transporter can be moved.

6. Vehicle Controls Subsystem—there are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter.

Note: In addition to the six subsystems identified above, *Mechanical Handling Design Report – Site Transporter* (Ref. B6.1.1) also includes a description of the site transporter "car body." Events associated with car body failure are screened from this analysis based on the results of the stress analysis contained in this reference.

A simplified block diagram of the functional subsystems on the site transporter is shown in Figure B6.2-2.



NOTE: AO = aging overpack.

Source: Original

Figure B6.2-2. Simplified Block Diagram of the Site Transporter Subsystems

B6.2.1.1 Site Transporter Crawler Tracks Subsystem Description

The site transporter moves by four tracks mounted on the crawler frames, with two on each side of the vehicle to increase stability when traversing terrain that includes sudden changes in elevation such as a drainage trough or curb. The site transporter is designed to negotiate roadways with a 5% grade and up to a 2% cross-slope (Ref. B6.1.2, Section 7.2.2-11). Special pads are included on the tracks to reduce the wear and tear on concrete or roadways.

Each track is driven by its own electric motor (50 hp at 900 rpm) through its own gear reduction and final chain drive reduction. During forward operations, motors on both sides of the machine drive are synchronized. During turns the outside tracks are driven faster, and for very sharp turns the tracks are counter-rotated to turn the site transporter about its own vertical centerline (Ref. B6.1.1, Section 2.1.2).

B6.2.1.2 Power Plant Subsystem Description

The power plant subsystem supplies the site transporter with 480 V AC, 3-phase power at 60 Hz. Because of the risk of contamination from their various fluids, there are no storage batteries or capacitors in the system. The generator is sized approximately at 110% of than the highest power requirement for the vehicle.

The 150 kW generator is sized for seven hours of continuous operation with a fuel tank containing approximately 100 gallons of diesel fuel (Ref. B6.1.1, Section 2.2.3). The fuel tank capacity is sized to minimize the amount of fuel taken inside the facilities but sufficient to transport a loaded aging overpack three miles and return to the site transporter's point of origin without refueling (Ref. B6.1.2, Section 7.2.2-2).

When entering a building the generator is shut down and a power source from the building is plugged into the site transporter integral receptacle to allow the site transporter to operate inside the building without a source of combustion.

The motor drive and current over load protection system prevents the site transporter from exceeding 2.5 mph (Ref. B6.1.1, Section 3.2.1).

B6.2.1.3 Rear Lift Forks Subsystem Description

The rear forks are only capable of moving up or down. Each fork is driven by its own gear reduction and 16 hp, 900 rpm electric motor. The output of the drive is a rotating ACME type screw, which, as it turns inside the rear forklift tube, drives an ACME nut that raises or lowers the fork. The height of the rear lift fork is controlled by limit switches as well as being mechanically unable to lift an aging overpack higher than 12 in. above the floor or ground (Ref. B6.1.1, Sections 2.1.4 and 2.2).

B6.2.1.4 Lift Support Arms Subsystem Description

The front support arms have constrained movement which consists of a clockwise/counterclockwise rotation and up and down movement. The right and left assemblies are mirror images of one another and move as a synchronous pair although they are each driven by their own gear reduction and 20 hp, 900 rpm electric motor (Ref. B6.1.1, Section 2.1.5).

The operator positions the lift support arms around the lifting forks. After the site transporter has been positioned properly around the aging overpack, the rear forks are raised to contact the bottom of the aging overpack's lifting slots. Limit and position switches ensure the lift support arms are in the correct position. Additional limit switches prevent the support arms from exceeding the 12-in. lift.

B6.2.1.5 Restraints Subsystem Description

When the load on the site transporter is ready to be lifted, the three arms of the restraint system are activated and moved to a location "near" the aging overpack. This location is determined by a combination of operator observation and integral limit switches.

After the aging overpack has been raised to the specified transportation height, the restraint arms are engaged to hold the aging overpack in place during movement. The arms are moved by linear electromechanical actuators. In addition, a locking pin is utilized to take extreme loads as well as serve as an interlock device. The three restraint arms must be properly pinned before the interlock will allow the site transporter to be moved (Ref. B6.1.3, Sheet 1 of 3).

B6.2.1.6 Vehicle Controls Subsystem Description

The site transporter can be operated in two modes: a remote (wireless) control and an operator controlled pendant (Ref. B6.1.1, Section 2.1.7). Both of these devices have the same capability. Table B6.2-1 contains a list of controls that are available on the controller and the corresponding activation device (Ref. B6.1.3, Sheet 3).

Table B6.2-1. Site Transporter Remote or Pendant Controls

Site Transporter Operation	Activation Device on Controller
Start/stop	Pushbutton
Emergency stop	Palm button
Restraint pin—engage (in)/disengage (out)	Selector switch
Maintenance—left side/right side/rear/all	Keyed selector switch
Track synch—left/right/both	Selector switch
Bypass—normal/bypass	Keyed selector switch
Support arms—in/out	Induction pushbutton
Support arms—raise/lower	Induction pushbutton
Forks—raise/lower	Induction pushbutton
Restraint—in/out	Induction pushbutton
Left Track—forward/reverse	Induction pushbutton
Right Track—forward/reverse	Induction pushbutton
Support Arms—off/in_out/raise_lower	Selector switch
Motion—off/tracks/restraints	Selector switch
Lift—off/forks/forks_support arms	Selector switch

Source: Original

All safety interlocks and controls of the site transporter are hard-wired between the specific relays, drives, circuit breakers, and other electrical equipment. No PLC or computer is used to control the machine.

B6.2.2 Normal Operations

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

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. Once the site transporter arrives at the facility, the operator stops the vehicle outside the Site Transporter Vestibule and turns off the diesel generator. An electrical umbilical cord is manually retrieved from inside the building and attached to the site transporter. The site transporter is never operated inside the RF on diesel power.

Once inside the building, the operator positions the site transporter in the Loading Room. When work is being performed on the aging overpack, the site transporter operator will remove the pins from the restraint arms and disengage them from the aging overpack. The movement interlock is engaged when the pins are removed. The operator will then lower the aging overpack to the

floor. The procedure is reversed when it is necessary to move the site transporter again inside the facility or to transport the aging overpack to some other location. Once outside the RF, the operator shuts down the site transporter and removes the electrical cable. Subsequent activities are addressed in the Intra-Site Operations analysis.

The operations used to move an unloaded aging overpack are identical but not considered in this analysis.

B6.2.3 Site Transporter Off-Normal Operations

There are four off normal conditions that could occur during the movement of an aging overpack in the RF. When any of these occur, the operator response encompasses only those actions to return the aging overpack to a safe state. These are:

1. Lowering the forks without electrical power
2. Rotating the lift support arms without electrical power
3. On-board generator fails to operate
4. Track belt fails.

In the event of a loss of power, the site transporter is designed to stop, retain its load and enter a locked mode. Upon the restoration of power the site transporter will stay in the locked mode until operator action is taken (Ref. B6.1.2, Section 7.2.3-5).

B6.2.4 Site Transporter Testing and Maintenance

Testing and maintenance of the site transporter is done on a periodic basis and does not affect the normal operations of the site transporter. Testing and/or maintenance are not performed on a site transporter loaded with an aging overpack. A site transporter that has malfunctioned or has a lighted warning light will be deemed unserviceable and turned in for maintenance. Unserviceable vehicles will not be used.

If an unserviceable state is identified during a lift/lower or movement activity, the site transporter shall immediately be placed in a safe state (as quickly as possible) and recovery actions for the site transporter will be invoked.

B6.2.5 Site Transporter System/Pivotal Event Success Criteria

A site transporter failure is the initiating event in five event sequences in the RF as shown in Table B6.2-2.

Table B6.2-2. Site Transporter Initiating Events by ESD

Site Transporter Initiating Event	Affected ESD
Site transporter spurious movement	ESD-06 Lifting and lowering a canister during transfer in CTM
Site transporter collision	ESD-07 Assembly and closure of aging overpack
Site transporter collision Site transporter rollover Site transporter load drop	ESD-08 Export of aging overpack from RF

Table B6.2-2. Site Transporter Initiating Events by ESD (Continued)

NOTE: CTM = canister transfer machine; ESD = event sequence diagram; RF = Receipt Facility.

Source: Original

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals can not be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

Requirements

Two means of stopping the site transporter are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that is the equivalent of a deadman switch.

On the loss of AC power from the facility, the site transporter immediately enters the lock mode state. The lock mode state is not reversible without specific operator action.

There is no maintenance or testing permitted on a site transporter loaded with an aging overpack.

Since the dominant contributor to site transporter collision in the facility is human error, no priority is given to either the remote or the pendant controllers.

Design Features

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

The site transporter can only perform one function at any time. It can lift an aging overpack or it can move it, but it can not perform both functions at the same time. This feature is accomplished by interlock and by power limitations inherent in the sizing of the power plant that ensures a limited amount of power for each of the electromechanical devices and drive system.

B6.3 DEPENDENCIES AND INTERACTIONS

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 B6.3-1 with the following dependencies:

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

Table B6.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Lift booms	-Material failure -ACME screw/nut	—	—	—	—
Lift support arms	-Material failure -ACME screw/nut	—	—	—	—
Restraint arms	-Material failure	—	—	—	—
Power plant	-Current overload protection fails -Safe state on	—	—	-Failure to stop -Failure to remove power cable	—
Remote control	-Spurious commands	—	—	-Improper command	-Collide with crane rigging
Tracks	—	—	—	-Failure to stop	—

Source: Original.

B6.4 RELATED FAILURE SCENARIOS

There are four basic site transporter fault trees developed for the RF. The top events for these fault trees and the variations are:

1. Site transporter collides with RF structures
2. Site transporter load drop during lift/movement
3. Site transporter tipover
4. Site transporter spurious movement.

B6.4.1 Site Transporter Collides with RF Structures (ESD-07, -08)

B6.4.1.1 Description

The fault trees for the collision events are identical. Collisions can occur as a result of human error or hardware failures (i.e., human error events are uniquely identified but all have the same screening value of 3E-3 with a lognormal error factor of 5). Hardware failures leading to a collision consist of: the site transporter fails to stop when commanded, the site transporter exceeding a safe speed, or the site transporter moves in the wrong direction.

B6.4.1.2 Success Criteria

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

The site transporter is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the site transporter 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 site transporter will immediately stop all movement and enter into lock mode safe state. The site transporter will remain in this locked mode until power is returned and the operator restarts the site transporter.

Runaway situations on the site transporter are prevented by hardware constraints. The maximum speed of the site transporter is limited by motor current overload protection (Ref. B6.1.1, Section 3.2.1). The site transporter motor speed and gearing prevents the site transporter from exceeding 2.5 mph.

The prevention of site transporter movements in the wrong direction is prevented by the limitation of the power plant that prevents simultaneous operations.

B6.4.1.3 Design Requirements and Features

The site transporter has two off-equipment control devices that have complete control over the site transporter.

The drive system consists of electric motors and a transmission constraint which will limit the maximum speed of the site transporter to 2.5 mph.

B6.4.1.4 Fault Tree Model

The fault tree model for "Site Transporter Collides with RF Structures" in the RF accounts for both human error and/or site transporter hardware problems that could result in collision. Movement within the facility is restricted and even at low speeds a collision can occur.

The fault tree considers mechanical failures that fail to stop the site transporter, events that could cause the site transporter to exceed safe speed, and events that could cause the site transporter to move in the wrong direction.

B6.4.1.5 Basic Event Data

Table B6.4-1 lists the basic events used in the site transporter collision fault tree. Uncertainty and cut set results are provide in Figures B6.4-1 and B6.4-2 respectively.

Table B6.4-1. Basic Event Probability for Site Transporter Collides with RF Structures

Basic Events Probability Report					
Project: Yucca-Mountain		Case: Current			
ST Collision in Facility		Units: Per Hour			
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-OPSTCOLLIDE2-HFI-NOD	1	3.00E-03	3.00E-03	0.00E+00	0.00E+00
200-ST---BRK001--BRK-FOD	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00
200-ST---CBP004-CBP--OPC	3	9.13E-08	0.00E+00	9.13E-08	1.00E+00
200-ST---CBP004-CBP--SHC	3	1.88E-08	0.00E+00	1.88E-08	1.00E+00

Table B6.4-1. Basic Event Probability for Site Transporter Collides with RF Structures (Continued)

Basic Events Probability Report					
Project: Yucca-Mountain		**Case: Current**			
ST Collision in Facility		**Units: Per Hour**			
Name	**Calc. Type[a]**	**Calc. Prob.**	**Fail. Prob.**	**Lambda**	**Miss. Time[a]**
200-ST---CT000---CT--FOD	1	4.00E-06	4.00E-06	0.00E+00	0.00E+00
200-ST---CT002---CT--FOH	3	6.88E-05	0.00E+00	6.88E-05	1.00E+00
200-ST---HC001--HC--FOD	1	1.74E-03	1.74E-03	0.00E+00	0.00E+00
200-ST---HC002---HC--SPO	3	5.23E-07	0.00E+00	5.23E-05	1.00E+00
200-ST---MOE000--MOE-FSO	3	1.35E-08	0.00E+00	1.35E-08	1.00E+00
200-ST---MOE021--MOE-FSO	3	1.35E-08	0.00E+00	1.35E-08	1.00E+00
200-ST---SC021---SC--FOH	3	1.28E-04	0.00E+00	1.28E-04	1.00E+00
200-ST---SC021---SC--SPO	3	3.20E-05	0.00E+00	3.20E-05	1.00E+00
200-ST---SEL021--SEL-FOH	3	4.16E-06	0.00E+00	4.16E-06	1.00E+00
LOSP-4	1	4.10E-06	4.16E-06	0.00E+00	0.00E+00

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

B6.4.1.5.1 Human Failure Events

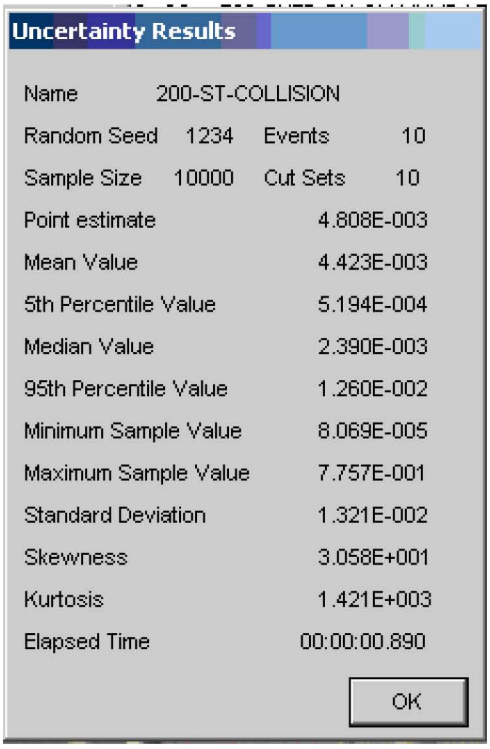
There is one human event in the collision trees for the site transporter and accounts for the site transporter operator causing the collision. This human error is set at the screening value of 3E-03 for all four ESD events.

B6.4.1.5.2 Common-Cause Failures

There are no common-cause events identified for the site transporter collision events.

B6.4.1.6 Uncertainty and Cut Set Generation Results

Figure B6.4-1 contains the uncertainty results obtained from running the fault tree for the "Site Transporter Collides with RF Structures" fault tree. Figure B6.4-2 provides the cut set generation results for the "Site Transporter Collides with RF Structures" fault tree, calculated using a 1E-15 cutoff. The fault trees are shown in Figures B6.4-3 through B6.4-5.



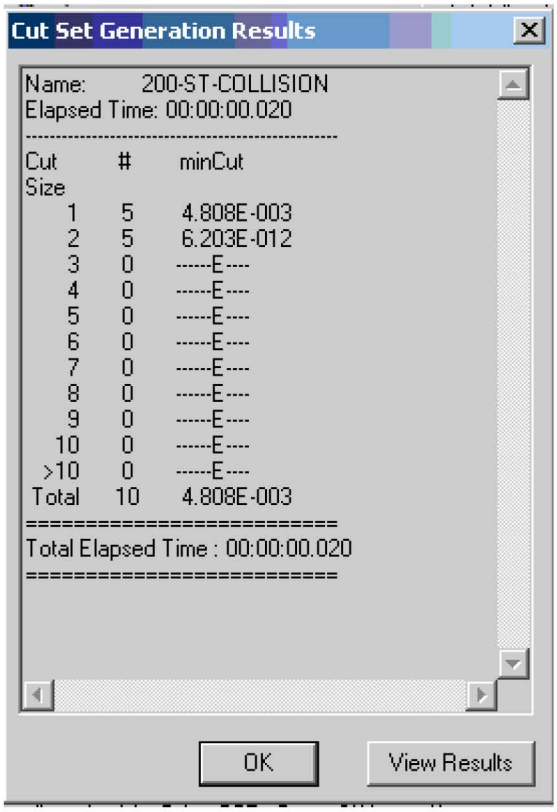
Uncertainty Results

Name	200-ST-COLLISION		
Random Seed	1234	Events	10
Sample Size	10000	Cut Sets	10
Point estimate			4.808E-003
Mean Value			4.423E-003
5th Percentile Value			5.194E-004
Median Value			2.390E-003
95th Percentile Value			1.260E-002
Minimum Sample Value			8.069E-005
Maximum Sample Value			7.757E-001
Standard Deviation			1.321E-002
Skewness			3.058E+001
Kurtosis			1.421E+003
Elapsed Time			00:00:00.890

OK

Source: Original

Figure B6.4-1. Uncertainty Results for the Site Transporter Collides with RF Structures Fault Tree



Source: Original

Figure B6.4-2. Cut Set Generation Results for the Site Transporter Collides with RF Structures Fault Tree

B6.4.1.7 Cut Sets

Table B6.4-2 contains the cut sets for the "Site Transporter Collides with RF Structures" fault tree.

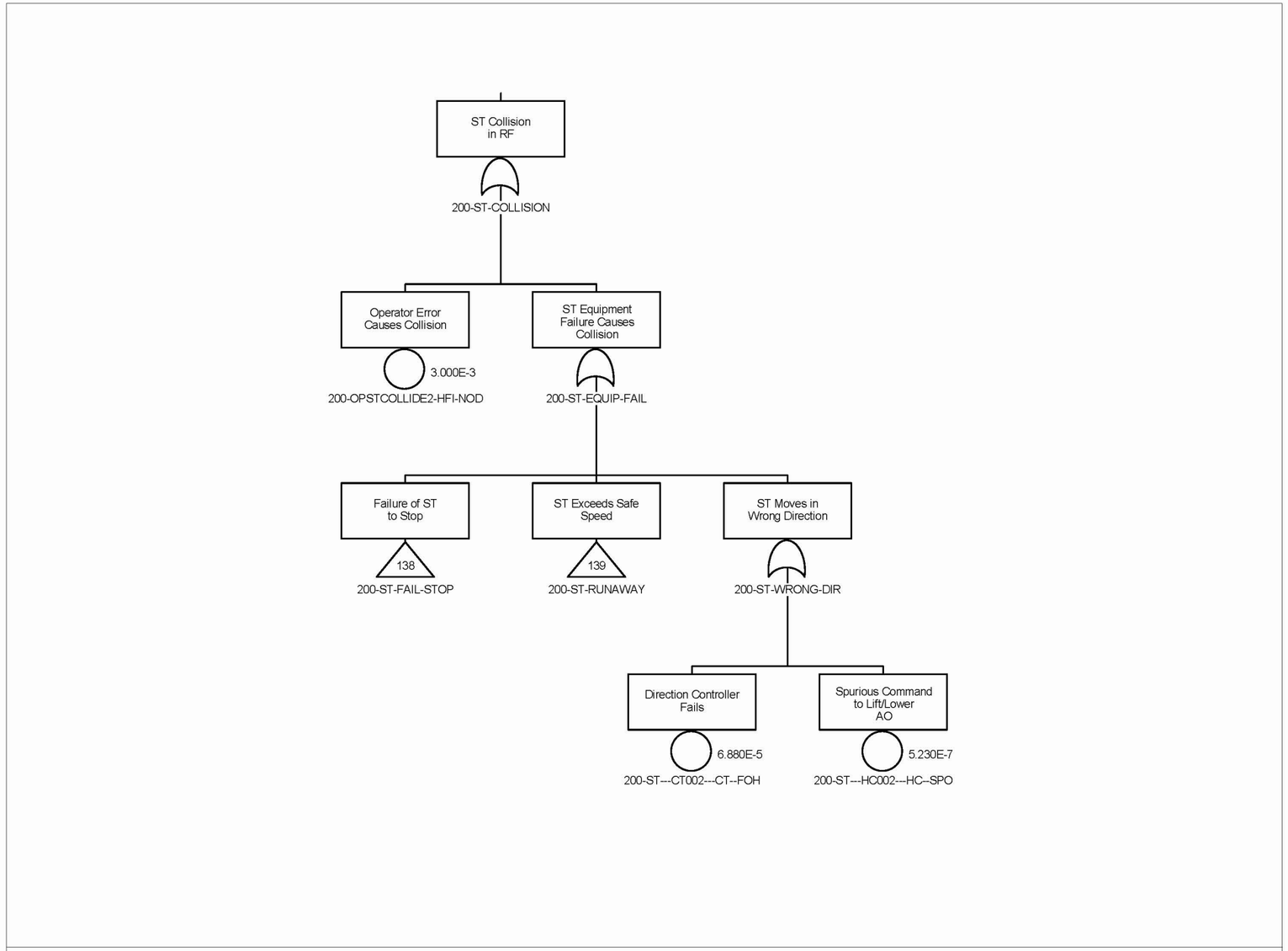
Table B6.4-2. Cut Sets for the Site Transporter Collision in Facility

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
200-ST-COLLISION	62.40	3.000E-003	200-OPSTCOLLIDE2-HFI-NOD	Operator error causes collision	3.000E-003
	36.19	1.740E-003	200-ST---HC001--HC--FOD	Remote control transmits wrong signal	1.740E-003
	1.43	6.880E-005	200-ST---CT002---CT--FOH	Direction controller fails	6.880E-005
	0.08	4.000E-006	200-ST---CT000---CT--FOD	ST primary stop switch fails	4.000E-006
	0.01	5.230E-007	200-ST---HC002---HC--SPO	Spurious command to lift/lower AO	5.230E-007
	0.00	5.986E-012	200-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-006
			LOSP-4	Failure of offsite power	4.100E-006
	0.00	1.333E-013	200-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-006
			200-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E-008
	0.00	5.535E-014	200-ST---MOE000--MOE-FSO	ST lock mode state fails on loss of power	1.350E-008
			LOSP-4	Failure of offsite power	4.100E-006
	0.00	2.745E-014	200-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-006
			200-ST---CBP004-CBP--SHC	ST power cable short circuit	1.880E-008
	0.00	1.233E-015	200-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E-008
			200-ST---MOE000--MOE-FSO	ST lock mode state fails on loss of power	1.350E-008
	4.808E-003		= Total		

NOTE: AO = aging overpack; ST = site transporter.

Source: Original

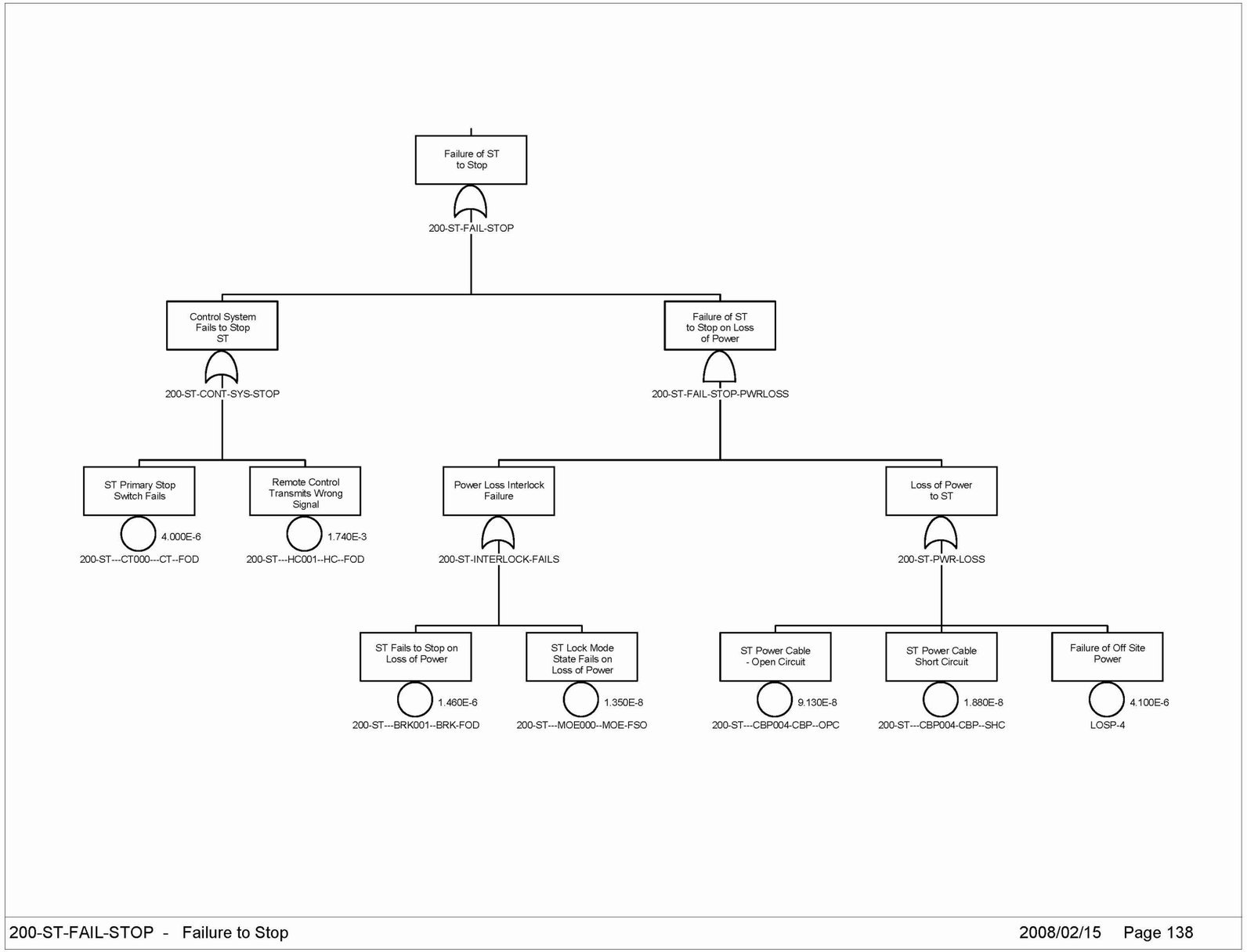
B6.4.1.8 Fault Trees



Source: Original

Figure B6.4-3. Site Transporter Collision in the RF

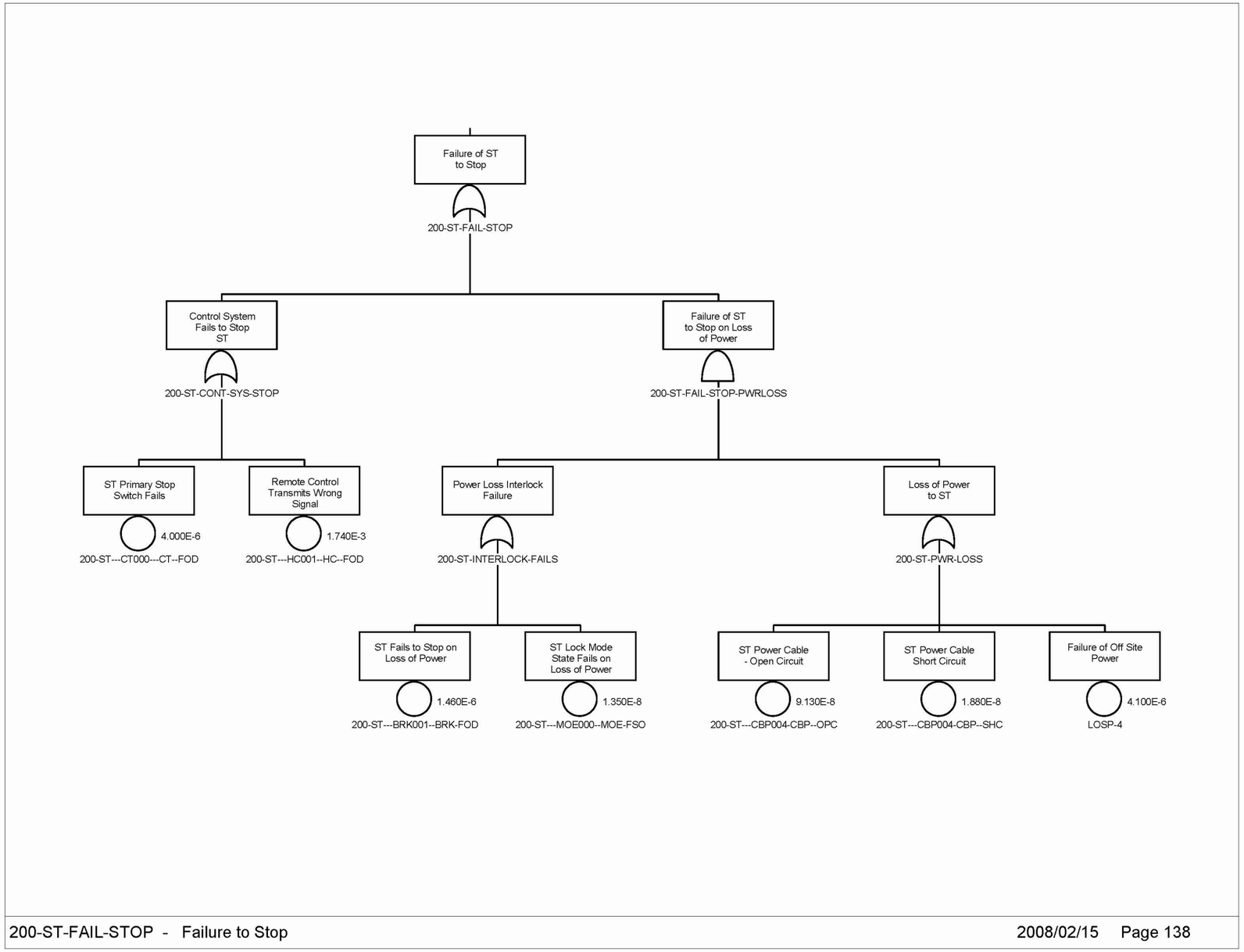
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-4. Failure to Stop

INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-5. Site Transporter Exceeds Safe Speed

INTENTIONALLY LEFT BLANK