- 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.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, 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 are 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.

B4.4.4.4 Fault Tree Model

The top event in this fault tree is "CTM collision." The CTM collision fault tree addresses potential end of run over travel events and collisions between the two CTMs. Faults considered in the evaluation of this top event include: human events that contribute to a collision and mechanical (structural) failures of the CTM components. The interlocks intended to prevent improper CTM movement are included in the model.

B4.4.4.5 Basic Event Data

Table B4.4-9 contains a list of basic events used in the CTM fault tree. Included are the HFEs and the CCF events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are 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 B4.4-9. Basic Event Probability for the CTM Collision Fault Tree

Name	Description	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	3	1.949E-006	—	4.450E-010	4.380E+003
050-CTM-BRIDGETR-MOE-FSO	CTM Shield Skirt-Bridge motor Interlock Failure	3	1.350E-008	—	1.350E-008	1.000E+000
050-CTM-BRIDGMTR-#CT-FOD	CTM bridge motor controller fails	1	4.000E-006	4.000E-006	—	—
050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motoer Interlock Failure	1	2.750E-005	2.750E-005	—	—
050-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.750E-005	2.750E-005	—	—
050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.750E-005	2.750E-005	—	—
050-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	1	3.990E-003	3.990E-003	—	—
050-CTM-TROLLEYT-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.350E-008	—	1.350E-008	1.000E+000
050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	3	1.949E-006	—	4.450E-010	4.380E+003
050-CTM-TROLYCNT-#HC-FOD	Hand Held Remote Controller Failure to Stop (on Demand)	1	1.740E-003	1.740E-003	—	—
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-008	4.000E-008	—	—
050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into endstop	1	1.000E+000	1.000E+00	—	—

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

CTM = canister transfer machine.

Source: Original

The impact modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. 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 test (i.e., mission time set to the average fault exposure time, one-half the test interval).

B4.4.4.5.1 Human Failure Events

Two basic events are associated with human error (Table B4.4-10). One addresses the movement of the CTM during a lift and the second addresses the potential overrun of the CTM (either the bridge trolley or the hoist/shield skirt trolley). The 050-OPCTIMPACT!-HFI-COD event was quantified considering human actions and the interlocks intended to prevent erroneous operator actions. The other event was quantified using screening HRA value.

Table B4.4-10. Human Failure Events

Name	Description
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor
050-OPCTMIMPACT5-HFI-COD	Operator overruns travel - collides into endstop

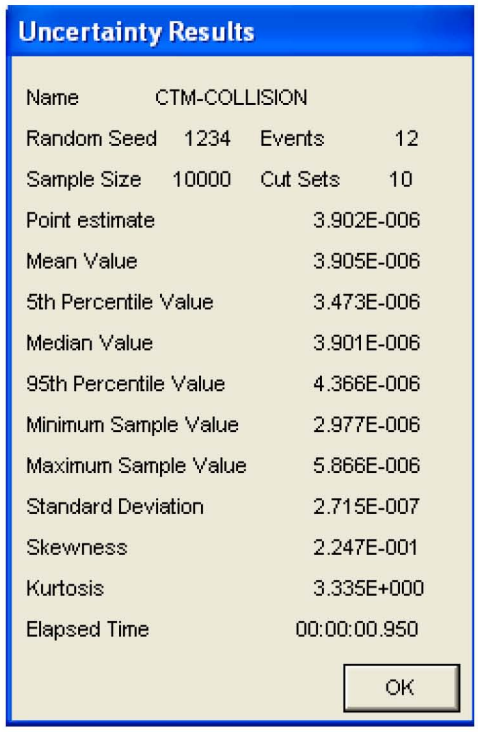
Source: Original

B4.4.4.5.2 Common-Cause Failures

There are no CCFs modeled in the CTM collision fault tree.

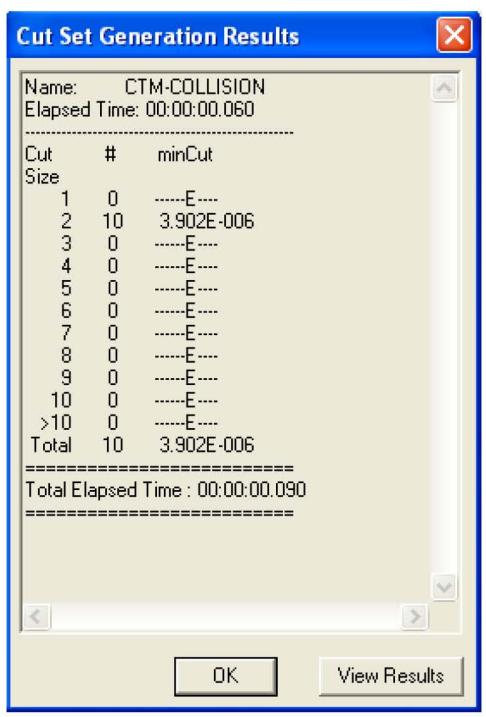
B4.4.4.6 Uncertainty and Cut Set Generation

Figure B4.4-37 contains the uncertainty results obtained from running the fault trees for the CTM collision using a cutoff at 1E-15. Figure B4.4-38 provides the cut set generation results for the CTM collision fault tree.



Source: Original

Figure B4.4-37. Uncertainty Results of the “CTM Collision” Fault Tree



Source: Original

Figure B4.4-38. Cut Set Generation Results for the “CTM Collision” Fault Tree

B4.4.4.7 Cut Sets

Table B4.4-11 contains the cut sets for the CTM collision fault tree.

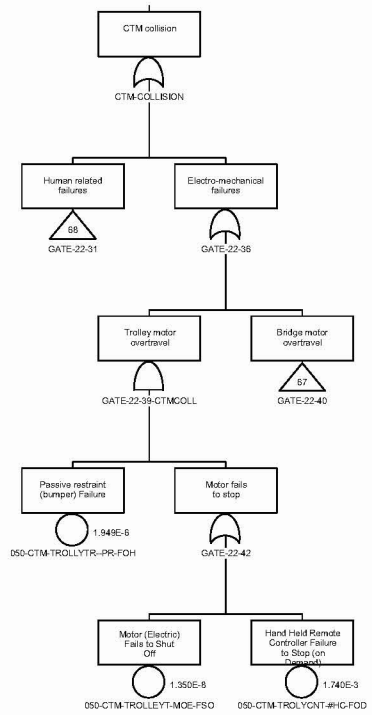
Table B4.4-11. Dominant Cut Sets for the CTM Collision Fault Tree

% Total	%Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
49.95	49.95	1.949E-006	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into endstop	1.000E+000
99.90	49.95	1.949E-006	050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into endstop	1.000E+000
99.99	0.09	3.391E-009	050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-TROLYCNT-#HC-FOD	Hand Held Remote Controller Failure to Stop (on Demand)	1.740E-003
99.99	0.00	1.596E-010	050-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	3.990E-003
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	7.796E-012	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-BRIDGMTR-#CT-FOD	CTM bridge motor controller fails	4.000E-006
99.99	0.00	1.100E-012	050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motoer Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	1.100E-012	050-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	1.100E-012	050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	2.631E-014	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-BRIDGETR-MOE-FSO	CTM Shield Skirt-Bridge motor Interlock Failure	1.350E-008

NOTE: CTM = canister transfer machine.

Source: Original

B4.4.4.8 Fault Trees

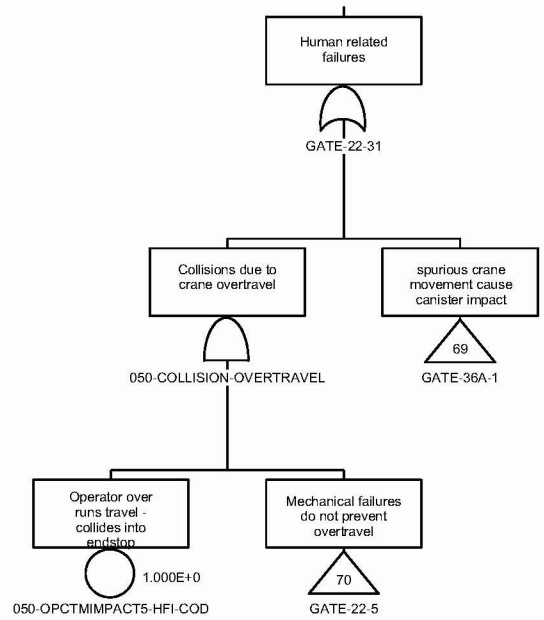


CTM-COLLISION - CTM collision 2008/03/03 Page 66

Source: Original

Figure B4.4-39. CTM Collision Sheet 1

INTENTIONALLY LEFT BLANK

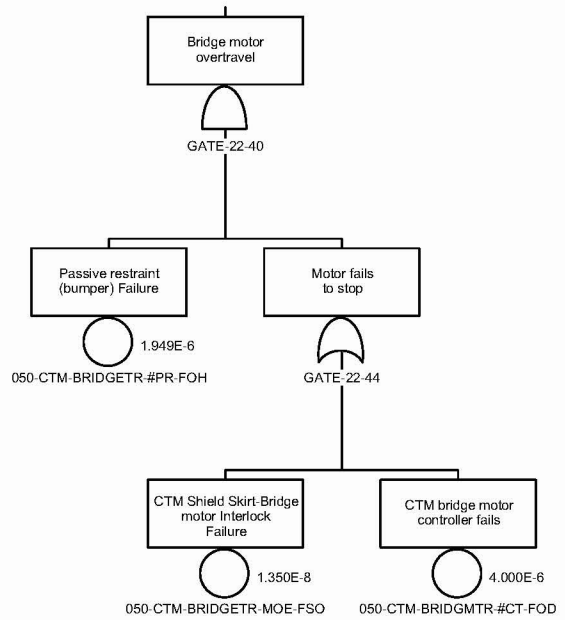


GATE-22-31 - Human related failures 2008/03/03 Page 68

Source: Original

Figure B4.4-40. CTM Collision Sheet 2

INTENTIONALLY LEFT BLANK

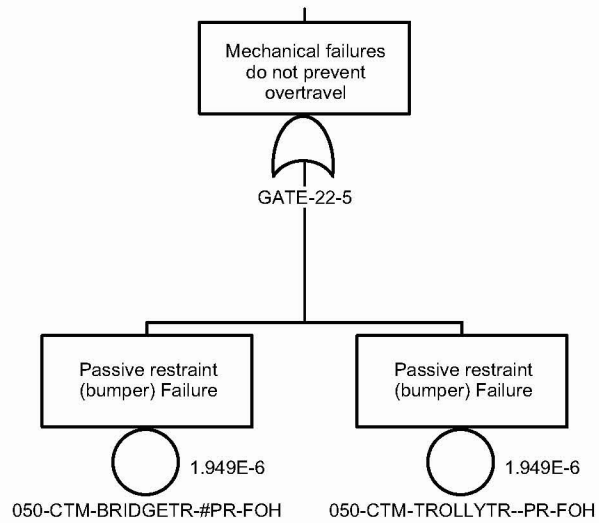


GATE-22-40 - Bridge motor overtravel 2008/03/03 Page 67

Source: Original

Figure B4.4-41. CTM Collision Sheet 3

INTENTIONALLY LEFT BLANK

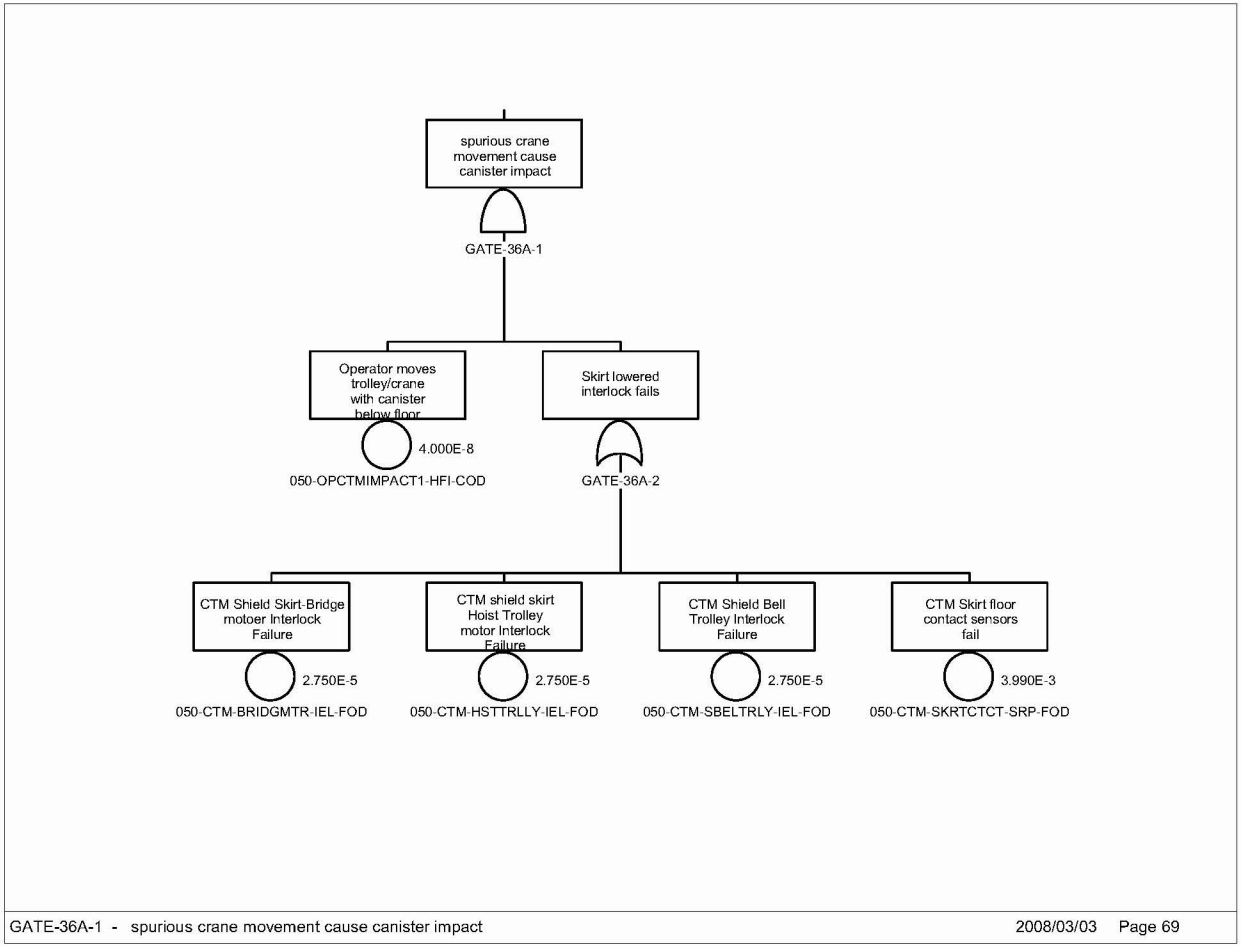


GATE-22-5 - Mechanical failures do not prevent overtravel 2008/03/03 Page 70

Source: Original

Figure B4.4-42. CTM Collision Sheet 4

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-43. CTM Collision Sheet 5

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 WHF 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 WHF 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, will stop 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.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, 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 are 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 WHF.

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 HFEs and the CCF events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are 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.

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.

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

Name	Description	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	1	2.930E-04	2.930E-04	—	—
050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	3	2.856E-02	—	8.050E-05	3.600E+02
050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	3	6.740E-08	—	6.740E-07	1.000E-01
050-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	3	6.740E-08	—	6.740E-07	1.000E-01
050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motorTorque limiter Failure	3	2.856E-02	—	8.050E-05	3.600E+02
050-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation - shear	3	3.650E-08	—	3.650E-07	1.000E-01
050-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3	3.650E-08	—	3.650E-07	1.000E-01
050-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation - shear	3	3.650E-08	—	3.650E-07	1.000E-01
050-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	3	6.740E-08	—	6.740E-07	1.000E-01
050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell MotorTorque limiter Failure	3	2.856E-02	—	8.050E-05	3.600E+02
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	—	—

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

B4.4.5.5.1 Human Failure Events

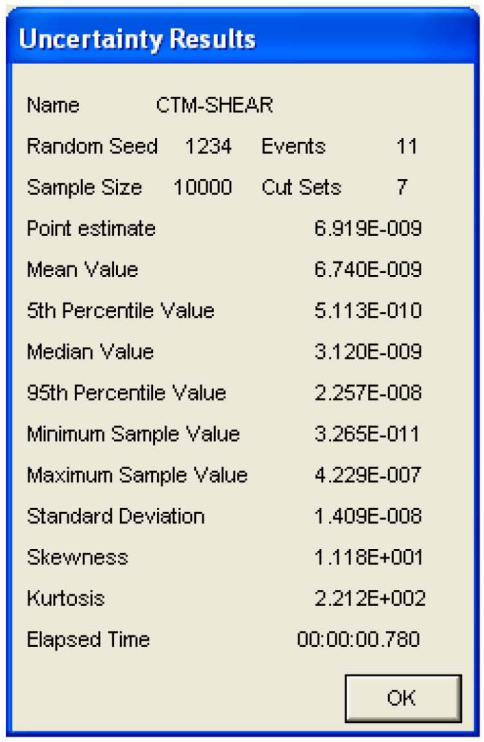
One basic event is associated with human error: 050-OPCTMIMPACT1-HFI-COD (operator moves trolley/crane with canister below floor). This event addresses the possible operator initiated movement of the bridge or trolleys while a canister is being lifted and is between WHF floors. This event was quantified using a detailed HRA that includes the human actions and the operation of interlocks intended to prevent erroneous actions.

B4.4.5.5.2 Common-Cause Failures

No CCFs apply to this fault tree.

B4.4.5.6 Uncertainty and Cut Set Generation

Figure B4.4-44 contains the uncertainty results obtained from running the fault trees for the CTM-SHEAR using a cutoff at 1E-15. Figure B4.4-45 provides the cut set generation results for the CTM-SHEAR fault tree.



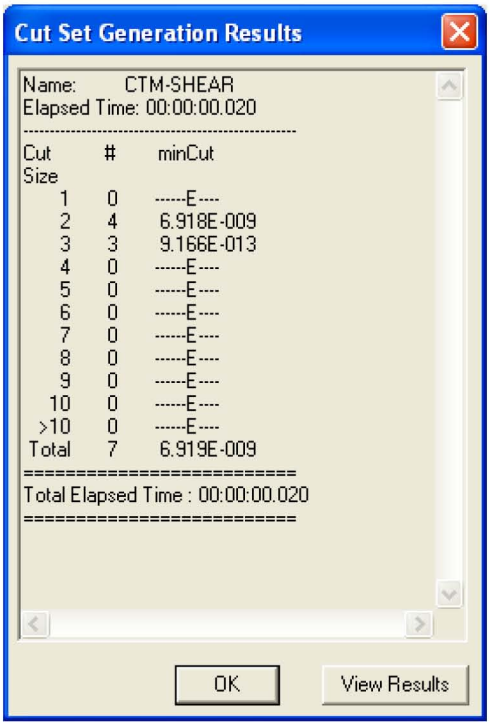
Uncertainty Results

Name	CTM-SHEAR		
Random Seed	1234	Events	11
Sample Size	10000	Cut Sets	7
Point estimate			6.919E-009
Mean Value			6.740E-009
5th Percentile Value			5.113E-010
Median Value			3.120E-009
95th Percentile Value			2.257E-008
Minimum Sample Value			3.265E-011
Maximum Sample Value			4.229E-007
Standard Deviation			1.409E-008
Skewness			1.118E+001
Kurtosis			2.212E+002
Elapsed Time			00:00:00.780

OK

Source: Original

Figure B4.4-44. Uncertainty Results of the “CTM Shear” Fault Tree



Source: Original

Figure B4.4-45. Cut Set Generation Results for the "CTM Shear" Fault Tree

B4.4.4.7 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 Shear Fault Tree

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
27.82	27.82	1.925E-09	050-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	6.740E-08
			050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell MotorTorque limiter Failure	2.856E-02
55.64	27.82	1.925E-09	050-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	6.740E-08
			050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motorTorque limiter Failure	2.856E-02
83.46	27.82	1.925E-09	050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	6.740E-08
99.97	16.51	1.143E-09	050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motorTorque limiter Failure	2.856E-02
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-08

Table B4.4-13. Dominant Cut Sets for the CTM Shear Fault Tree (Continued)

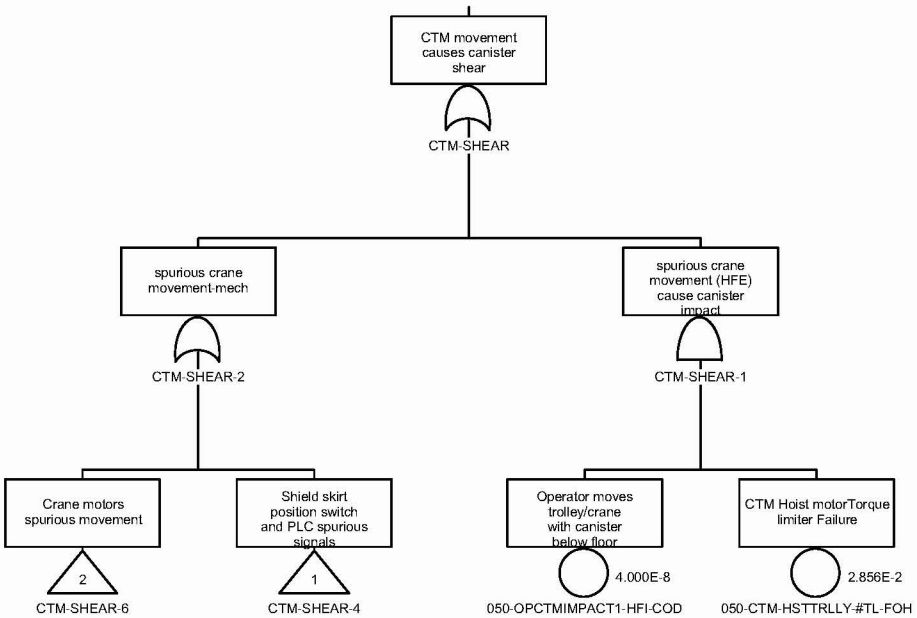
% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
99.97	0.00	3.055E-13	050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	2.930E-04
			050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			050-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3.650E-08
99.97	0.00	3.055E-13	050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	2.930E-04
			050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motorTorque limiter Failure	2.856E-02
			050-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -shear	3.650E-08
99.97	0.00	3.055E-13	050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	2.930E-04
			050-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3.650E-08
			050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell MotorTorque limiter Failure	2.856E-02

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

Source: Original

B4.4.5.8 Fault Tree

INTENTIONALLY LEFT BLANK

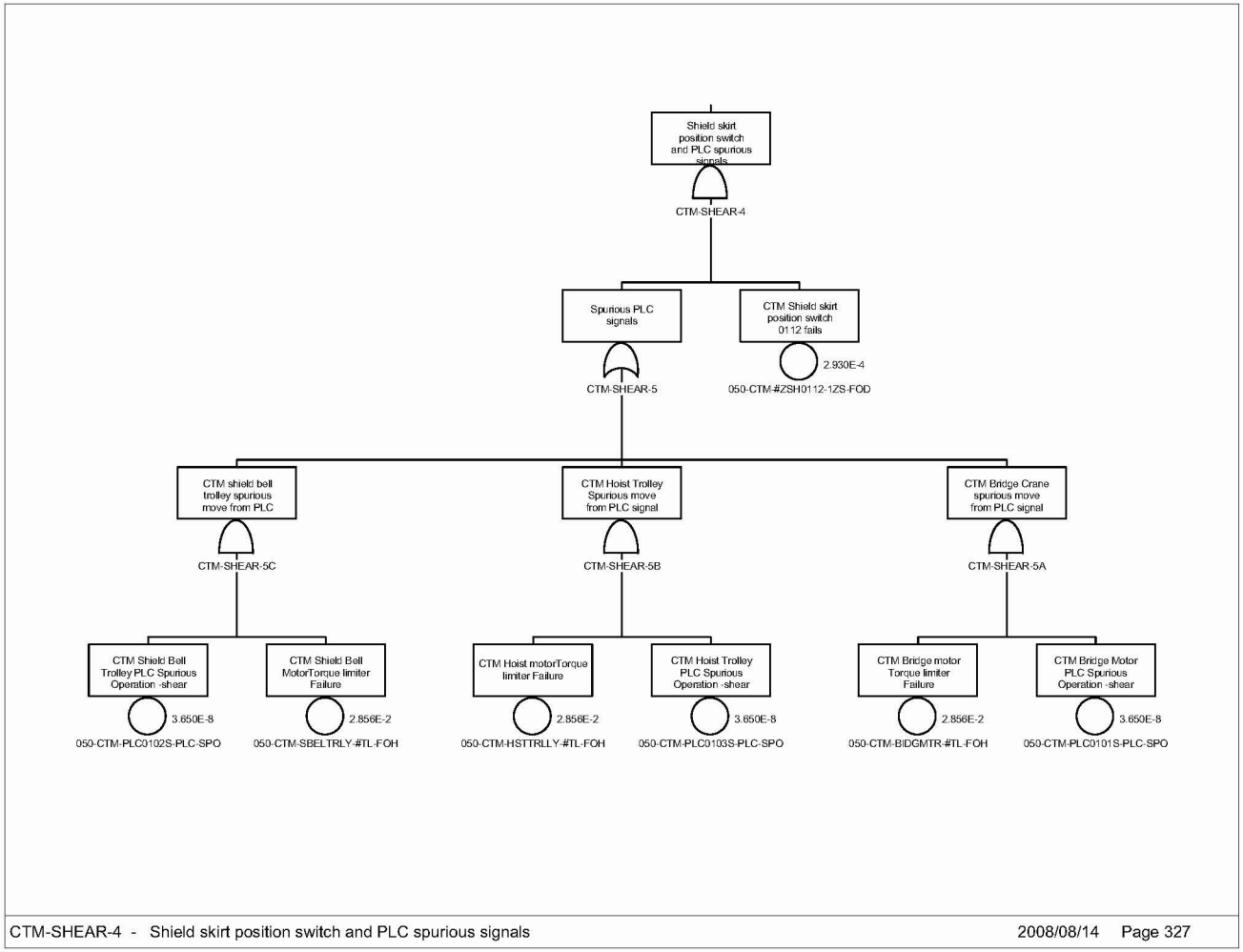


CTM-SHEAR - CTM movement causes canister shear 2008/03/03 Page 333

Source: Original

Figure B4.4-46. CTM Shear Sheet 1

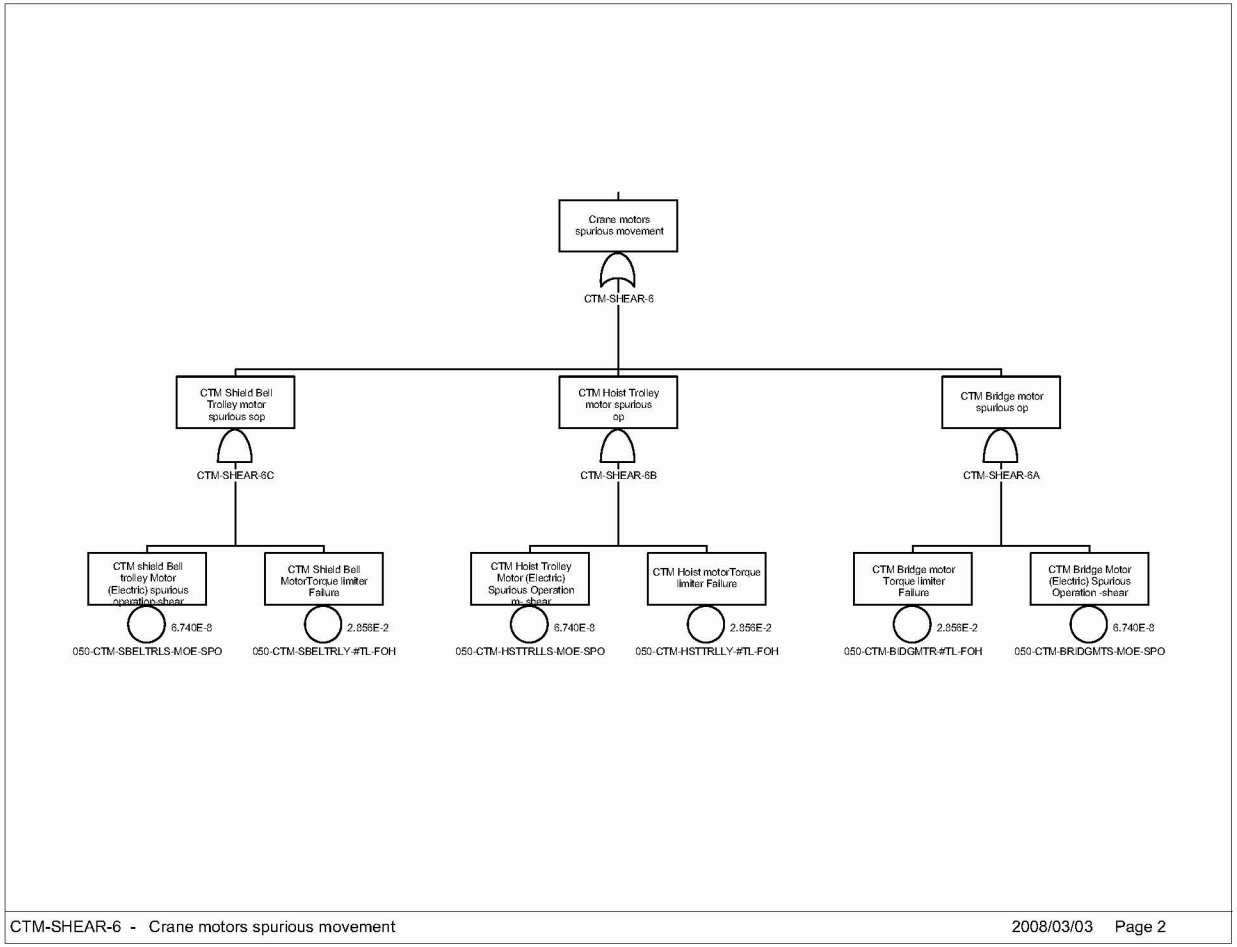
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-47. CTM Shear Sheet 2

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-48. CTM Shear Sheet 3

INTENTIONALLY LEFT BLANK

B5 CASK COOLING SYSTEM– 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.

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.

B5.1.1 *BSC (Bechtel SAIC Company) 2007. *Cask and Canister Cooling System Calculation.* 050-M0C-MRC0-00100-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071030.0009.

B5.1.2 *BSC 2007. *Wet Handling Facility Preparation Station #1 Cask Cooling System Piping & Instrument. Diagram.* 050-M60-MRC0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071218.0015.

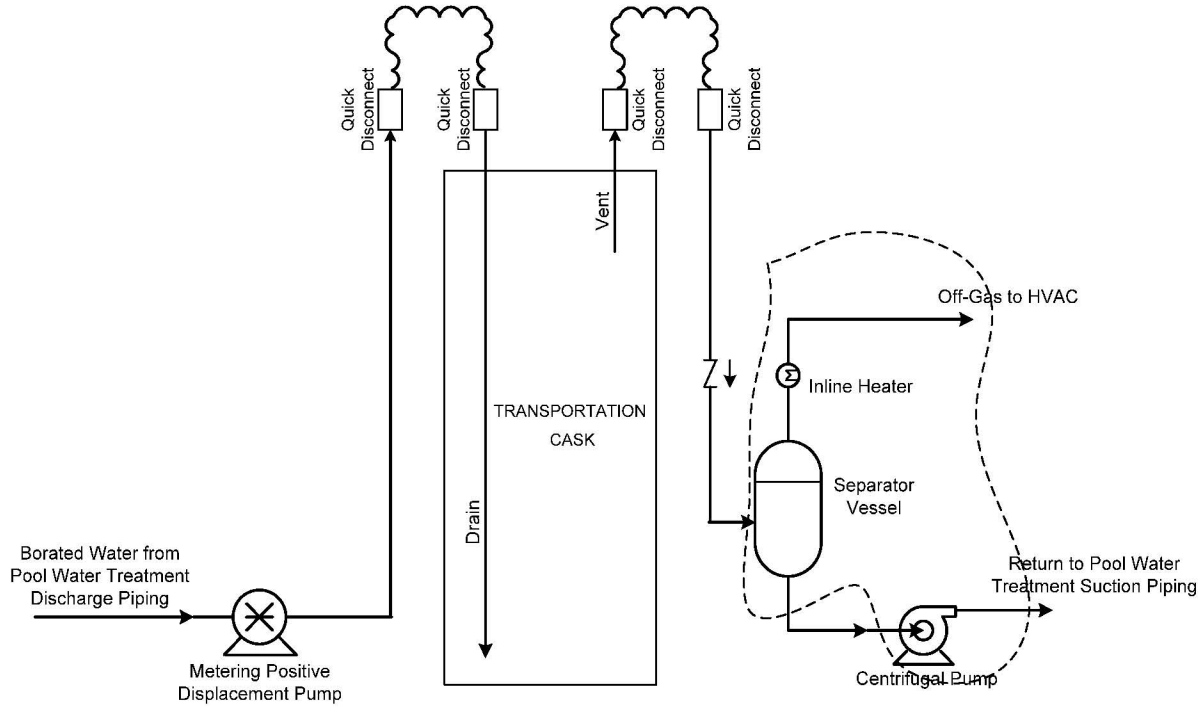
B5.2 CASK COOLING DESCRIPTION

B5.2.1 System Description

The cask cooling system, Figure B5.2-1, is a pump driven system that will be used to cool casks by introducing borated water into the cask. The system consists of two motor-driven pumps, a pressure relief valve, two interlocks, water piping, four quick disconnects, two sections of flexible tubing, and a separator vessel (Ref. B5.1.1).

The pumps serve to direct water from the pool, into the cask, and back to the pool. The positive displacement pump drives water out of the pool and into the cask, while the centrifugal pump directs water out of the cask and back into the pool for reuse. Borated water is injected via the drain pipe which is below the bottom of the spent fuel assemblies. Steam leaves the cask through the vent piping.

The water delivery and removal systems consist of a series of pipes, tubing, and quick disconnects. The flexible tubing connects the supply and return piping to the cask, with connections provided by quick disconnects. System piping runs from the pool to the flexible tubing which supplies the cask, and from the cask return to the separator vessel.



NOTE: HVAC = heating, ventilation, and air conditioning.

Source: Modified from Ref. B5.1.2

Figure B5.2-1. Cask Cooling System (Components within dashed line added for completeness)

Two lines of piping follow out of the separator vessel: one provides water for treatment and the other routing air to off-gas treatment. The separator vessel serves the purpose of separating air and water delivered from the cask.

B5.2.2 Operations

The cask handling crane places the cask into the preparation station. At the preparation station, the gas sampling port is opened and the drain valve and drain port cover plates are removed. The borated water line is connected to the drain port, and the vent line is connected to the gas sampling port. Borated water is then introduced into the cask as the steam is vented. Once the cask is satisfactorily cooled, the lines are disconnected, and the cover plates are reinstalled.

B5.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, 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

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Interlocks	Senses HI-HI water level and shuts down pump (Non-ITS)	—	—	Error point set too high	—
Positive Displacement Pump	Pumps water into the cask	—	—	Pump rate set too high	—
Flex lines and quick disconnects	Directs and contains water flowing into and out of the cask	—	—	—	Rupture or break of the line
Piping lines	Directs and contains water flowing into and out of the cask	—	—	—	Rupture or break of the line

NOTE: ITS = important to safety.

Source: Original

B5.4 CASK RELATED FAILURE SCENARIOS

There are two fault trees associated with the cask cooling system:

1. Break of non-pressurized sample line
2. Cask over-pressurization.

Table B5.4-1 provides a cross reference between the ESD and the fault trees that support them.

Table B5.4-1. ESD Cross Reference with Cask Cooling Fault Trees

WHF ESD Number	Fault Tree	Non-pressurized leak	Overpressurization
WHF-ESD16-CSNF	ESD16-PREP-OVERPRESSURE	N/A	X
WHF-ESD16-CSNF	ESD16-PREP-SAMPLE	X	N/A
WHF-ESD17-DPC	ESD17-PREP-OVERPRESSURE	N/A	X
WHF-ESD17-DPC	ESD17-PREP-SAMPLE	X	X

NOTE: ESD = event sequence diagram; WHF = Wet Handling Facility.

Source: Original

B5.4.1 Break of Non-pressurized Sample Line

B5.4.1.1 Description

The cask cooling fault tree describes the break of a non-pressurized sample line during cask cooling to satisfy WHF-ESD16-CSNF and WHF-ESD17-DPC, initiating event "Sampling line break." The top event is "Release During DPC Sampling" which is defined as the break of a sample line while the cask is being cooled. This fault tree is shown in Figures B5.4-3 through B5.4-5. The top event is "Release During CSNF Sampling" is described by identical fault trees which are not replicated here.

Breaks that can impact the release of contaminated water/steam are between the gas sampling port and separator vessel. This includes the two quick disconnects, flex line, and piping. The quick disconnect at the gas sampling port cannot fail independently of a clapper closure failure.

B5.4.1.2 Success Criteria

Success criteria for cooling a cask using borated water requires the contaminated water to remain contained.

Before filling the cask, the positive displacement pump is set to pump at a pre-determined rate based on the cask type. Should this pump allow a higher flow rate than determined, there exists a potential for contaminated water to breach the system due to cask over pressurization. Similarly, failure of the centrifugal pump also has the potential to lead to the release of contaminated water.

During the cask cooling process, a breach of any of the piping or tubing (including quick disconnects) venting the cask would result in a release of contaminated steam. Blockages of the same piping or tubing can result in a release due to over-pressurization of the cask.

The pump failures and blockages which can cause cask over pressurization are controlled by a pressure relief valve. In the advent of an overpressure condition, the pressure relief valve relieves the pressure.

B5.4.1.3 Design Features and Requirements

A pressure relief valve shall remedy a cask overfilling or over-pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition.

B5.4.1.4 Fault Tree Model

The fault tree in Figures B5.4-3 and B5.4-4 show two types of non-pressurized breaches or ruptures that can cause release from the cask cooling system:

1. Ruptures or leaks in discharge piping downstream of the cask
2. Ruptures or leaks in the quick disconnect valves or flex piping.

The most likely failure of the flex piping is a disconnection from the quick disconnect valve. Ruptures or leaks are single point failures with the exception of a rupture of flex piping downstream of quick disconnect valve 01 that is attached directly to the vent line. In this case, the quick disconnect valve would close (check) and isolate the leak. This checking action must also fail to cause a leak.

B5.4.1.5 Basic Events Data

Table B5.4-2 contains a list of basic events used in the fault tree for a sample line break (non-pressurized).

Table B5.4-2. Basic Event Probabilities for a Sample Line Break Non-Pressurized

Name	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission time[a]
050-CCS-CSKVLV1-CKV-FOD	1	6.62E-04	6.62E-04	—	—
050-CCS-DRNHOSE-HOS-RUP	3	1.48E-06	—	1.48E-06	8.00E+00
050-CCS-DRNQD01-QDV-FOH	3	4.26E-06	—	4.26E-06	1.00E+00
050-CCS-DRNQD02-QDV-FOH	3	4.26E-06	—	4.26E-06	1.00E+00
050-CCS-PIPBW03-PPL-RUP	3	3.54E-06	—	4.42E-07	8.00E+00
050-CCS-PIPBW04-PPL-RUP	3	3.54E-06	—	4.42E-07	8.00E+00
050-CCS-PIPBW05-PPL-RUP	3	3.54E-06	—	4.42E-07	8.00E+00
050-OPSAMPLEREL2-HFI-NOD	1	5.000E-003	5.00E-003	—	—

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time. See Table 6.3-1 for definitions of calculation types.

Source: Original

B5.4.1.5.1 Human Failure Events

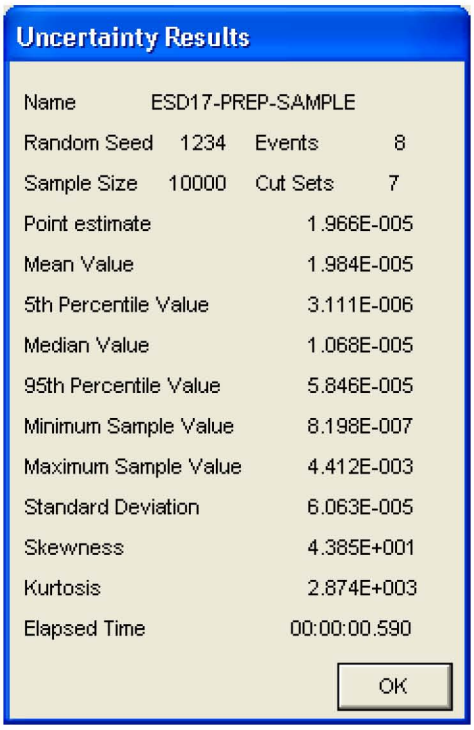
There is one human failure event involving operator release of material from the sample line.

B5.4.1.5.2 Common-Cause Failures

There is no common-cause failure event associated with this fault tree.

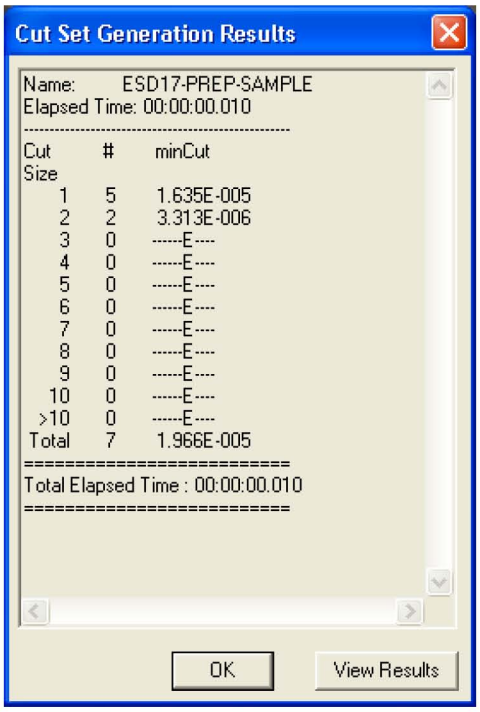
B5.4.1.6 Uncertainty and Cut Set Generation Results

Figure B5.4-1 contains the uncertainty results obtained from running the fault trees for a sample line break. Figure B5.4-2 provides the cut set generation results for a sample line break.



Source: Original

Figure B5.4-1. Uncertainty Results of the "Sample Line Break Non-Pressurized" Fault Tree



Source: Original

Figure B5.4-2. Cut Set Generation Results of the "Sample Line Break Non-Pressurized" Fault Tree

B5.4.1.7 Cut Sets

Table B5.4-3 contains the cut sets for a non-pressurized sample line during cask cooling. The total probability per cask is 1.75E-04.

Table B5.4-3. Cut Sets for a Non-Pressurized Sample Line Break

Fault Tree	% Cut Set	Probability/ Frequency	Basic Event	Description	Probability
ESD17-PREP-SAMPLE	21.67	4.260E-006	050-CCS-DRNQD01-QDV-FOH	Cask cooling QD Valve Fails	4.260E-006
	17.99	3.536E-006	050-CCS-PIPBW03-PPL-RUP	Drain Piping Catastrophic - Line BW-0003	3.536E-006
	17.99	3.536E-006	050-CCS-PIPBW04-PPL-RUP	Drain Piping Catastrophic - Line BW-0004	3.536E-006
	17.99	3.536E-006	050-CCS-PIPBW05-PPL-RUP	Drain Piping Catastrophic - Line BW-0005	3.536E-006
	16.84	3.310E-006	050-CCS-CSKVLV1-CKV-FOD	Cask Check Valve 1 Fails to Check	6.620E-004
			050-OPSAMPLEREL2-HFI-NOD	Operator Releases Material from Sample Line - QD Valve	5.000E-003
	7.53	1.480E-006	050-CCS-DRNHOSE-HOS-RUP	Cask Cooling Drain Hose Ruptures	1.480E-006
	0.01	2.820E-009	050-CCS-CSKVLV1-CKV-FOD	Cask Check Valve 1 Fails to Check	6.620E-004
			050-CCS-DRNQD02-QDV-FOH	Cask cooling QD 02 Valve Fails	4.260E-006

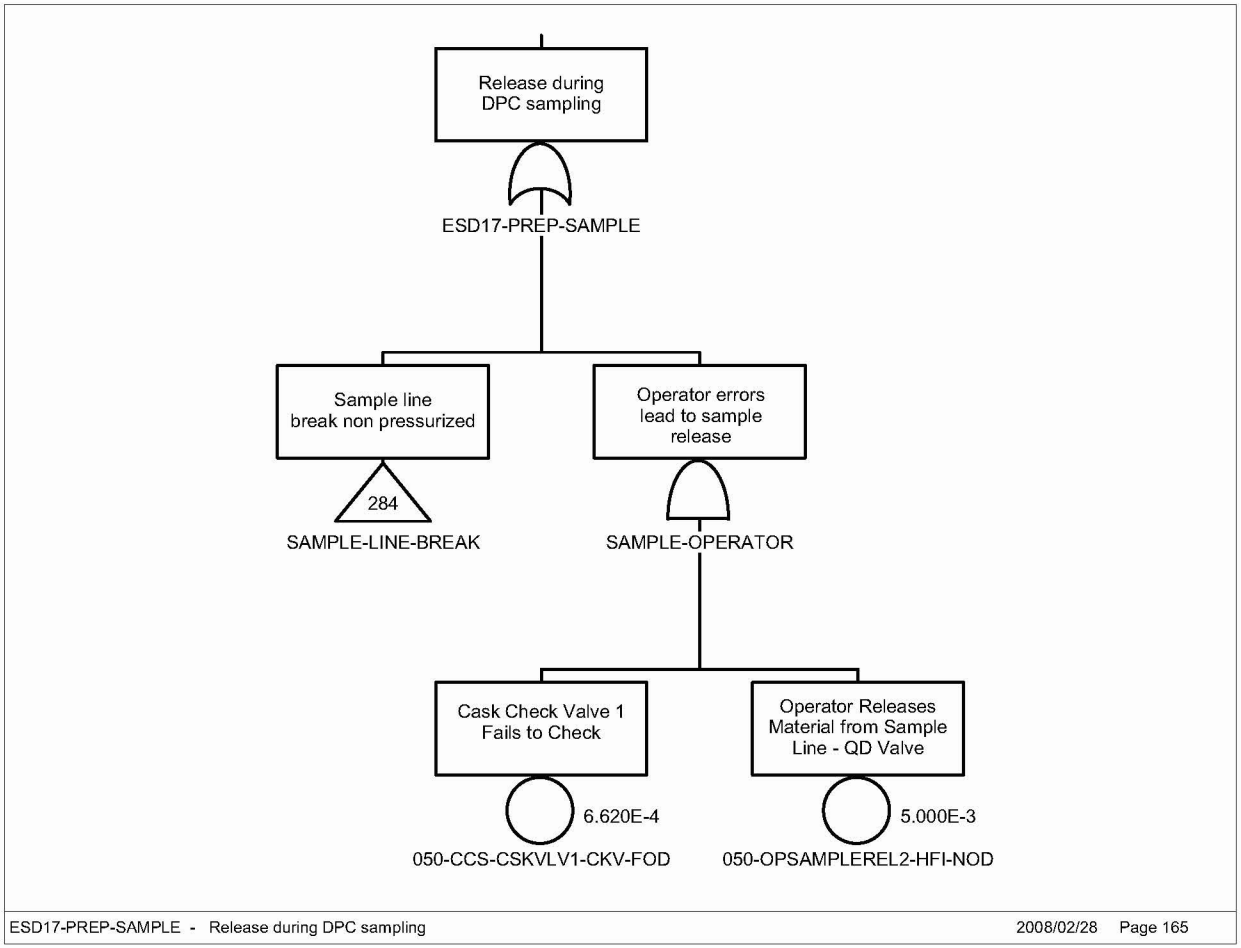
NOTE: QD = quick disconnect.

Source: Original

B5.4.1.8 Fault Tree

Figures B5.4-3 through B5.4-5 display the Fault Trees for a Non-Pressurized Sample Line Break.

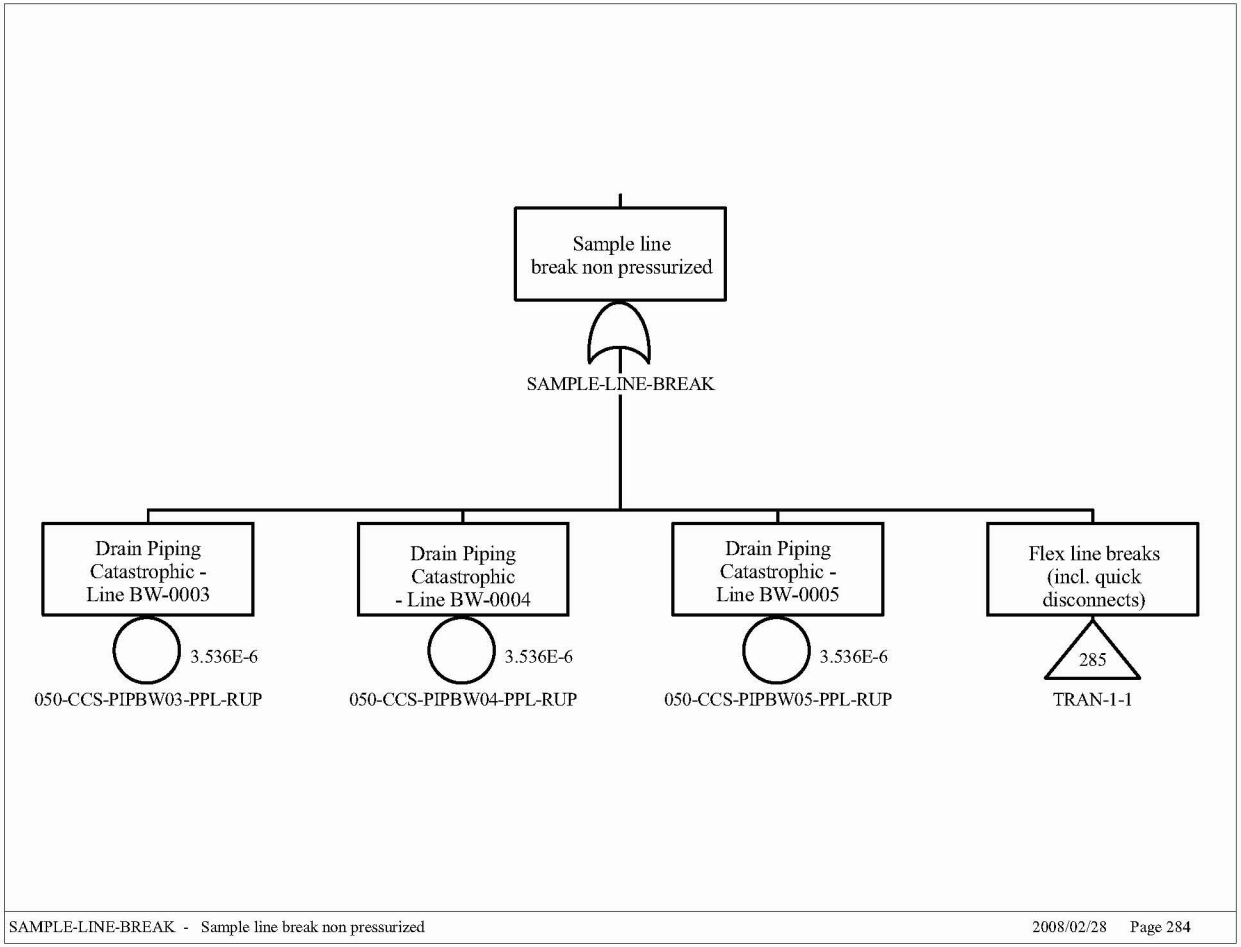
INTENTIONALLY LEFT BLANK



Source: Original

Figure B5.4-3. Fault Tree for a Non-Pressurized Sample Line Break

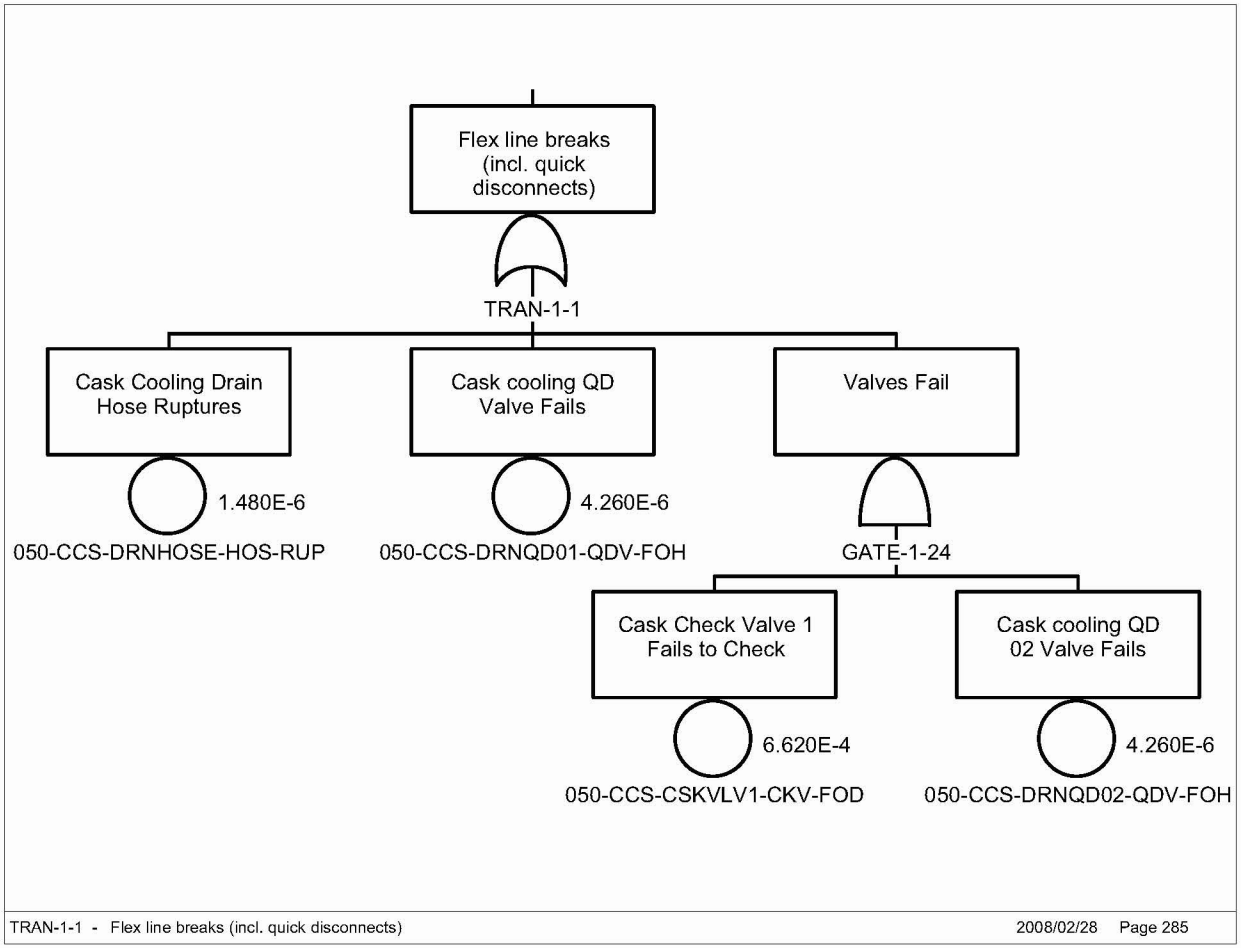
INTENTIONALLY LEFT BLANK



Source: Original

Figure B5.4-4. Sample Line Break

INTENTIONALLY LEFT BLANK



Source: Original

Figure B5.4-5. Fault Tree for a Non-Pressurized Sample Line Break (Transfer 1-1)

INTENTIONALLY LEFT BLANK

B5.4.2 Cask Over Pressurization

B5.4.2.1 Description

This fault tree describes the over pressurization of the cask to satisfy WHF-ESD16-CSNF and WHF-ESD17-DPC, initiating event "Over pressurization of canister." The top event is "cask/sample line over pressurized" which is defined as the abundance of pressure in the cask or sample line resulting in an unplanned escape of water into the facility during cask cooling. This fault tree is shown in Figures B5.4 -8 and B5.4-9.

The existence of an excess of pressure is caused by an excess of water introduced into the cask and a failure to reduce this excess. The existence of excess water can be caused by the metering pump running too fast, a blockage in piping, or the failure of the venting pump to run.

B5.4.2.2 Success Criteria

A pressure relief valve shall be part of the system as a final resource to remedy a cask overfilling or over pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition[1].

B5.4.2.3 Design Features and Requirements

A pressure relief valve shall remedy a cask overfilling or over-pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition. Mission time is set to eight hours which equates to nominal DPC cooling time.

B5.4.2.4 Fault Tree Model

The fault trees in Figures B5.4-8 through B5.4-9 show two types of pressurized breaches or ruptures can cause release from the cask cooling system:

1. Operator error initiated over pressurization
2. Mechanical failure initiated over pressurization.

For both of these events, failure of the pressure relief valve is considered as a preventative measure in relieving overpressure.

[1] There are two interlocks in this system to control the positive displacement pump, should an excess of water be detected. One interlock detects a high level of water entering the cask and the other interlock detects a high level of water leaving the cask. In either case, the interlock is designed to shut down the pump which delivers water to the cask. However, these interlocks depend upon PLCs and are not credited in the fault tree analysis. The pressure relief valve is the only credited safety feature.

B5.4.2.5 Basic Events Data

Table B5.4-4 contains a list of basic events used in the fault tree for cask/sample line over pressurization.

Table B5.4-4. Basic Event Probabilities for Over pressurization

Name	Calculation Type	Calculation Probability	Failure Probability	Lambda	Mission time
050-CCS-VNTPIPE-PPM-PLG	3	5.81E-06	—	7.26E-07	8.00E+00
050-CCS-PLCSPUR-PLC-SPO	3	2.92E-06	—	3.65E-07	8.00E+00
050-CCS-PMTRFST-MSC-FOH	3	1.02E-03	—	1.28E-04	8.00E+00
050-CCS-PUMPSTP-PMD-FTR	3	2.76E-04	—	3.45E-05	8.00E+00
050-CCS-RLFVLVF-PRV-FOD	1	6.54E-03	6.54E-03	—	—
050-CCS-THVLVFL-NZL-FOH	3	2.28E-05	—	2.85E-06	8.00E+00
050-OPDPC-OVP01-HFI-NOW	1	7.00E-08	7.00E-08	—	—

Source: Original

B5.4.2.5.1 Human Failure Events

There is one human failure event associated with this fault tree—050-OPDPC-OVPR01-HFI-NOD.

As described in detail in Attachment E, this HFE addresses potential failures during operator preparation activities when the DPC is filled and flushed with water to prevent a crud burst when put into the pool.

B5.4.2.5.2 Common Cause Failures

There is no CCF event associated with this fault tree.

B5.4.2.6 Uncertainty and Cut set Generation Results

Figure B5.4-6 contains the uncertainty results obtained from running the fault trees for cask/sample line over pressurization. Figure B5.4-7 provides the cut set generation results for a sample line break.

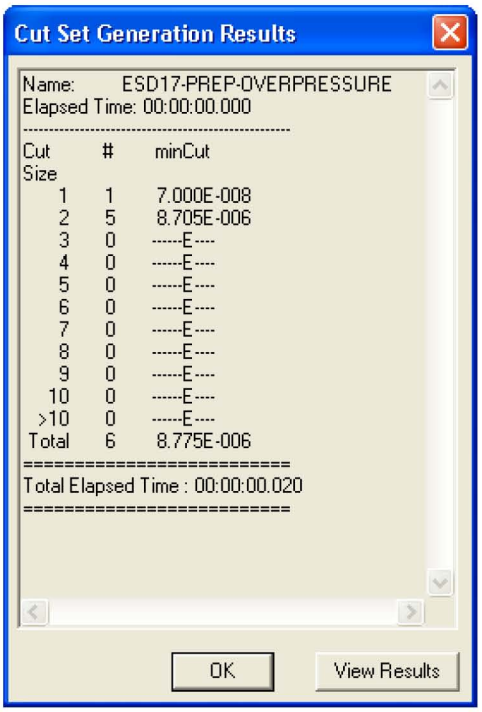
Uncertainty Results

Name	ESD17-PREP-OVERPRESSURE		
Random Seed	1234	Events	7
Sample Size	10000	Cut Sets	6
Point estimate			8.775E-006
Mean Value			7.792E-006
5th Percentile Value			3.913E-008
Median Value			7.496E-007
95th Percentile Value			2.850E-005
Minimum Sample Value			2.482E-009
Maximum Sample Value			3.779E-003
Standard Deviation			5.092E-005
Skewness			4.473E+001
Kurtosis			3.063E+003
Elapsed Time			00:00:00.610

OK

Source: Original

Figure B5.4-6. Uncertainty Results of the “Sample Line Break Overpressurized” Fault Tree



Source: Original

Figure B5.4-7. Cut Set Generation Results of the "Sample Line Break Overpressurized" Fault Tree

B5.4.2.7 Cut Sets

Table B5.4-5 contains the cut sets for cask/sample line over pressurization. The total probability per cask is 8.08E-6.

Table B5.4-5. Cut Sets for Over Pressurization

Fault Tree	% Cut Set	Probability/ Frequency	Basic Event	Description	Probability
OVERPRESSURIZATION	76.28	6.694E-006	050-CCS-PMTRFST-MSC-FOH	Pump motor runs too fast	1.023E-003
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
	20.57	1.805E-006	050-CCS-PUMPSTP-PMD-FTR	Pump P-00002 fails to run	2.760E-004
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
	1.70	1.491E-007	050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
			050-CCS-THVLVFL-NZL-FOH	Throttle valve to pump fails open	2.280E-005
	0.80	7.000E-008	050-OPDPC-OVP01-HFI-NOW	Operator causes overpressurization	7.000E-008
	0.43	3.798E-008	050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
			050-CCS-VNTPIPE-PPM-PLG	Pipe BW-0003 plugs	5.808E-006
	0.22	1.910E-008	050-CCS-PLCSPUR-PLC-SPO	PLC spurious operation causes pump motor to run too fast	2.920E-006
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003

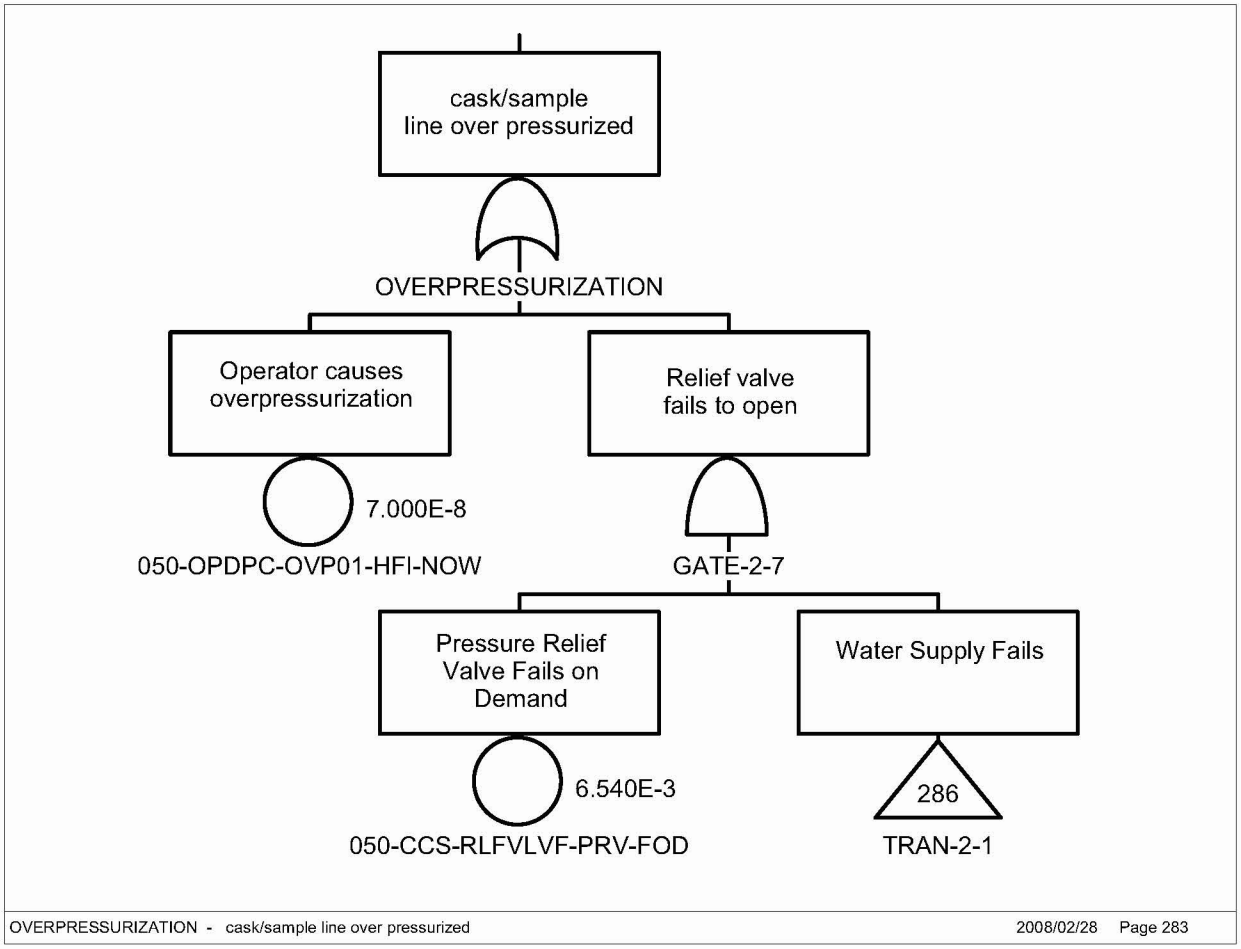
NOTE: PLC = programmable logic controller.

Source: Original

B5.4.2.8 Fault Tree

Figures B5.4-8 and B5.4-9 display the fault trees for “Cask/Sample Line Over Pressurization”.

INTENTIONALLY LEFT BLANK



Source: Original

Figure B5.4-8. Fault Tree for an Over Pressurization