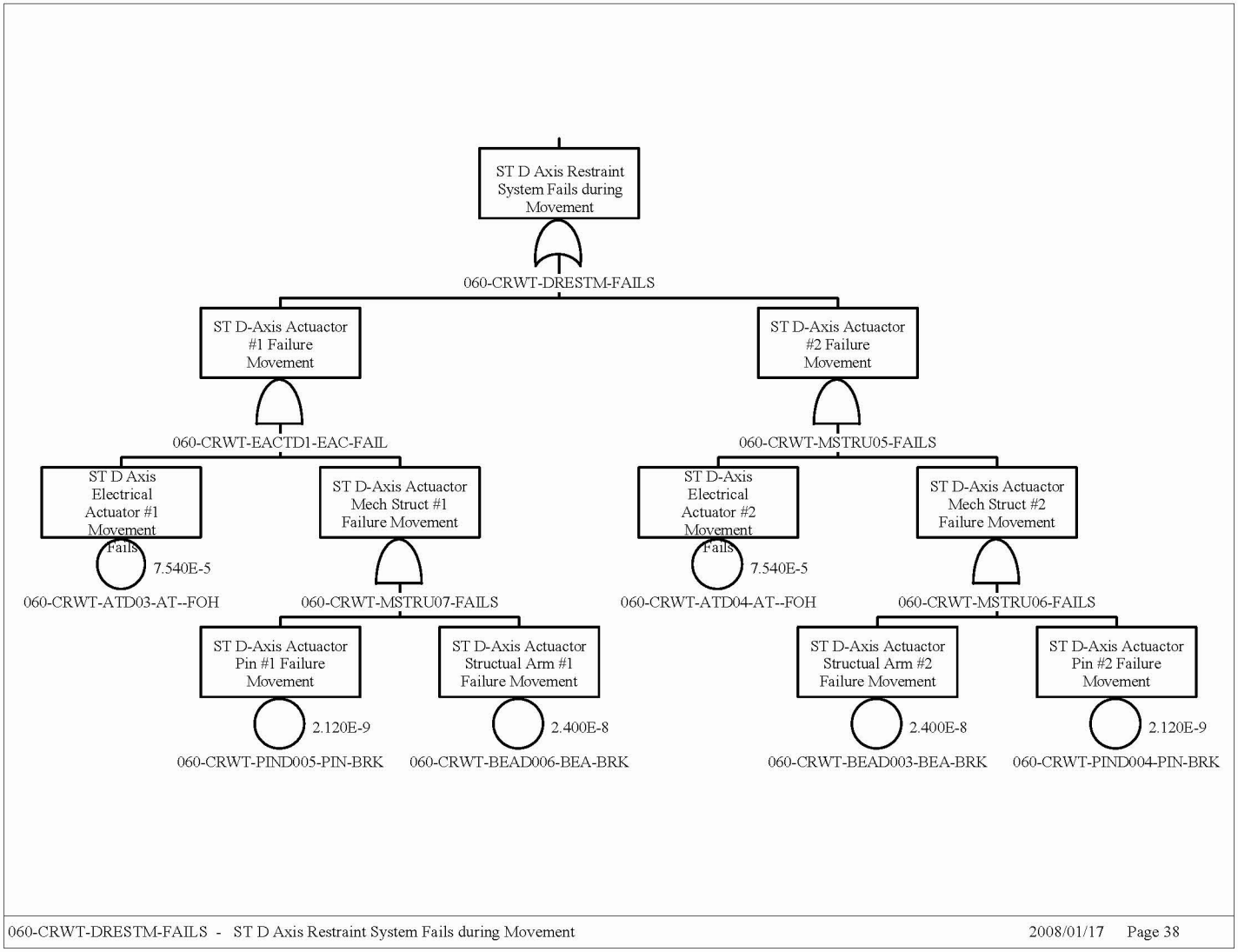
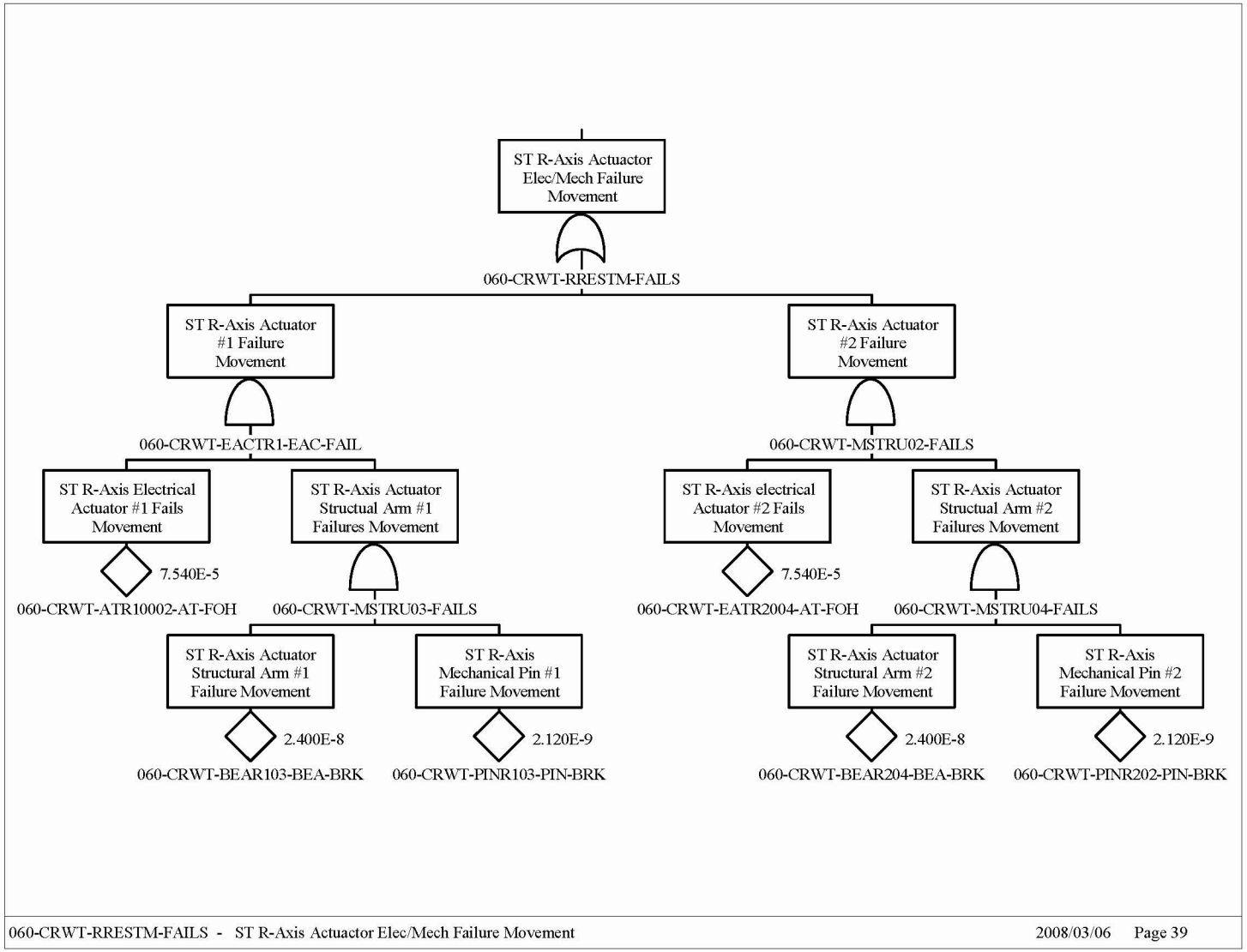


Source: Original

Figure B6.4-18. Site Transporter Drop Axis Restraint System Fails during Movement



Source: Original

Figure B6.4-19. Site Transporter Roll-Axis Actuator Electrical/Mechanical Failure Movement

B6.4.3 Site Transporter Rollover (Tipover) (ESD-02, ESD-16)

B6.4.3.1 Description

Although the site transporter has been designed to have a low center of gravity and a wide footprint, there is a possibility of a rollover caused by a track failure with a subsequent operator failure to stop the site transporter upon loss of a track. The track would have to fail in a manner such that it binds (i.e., rolls up), the site transporter drives over the failed track, and the site transporter tilts to an angle that results in a tipover condition.

B6.4.3.2 Success Criteria

The design of the site transporter prevents the majority of events that could potentially cause a site transporter rollover. The site transporter is designed to negotiate a 5% grade and a 2% cross-slope. In addition, the aging overpack is mechanically prevented from being lifted more than 12 inches. The combination of the low lift height of the aging overpack, the low center of gravity, and the wide footprint of the site transporter results in stable platform during movement.

During movement, a site transporter track failure could result in a potential tipover situation. There is no design constraint for this failure mode, preventing this situation relies on operator awareness and response time to this situation to initiate an emergency stop command. The operator has several seconds to respond to the track failure; however, since this is a recovery action, no credit is taken for the operator response.

B6.4.3.3 Design Requirements and Features

Requirements

Operator has the capability of stopping the site transporter in sufficient time to keep the site transporter from running off the end of a broken track.

Features

The center of gravity of a loaded site transporter with aging overpack, ensures stability.

The site transporter operator has the capability to stop the operation of the site transporter during abnormal conditions.

B6.4.3.4 Fault Tree Model

Human error is conservatively postulated to result in a rollover/tipover if the operator does not stop the site transporter in sufficient time to prevent the site transporter from running off the broken track.

B6.4.3.5 Basic Events

Table B6.4-6 lists the basic events used in the site transporter drop load during lift/movement fault tree. Uncertainty and cut set results are provided in Figures B6.4-20 and B6.4-21 respectively.

Table B6.4-6. Basic Event Probability for the Site Transporter Rollover

Basic Events Probability Report					
Project: Yucca-Mountain		Case : Current			
ST Rollover	Calc.	Units: Per Hour			
Name	Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-CRWT-TRD0001-TRD-FOH	3	5.89E-007	0.00E+00	5.89E-007	1.00E+00
060-CRWT-TRD0002-TRD-FOH	3	5.89E-007	0.00E+00	5.89E-007	1.00E+00
060-CRWT-TRD0003-TRD-FOH	3	5.89E-007	0.00E+00	5.89E-007	1.00E+00
060-CRWT-TRD0004-TRD-FOH	3	5.89E-007	0.00E+00	5.89E-007	1.00E+00
060-CRWT-TRK0001-TRD-FOH	3	5.89E-007	0.00E+00	5.89E-007	1.00E+00
060-OP-FAILSTOP-HFI-NOD	1	1.00E+000	1.00E+00	0.00E+000	1.00E+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; ST = site transporter.

Source: Original

B6.4.3.5.1 Human Failure Events

There is one human error failure event included in this model. It is conservatively set to a value of 1E+0 because unsafe actions that require an equipment failure to cause an initiating event are generically assigned a screening HEP of 1.0 (Table E6.4-1).

B6.4.3.5.2 Common-Cause Failures

There is no common-cause failure identified for this fault tree in that the failure of one track could potentially result in a rollover (tipover).

B6.4.3.6 Uncertainty and Cut Set Generation

Figures B6.4-20 and B6.4-21 contain the uncertainty and the cut set generation results for the "Site Transporter Rollover (Tipover)" fault tree using a cutoff probability of 1E-15.

Uncertainty Results

Name	060-2-ST-ROLLOVER		
Random Seed	1234	Events	5
Sample Size	10000	Cut Sets	4
Point estimate			2.356E-006
Mean Value			2.327E-006
5th Percentile Value			5.164E-007
Median Value			1.778E-006
95th Percentile Value			6.019E-006
Minimum Sample Value			6.265E-008
Maximum Sample Value			2.504E-005
Standard Deviation			1.929E-006
Skewness			2.677E+000
Kurtosis			1.582E+001
Elapsed Time			00:00:00.710

OK

Source: Original

Figure B6.4-20. Uncertainty Results for the Site Transporter Rollover (Tipover) Fault Tree

Cut Set Generation Results

Name: 060-2-ST-ROLLOVER
Elapsed Time: 00:00:00.000

Cut Sets Size	#	UpperBound
1	0	------E----
2	4	2.356E-006
3	0	------E----
4	0	------E----
5	0	------E----
6	0	------E----
7	0	------E----
8	0	------E----
9	0	------E----
10	0	------E----
>10	0	------E----
Total	4	2.356E-006

OK

Source: Original

Figure B6.4-21. Cut Set Generation Transporter Rollover Results for the Site Transporter Rollover (Tipover) Fault Tree

B6.4.3.7 Cut Sets

Table B6.4-7 contains the cut sets for the "Site Transporter Rollover" fault tree.

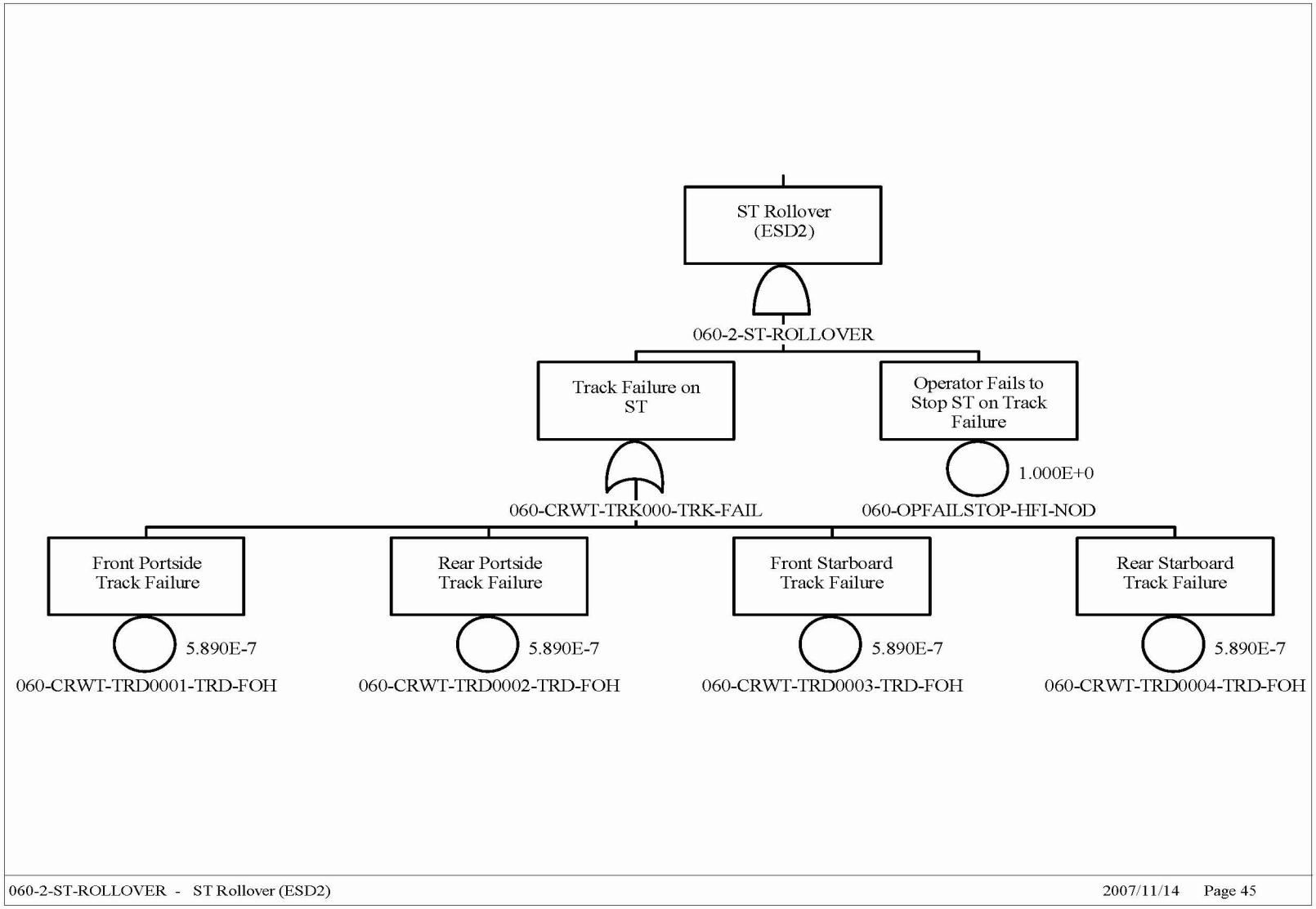
Table B6.4-7. Cut Sets for the Site Transporter Rollover (Tipover)

Project: Yucca Mountain Analysis: RANDOM	Fault Tree Cutsets (Detailed) Report			
		Case : Current Units: Per Hour		
Cut Set %	Prob./Freq.	Basic Event	Description	Probability
25	5.89E-07	060-CRWT-TRD0001-TRD-FOH	Front Portside Track Failure	5.90E-07
		060-OP-FAILSTOP-HFI-FOD	Operator Fails to Stop ST on Track Failure	1.00E+00
25	5.89E-07	060-CRWT-TRD0002-TRD-FOH	Rear Portside Track Failure	5.90E-07
		060-OP-FAILSTOP-HFI-FOD	Operator Fails to Stop ST on Track Failure	1.00E+00
25	5.89E-07	060-CRWT-TRD0003-TRD-FOH	Front Starboard Track Failure	5.90E-07
		060-OP-FAILSTOP-HFI-FOD	Operator Fails to Stop ST on Track Failure	1.00E+00
25	5.89E-07	060-CRWT-TRD0004-TRD-FOH	Rear Starboard Track Failure	5.90E-07
		060-OP-FAILSTOP-HFI-FOD	Operator Fails to Stop ST on Track Failure	1.00E+00

NOTE: Freq. = frequency, Prob. = probability; ST = site transporter.

Source: Original

B6.4.3.8 Fault Tree



Source: Original

Figure B6.4-22. Operator causes Site Transporter Tipover

B6.4.4 Site Transporter Spurious Movement (ESD--09)

B6.4.4.1 Description

The fault tree for "Site Transporter Spurious Movement" in this event sequence addresses activities associated with site transporter transfers of aging overpack canisters to or from staging in the Cask Unloading Room.

B6.4.4.2 Success Criteria

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 lift/lower an 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 cable disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

B6.4.4.3 Design Requirements and Features

Requirements

Site transporter power and the remote control pendant are removed by the operator from the site transporter when it has been positioned within the Cask Unloading Room.

On removal of AC power derived from the facility, the site transporter performs a controlled stop. Once stopped it enters the "lock mode," safe state. The "lock mode," safe state is not reversible without specific operator action.

Features

There are no electrical storage devices capable of propelling the site transporter with electrical energy when the AC power cable is removed. When the AC power cable is removed, the on board diesel generator must be operating to cause the site transporter to move.

A shield door interlock ensures that facility power has been removed from the site transporter.

B6.4.4.4 Fault Tree Model

The fault tree model for "Site Transporter Spurious Movement in Cask Unloading Room" accounts for the failure to remove facility power and the possibility of the site transporter receiving a spurious movement command for the remote control device.

B6.4.4.5 Basic Event Data

Table B6.4-8 lists the basic events used in the "Site Transporter Spurious Movement" fault tree.

Table B6.4-8. Basic Event Probability for Site Transporter Spurious Movement

Basic Events Probability Report					
Project: Yucca-Mountain	Case : Current	Units: Per Hour			
ST Spurious Movement					
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-CR---IEL00A--IEL-FOD	1	2.75E-05	2.75E-05	0.00E+00	1.00E+00
060-CR---IEL00B--IEL-FOD	1	2.75E-05	2.75E-05	0.00E+00	1.00E+00
060-CR---IELCCF--IEL-CCF	C [b]	1.30E-06	—	—	—
060-OPNOUNPLUGST-HFI-NOD	1	1.00E-03	1.00E-03	0.00E+00	1.00E+00
060-ST---HC000--HC--SPO	3	5.23E-07	0.00E+00	5.23E-07	1.00E+00
060-ST---SC002--SC--FOH	3	1.28E-04	0.00E+00	1.28E-04	1.00E+00
060-ST---SC021---SC--SPO	3	3.20E-05	0.00E+00	3.20E-05	1.00E+00

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

[b] A calculation of type "C", i.e., "compound event" is used to evaluate CCFs. For this type of calculation, SAPHIRE uses 1) information on the failure rate or failure probability of the underlying components and 2) information on the probability distribution of the alpha factors involved in the CCF to internally evaluate the probability distribution of the resulting basic event (see Attachment C, Section C3). The number shown in the "Basic event mean probability" column is actually a point estimate which approximates the mean.

Calc. = Calculation; Fail. = failure; Miss. = mission; Prob. = probability; ST = site transporter.

Source: Original

B6.4.4.5.1 Human Failure Events

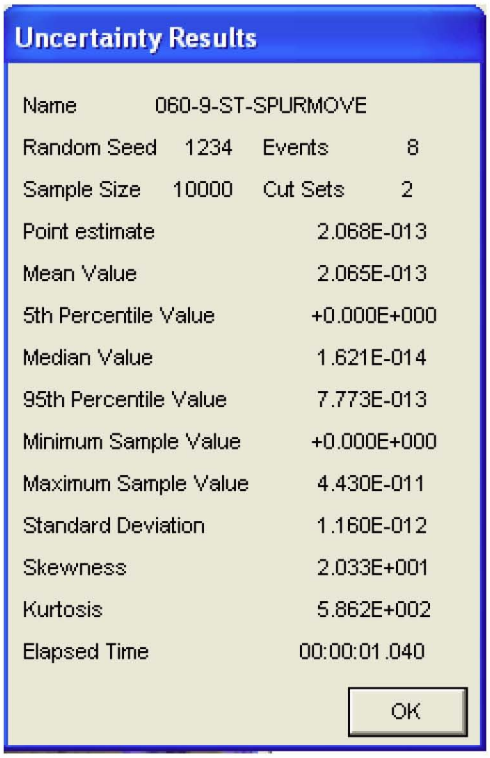
There is one human error associated with this fault tree that addresses an operator failure to unplug the site transporter power cable after it has been parked in the Cask Unloading Room.

B6.4.4.5.2 Common-Cause Failures

There is one common-cause failure associated with two interlock failures on the slide gates. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criteria (Table C3-1, CCCG = 2).

B6.4.4.6 Uncertainty and Cut Set Generation

Figures B6.4-23 and B6.4-24 contain the uncertainty and the cut set generation results for "Site Transporter Spurious Movement" fault tree using a cutoff probability of 1E-15.



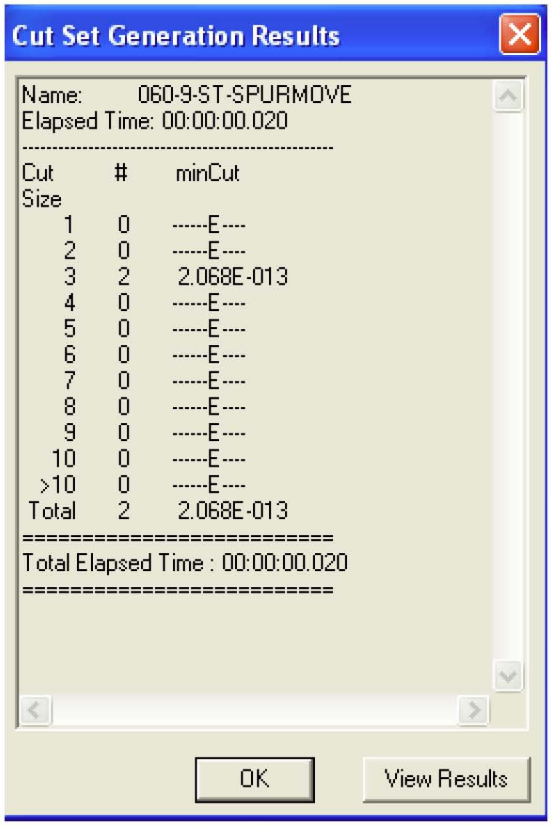
Uncertainty Results

Name	060-9-ST-SPURMOVE		
Random Seed	1234	Events	8
Sample Size	10000	Cut Sets	2
Point estimate			2.068E-013
Mean Value			2.065E-013
5th Percentile Value			+0.000E+000
Median Value			1.621E-014
95th Percentile Value			7.773E-013
Minimum Sample Value			+0.000E+000
Maximum Sample Value			4.430E-011
Standard Deviation			1.160E-012
Skewness			2.033E+001
Kurtosis			5.862E+002
Elapsed Time			00:00:01.040

OK

Source: Original

Figure B6.4-23. Uncertainty Results Site Transporter Spurious Movement Fault Tree



Source: Original

Figure B6.4-24. Cut Set Generation Results for the Site Transporter Spurious Movement Fault Tree

B6.4.4.7 Cut Sets

Table B6.4-9 contains the cut sets for the "Site Transporter Spurious Movement" fault tree.

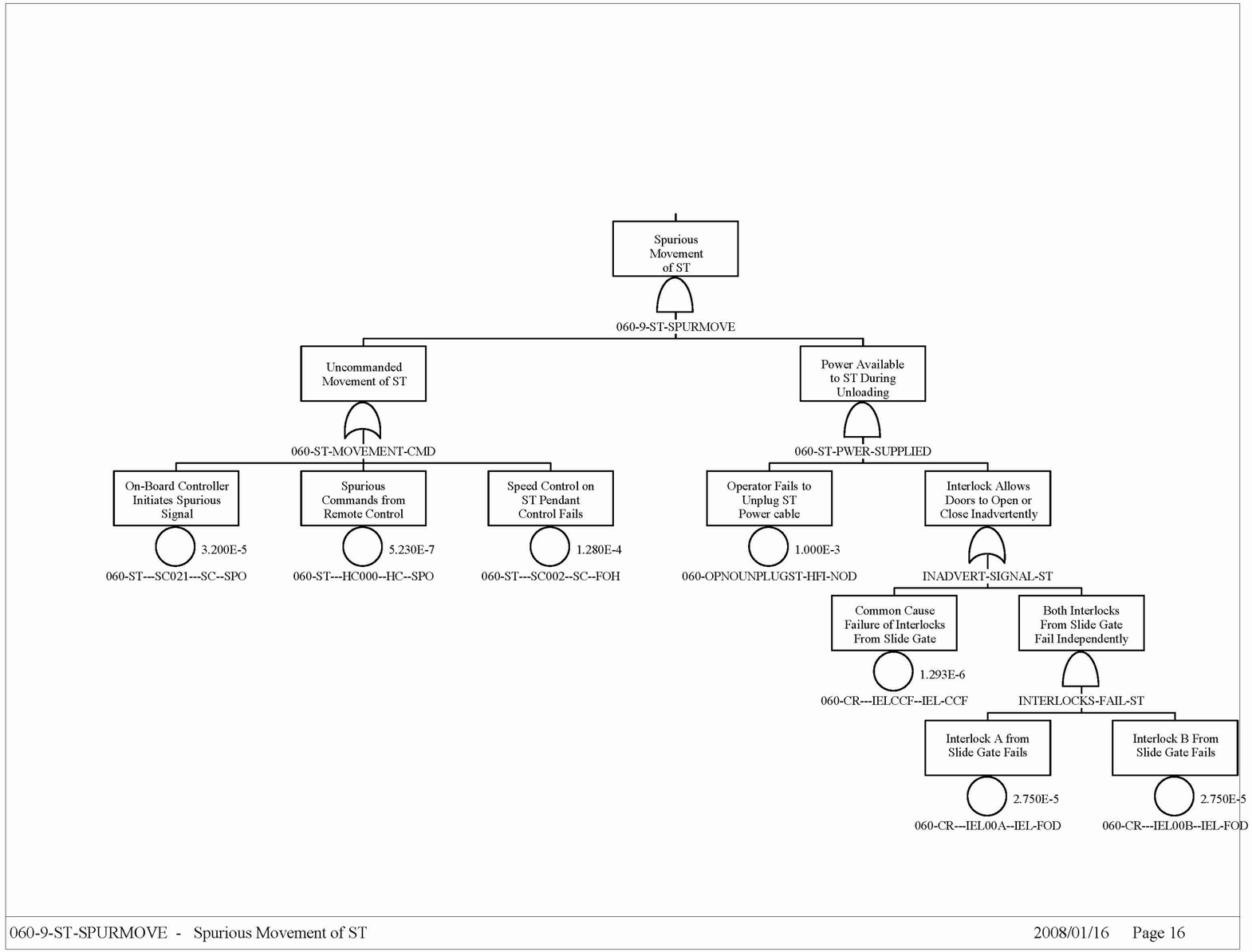
Table B6.4-9. Cut Sets for the Site Transporter Spurious Movement

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-9-ST-SPURMOVE	79.98	1.654E-013	060-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			060-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			060-ST---SC002--SC--FOH	Speed Control on ST Pendant Control Fails	1.3E-004
	20.00	4.136E-014	060-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			060-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			060-ST---SC021---SC--SPO	On-Board Controller Initiates Spurious Signal	3.2E-005
		2.068E-013	= Total		

NOTE: AO = aging overpack; Freq. = frequency, Prob. = probability; ST = site transporter; STC = shielded transfer cask.

Source: Original

B6.4.4.8 Fault Tree



Source: Original

Figure B6.4-25. Spurious Movement of Site Transporter

INTENTIONALLY LEFT BLANK

B6.4.5 Site Transporter Spurious Movement (ESD-05, ESD-12)

B6.4.5.1 Description

Site transporter impact fault trees for these ESDs are identical. The fault tree addresses site transporter impacts with the aging overpack due to spurious movement due to both human error and equipment failure.

B6.4.5.2 Success Criteria

The success criteria for preventing an impact to the site transporter include safety design features for hardware failures resulting in spurious commands and the site transporter operator maintaining situational awareness and proper control of the movement of the site transporter.

B6.4.5.3 Design Requirements and Features

Requirements

The operational control of the site transporter, when inside facility is performed, as a minimum, by a two crewmember team.

One crewmember controls the movement of the site transporter and the other performs spotter functions.

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

Features

All vehicles in the CRCF have limiters to restrict speed.

B6.4.5.4 Fault Tree Model

The fault tree model for site transporter impact due to spurious movement addresses one human errors and the possibility of the site transporter receiving a spurious movement or speed commands for the remote control device.

B6.4.5.5 Basic Event Data

Table B6.4-10 lists the basic events used in the site transporter spurious movement. Uncertainty and cut set results are provided in Figures B6.4-26 and B6.4-27 respectively.

Table B6.4-10. Basic Event Probability for Site Transporter Spurious Movement

Basic Events Probability Report					
Project: Yucca-Mountain		Case : Current			
ST Impact		Units: Per Hour			
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-ST---SC002--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
060-ST---SC021---SC--SPO	3	3.200E-005	0.000E+000	3.200E-005	1.000E+000
060-OPSPURMOVE01-HFI-NOD	1	1.000E-004	1.000E-004	0.000E+000	1.000E+000
060-ST---HC000--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000

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

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

Source: Original

B6.4.5.5.1 Human Failure Events

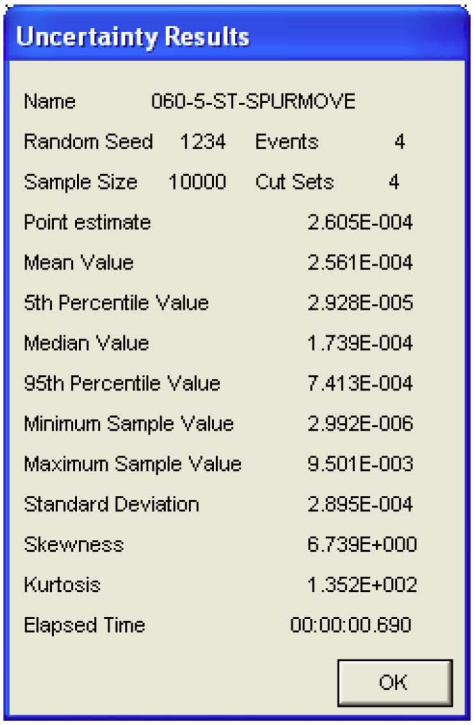
The human failure associated with this fault tree is 060-OPSPURMOVE01-HFI-NOD—the site transporter operator initiates a spurious movement which is set to a screening value of 1E-04.

B6.4.5.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

B6.4.5.6 Uncertainty and Cut Set Generation

Figures B6.4-26 and B6.4-27 contain the uncertainty and the cut set generation results for the "Site Transporter Spurious Movement" fault tree using a cutoff probability of 1E-15.



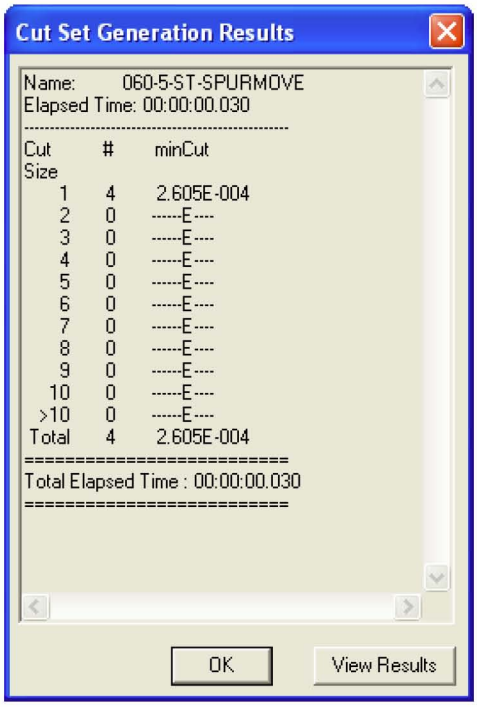
Uncertainty Results

Name	060-5-ST-SPURMOVE		
Random Seed	1234	Events	4
Sample Size	10000	Cut Sets	4
Point estimate			2.605E-004
Mean Value			2.561E-004
5th Percentile Value			2.928E-005
Median Value			1.739E-004
95th Percentile Value			7.413E-004
Minimum Sample Value			2.992E-006
Maximum Sample Value			9.501E-003
Standard Deviation			2.895E-004
Skewness			6.739E+000
Kurtosis			1.352E+002
Elapsed Time			00:00:00.690

OK

Source: Original

Figure B6.4-26. Uncertainty Results Site Transporter Spurious Movement



Cut Set Generation Results

```
Name:        060-5-ST-SPURMOVE
Elapsed Time: 00:00:00.030
-------------------------------------------
Cut      #      minCut
Size
    1    4      2.605E-004
    2    0      ------E----
    3    0      ------E----
    4    0      ------E----
    5    0      ------E----
    6    0      ------E----
    7    0      ------E----
    8    0      ------E----
    9    0      ------E----
   10    0      ------E----
  >10    0      ------E----
 Total   4      2.605E-004
==========================
Total Elapsed Time : 00:00:00.030
==========================
```

OK View Results

Source: Original

Figure B6.4-27. Cut Set Generation Results for the Site Transporter Spurious Movement Fault Tree

B6.4.5.7 Cut Sets

Table B6.4-11 contains the cut sets for the "Site Transporter Spurious Movement" fault tree.

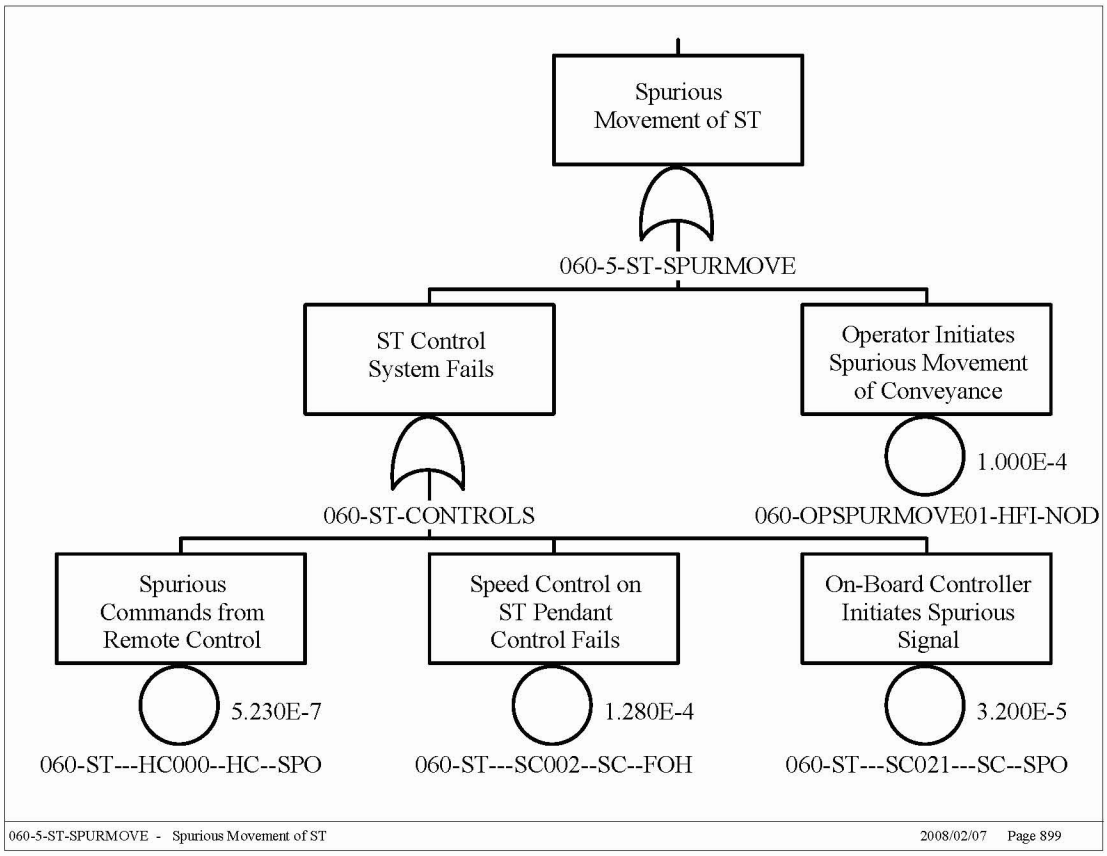
Table B6.4-11. Cut Sets for Site Transporter Spurious Movement

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-5-ST-SPURMOVE	49.13	1.280E-004	060-ST---SC002--SC--FOH	Speed Control on ST Pendant Control Fails	1.3E-004
	38.39	1.000E-004	060-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement of Conveyance	1.0E-004
	12.28	3.200E-005	060-ST---SC021---SC--SPO	On-Board Controller Initiates Spurious Signal	3.2E-005
	0.20	5.230E-007	060-ST---HC000--HC--SPO	Spurious Commands from Remote Control	5.2E-007
		2.605E-004	= Total		

NOTE: Freq. = frequency, Prob. = probability; ST = site transporter.

Source: Original

B6.4.5.8 Fault Tree



Source: Original

Figure B6.4-28. Impact to ST with AO

B7 HEATING VENTILATION AND AIR CONDITIONING FAULT TREE ANALYSIS

B7.1 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.

B7.1.1 Not Used.

B7.1.2 Not Used.

B7.1.3 BSC 2007. *CRCF 1 Composite Vent Flow Diagram Tertiary Conf ITS Exhaust & Non-ITS HVAC Supply Systems.* 060-M50-VCT0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071227.0013.

B7.1.4 BSC 2007. *CRCF 1 ITS Confinement Areas HEPA Exhaust System—Train A Ventilation & Instrumentation Diagram.* 060-M80-VCT0-00103-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0005.

B7.1.5 BSC 2007. *CRCF 1 ITS Confinement Areas HEPA Exhaust System—Train B Ventilation & Instrumentation Diagram.* 060-M80-VCT0-00104-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0006.

B7.1.6 BSC 2007. *CRCF 1 Equipment Sizing and Selection Calculation (ITS).* 060-M8C-VCT0-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0032.

Design Constraints

B7.1.7 NRC (Nuclear Regulatory Commission) 2007. *Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program.* HLWRS-ISG-03. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20070918.0096.

B7.2 IMPORTANT TO SAFETY HVAC DESCRIPTION

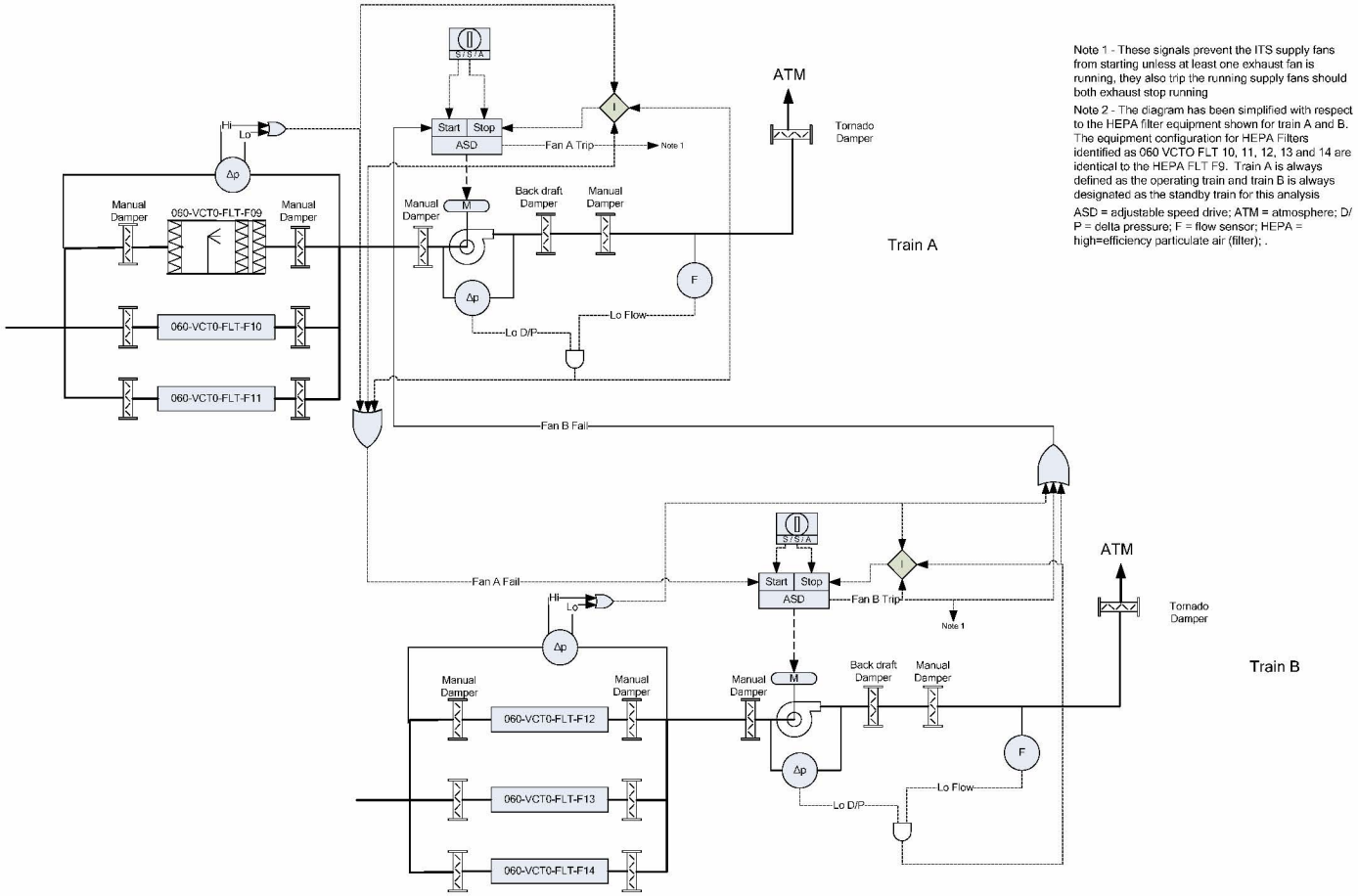
B7.2.1 Overview

The ITS HVAC provides HEPA filtered exhaust from the CRCF waste handling areas denoted as tertiary confinement (C2) zones. This minimizes the potential of discharging radioactive material released during waste handling operations to the environment. The ITS HVAC system consists of two identical trains. Each train consists of one exhaust fan, three parallel HEPA filtered exhaust plenums, isolation and backdraft dampers, and associated instrumentation and controls. The normal system lineup is with one train operating and the other train in standby. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. A backdraft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

A simplified schematic of the system and its associated controls is given in Figure B7.2-1.

Air distribution, ventilation rates, and transport velocities required to maintain design negative pressures and flows within the (C2) zones is provided in Ref. B7.1.6, Section 6.1.

Major components comprising the HVAC system include; a series of dampers that isolate components, and prevent reverse flow through the system, six HEPA filter plenums (three in each train) that remove particulate matter from the exhaust, and two exhaust fans (one in each train). Normal system control is provided by the digital control and management information system (DCMIS) through ASDs associated with each fan. ITS controls are hardwired bypassing the DCMIS to the fan ASD.



NOTE: It should be noted that, the diagram has been simplified with respect to the HEPA filter equipment shown for train A and B. The equipment configuration for HEPA Filters identified as 060 VCTO FLT 10, 11, 12, 13 and 14 are identical to the HEPA FLT 9. In addition, train B has the same input/output dampers shown for train A. Train A is always defined as the operating train and train B is always designated as the standby train.

ASD = adjustable speed drive; ATM = atmosphere; D/P = delta pressure; F = flow sensor; ITS = important to safety; HEPA = high=efficiency particulate air (filter).

Source: Original

Figure B7.2-1. Block Diagram of the CRCF ITS HVAC System

B7.2.2 Damper Subsystem Description

The ITS HVAC system uses manual, backdraft and tornado dampers to control flow and pressure inside the containment area, isolate components, and prevent backflow through the standby system. With the exception of the tornado and backdraft dampers, all control dampers in the ITS HVAC system are manual dampers. These dampers may be closed when maintenance is required on the standby train.

Manual dampers are located on the input and output sides of the HEPA filter plenum. These dampers are used to isolate the HEPA filter plenum, if required, during maintenance. There is a manual damper on the input side of the exhaust fan that is used to isolate the entire HEPA filter subsystem for maintenance on the HEPA filters or the exhaust fan. One additional manual damper is located between the backdraft and the tornado damper which can be used to isolate the entire train.

A backdraft damper is located on the exhaust side of the fan. This damper is normally open for the operating train and closed on the standby train. This damper prevents reverse airflow through the standby system as a result of the negative delta pressure in the C2 areas.

A tornado damper is used to control airflow automatically to prevent the transmission of tornado pressure surges from outside the facility.

Failure modes considered for these dampers are summarized in Table B7.2-1.

Table B7.2-1 HVAC Damper Failure Modes

Damper Type	Failure Mode	Discussion
Manual Dampers	Fail to remain open	These dampers are normally open dampers that are used to isolate equipment. They will block flow within a train if they fail to a closed position or were not restored to an open position if they were closed to isolate a component for maintenance.
Backdraft Dampers	Fail to open	Backdraft dampers close when the exhaust fan is not running to prevent backflow through the system. They are supposed to open when the exhaust fan starts. If the damper fails to open flow will be blocked, failing the train
	Fail to remain open	If the backdraft damper fails to remain open while the exhaust fan is running, flow through the train will be lost.
Tornado Dampers	Fail to remain open	The tornado damper is intended to close and isolate its associated HVAC train from pressure transients caused by a tornado. If it closes at any time other than when tornado conditions exist, it will block flow and defeat the train. If it operates as it is supposed to when tornado conditions exist it will close, blocking flow and defeating its associated HVAC train. Both conditions are captured in the tornado damper fails closed event in the HVAC fault tree.
	Fail to close	If the tornado damper fails to close when tornado conditions exist it would allow pressure transients within the train that could damage ducting or components.

B7.2.3 HEPA Filters

In each train there are three parallel HEPA filter plenums. Each plenum contains a preliminary bank of medium-efficiency roughing filters; followed by two banks of high-efficiency particulate air (HEPA) filters for particulate removal. The unit also contains a mister/demister for maintaining proper humidity levels and a water deluge system for fire suppression. The roughing filters are 60%-90% efficient in removing particulates and the HEPA filters remove particulates with 99.97% efficiency (Ref. B7.1.6, Appendix B). The HEPA plenums also contain an inlet test section, a combination test section, an outlet test section; these sections and the deluge system are not modeled in the fault tree analysis:

The preliminary bank of roughing filters consists of a 3 × 3 array (nine filters). The roughing filters are followed by two banks of HEPA filters. Each bank consists of 3 × 3 array (nine filters) for a total of 18 filters. Each filter plenum is sized for a maximum flow of 1,500 cfm Project Design Criteria Document (Ref. B7.1.6, Section 3.2.2).

Failure modes associated with the filter plenums (Table B7.2-2) considered in the analysis includes the HEPA filter bank for plugs and leaks, mister/demister for humidity control, and the medium roughing filter. A bag-in/bag-out procedure is used to replace the HEPA filters

Table B7.2-2 HEPA Plenum Failure Modes

Plenum Component	Failure Mode	Discussion
Mister/Demister	Plugs	The demister removes entrained moisture from the air by causing the air to rapidly change direction as it flows through the demister panel. This panel can become plugged with a combination of particulates and moisture over time.
Filters including the HEPA and roughing filters	Plug	Plugging of the filters will reduce flow, failing the train. When the supply fans are operating the flow rates require all three filter plenums to be operating in parallel to maintain the desired D/P. If the supply fans are inoperable the flow rates required to maintain the desired D/P are low enough that only two of the three filter plenums need to be in operation.
	Leak	Leaks through the filters can be from catastrophic failures that will be indicated by a large decrease in D/P across the filter plenum which would cause the control system to stop the operating train and start the standby train. Small leaks, such as those that might occur around the filter housing seals, however, may not be accompanied by a decrease in plenum D/P of sufficient magnitude to initiate an automatic switch over to the standby system. In this case the reduced D/P could be accompanied by increased radiation levels indicated in the discharge ducting. In this particular case the operator must recognize the indications of a small leak and initiate a manual switch over. Because leak data is does not differentiate between small and large leaks the leak failure modeled in the fault tree is accompanied by either a failure of the D/P sensing system or a failure of the operator to recognize the leaking condition.

B7.2.4 Direct Drive Exhaust Fan and Motor

The exhaust fan and motor are sized to provide a maximum airflow rate of 40,500 cfm with an exhaust fan motor rated at 200 horsepower CRCF 1 Air Pressure Drop Calculation (ITS) (Ref. B7.1.6, Section 6.1.2)). To meet delta pressure requirements for the CRCF, the exhaust system must provide an airflow rate of 35,010 cfm CRCF 1 Equipment Sizing and Selection Calculation (ITS) (Ref. B7.1.6, Appendix A, Table A-1)). At this airflow rate, the exhaust system provides for a total of 14.2 inches of water column required to maintain delta pressure in the facility CRCF 1 Equipment sizing and Selection Calculation (ITS) (Ref.B7.1.6, Section 3.1.4)).

The exhaust fan motor is rated at 1800 rpm (Ref. B7.1.6, Section 3.1.5) but the actual speed is controlled by the ASD. The ASD adjusts the speed to maintain delta pressure when facility doors are opened, HEPA filters lose efficiency, or when external winds affect room pressures within the facility.

The failure modes for the exhaust fans are fail to start and fail to run.

B7.2.5 Supply Fans

Two parallel AHUs supply ventilation to the Loadout area (Rm 1015) and two parallel AHUs supply ventilation to the Prep area (Rm 1026). These AHUs mix air recalculated from their associated areas with outside air to replenish leakage air flow that is exhausted by the ITS HVAC exhaust system. These systems are considered non-ITS and are not necessary for the successful operation of the ITS HVAC exhaust system. They do however determine the amount of air that must be exhausted by the operating ITS HVAC exhaust system to maintain cascaded air flow and Δp within the C2 zone. When the supply fans are operating more air must be exhausted by the operating exhaust fan and all three filter plenums in the operating exhaust train must be operating to maintain the required flow. When the supply fans are not operating less air needs to be exhausted and the flow through two HEPA plenums in the operating train are sufficient to maintain cascaded flow and Δp.

B7.2.6 Control Circuitry

Normal operation of the HVAC system is controlled by the DCMIS which controls each trains operating mode as determined by the operator (Start, Stop or Auto). The DCMIS also controls fan speed through an ASD to maintain facility flow and pressures within normal operating limits. Functions considered important to safety such as auto start of the standby train when the operating train fails are provided by hardwired interlocks that bypass the normal controls provided by the DCMIS.

The exhaust fan speed is controlled by an ASD which receives duct differential pressure signals from the DCMIS. The non-programmable ASD adjusts the exhaust fan speed to maintain these parameters within the specified operating band.

ASDs associated with the supply fans adjust the fans speed in response to temperature monitored in the room they supply. (Ref. B7.1.4, Ref. B7.1.5, and Ref. B7.1.3). The supply fans are used to stabilize the airflow within the CRCF. Although these fans are non-ITS their operation impacts

the air flow required to maintain Δp; consequently they are accounted for in the loss of HEPA filter plenum section of the fault tree model.

Automatic transfer from the operating train to the standby train is accomplished when the following conditions are sensed in the operating train.

1. Low flow sensed in the discharge plenum occurring concurrently with a low Δp sensed across the exhaust fan, or

2. Operating fan trip signal provided by the operating fan ASD indicating the fan has tripped, or

3. High Δp across the operating train filter plenums indicating the plenum is plugged, or

4. Low Δp across the operating train filter plenums, indicating the plenum is leaking.

Under normal operations with non-ITS supply fans working, all three HEPA filter plenums in the train must be working to achieve the exhaust flow rate of 35,010 cfm (Ref. B7.1.6, Section 6.1.1 (1)). Each HEPA filter plenum can filter 13,500 cfm at maximum efficiency (Ref. B7.1.6, Section 6.1.1 (2)). The design has some reserve capacity but not enough to maintain the required delta pressure if one of the HEPA filters fails when the supply fans are operating. Under normal operations, the only redundancy in the design is the second train.

B7.2.7 Equipment Door Interlocks

In order to maintain Δp in the C2 zone during receipt or export of transportation casks, aging overpacks or waste packages CRCF equipment access doors have been interlocked to preclude loss of Δp.

Equipment doors relied upon to maintain Δp in the prep area (Rm 1026) are the cask unloading room shield doors (060-CR00-DR-001 and 060-CR00-DR-002) and the confinement doors (060-CR00-DR-0010 and 060-CR00-DR-0011, and 060-CR00-DR-0012). The shield doors are interlocked with the confinement doors and their associated cask unloading room shield port to prevent them from opening unless all of the confinement doors and the port gate are closed. The confinement doors are interlocked with the shield doors to prevent them from opening unless both cask unloading room shield doors are closed.

Equipment doors that help maintain ΔP in the loadout area and the WP positioning room are the inner shield doors (060-CR00-DR-003 and 060-CR00-DR-004) between the loadout area and the WP positioning room and the outer shield doors (060-CR00-DR-005 and 060-CR00-DR-006) between the loadout room and the WP loadout vestibule. The inner doors are interlocked to prevent them from opening unless both outer shield doors are closed, the WP port slide gate is closed and personnel access doors to the area are closed. The outer shield doors are only interlocked with a radiation detector in the loadout area that prevents them from opening if a high radiation level exists in the loadout area. The outer shield doors are not prevented from opening if the WP positioning room shield doors are already open. These interlocks are summarized in Table B7.2-3.

Table B7.2-3 CRCF Confinement and Shield Door Interlocks

Door	Location	Function	Open Permissives	Close Permissives	Auto Opens	Auto Closes	Emergency Override
060-CR00-DR-000001	Between Cask Preparation Room (1026) and North Cask Unloading room (1023)	Shield Door	Conf DR 10 Closed	None	None	None	Yes
			Conf DR 11 Closed				
			Conf DR 12 Closed				
			North Cask Port Slide Gate Closed				
060-CR00-DR-000002	Between Cask Preparation room (1026) and South Cask Unloading room (1024)	Shield Door	Conf DR 10 Closed	None	None	None	Yes
			Conf DR 11 Closed				
			Conf DR 12 Closed				
			South Cask Port Slide Gate Closed				
060-CR00-DR-000003	Between North WP Positioning Room (1018) and WP Loadout Room (1015)	Shield Door	North WP Port Slide Gate Closed	None	None	None	Yes
			North WP Loadout Rm Shield Dr (05) Closed				
			South WP Loadout Rm Shield Dr (06) Closed				
			1st Floor North Personnel Access Dr (07) Closed				
			1st Floor South Personnel Access Dr (08) Closed				
			WP Loadout Rm Crane Access Dr (09) Closed				
060-CR00-DR-000004	Between South WP Positioning Room (1019) and WP Loadout Room (1015)	Shield Door	South WP Port Slide Gate Closed	None	None	None	Yes
			North WP Loadout Rm Shield Dr (05) Closed				
			South WP Loadout Rm Shield Dr (06) Closed				
			1st Floor North Personnel Access Dr (07) Closed				
			1st Floor South Personnel Access Dr (08) Closed				
			WP Loadout Rm Crane Access Dr (09) Closed				

Table B7.2-3 CRCF Confinement and Shield Door Interlocks (Continued)

Door	Location	Function	Open Permissives	Close Permissives	Auto Opens	Auto Closes	Emergency Override
060-CR00-DR-000005	North Door between WP Loadout Room (1015) and WP Loadout Vestibule (1014)	Shield Door	Radiation Level in WP Loadout Rm Not High	None	None	None	Yes
060-CR00-DR-000006	South Door between WP Loadout Room (1015) and WP Loadout Vestibule (1014)	Shield Door	Radiation Level in WP Loadout Rm Not High	None	None	None	Yes
060-CR00-DR-000010	South end of Cask Preparation Room (1026) to Transportation Cask Vestibule	Confinement	North Cask Unloading Rm Shield Dr (01) Closed South Cask Unloading Rm Shield Dr (02) Closed	None	None	None	No
060-CR00-DR-000011	East end of Cask Preparation Room (1026) to North access to ST Vestibule	Confinement	North Cask Unloading Rm Shield Dr (01) Closed South Cask Unloading Rm Shield Dr (02) Closed	None	None	None	No
060-CR00-DR-000012	East end of Cask Preparation Room (1026) to South access to ST Vestibule	Confinement	North Cask Unloading Rm Shield Dr (01) Closed South Cask Unloading Rm Shield Dr (02) Closed	None	None	None	No

ITS HVAC Normal Operations

Under normal operations with non-ITS supply fans working, all three HEPA filter plenums in the train must be working to achieve the exhaust flow rate of 35,010 cfm (Ref. B2.1.6, Section 6.1.1 (1)). Each HEPA filter plenum can filter 13,500 cfm at maximum efficiency (Ref. B2.1.6, Section 6.1.1 (2)). The design has some reserve capacity but not enough to maintain the required delta pressure if one of the HEPA filters fails when the supply fans are operating. Under normal operations, the only redundancy in the design is the second train.

B7.2.8 ITS HVAC Degraded Operations

The ITS HVAC system maintains proper delta pressure throughout Class C2 designated containment areas. Exhausted air from the CRCF is made-up from opening/closing doors to the outside, leaks in the structure and from one of two supply fans which are controlled by the ASD on the operating train. One of these fans in conjunction with other air makeup sources can provide sufficient airflow through the C2 containment areas for the HVAC to maintain delta pressure. These supply fans are not ITS and therefore, they are not connected to the ITS power system for the CRCF. Should these fans shut down, it becomes possible to maintain delta pressure with two of three HEPA filters. This special case has been added to the fault trees for the failure to maintain delta pressure in the CRCF. In this case, there is redundancy within the train and a common-cause failure mode has been added to the fault tree.

B7.2.9 ITS HVAC Testing and Maintenance

Under normal operations train A continues to operate until a failure is detected or the train is shut down for maintenance. Normal maintenance renders train B unavailable 40 hours per year (the majority of operational-level maintenance can be performed on the operational train and therefore does not affect the overall availability of the standby train). During maintenance, the train B "start/stop/auto" switch is placed in the stop position. When maintenance is completed, the standby system (train B) is started and operational system (train A) is shut down and is now considered to be the standby train (train A). Maintenance may be scheduled consecutively for this train or at some future date. Under normal operations, maintenance does not result in the loss of/or the inability of the operating train to perform its intended function.

Testing is considered part of routine maintenance. When the maintenance has been completed, maintenance personnel turns the standby train on and check for normal operations including delta pressure, flow rate, and that all failure indicators are reset/off. Maintenance personnel also observe the forced shutdown of the operating system as the standby train is turned on.

Flow rates are monitored as part of testing to ensure that airflow balance is maintained.

B7.3 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 B7.3-1 with the following dependencies:

1. Functional dependence

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

Table B7.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
ASD	Flow and pressure sensors	—	—	—	—
	Speed control for fan/motor	—	—	—	—
ΔP Exhaust Fans	—	Wind speed	—	—	—
Stop/Start/Auto Switch Position	—	—	—	Wrong position	—
Dampers	—	—	—	Wrong position	—
ITS Power	HVAC shuts down	—	—	—	—
Non-ITS Power	—	—	—	—	Supply fans stop
HEPA	—	—	—	Failure to notice leak	—
HVAC Maintenance	—	—	—	Trains can not switch	—
Vestibule Doors	Prep area and WP loadout area equipment doors are interlocked as described in Table 7.2-nnn	—	—	—	—
Alarm Panel (Non-ITS)	—	—	—	Failure to Respond to HVAC Alarm	—

NOTE: ASD = adjustable speed drive; ΔP = delta pressure; HEPA = high-efficiency particulate air (filter); HVAC = heating, ventilation, and air-conditioning; ITS = important to safety.

Source: Original

B7.4 HVAC RELATED FAILURE SCENARIO

There is a single top event for ITS HVAC failure which is stated as; Confinement zone exhaust system fails to maintain HEPA filtered flow. This model is also applicable to CRCF 2 and 3.

B7.4.1 Description

The ITS HVAC fault tree models component, system and human failures that contribute to failing to exhaust air from the C2 confinement zones through HEPA filters to the atmosphere. This includes loss of flow from the operating and standby trains and failures that bypass the HEPA filters while maintaining flow.

B7.4.2 Success Criteria

The purpose of the ITS HVAC system is to maintain a positive airflow from the confinement boundary through the operating areas to the HEPA filters, and into the atmosphere. The design of the system accomplishes this objective by functionally cascading Δps to maintain airflow toward the center of the facility where it is exhausted through HEPA filters to the atmosphere. Consequently the success criterion for the ITS HVAC is to maintain these Δps and associated exhaust flow through HEPA filters.

To accomplish this one of two HVAC trains must be operational with all exhaust flow passing through the HEPA filters before it is discharged to the atmosphere. The sizing of the exhaust motor and fan assembly will maintain the required Δps in sustained winds of up to 40 mph with less than 3 second gusts up to 90 mph. In addition, Δps may be lost for a period of time not to exceed 7 minutes in the CRCF if and only if one of the shield or confinement doors is open.

B7.4.3 Design Requirements and Features

Requirements

There is only one HVAC train in operation at anytime. The second train is on standby except when it is off-line for maintenance.

Alarms are on a panel in the continuously manned central control station and responded to by operators. Alarm conditions are: fan tripped, fan failure, fan low Δp, and low discharge flow. Operators are not required to respond to the alarm (ITS-HVAC trains are switched automatically); however, operators are expected to notify maintenance that a switch has occurred and maintenance is required to determine the cause of the failure and correct it.

Design Features

ITS HVAC system is in normal operation with three HEPA filter plenums. Each HEPA filter plenum consists of one 3 × 3 medium filter array and two 3 × 3 HEPA arrays.

B7.4.4 Testing and Maintenance

Requirements

HVAC maintenance personnel are notified when an alarm condition exists. Repairs are performed as soon as possible to return train to operational status.

While a HVAC train is undergoing maintenance, the train is not available for service.

Testing that requires the exhaust fan to run is performed on the active HVAC system.

Features

Normal maintenance is performed in accordance with manufacturer's recommendations.

B7.4.5 Fault Tree Model

The top event in this fault tree is "Delta Pressure not Maintained in CRCF Facility." This is defined as the inability of the ITS HVAC system to maintain delta pressure within the facility. The ITS HVAC system is a two train system. The configuration of the ITS HVAC systems in the CRCF facilities is essentially identical.

The fault tree model for the failure to maintain delta pressure in the facility includes those components that have been designated as ITS. There is only one exception and that is the inclusion of non-ITS supply fans that impact the exhaust fan run speed required to maintain Δp.

Interlocks in the ITS HVAC system addresses the potential for opening two or more of the confinement and shield doors as discussed under the door interlocks. (Note: There is no physical connection between this door interlock and the HVAC system.)

The mission time for the ITS HVAC system is set to 720 hours Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program (Ref. B7.1.7). This mission time applies to the ITS HVAC train that is in operation at the time the initiating event occurs. Should this train fail, the standby train is actuated and takes over the mission of maintaining an adequate delta pressure within the facility, for the rest of the time between the failure of the first train until the end of the 720 hours after the initiating event. Considering that a failure of the first train can randomly occur at any time over the mission time of 720 hours, the standby ITS HVAC train, if needed, will have a mission time that is in average half the mission time of the first train, i.e., 720/2 = 360 hours. This reduced mission time is applied in SAPHIRE to the standby ITS HVAC train.

B7.4.6 Basic Event Data

Table B7.4-1 contains a list of basic events used in the loss of delta pressure in the CRCF. The model contains undeveloped transfers to ITS power systems. These failures are addressed in Attachment B8. Reliability data for basic events is detailed in Attachment C with the following exceptions:

A. Three are associated with human error. HFE detailed analysis is in Section 6.4 and Attachment E:

   1. Opening two or more equipment doors.
   2. Failure to properly restore system after maintenance.
   3. Failure to notice HEPA filter leak.

B. Unavailability of the standby train due to scheduled maintenance which is based on a conservative estimate.

C. Loss of delta pressure as a direct result of opening a vestibule door and the time it takes for the HVAC exhaust fans to re-establish delta pressure.

D. Two common-cause failures:

1. Common-cause failures of the HEPA filters in the degraded mode.
2. Common-cause failures of the non-ITS supply fans.

Table B7.4-1. Basic Event Probability for the Failure to Maintain Delta Pressure in the CRCF Fault Tree

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-EXCESSIVE-WIND-SPEED	Loss of dp due to sustained wind speeds exceeding 30 MPH	1	4.700E-03	4.700E-03	0.000E+00	0.000E+00
060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCTO-AHU0013-FAN-FTR	AHU 013 fan fails to run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCTO-AHU0014-FAN-FTR	AHU 014 fan fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
060-VCTO-BDMP00A-UDM-FOH	Damper (Backdraft) Failure	3	1.614E-02	0.000E+00	2.260E-05	7.200E+02
060-VCTO-BDMP00B-UDM-FOH	Train B fan discharge backdraft damper fails closed	3	8.103E-03	0.000E+00	2.260E-05	3.600E+02
060-VCTO-BDMP00B-DTM-FOD	Train B backdraft damper fails to open when fan starts	1	8.710E-04	8.710E-04	0.000E+00	0.000E+00
060-VCTO-DCT0A-DTC-RUP	Train A Duct Ruptures	3	2.675E-03	0.000E+00	3.720E-06	7.200E+02
060-VCTO-DCT0B-DTC-RUP	Train B Duct Ruptures	3	1.338E-03	0.000E+00	3.720E-06	3.600E+02
060-VCTO-DMP000A-DMP-FRO	Train A fan discharge manual isolation damper fails closed	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-DMP000B-DMP-FRO	Train B fan discharge manual isolation damper fails closed	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-DMPF00A-DMP-FRO	Train A fan inlet manual isolation damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-DMPF00B-DMP-FRO	Train B fan inlet manual isolation damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-DR0001-HFI-NOD	Operator opens 1 inner door and 1 outer door	1	1.000E-02	1.000E-02	0.000E+00	0.000E+00
060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCTO-FAN00A-PRM-FOH	Train A exhaust fan fails due to ASD malfunction	3	3.873E-04	0.000E+00	5.380E-07	7.200E+02
060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02

Table B7.4-1. Basic Event Probability for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-VCTO-FAN00B-FAN-FTS	Train B exhaust fan fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
060-VCTO-FAN00B-PRM-FOH	Train B exhaust fan fails due to ASD malfunction	3	1.937E-04	0.000E+00	5.380E-07	3.600E+02
060-VCTO-FANBASD-CTL-FOD	Train B ASD start logic signal fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCTO-HEPA-CCF	CCF of 2 of 3 filter plenums	C	9.531E-05	---	---	---
060-VCTO-HEPAB-CCF	Common Cause Failure of HEPA Filters (2 of 3)	C	4.769E-05	---	---	---
060-VCTO-HEPALK-HFI-NOD	Operator fails to shift trains when alarm occurs	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1	1.000E-01	1.000E-01	0.000E+00	0.000E+00
060-VCTO-IEL0001-IEL-FOD	CRCF Door Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
060-VCTO-IEL0002-IEL-FOD	Interlock Failure on Demand	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
060-VCTO-PLEN09-DMS-FOH	Train A plenum 09 moisture separator/demister plugs	3	6.545E-03	0.000E+00	9.120E-06	7.200E+02
060-VCTO-PLEN09-HEP-LEK	Train A Plenum 9 HEPA filters leak	3	2.158E-03	0.000E+00	3.000E-06	7.200E+02
060-VCTO-PLEN09-HEP-PLG	Train A Plenum 9 HEPA filters plug	3	3.070E-03	0.000E+00	4.270E-06	7.200E+02
060-VCTO-PLEN09I-DMP-FRO	Train A filter plenum 09 inlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN09O-DMP-FRO	Train A filter plenum 09 outlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN10-DMS-FOH	Train A plenum 10 moisture separator/demister plugs	3	6.545E-03	0.000E+00	9.120E-06	7.200E+02
060-VCTO-PLEN10-HEP-LEK	Train A Plenum 10 HEPA filters leak	3	2.158E-03	0.000E+00	3.000E-06	7.200E+02
060-VCTO-PLEN10-HEP-PLG	Train A Plenum 10 HEPA filters plug	3	3.070E-03	0.000E+00	4.270E-06	7.200E+02
060-VCTO-PLEN10I-DMP-FRO	Train A filter plenum 10 inlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN10O-DMP-FRO	Train A filter plenum 10 outlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN11-DMS-FOH	Train A plenum 11 moisture separator/demister plugs	3	6.545E-03	0.000E+00	9.120E-06	7.200E+02

Table B7.4-1. Basic Event Probability for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-VCTO-PLEN11-HEP-LEK	Train A Plenum 11 HEPA filters leak	3	2.158E-03	0.000E+00	3.000E-06	7.200E+02
060-VCTO-PLEN11-HEP-PLG	Train A Plenum 11 HEPA filters plug	3	3.070E-03	0.000E+00	4.270E-06	7.200E+02
060-VCTO-PLEN11I-DMP-FRO	Train A filter plenum 11 inlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN11O-DMP-FRO	Train A filter plenum 11 outlet damper fails to remain open	3	6.033E-05	0.000E+00	8.380E-08	7.200E+02
060-VCTO-PLEN12-DMS-FOH	Train B plenum 12 moisture separator/demister plugs	3	3.278E-03	0.000E+00	9.120E-06	3.600E+02
060-VCTO-PLEN12-HEP-LEK	Train B Plenum 12 HEPA filters leak	3	1.079E-03	0.000E+00	3.000E-06	3.600E+02
060-VCTO-PLEN12-HEP-PLG	Train B Plenum 12 HEPA filters plug	3	1.536E-03	0.000E+00	4.270E-06	3.600E+02
060-VCTO-PLEN12I-DMP-FRO	Train B filter plenum 12 inlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-PLEN12O-DMP-FRO	Train B filter plenum 12 outlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-PLEN13-DMS-FOH	Train B plenum 13 moisture separator/demister plugs	3	9.120E-06	0.000E+00	9.120E-06	0.000E+00
060-VCTO-PLEN13-HEP-LEK	Train B Plenum 13 HEPA filters leak	3	3.000E-06	0.000E+00	3.000E-06	0.000E+00
060-VCTO-PLEN13-HEP-PLG	Train B Plenum 13 HEPA filters plug	3	1.536E-03	0.000E+00	4.270E-06	3.600E+02
060-VCTO-PLEN13I-DMP-FRO	Train B filter plenum 13 inlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-PLEN13O-DMP-FRO	Train B filter plenum 13 outlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-PLEN14-DMS-FOH	Train B plenum 14 moisture separator/demister plugs	3	3.278E-03	0.000E+00	9.120E-06	3.600E+02
060-VCTO-PLEN14-HEP-LEK	Train B Plenum 14 HEPA filters leak	3	3.000E-06	0.000E+00	3.000E-06	0.000E+00
060-VCTO-PLEN14-HEP-PLG	Train B Plenum 14 HEPA filters plug	3	1.536E-03	0.000E+00	4.270E-06	3.600E+02
060-VCTO-PLEN14I-DMP-FRO	Train B filter plenum 14 inlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02
060-VCTO-PLEN14O-DMP-FRO	Train B filter plenum 14 inlet damper fails to remain open	3	3.017E-05	0.000E+00	8.380E-08	3.600E+02

Table B7.4-1. Basic Event Probability for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
060-VCTO-RSH005-SRR-FOH	High rad door interlock permissive fails	3	8.804E-02	0.000E+00	1.280E-04	7.200E+02
060-VCTO-RSH114-SRR-FOH	Exhaust high rad alarm fails	3	2.000E-05	0.000E+00	2.000E-05	0.000E+00
060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	3	1.614E-02	0.000E+00	2.260E-05	7.200E+02
060-VCTO-TDMP00B-DTM-FOH	Train B tornado damper fails closed when tornado conditions don't exist	3	8.103E-03	0.000E+00	2.260E-05	3.600E+02
060-VCTO-TRAINB-MAINT	Train B unavailable due to maintenance	1	4.570E-03	4.570E-03	0.000E+00	0.000E+00
060-VCTO-TRATRIP-CTL-FOD	Logic Controller Fails on Demand	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-WP-LORM-NOT	High radiation source not present	1	9.500E-01	9.500E-01	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. See Table 6.3-1 for calculation type definitions.

Calc. = calculation; CRCF = Canister Receipt and Closure Facility; DP = delta pressure; Fail. = failure; Miss. = mission; P = pressure; Prob. = probability.

Source: Original

B7.4.6.1 Human Failure Events

There are three basic human failure events (HFE) associated with human error listed in Table B7.4-2. They are for inadvertently opening two or more vestibule doors at the same time, failure to notice that there is a HEPA leak and leaving the "start/stop/auto" switch on the standby train in the wrong position.

Table B7.4-2. Human Failure Events

Basic Event Name	Basic Event Description
060-VCTO-DR00001-HFI-NOD	Operator opens 1 inner and 1 outer door
060-VCTO-HEPALK-HFI-NOD	Operator fails to shift trains when alarm occurs
060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position

NOTE: CRCF = Canister Receipt and Closure Facility; HEPA = high-efficiency particulate air (filter).

Source: Original

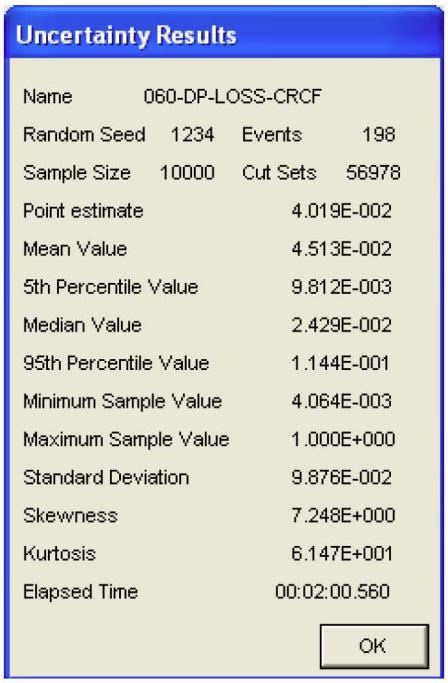
B7.4.6.2 Common-Cause Failures

There are two common-cause failures identified in the HVAC model. Two of the common-causes are associated with the potential of a HEPA filter failure in the degraded mode of operation for the HVAC (operation with the supply fans inoperable). In the degraded mode the HEPA filters operate in a two-of-three success situation. The CCF compound event is developed

from the appropriate alpha factors from Attachment C section C3 and the HEPA random failure probabilities for plugged failure.

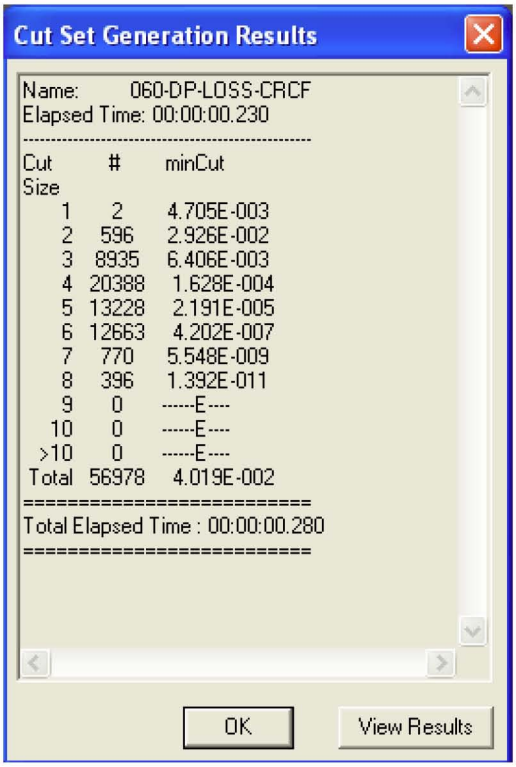
B7.4.7 Uncertainty and Cut Set Generation

Figure B7.4-1 contains the uncertainty results obtained from running the fault trees for "Failure to Maintain Delta Pressure" using a cutoff probability of 1E-15. Figure B7.4-2 provides the cut set generation results for the "Failure to Maintain Delta Pressure" fault tree. These results are for the HVAC system coupled with loss of electrical power, which is discussed separately in Section B8. If loss of electrical power is not included in the HVAC tree, the mean failure probability and standard deviation of the HVAC system alone is 3.1E-02 and 6.0E-02.



Source: Original

Figure B7.4-1. Uncertainty Results of the Failure to Maintain Delta Pressure Fault Tree



Source: Original

Figure B7.4-2. Cut Set Generation Results for the Failure to Maintain Delta Pressure Fault Tree

B7.4.8 Cut Sets

Table B7.4-3 contains the top 40 cut sets for the "Failure to Maintain Delta Pressure" fault tree.

Table B7.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure Fault Tree

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-DP-LOSS-CRCF	23.64	9.500E-003	060-VCTO-DR0001-HFI-NOD	Operator opens 1 inner door and 1 outer door	1.000E-002
			060-WP-LORM-NOT	High radiation source not present	9.500E-001
	12.59	5.059E-003	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	11.69	4.700E-003	060-EXCESSIVE-WIND-SPEED	Loss of dp due to sustained wind speeds exceeding 30 MPH	4.700E-003
	4.41	1.772E-003	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-001
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-001
			LOSP	Loss of offsite power	2.990E-003
	4.02	1.614E-003	060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
			060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	1.614E-002
	4.02	1.614E-003	060-VCTO-BDMP00A-UDM-FOH	Damper (Backdraft) Failure	1.614E-002
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	3.22	1.296E-003	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	2.562E-002
	2.19	8.804E-004	060-VCTO-DR0001-HFI-NOD	Operator opens 1 inner door and 1 outer door	1.000E-002
			060-VCTO-RSH005-SRR-FOH	High rad door interlock permissive fails	8.804E-002
	1.34	5.378E-004	060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	5.378E-003
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	1.03	4.135E-004	060-VCTO-BDMP00A-UDM-FOH	Damper (Backdraft) Failure	1.614E-002
			060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	2.562E-002
	1.03	4.135E-004	060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	2.562E-002
			060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	1.614E-002
	1.02	4.099E-004	060-VCTO-BDMP00B-UDM-FOH	Train B fan discharge backdraft damper fails closed	8.103E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
	1.02	4.099E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-TDMP00B-DTM-FOH	Train B tornado damper fails closed when tornado conditions don't exist	8.103E-003

Table B7.4-3. Dominant Cut Sets for The Loss of Delta Pressure in The CRCF (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-DP-LOSS-CRCF (Continued)	0.95	3.816E-004	060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 Feed Breaker Spurious Operation	3.816E-003
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	0.95	3.816E-004	060-#EEE-LDCNTRA-C52-SPO	Load Center A Feed Circuit Breaker (AC) Spurious Operation	3.816E-003
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	0.73	2.937E-004	060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-001
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS SWGR A feed Breaker Spurious Operation	3.816E-003
	0.73	2.937E-004	060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-001
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-003
	0.68	2.732E-004	060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
			26D-#EEESWGRDGA-AHU-FTR	13.8kV ITS Switchgear room Air Handling Unit Fails	2.732E-003
	0.68	2.721E-004	060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 Failure	5.378E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
	0.64	2.559E-004	060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-002
			060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	5.059E-002
			060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
	0.58	2.312E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-TRAINB-MAINT	Train B unavailable due to maintenance	4.570E-003
	0.57	2.302E-004	060-VCTO-HFIA000-HFI-NOM	HVAC Train B control switch in wrong position	1.000E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-001
			LOSP	Loss of offsite power	2.990E-003
	0.48	1.930E-004	060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 Feed Breaker Spurious Operation	3.816E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
	0.48	1.930E-004	060-#EEE-LDCNTRB-C52-SPO	CRCF ITS Load Center Circuit Breaker (AC) Spur Op	3.816E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002

Table B7.4-3. Dominant Cut Sets for The Loss of Delta Pressure in The CRCF (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-DP-LOSS-CRCF (Continued)	0.41	1.658E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-PLEN14-DMS-FOH	Train B plenum 14 moisture separator/demister plugs	3.278E-003
	0.41	1.658E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-PLEN12-DMS-FOH	Train B plenum 12 moisture separator/demister plugs	3.278E-003
	0.37	1.486E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-001
			26D-#EEY-OB-SWGB-C52-SPO	13.8kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-003
	0.37	1.486E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-001
			27A-#EEE-BUS3DGB-C52-SPO	13.8kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-003
	0.34	1.382E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			26D-#EEE-SWGRDGB-AHU-FTR	EDGB Switchgear Room Air Handling Unit Failure to Run	2.732E-003
	0.34	1.378E-004	060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	5.378E-003
			060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	2.562E-002
	0.33	1.308E-004	060-VCTO-BDMP00A-UDM-FOH	Damper (Backdraft) Failure	1.614E-002
			060-VCTO-BDMP00B-UDM-FOH	Train B fan discharge backdraft damper fails closed	8.103E-003
	0.33	1.308E-004	060-VCTO-BDMP00B-UDM-FOH	Train B fan discharge backdraft damper fails closed	8.103E-003
			060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	1.614E-002
	0.33	1.308E-004	060-VCTO-BDMP00A-UDM-FOH	Damper (Backdraft) Failure	1.614E-002
			060-VCTO-TDMP00B-DTM-FOH	Train B tornado damper fails closed when tornado conditions don't exist	8.103E-003
	0.33	1.308E-004	060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	1.614E-002
			060-VCTO-TDMP00B-DTM-FOH	Train B tornado damper fails closed when tornado conditions don't exist	8.103E-003

Table B7.4-3. Dominant Cut Sets for The Loss of Delta Pressure in The CRCF (Continued)

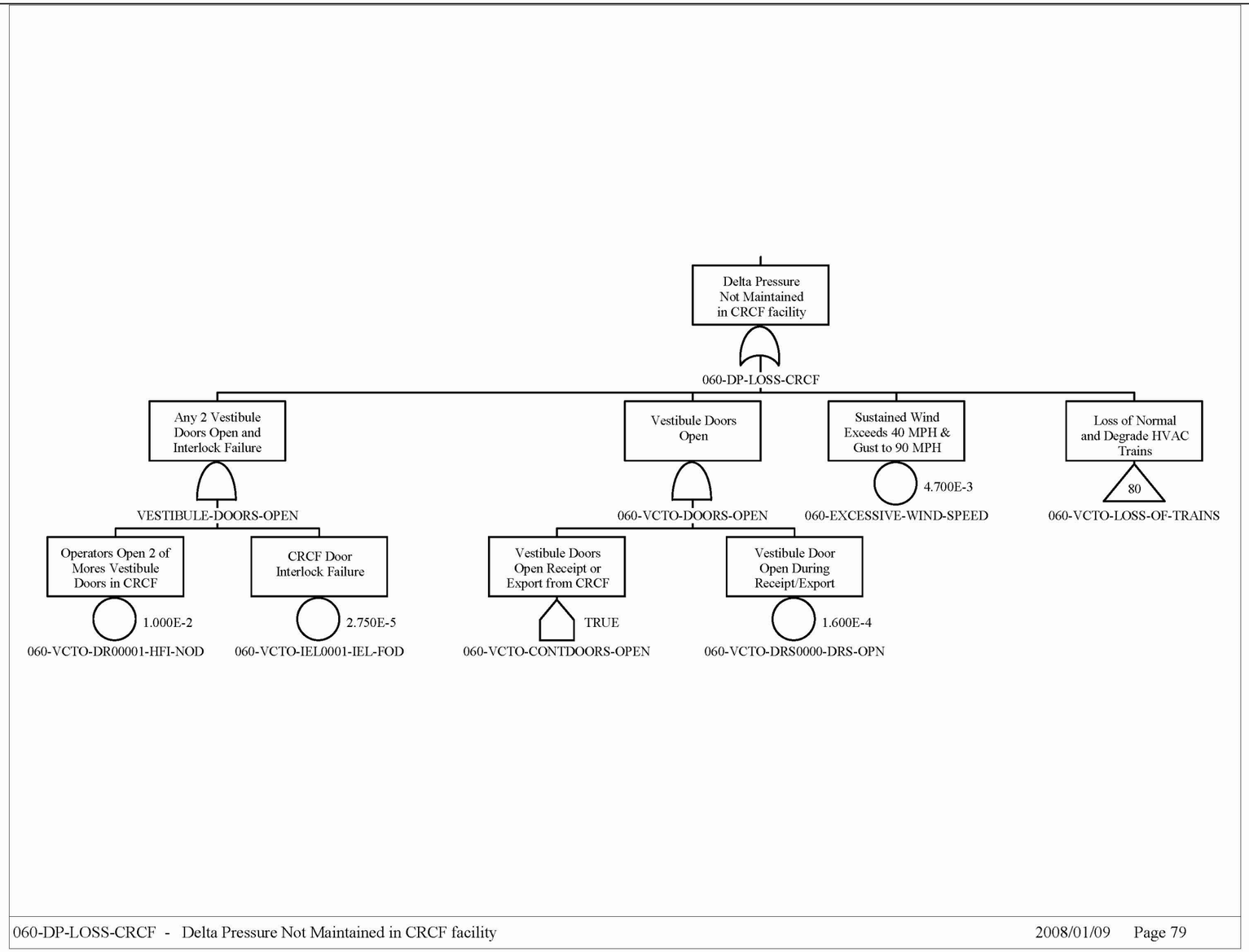
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-DP-LOSS-CRCF (Continued)	0.32	1.295E-004	060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-002
			060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh. Fan 8 Fails to Run	5.059E-002
	0.29	1.164E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-001
			LOSP	Loss of offsite power	2.990E-003
	0.26	1.027E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-TRATRIP-CTL-FOD	Logic Controller Fails on Demand	2.030E-003
	0.26	1.027E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-FANBASD-CTL-FOD	Train B ASD start logic signal fails	2.030E-003
	0.25	1.022E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.059E-002
			060-VCTO-FAN00B-FAN-FTS	Train B exhaust fan fails to start	2.020E-003
	0.24	9.777E-005	060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 Feed Breaker Spurious Operation	3.816E-003
			060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	2.562E-002

NOTE: AC = alternating current; CRCF = canister receipt and closure facility; DG = diesel generator; Elec = electrical; Exh = exhaust; Freq. = frequency; HEPA = high efficiency particulate air; ITS = important-to-safety; MCC = motor control center; Prob. = probability; SWGR = switchgear

Source: Original

B7.4.9 HVAC Fault Trees

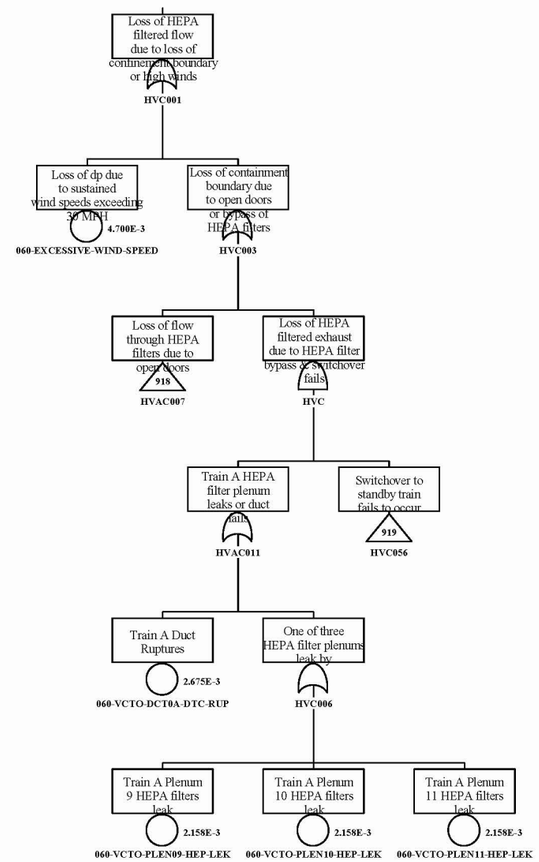
The following fault trees show the transfers to the ITS electrical system for the HVAC equipment. For specifics on the electrical system, refer to the "AC Power System Fault Tree Analysis" in Attachment B8.



Source: Original

Figure B7.4-3. Delta Pressure Not Maintained in CRCF Facility

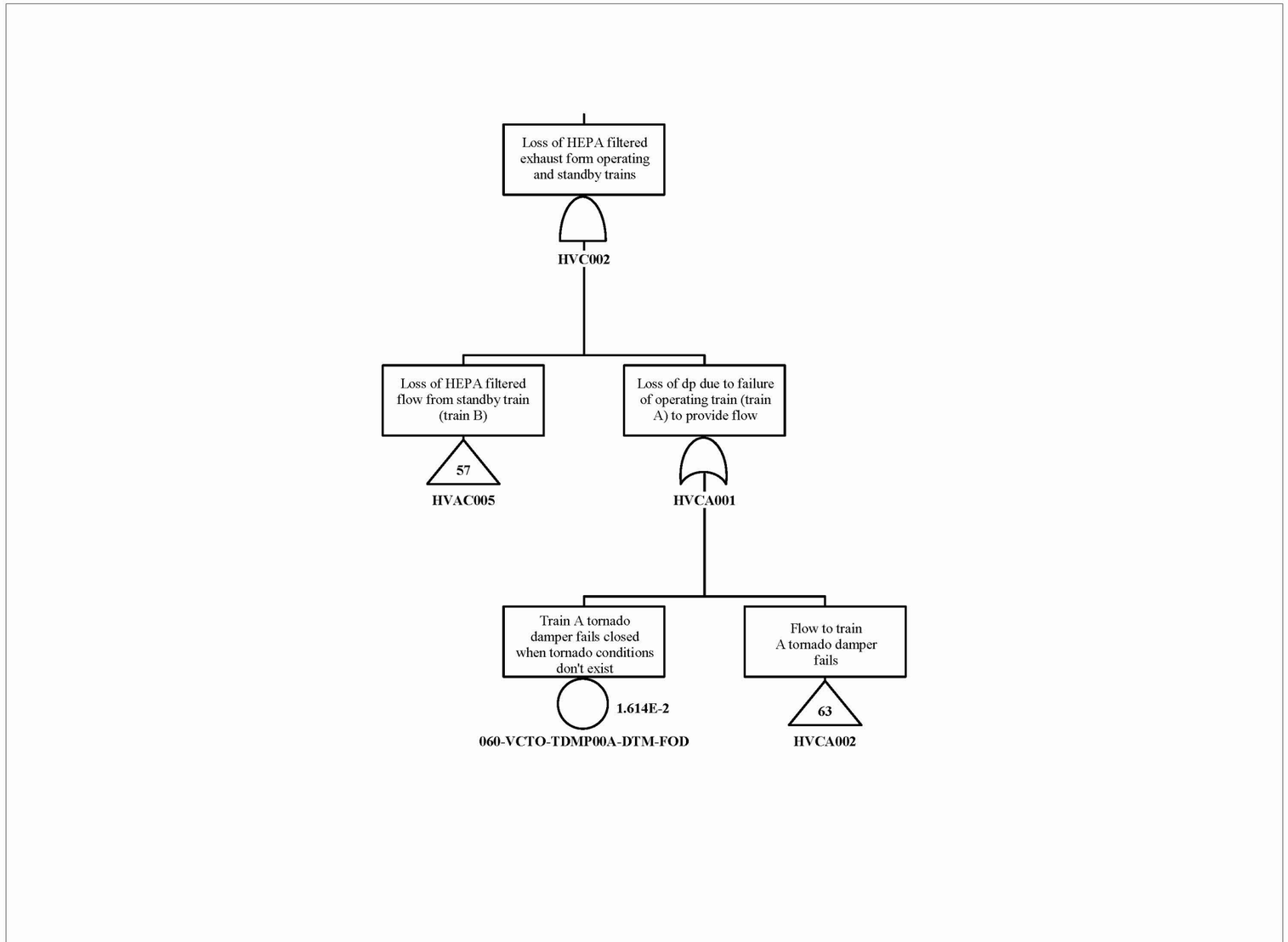
INTENTIONALLY LEFT BLANK



Source: Original

Figure B7.4-4. Loss of HEPA Filtered Flow due to Loss of Confinement Boundary or High Winds

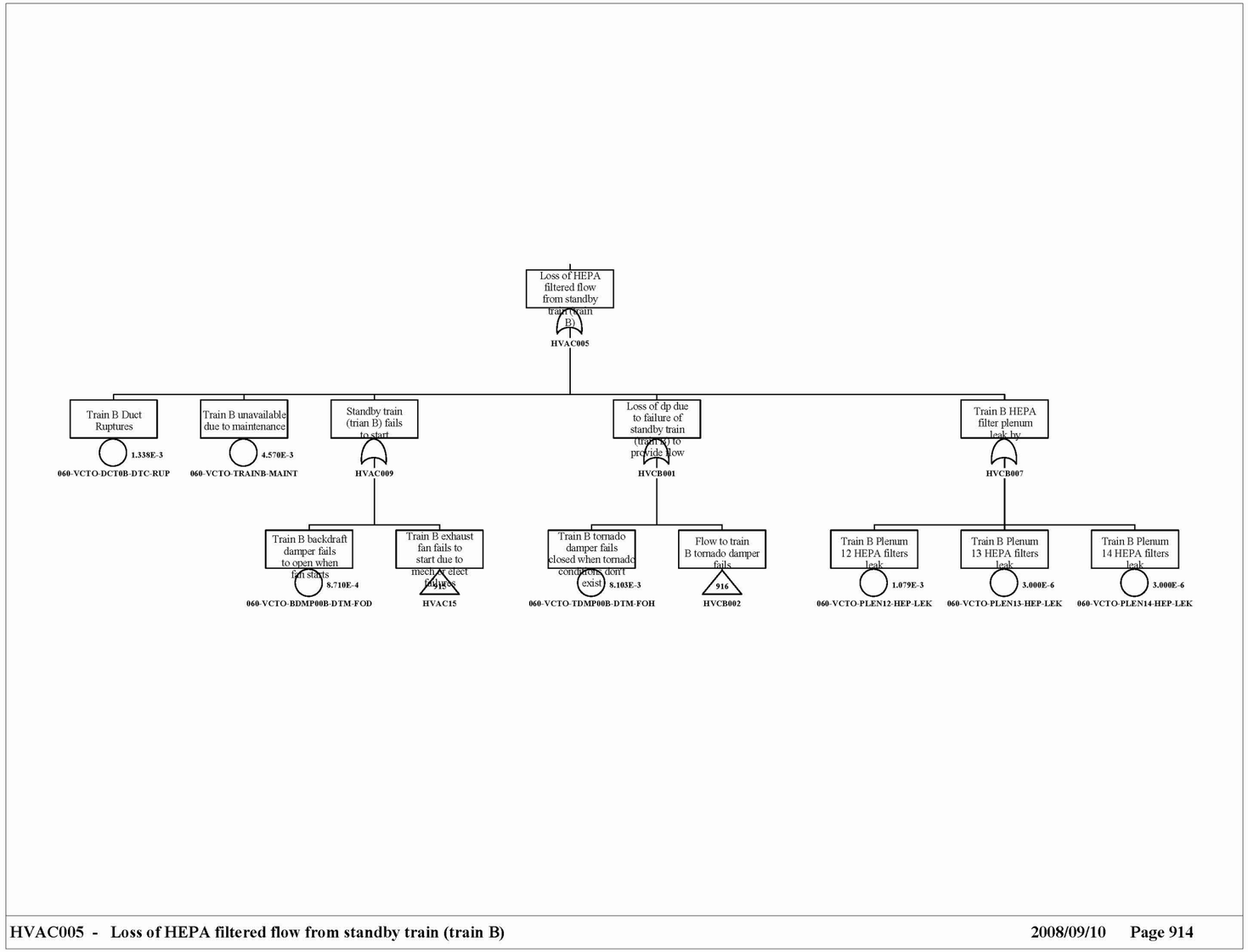
INTENTIONALLY LEFT BLANK



Source: Original

Figure B7.4-5. Loss of HEPA Filtered Exhaust from Operating and Standby Trains

INTENTIONALLY LEFT BLANK



Source: Original

Figure B7.4-6. Loss of HEPA Filtered Flow from Standby Train (Train B)

INTENTIONALLY LEFT BLANK