B6.4.2 Site Transporter Load Drop during Lift/Movement (ESD-08)

B6.4.2.1 Description

The site transporter conducts lift/lowering and movement operations at the aging pads and inside the facilities. Since the site transporter is only capable of performing one operation at a time it is not possible to move an aging overpack while it is being lifted/lowered. For activities associated with this ESD, there are four distinct failure modes. Those associated with electrical failures, site transporter controller failures, mechanical failures during lifting and lowering, and mechanical failures during movement.

B6.4.2.2 Success Criteria

The potential for a load drop exists when there is a loss of site transporter power, a hardware failure of the lift/lowering devices, aging overpack restraint device failure during movement, or a failure of the site transporter control system during these operations.

If there is a failure of the electrical system during lifting/lower or movement, the ACME screw/nuts prevent the rear forks and the lift support arms from moving. There is a potential for a common-cause failure of the forks.

The ACME devices also serve to prevent a load drop when there is a lift boom failure. There are four of these devices: one on each of the rear forks and one on each of the lift support arms.

The aging overpack restraint system is engaged after the lift has been accomplished and released prior to performing a lowering operation. These devices restrict the movement of the aging overpack during transport. There are three of these restraints that prevent/restrict movement in the X-Y axis. Pins are used in these devices that prevent the release of the restraint in the advent of an electromechanical failure that controls the position of these devices.

There is an interlock built-in to the restraint system. Movement of the site transporter is prevented until the three pins in the restraint system have been properly installed. These pins also preclude an inadvertent release of the restraint system since they have to be removed from their engaged position before the restraints can be released.

The receipt of inadvertent command signals is also prevented in that the site transporter can only perform one operation at a time due to the limitations in the power plant.

B6.4.2.3 Design Requirements and Features

Requirements

Facility power is removed from the site transporter when it has been properly position within the Loading Room.

On the loss or removal of AC power derived from the facility, the site transporter performs a controlled stop. Once stopped the site transporter 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 in the design of the site transporter. When the facility AC power cable is removed, the site transporter is incapable of movement.

Two operators have the capability of stopping any operation performed by the site transporter when it is inside a facility.

B6.4.2.4 Fault Tree Model

The fault tree model for site transporter drop load during lift and movement addresses:

- Electrical failures including motor and distribution events and the failure to enter a lock mode safe state.
- A load drop during the lifting or lowering of the aging overpack which includes mechanical failure of the lifting booms and restraint/lifting arms.
- Failure of the aging overpack restraint subsystem during the lift/lowering/moving of the site transporter.
- Failure of the site transporter control subsystem.

NOTE: The fault tree defines the movement of the aging overpack in a three axis system as:

1. A roll movement side-to-side as the "R-axis."
2. A pitch movement front-to-back as the "P-axis."
3. A drop movement as the "D-axis."

B6.4.2.5 Basic Events Data

Table B6.4-3 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 B6.4-6 and B6.4-7 respectively.

Table B6.4-3. Basic Event Probability for the Load Drop during Lift/Movement

Basic Events Probability Report					
Project: Yucca-Mountain		Case: Current			
ST Load Drop Lift/Movement		Units: Per Hour			
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-CRWT-ATB1001-AT--FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATB1011-AT--FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATB2002-AT--FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATB222-AT--FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATD0002-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATD001-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATD03-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000

Table B6.4-3. Basic Event Probability for the Load Drop during Lift/Movement (Continued)

Basic Events Probability Report					
Project: Yucca-Mountain		**Case: Current**			
ST Load Drop Lift/Movement		**Units: Per Hour**			
Name	**Calc. Type[a]**	**Calc. Prob.**	**Fail. Prob.**	**Lambda**	**Miss. Time[a]**
200-CRWT-ATD04-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATP002-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATR10002-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-ATR2004-AT-FOH	3	7.540E-005	0.000E+000	7.540E-005	1.000E+000
200-CRWT-BEA#1-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEA22-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAB202-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAD003-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAD006-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAP02-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAR103-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-BEAR204-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-CBP0000-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
200-CRWT-CON0000-CON-FOH	3	7.140E-005	0.000E+000	7.140E-005	1.000E+000
200-CRWT-CTSHC000-CT-SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
200-CRWT-DROP11-BEA-BRK	3	2.400E-008	0.000E+000	2.400E-008	1.000E+000
200-CRWT-ECP0000-ECP-FOH	3	1.790E-006	0.000E+000	1.790E-006	1.000E+000
200-CRWT-ELEC-MOE-FOD	1	6.000E-005	6.000E-005	0.000E+000	0.000E+000
200-CRWT-IEL0001-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
200-CRWT-LC000011-LC-FOD	1	6.250E-004	6.250E-004	0.000E+000	0.000E+000
200-CRWT-LVRD01-LVR-FOH	3	2.100E-006	0.000E+000	2.100E-006	1.000E+000
200-CRWT-LVRD02-LVR-FOH	3	2.100E-006	0.000E+000	2.100E-006	1.000E+000
200-CRWT-PIND004-PIN-BRK	3	2.120E-009	0.000E+000	2.120E-009	1.000E+000
200-CRWT-PIND005-PIN-BRK	3	2.120E-009	0.000E+000	2.120E-009	1.000E+000
200-CRWT-PINP04-PIN-BRK	3	2.120E-009	0.000E+000	2.120E-009	1.000E+000
200-CRWT-PINR103-PIN-BRK	3	2.120E-009	0.000E+000	2.120E-009	1.000E+000
200-CRWT-PINR202-PIN-BRK	3	2.120E-009	0.000E+000	2.120E-009	1.000E+000
200-CRWT-SJKB011-SJK-FOH	3	8.140E-006	0.000E+000	8.140E-006	1.000E+000
200-CRWT-SJKB101-SJK-FOH	3	8.140E-006	0.000E+000	8.140E-006	1.000E+000
200-CRWT-SJKB202-SJK-FOH	3	8.140E-006	0.000E+000	8.140E-006	1.000E+000
200-CRWT-SJKB22-SJK-FOH	3	8.140E-006	0.000E+000	8.140E-006	1.000E+000
200-CRWT-ZSD00005-ZS-FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
200-CRWT-ZSD0006-ZS-FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
200-CRWT-ZSP00003-ZS-FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
200-CRWT-ZSR00005-ZS-FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
200-ST-MOE0001-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	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; ST = site transporter.

Source: Original

B6.4.2.5.1 Human Failure Events

There are two human error events incorporated in the tree. These are:

- Operator action which results in a load drop. This is set to a screening value of 1E-03.
- Operator sends wrong command which results in a load drop. This event is also set to a screening value of 1E-03.

B6.4.2.5.2 Common-Cause Failures

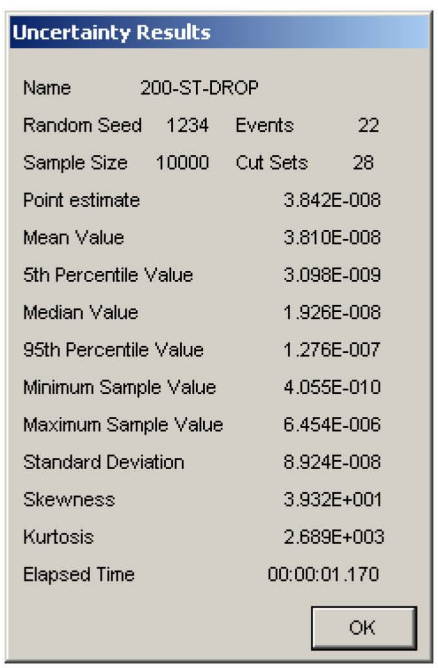
There are no CCFs identified in this fault tree.

B6.4.2.6 Uncertainty and Cut Set Generation Results

Figure B6.4-6 contains the uncertainty results obtained from running the fault tree for the "Site Transporter Load Drop during Lift and Movement" fault tree. Figure B6.4-7 provides the cut set generation results for the "Site Transporter Load Drop during Lift and Movement" fault tree, calculated using a 1E-15 cutoff. The fault trees are shown in Figures B6.4-8 through B6.4-19.

B6.4.2.7 Cut Sets

Table B6.4-4 contains the cut sets for the "Site Transporter Load Drop during Lift and Movement" fault tree.



Uncertainty Results

Name	200-ST-DROP		
Random Seed	1234	Events	22
Sample Size	10000	Cut Sets	28
Point estimate			3.842E-008
Mean Value			3.810E-008
5th Percentile Value			3.098E-009
Median Value			1.926E-008
95th Percentile Value			1.276E-007
Minimum Sample Value			4.055E-010
Maximum Sample Value			6.454E-006
Standard Deviation			8.924E-008
Skewness			3.932E+001
Kurtosis			2.689E+003
Elapsed Time			00:00:01.170

OK

Source: Original

Figure B6.4-6. Uncertainty Results for the Site Transporter Load Drop during Lift and Movement Fault Tree

Cut Set Generation Results

Name: 200-ST-DROP

Elapsed Time: 00:00:00.000

Cut Sets Size	#	UpperBound
1	0	------E----
2	18	3.842E-008
3	10	5.502E-013
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	28	3.842E-008

OK

Source: Original

Figure B6.4-7. Cut Set Generation Results for the Site Transporter Load Drop during Lift and Movement Fault Tree

Table B6.4-4. Cut Sets for the Site Transporter Load Drop during Lift and Movement Fault Tree

Fault Tree	Cut Set%	Prob./Freq.	Basic Event	Description	Probability
200-ST-DROP	36.92	1.419E-008	200-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E-005
			200-CRWT-LC000011-LC-FOD	ST lift/lower selector level fails	6.250E-004
	20.97	8.057E-009	200-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-005
			200-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	2.930E-004
	20.97	8.057E-009	200-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-005
			200-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	2.930E-004
	20.97	8.057E-009	200-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-005
			200-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	2.930E-004
	0.11	4.063E-011	200-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E-005
			200-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	1.790E-006
	0.02	7.032E-012	200-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	2.400E-008
			200-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-004
	0.02	7.032E-012	200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-008
			200-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-004
	0.00	1.810E-012	200-CRWT-ATD0002-AT-FOH	ST D-axis Electrical Actuator #2 fails lift/lower	7.540E-005
			200-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	2.400E-008
	0.00	1.810E-012	200-CRWT-ATD001-AT-FOH	ST D-axis Electrical Actuator #1 fails lift/lower	7.540E-005
			200-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	2.400E-008
	0.00	1.810E-012	200-CRWT-ATD0002-AT-FOH	ST D-axis Electrical Actuator #2 fails lift/lower	7.540E-005
			200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-008
	0.00	1.810E-012	200-CRWT-ATD001-AT-FOH	ST D-axis Electrical Actuator #1 fails lift/lower	7.540E-005
			200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-008
	0.00	9.639E-013	200-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	7.140E-005
			200-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E-008
	0.00	8.100E-013	200-CRWT-ELEC-MOE-FOD	ST electric motor failure	6.000E-005
			200-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E-008
	0.00	1.798E-013	200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-005
			200-CRWT-SJKB011-SJK-FOH	Screw lift on Boom #1 fails	8.140E-006
			200-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-004

Table B6.4-4. Cut Sets for the Site Transporter Load Drop during Lift and Movement Fault Tree (Continued)

Fault Tree	Cut Set%	Prob./Freq.	Basic Event	Description	Probability
200-ST-DROP (continued)	0.00	1.798E-013	200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-005
			200-CRWT-SJKB202-SJK-FOH	Screw lift on Boom #2 fails	8.140E-006
			200-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-004
	0.00	5.040E-014	200-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	2.400E-008
			200-CRWT-LVRD01-LVR-FOH	ST D-axis Actuator Structural Arm #1 failure	2.100E-006
	0.00	5.040E-014	200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-008
			200-CRWT-LVRD01-LVR-FOH	ST D-axis Actuator Structural Arm #1 failure	2.100E-006
	0.00	5.040E-014	200-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	2.400E-008
			200-CRWT-LVRD02-LVR-FOH	ST D-axis Actuator Structural Arm #2 failure	2.100E-006
	0.00	5.040E-014	200-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-008
			200-CRWT-LVRD02-LVR-FOH	ST D-axis Actuator Structural Arm #2 failure	2.100E-006
	0.00	4.627E-014	200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-005
			200-CRWT-ATD0002-AT-FOH	ST D-axis Electrical Actuator #2 fails lift/lower	7.540E-005
			200-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	8.140E-006
	0.00	4.627E-014	200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-005
			200-CRWT-ATD001-AT-FOH	ST D-axis Electrical Actuator #1 fails lift/lower	7.540E-005
			200-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	8.140E-006
	0.00	4.627E-014	200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-005
			200-CRWT-ATD0002-AT-FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E-005
			200-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	8.140E-006
	0.00	4.627E-014	200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-005
			200-CRWT-ATD001-AT-FOH	ST D-axis Electrical Actuator #1 fails lift/lower	7.540E-005
			200-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	8.140E-006
	0.00	1.289E-015	200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-005
			200-CRWT-LVRD01-LVR-FOH	ST D-axis Actuator Structural Arm #1 failure	2.100E-006
			200-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	8.140E-006
	0.00	1.289E-015	200-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-005
			200-CRWT-LVRD02-LVR-FOH	ST D-axis Actuator Structural Arm #2 failure	2.100E-006
			200-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	8.140E-006
	0.00	1.289E-015	200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-005
			200-CRWT-LVRD01-LVR-FOH	ST D-axis Actuator Structural Arm #1 failure	2.100E-006
			200-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	8.140E-006

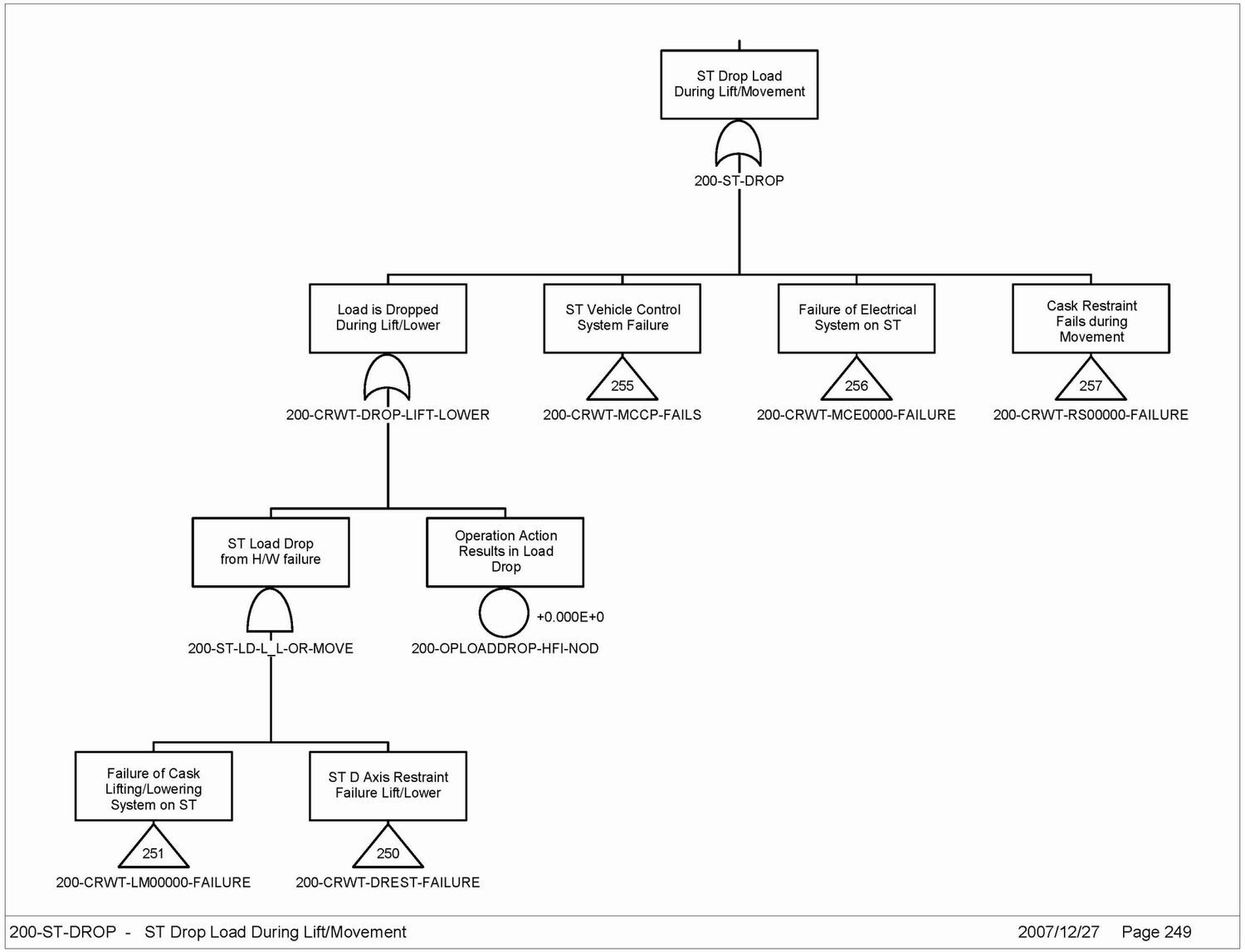
Table B6.4-4. Cut Sets for the Site Transporter Load Drop during Lift and Movement Fault Tree (Continued)

Fault Tree	Cut Set%	Prob./Freq.	Basic Event	Description	Probability
200-ST-DROP (continued)	0.00	1.289E-015	200-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-005
			200-CRWT-LVRD02-LVR-FOH	ST D-axis Actuator Structural Arm #2 failure	2.100E-006
			200-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	8.140E-006
	0.00	1.233E-015	200-CRWT-CBP0000-CBP-OPC	Electrical power dist cable failure on ST	9.130E-008
			200-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E-008
	3.842E-008		= Total		

NOTE: AO = aging overpack; CCF = common-cause failure; ST = site transporter.

Source: Original

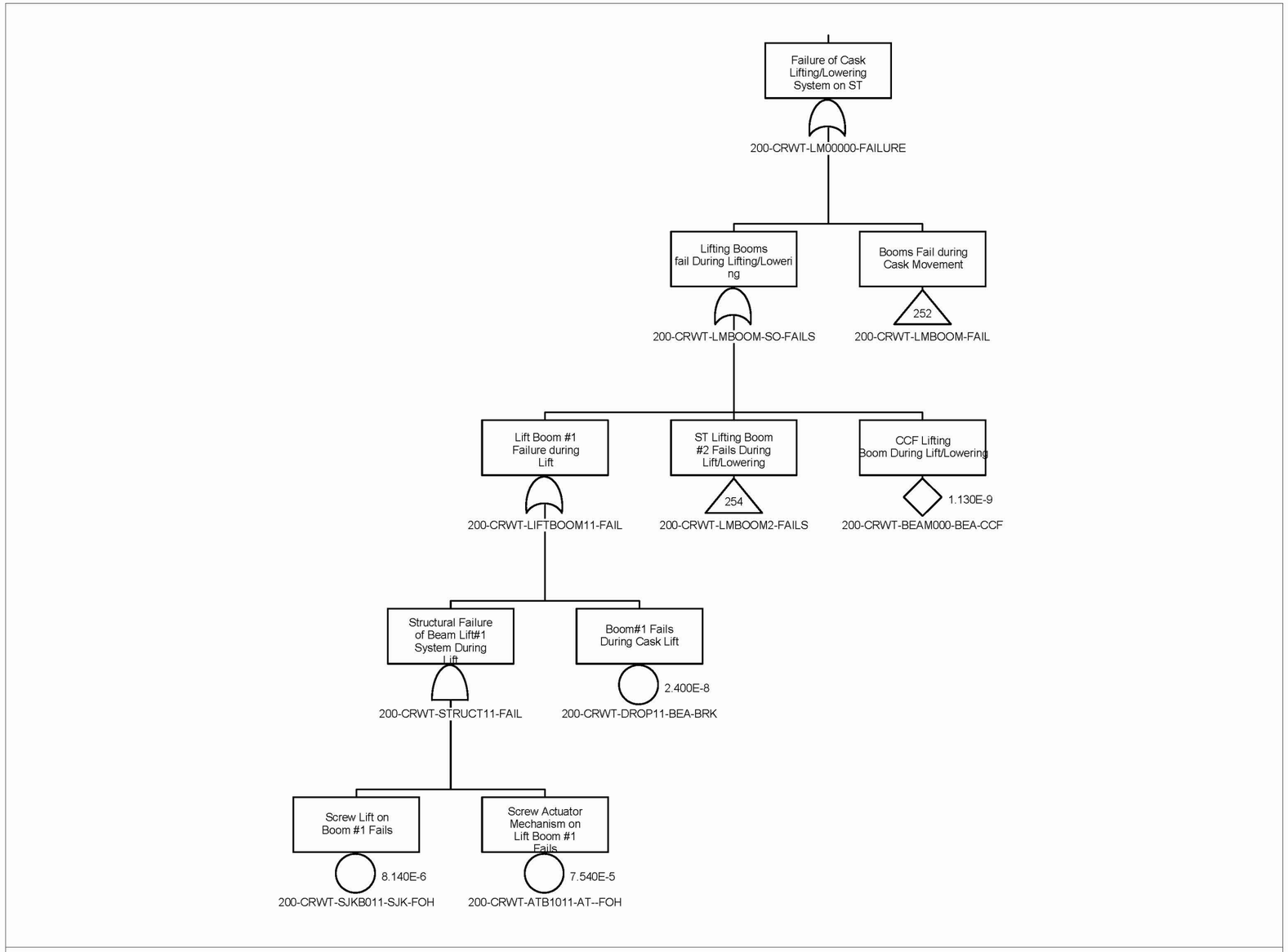
B6.4.2.8 Fault Trees



Source: Original

Figure B6.4-8. Site Transporter Drop Load during Lift/Movement

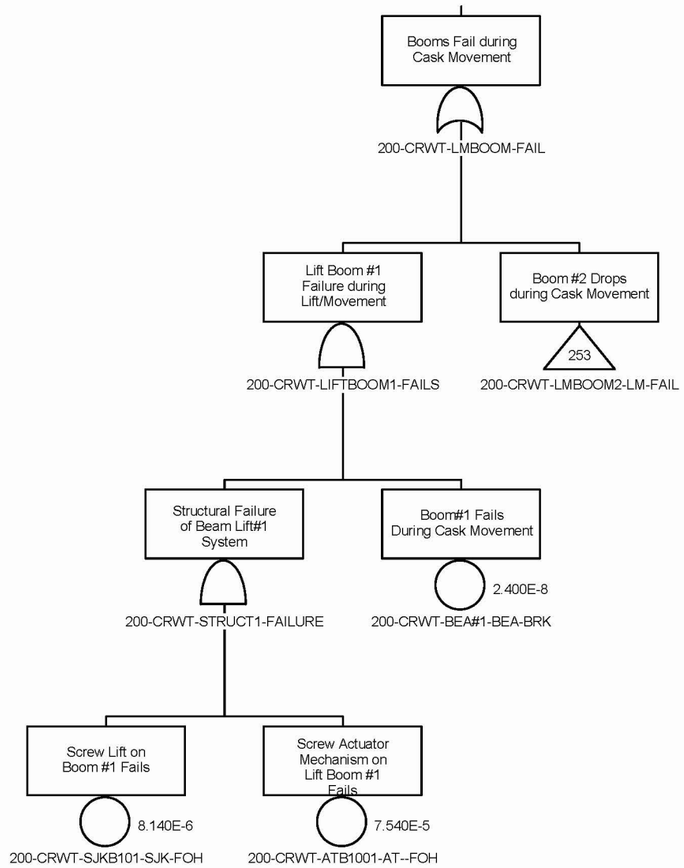
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-9. Failure of Cask Lifting/Lowering System on Site Transporter

INTENTIONALLY LEFT BLANK

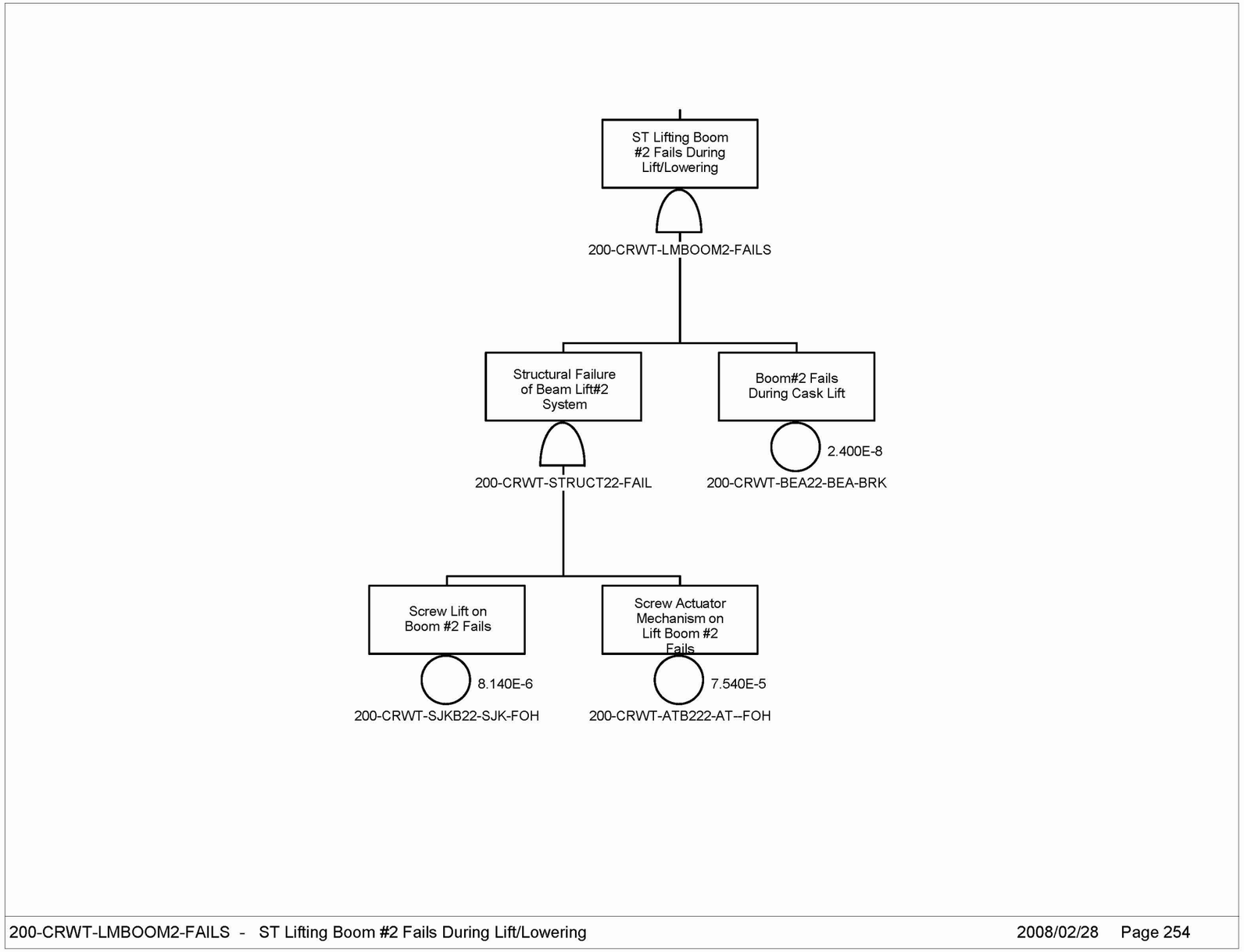


200-CRWT-LMBOOM-FAIL - Booms Fail during Cask Movement 2008/02/28 Page 252

Source: Original

Figure B6.4-10. Booms Fail during Cask Movement

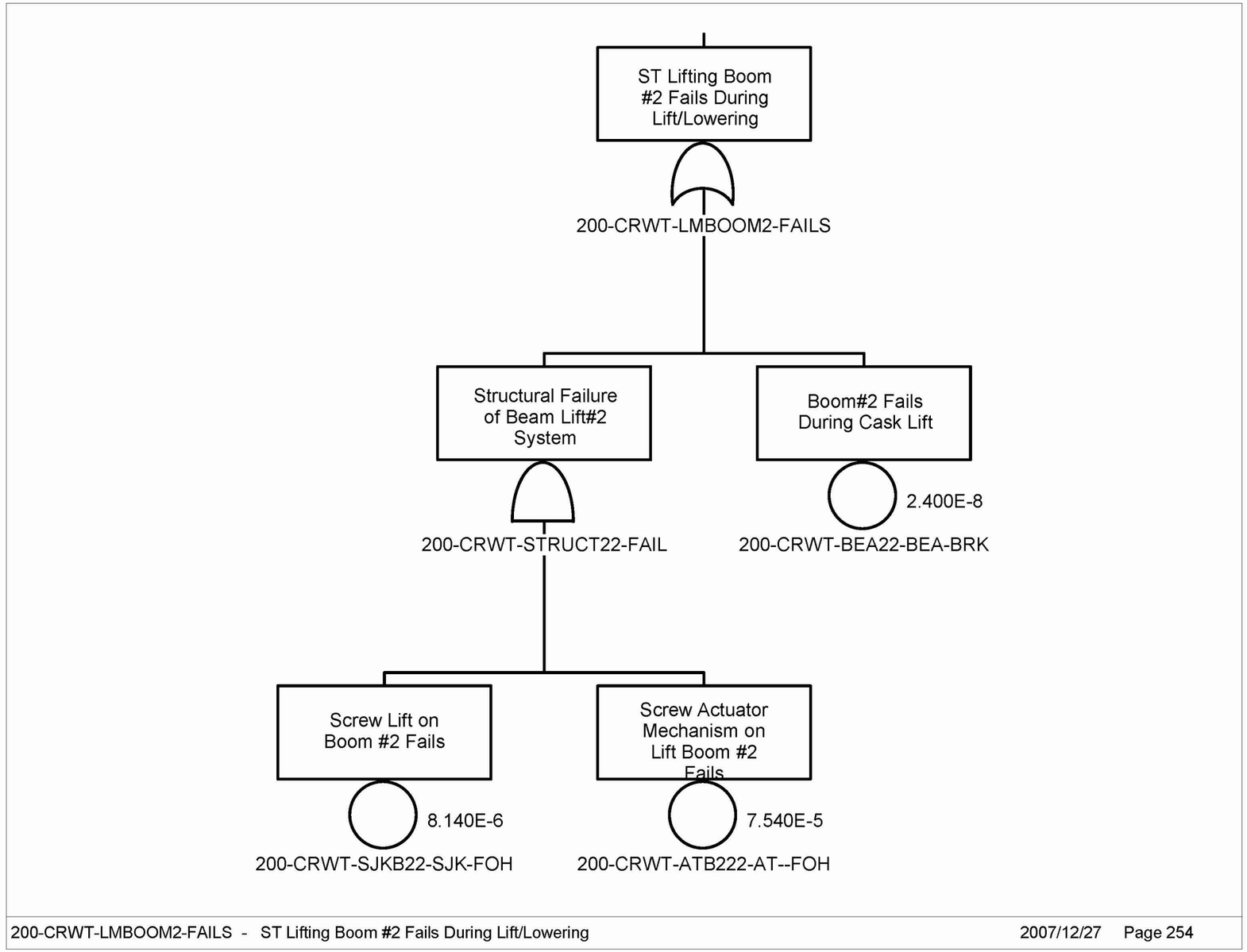
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-11. Boom #2 Drops during Cask Movement

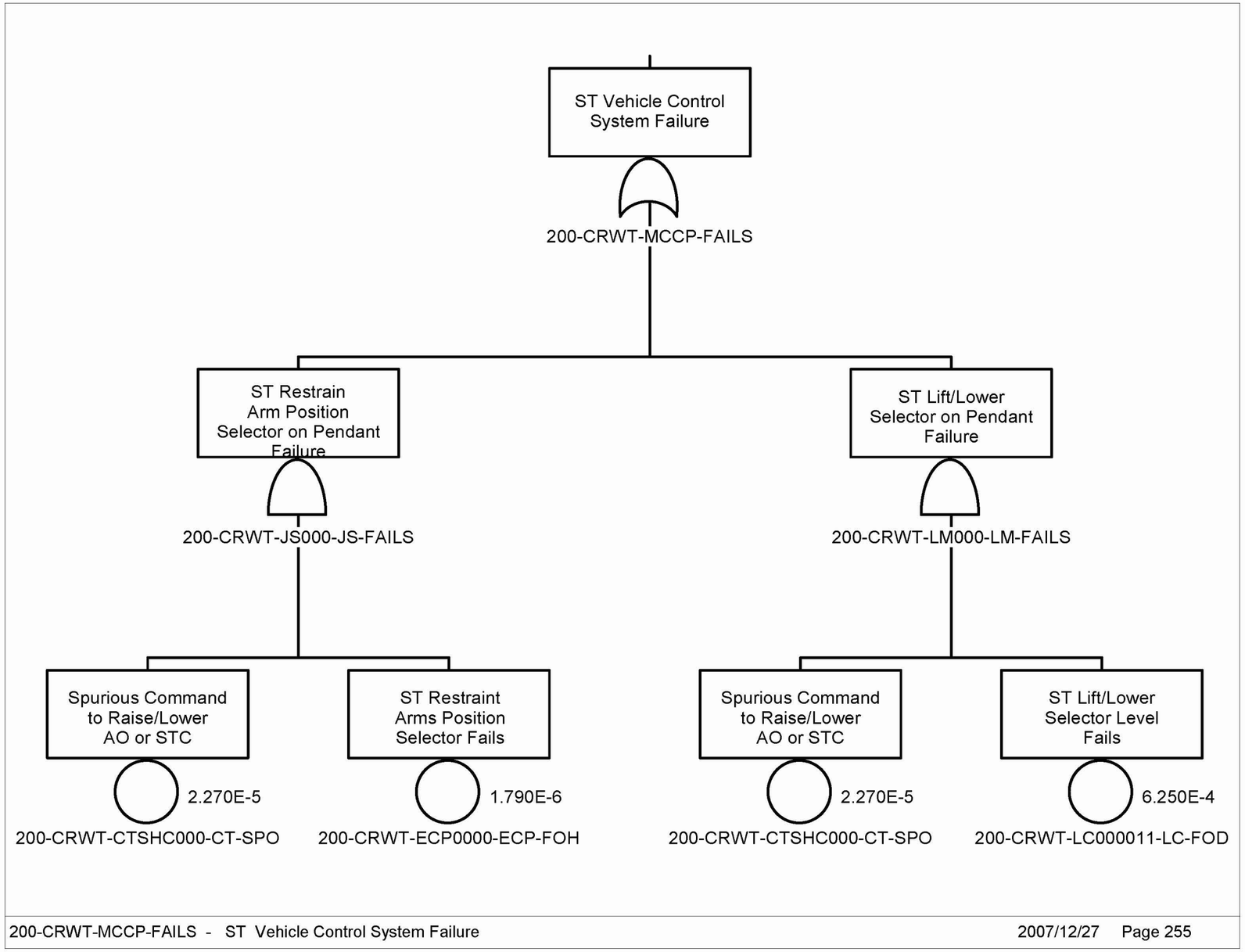
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-12. Site Transporter Lifting Boom #2 Fails During Lift/Lowering

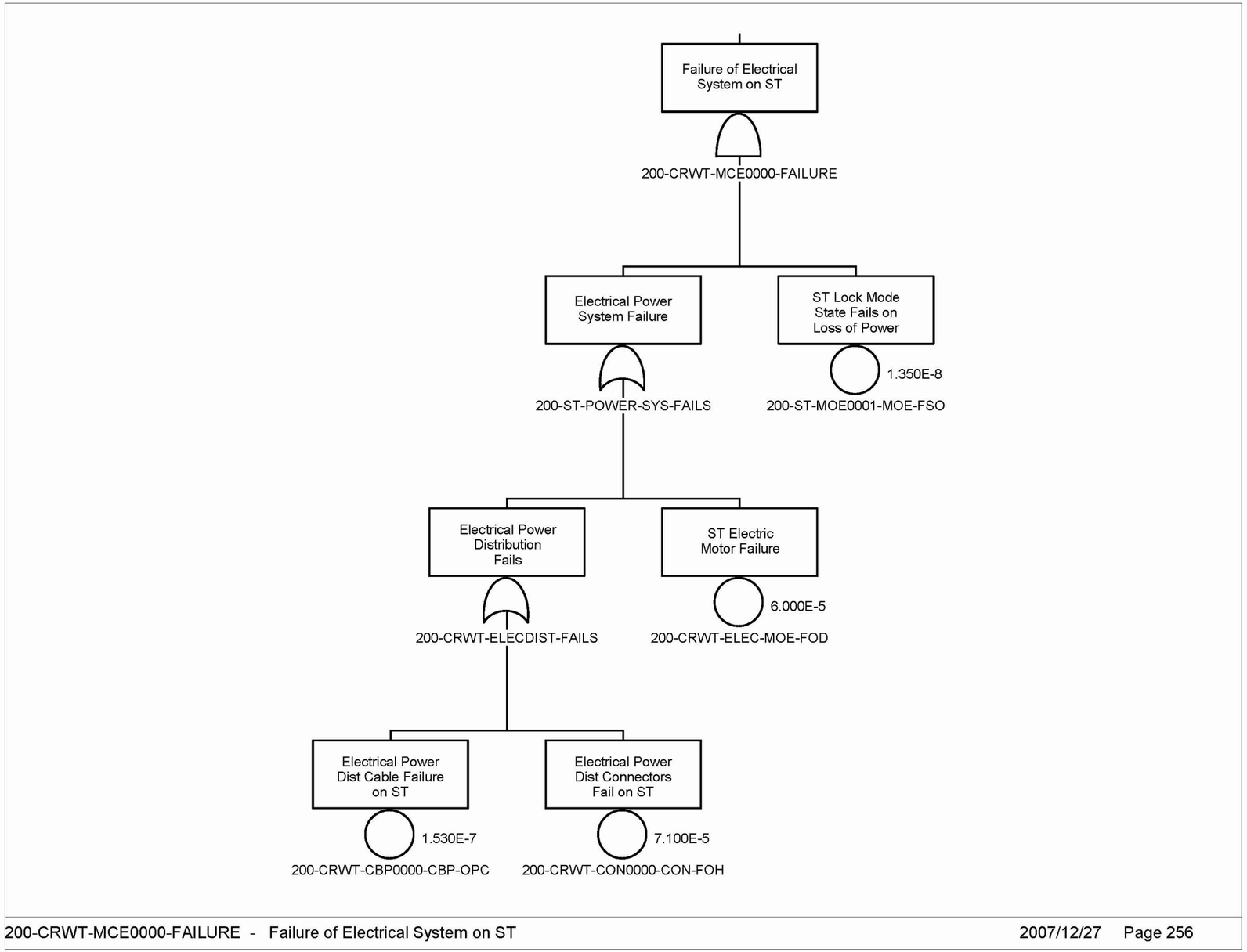
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-13. Site Transporter Vehicle Control System Failure

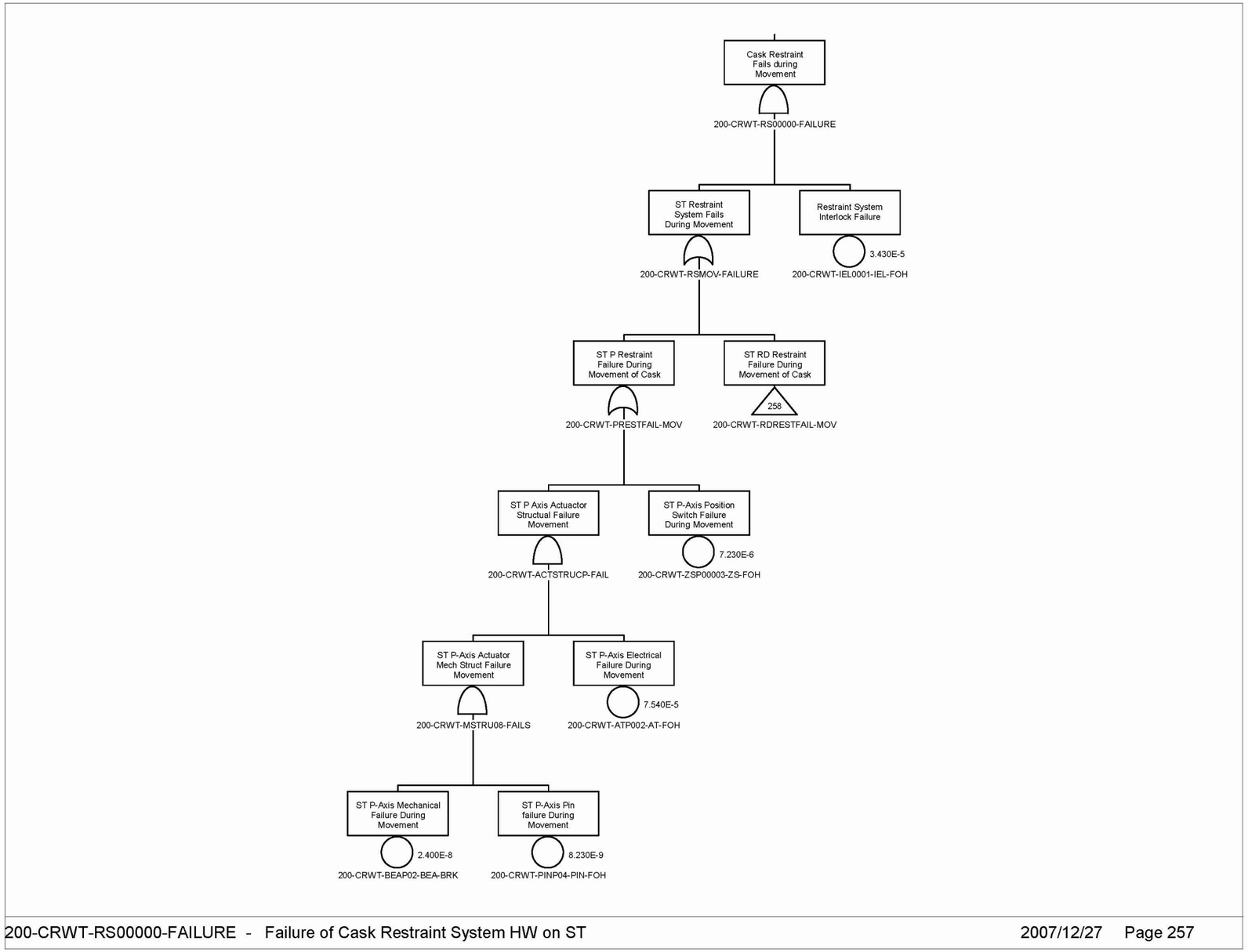
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-14. Failure of Electrical System on Site Transporter

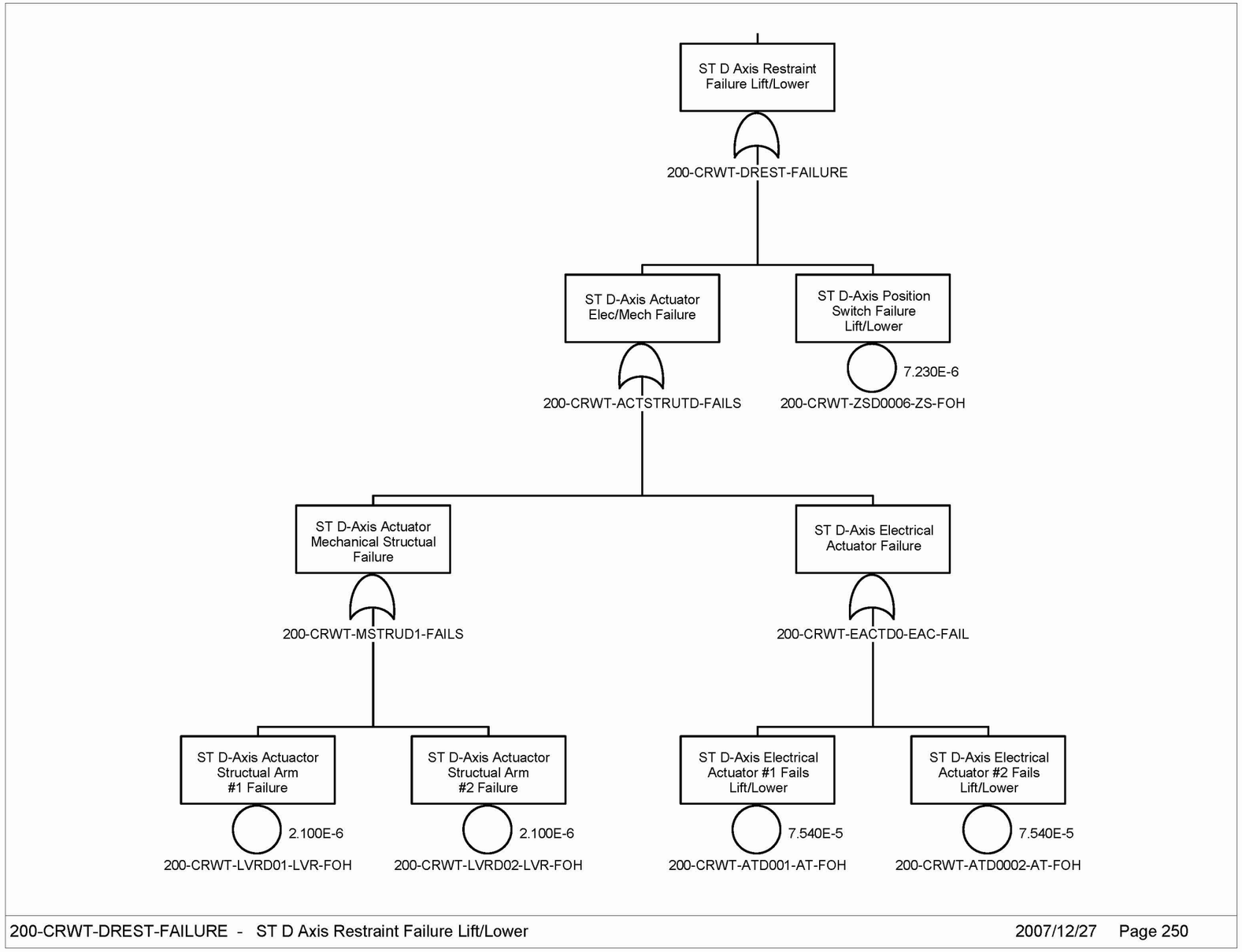
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-15. Cask Restraint Fails During Movement

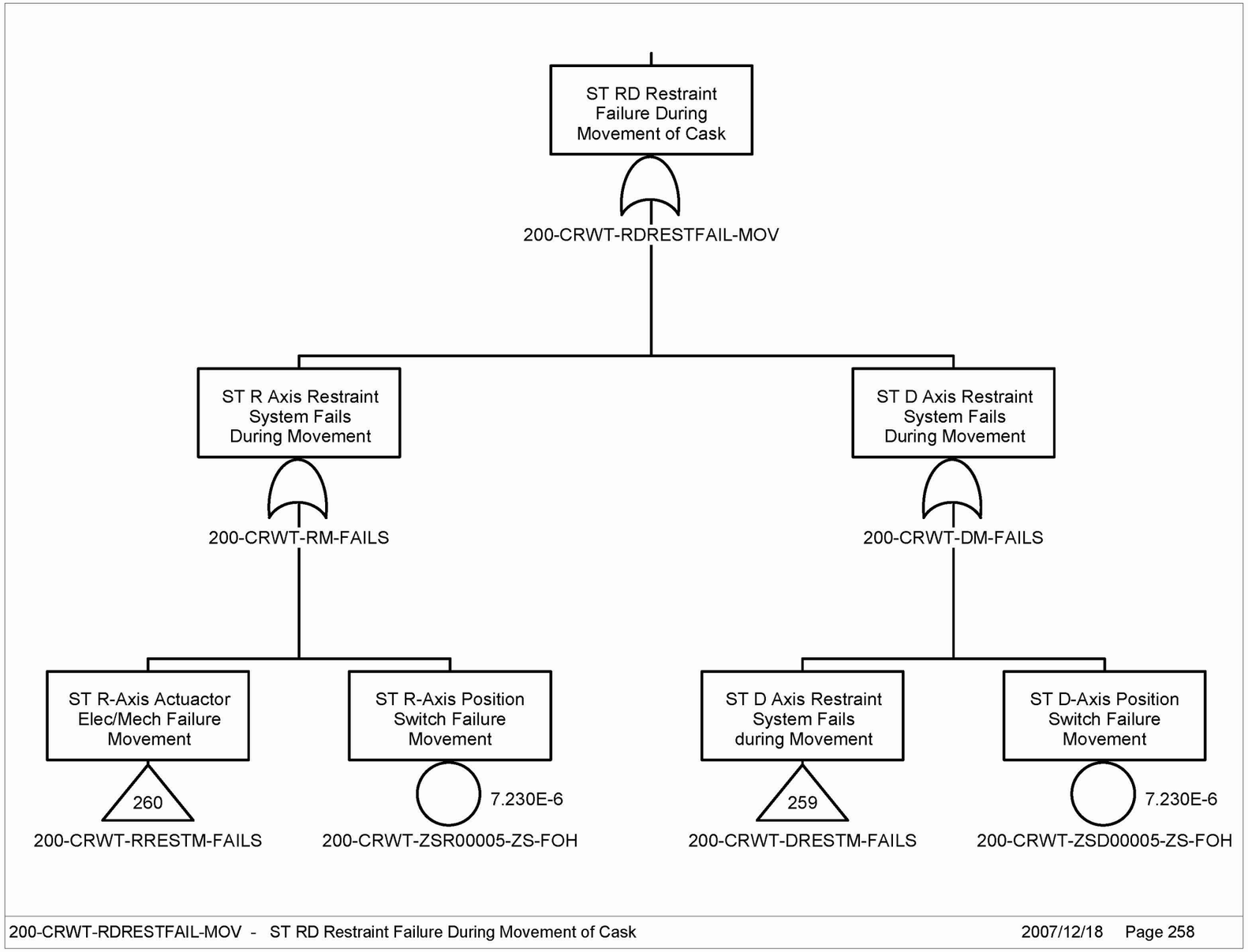
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-16. Site Transporter D-Axis Restraint Failure Lift/Lower

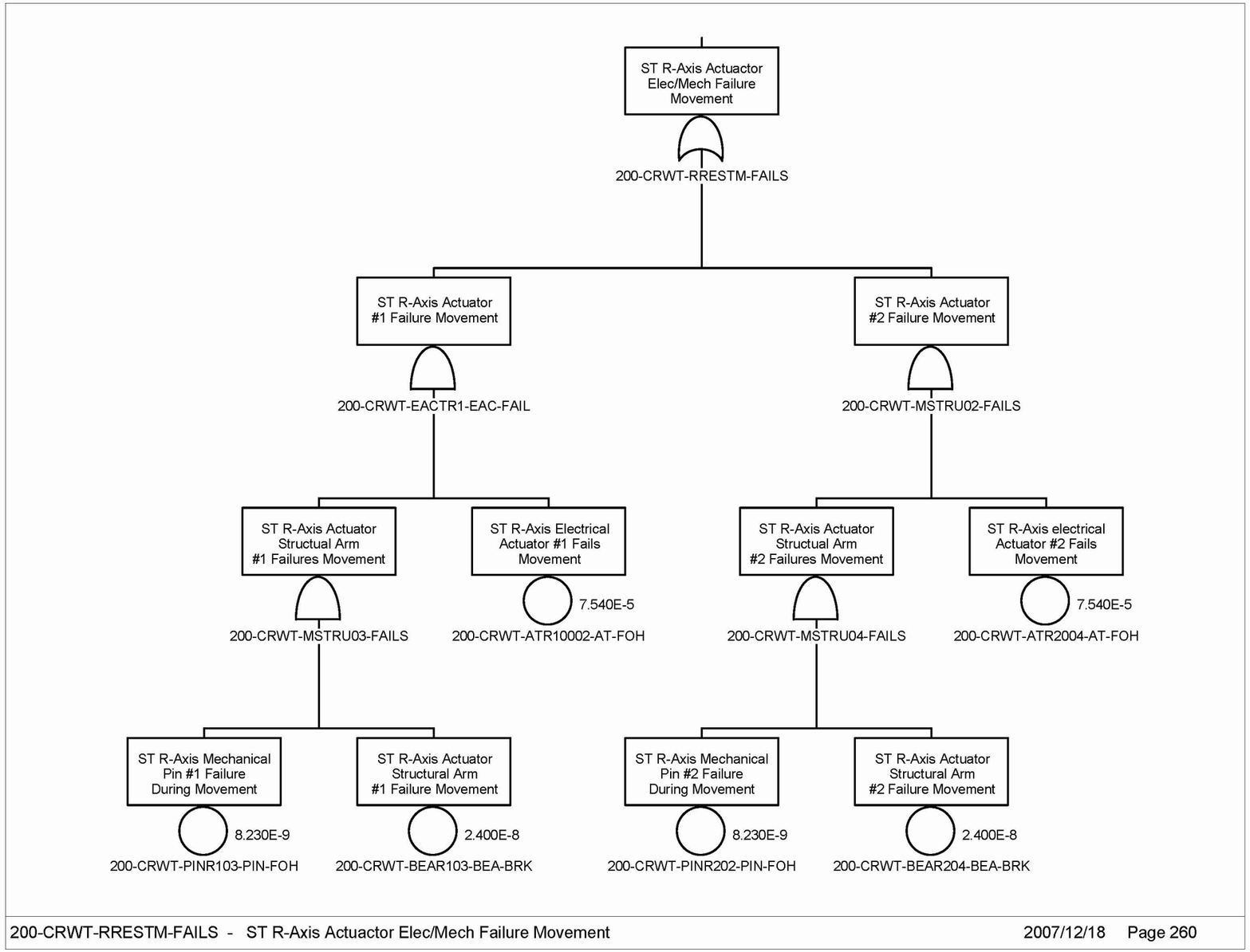
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-17. Site Transporter R- and D-Axis Restraint Failure during Movement of Cask

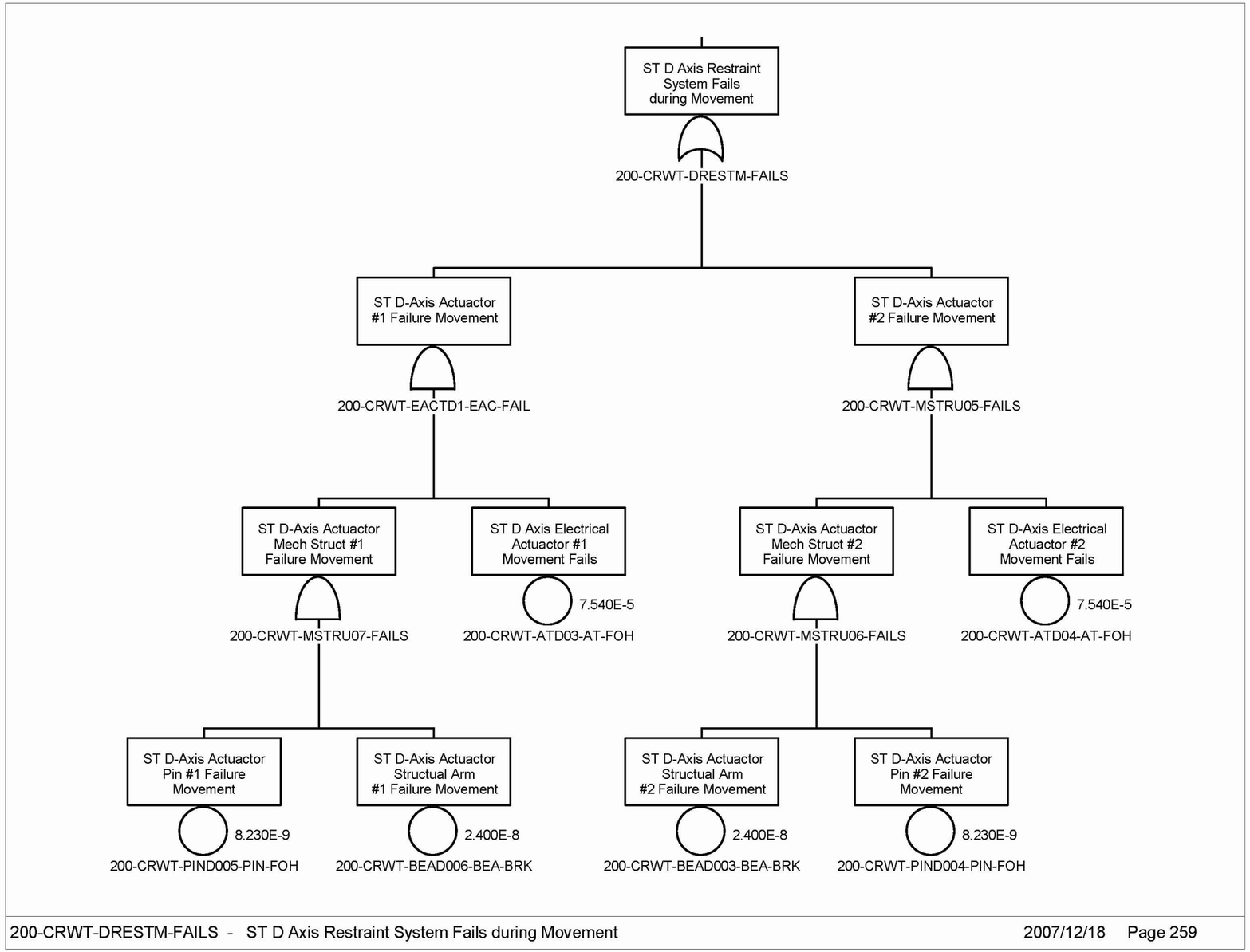
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-18. Site Transporter R-Axis Actuator Electrical/Mechanical Failure Movement

INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-19. Site Transporter D-Axis Restraint System Fails during Movement

INTENTIONALLY LEFT BLANK

B6.4.3 Site Transporter Rollover (Tipover) (ESD-08)

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 scenarios 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 physically prevented from being lifted more than 12 in. The combination of the low lift of the aging overpack, the low center of gravity, and wide footprint of the site transporter results in a stable platform during movements.

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 an operator awareness and response 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

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

Design Feature

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 Event Data

Table B6.4-5 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 B6.4-5. Basic Event Probability for the Site Transporter Rollover

Basic Events Probability Report					
Project: Yucca-Mountain	--	Case: Current	--	--	--
ST Rollover	--	Units: Per Hour	--	--	--
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-CRWT-TRD0001-TRD-FOH	3	5.890E-007	1.000E+000	5.890E-007	1.000E+000
200-CRWT-TRD0002-TRD-FOH	3	5.890E-007	1.000E+000	5.890E-007	1.000E+000
200-CRWT-TRD0003-TRD-FOH	3	5.890E-007	1.000E+000	5.890E-007	1.000E+000
200-CRWT-TRD0004-TRD-FOH	3	5.890E-007	1.000E+000	5.890E-007	1.000E+000
200-CRWT-TRK0001-TRD-FOH	3	5.890E-007	1.000E+000	5.890E-007	1.000E+000
200-OP-FAILSTOP-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000

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

Source: Original

B6.4.3.5.1 Human Failure Events

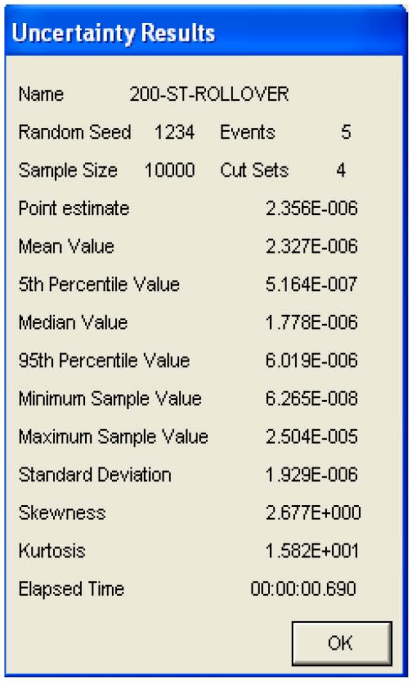
There is one human error failure event included in this model. It is conservatively set to a value of 1E+0 because unsafe actions that require an equipment failure to cause an initiating event are generically assigned a screening human error probability (HEP) of 1.0 (Table E6.4-1).

B6.4.3.5.2 Common-Cause Failures

There are no common-cause failures 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

Figure B6.4-20 contains the uncertainty results obtained from running the fault tree for the "Site Transporter Rollover" fault tree. Figure B6.4-21 provides the cut set generation results for the "Site Transporter Rollover" fault tree, calculated using a 1E-15 cutoff. The fault tree can be found on Figure B6.4-22.



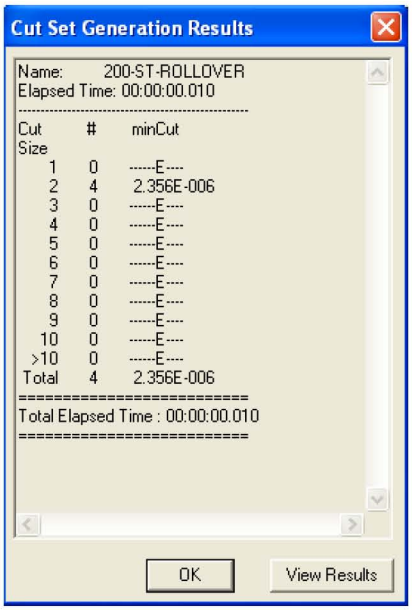
Uncertainty Results

Name	200-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			00:00:00.690

OK

Source: Original

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



Cut Set Generation Results

```
Name:        200-ST-ROLLOVER
Elapsed Time: 00:00:00.010
-------------------------------------------
Cut        #      minCut
Size
    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
==========================
Total Elapsed Time : 00:00:00.010
==========================
```

OK View Results

Source: Original

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

B6.4.3.7 Cut Sets

Table B6.4-6 contains the cut sets for the “Site Transporter Rollover” fault tree.

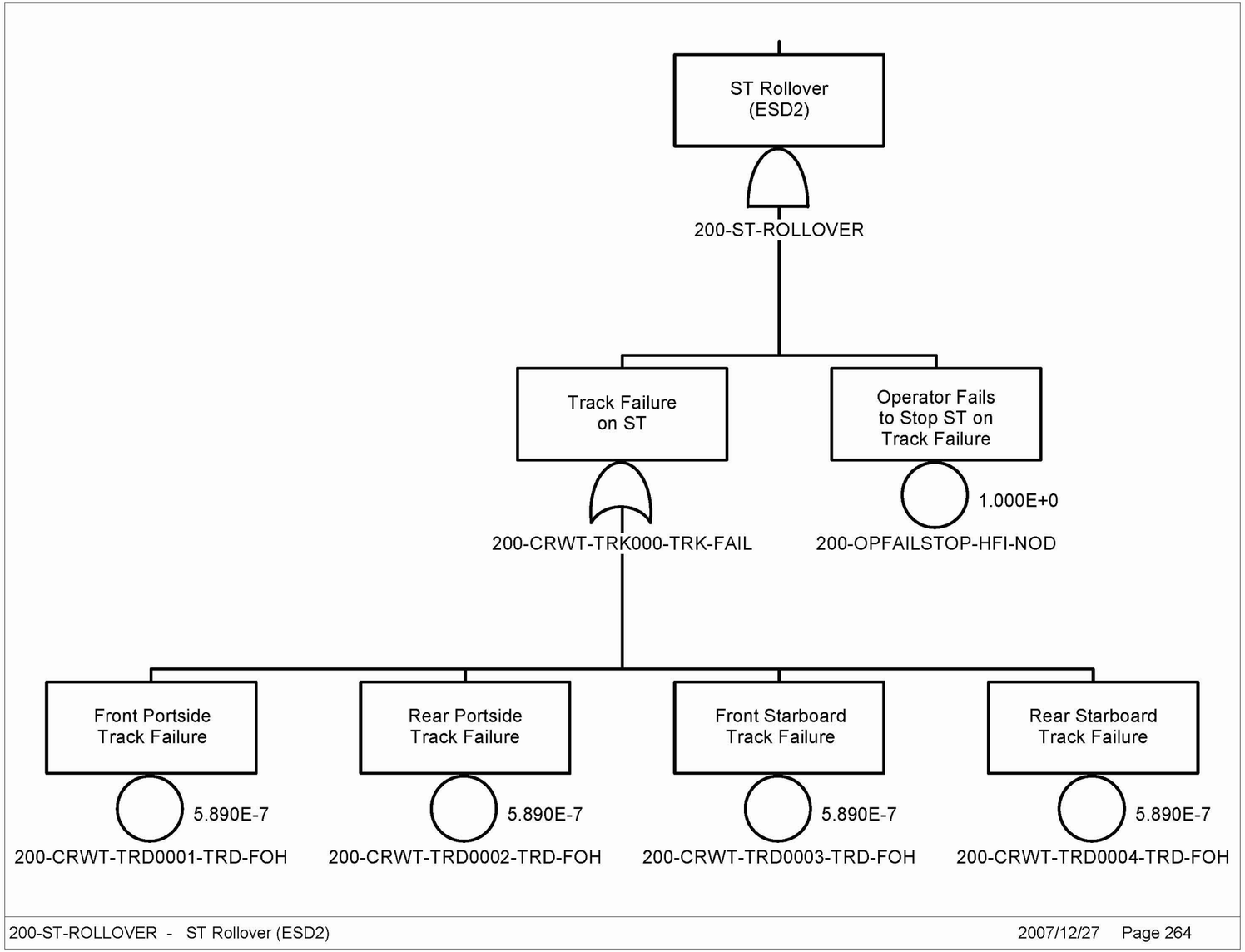
Table B6.4-6. Cut Sets for the Site Transporter Rollover (Tipover)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
200-ST-ROLLOVER	25.00	5.890E-007	200-CRWT-TRD0001-TRD-FOH	Front portside track failure	5.9E-007
			200-OPFAILSTOP-HFI-NOD	Operator fails to stop ST on track failure	1.0E+000
	25.00	5.890E-007	200-CRWT-TRD0002-TRD-FOH	Rear portside track failure	5.9E-007
			200-OPFAILSTOP-HFI-NOD	Operator fails to stop ST on track failure	1.0E+000
	25.00	5.890E-007	200-CRWT-TRD0003-TRD-FOH	Front starboard track failure	5.9E-007
			200-OPFAILSTOP-HFI-NOD	Operator fails to stop ST on track failure	1.0E+000
	25.00	5.890E-007	200-CRWT-TRD0004-TRD-FOH	Rear starboard track failure	5.9E-007
			200-OPFAILSTOP-HFI-NOD	Operator fails to stop ST on track failure	1.0E+000
	2.356E-006		= Total		

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

INTENTIONALLY LEFT BLANK

B6.4.4 Site Transporter Spurious Movement (ESD-06)

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 to or from staging in the Loading 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 command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals can not be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

B6.4.4.3 Design Requirements and Features

Requirements

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

It shall be required to remove facility power and the control pendant from the site transporter when it has been properly position within the Loading Room. On removal of facility AC power, the site transporter immediately enters the "lock mode" safe state. The "lock mode" safe state is not be 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 the Loading Room accounts for 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 B6.4-7 lists the basic events used in the "Site Transporter Spurious Movement" fault tree.

Table B6.4-7. Basic Event Probability for Site Transporter Spurious Movement

Basic Events Probability Report					
Project: Yucca-Mountain	Case: Current	--	--	--	--
ST Spurious Movement	--	Units: Per Hour	--	--	--
Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
200-CR---IEL001--IEL-FOD	1	2.75E-05	2.75E-05	---	---
200-CR---IEL002--IEL-FOD	1	2.75E-05	2.75E-05	---	---
200-CR---IELCCF--IEL-CCF	C	1.29E-06	---	---	---
200-OPNOUNPLUGST-HFI-NOD	1	1.00E-03	1.00E-03	---	---
200-ST---HC000--HC--SPO	3	5.23E-07	0.00E+00	5.23E-07	1.00E+00
200-ST---SC002--SC--FOH	3	1.28E-04	0.00E+00	1.28E-04	1.00E+00
200-ST---SC021---SC---SPO	3	3.20E-05	0.00E+00	3.20E-05	1.00E+00

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

Source: Original

B6.4.4.5.1 Human Failure Events

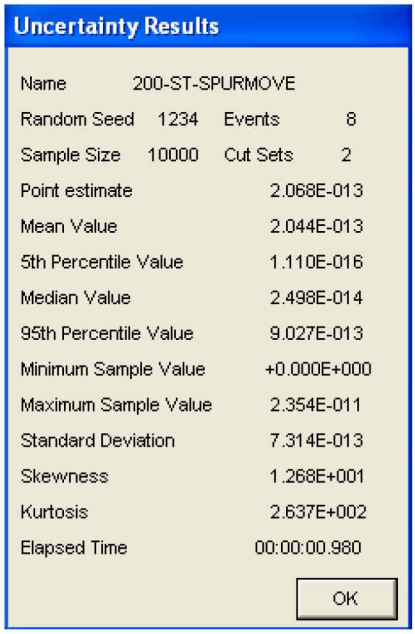
There is one human error associated with this fault tree that addresses an operator failure to unplug the site transporter power cable after it has been parked in the Unloading Room.

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, CCCF = 2).

B6.4.4.6 Uncertainty and Cut Set Generation Results

Figure B6.4-23 contains the uncertainty results obtained from running the fault tree for the "Site Transporter Spurious Movement" fault tree. Figure B6.4-24 provides the cut set generation results for the "Site Transporter Spurious Movement" fault tree, calculated using a 1E-15 cutoff. The fault tree can be found on Figure B6.4-25.



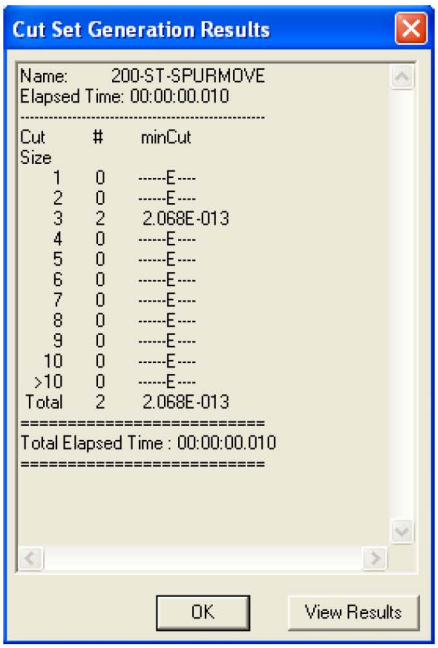
Uncertainty Results

Name	200-ST-SPURMOVE		
Random Seed	1234	Events	8
Sample Size	10000	Cut Sets	2
Point estimate			2.068E-013
Mean Value			2.044E-013
5th Percentile Value			1.110E-016
Median Value			2.498E-014
95th Percentile Value			9.027E-013
Minimum Sample Value			+0.000E+000
Maximum Sample Value			2.354E-011
Standard Deviation			7.314E-013
Skewness			1.268E+001
Kurtosis			2.637E+002
Elapsed Time			00:00:00.980

OK

Source: Original

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



Cut Set Generation Results

```
Name:        200-ST-SPURMOVE
Elapsed Time: 00:00:00.010
-------------------------------------------
Cut      #      minCut
Size
   1     0      ------E----
   2     0      ------E----
   3     2       2.068E-013
   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    2       2.068E-013
==========================
Total Elapsed Time : 00:00:00.010
==========================
```

OK View Results

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 B6.4-8 contains the cut sets for the Site Transporter Spurious Movement fault tree.

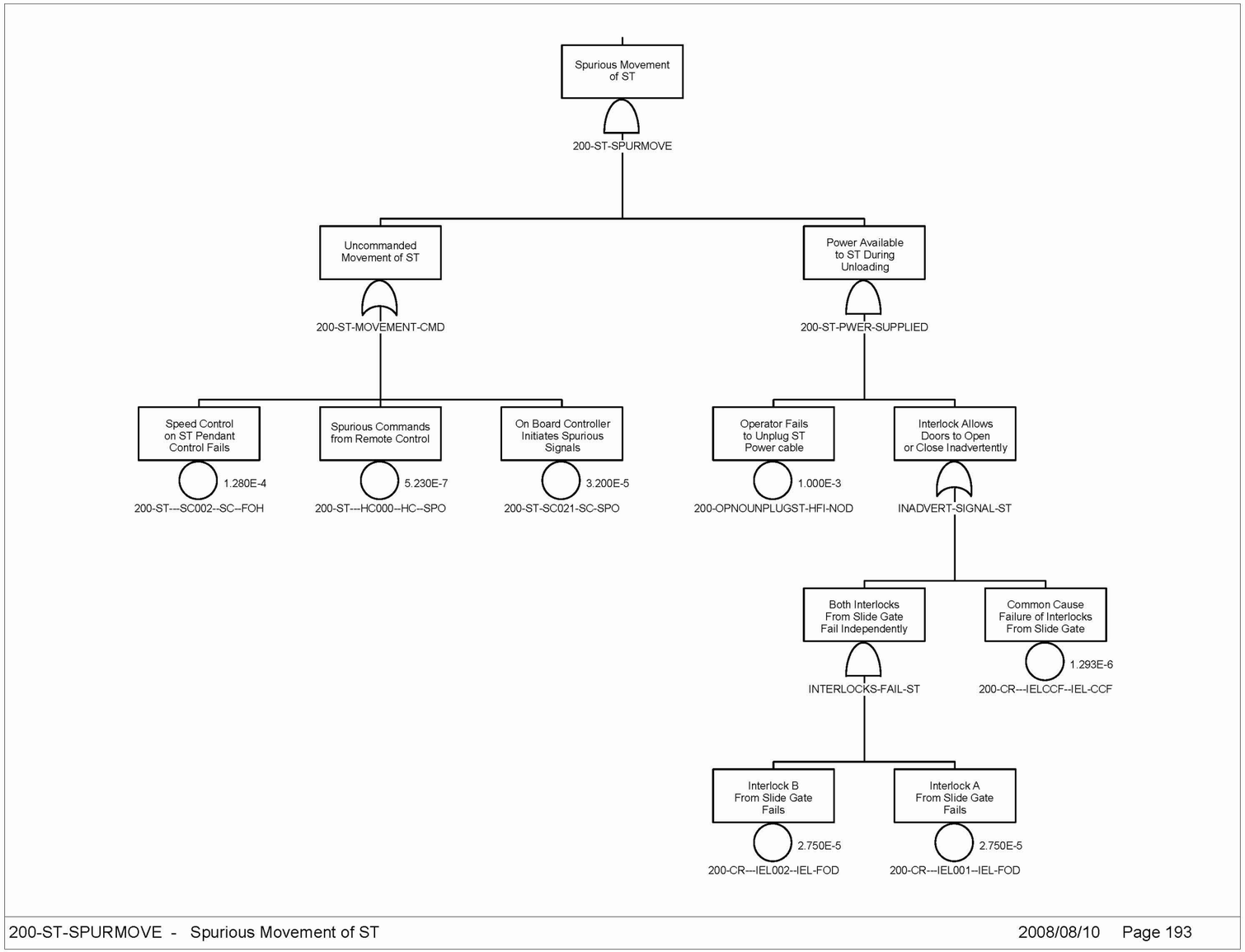
Table B6.4-8. Cut Sets for the Site Transporter Spurious Movement

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
200-ST-SPURMOVE	79.98	1.654E-013	200-CR---IELCCF—IEL-CCF	Common-cause failure of interlocks from slide gate	1.3E-006
			200-OPNOUNPLUGST-HFI-NOD	Operator fails to unplug ST power cable	1.0E-003
			200-ST---SC002--SC--FOH	Speed control on ST pendant control fails	1.3E-004
	20.02	4.136F-014	200-CR---IELCCF—IEL-CCF	Common-cause failure of interlocks from slide gate	1.3E-006
			200-OPNOUNPLUGST-HFI-NOD	Operator fails to unplug ST power cable	1.0E-003
			200-ST---SC021---SC--SPO	On-board controller initiates spurious signal	3.2E-005
		2.048E-013	= Total		

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

Source: Original

B6.4.4.8 Fault Tree



Source: Original

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

INTENTIONALLY LEFT BLANK

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 BSC 2007. *Receipt Facility Composite Vent Flow Diagram Tertiary Confinement Non-ITS HVAC Supply Sys & ITS Exhaust*. 200-M50-VCT0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0021.

B7.1.3 BSC 2007. *Receipt Facility ITS Confinement Areas HEPA Exhaust System - Train A Ventilation & Instrumentation Diagram*. 200-M80-VCT0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0017.

B7.1.4 BSC 2007. *Receipt Facility ITS Confinement Areas HEPA Exhaust System - Train B Ventilation & Instrumentation Diagram*. 200-M80-VCT0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0018.

B7.1.5 Not used.

B7.1.6 BSC 2007. *RF Equipment Sizing and Selection Calculation (ITS)*. 200-M8C-VCT0-00500-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0033.

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 HEATING, VENTILATION, AND AIR CONDITIONING DESCRIPTION

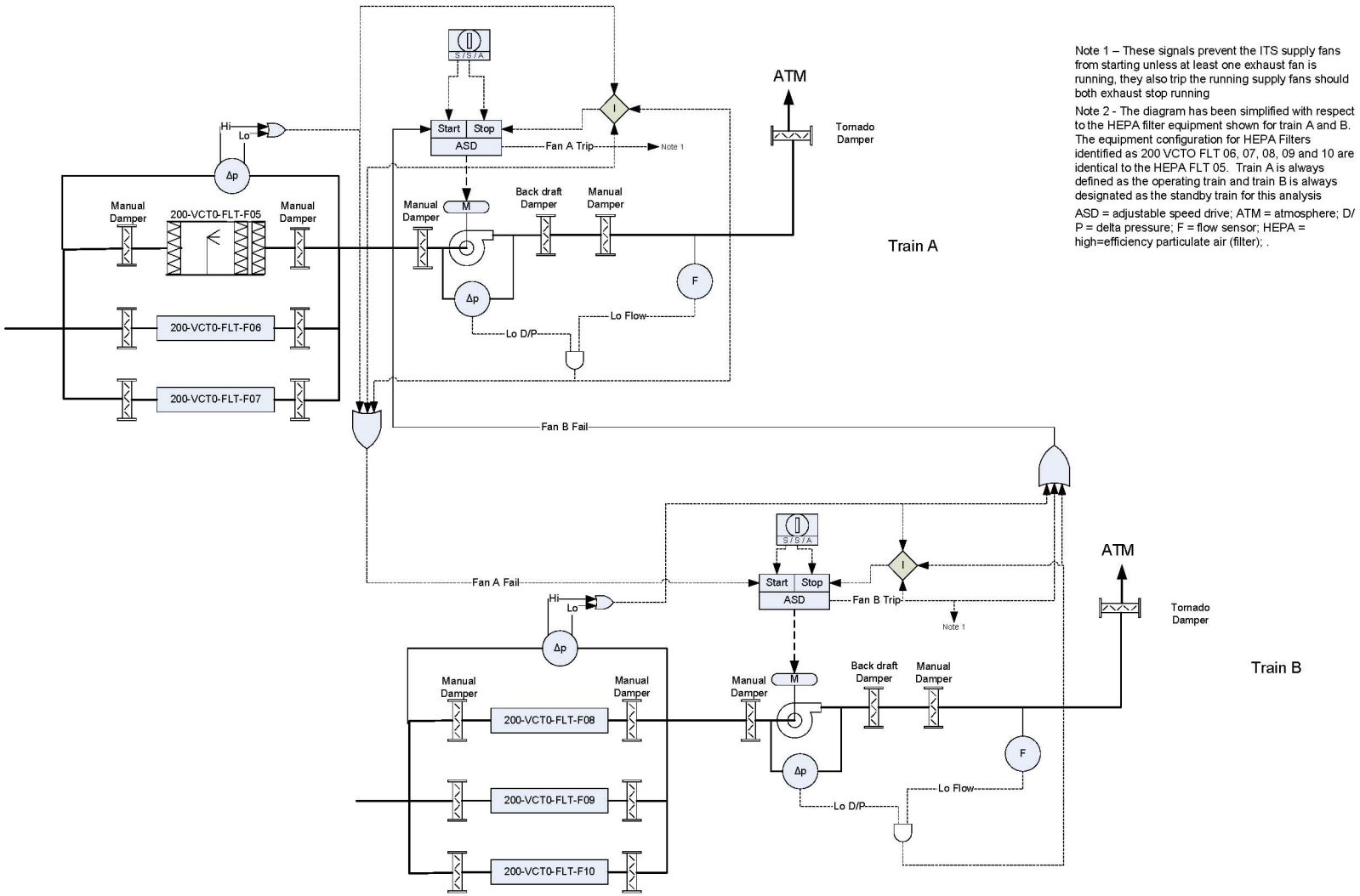
B7.2.1 Overview

The ITS heating, ventilation, and air conditioning (HVAC) provides high-efficiency particulate air (HEPA) filtered exhaust from the RF 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.

Additional information related to equipment sizing, air distribution, ventilation rates, and transport velocities required to maintain design negative pressures and flows within the C2 zones is provided in *RF Equipment Sizing and Selection Calculation (ITS)* (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.



Source: Original

Figure B7.2-1. Block Diagram of the RF 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 the following 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.

NOTE: HVAC = heating, ventilation, and air conditioning

Source: Original

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 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 to 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 three by three array (nine filters). The roughing filters are followed by two banks of HEPA filters. Each bank consists of three by three array (nine filters), for a total of 18 filters.

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.

NOTE: D/P = delta pressure; HEPA = high-efficiency particulate air; HVAC = heating, ventilation, and air conditioning.

Source: Original

B7.2.4 Direct Drive Exhaust Fan and Motor

The exhaust fan and motor are sized to provide a maximum airflow rate sufficient to maintain the necessary delta pressure and air flow. The exhaust fan motor speed is controlled by the ASD (Ref. B7.1.6). 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 air handling units (AHUs) supply air to the Loading Room (1013), the Cask Unloading Room (1015), the Cask Preparation Room (1017), and the Cask Preparation Annex (1017A). These AHUs draw directly from the environment and do not circulate air from any facility area. 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 delta pressure 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 delta pressure.

B7.2.6 Control Circuitry

Normal operation of the HVAC system is controlled by the DCMIS which controls each train's 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. B7.1.3), (Ref. B7.1.4), and (Ref. B7.1.2)). The supply fans are used to stabilize the airflow within the RF. Although these fans are non-ITS, their operation impacts the air flow required to maintain delta pressure; consequently, they are accounted for in the loss of HEPA filter plenum section of the fault tree model.