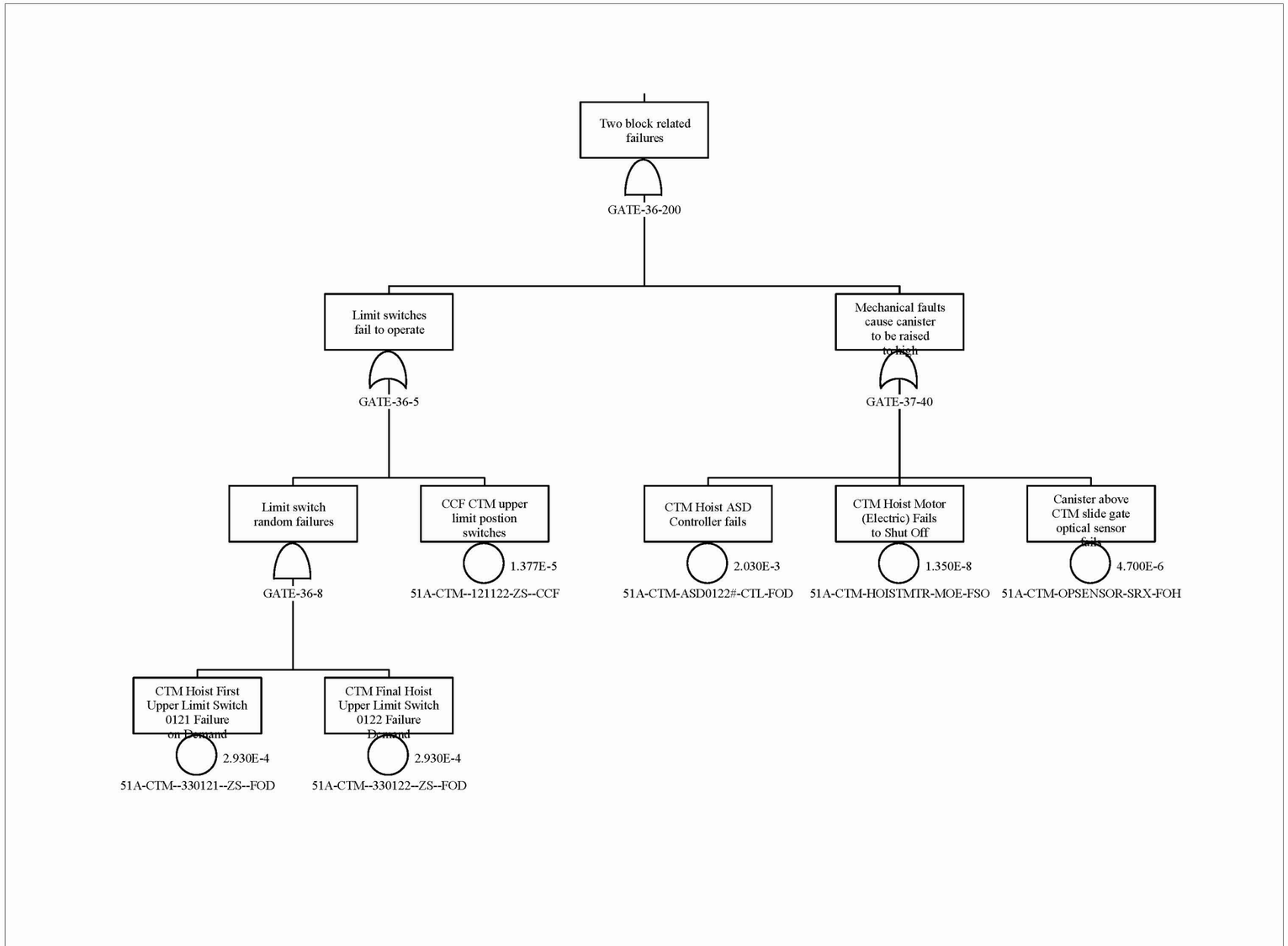


Source: Original

Figure B4.4-19. CTM High Drops from Two Blocking Event Sheet 3

INTENTIONALLY LEFT BLANK

B4.4.3 Drop of Object onto Canister

B4.4.3.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of an object onto canisters. Cask lids, handling equipment, auxiliary grapples are handled during the canister transfer process. At times these objects are over the canister and could be dropped onto the canister.

B4.4.3.2 Success Criteria

The success criterion for the CTM is the prevention of a drop of any object onto the canister from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.3.3 Design Requirements and Features

Requirements

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

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

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

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

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

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

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

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

Design Features

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

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

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

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

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

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

B4.4.3.4 Fault Tree Model

The top event in this fault tree is "Drop of Object onto Canister." This is defined as a drop of an object onto a canister during transfer operations. Faults considered in the evaluation of this top event include: human events that contribute to a drop (considered in conjunction with the interlocks intended to prevent the erroneous human action) and mechanical (structural) failures of the CTM components. The interlocks and safety features (position controls, load cells, and drum and holding brakes) intended to either prevent CTM failure or given failure of the CTM to prevent a load drop are included in the model.

Structural failures of components including the hoist cables, sheaves, drum, and grapples can result in canister drops. Operator events are addressed for actions including improper grapple connections, misalignments of the hoist and the canister, improper hoist activities and improper lateral movement of the CTM. Protection from these actions are provided by hard-wired interlocks keyed to the position of the CTM (both hoist position and CTM lateral position), slide and port gate doors, and the shield bell skirt. Also considered in the analysis is a canister drop initiated by improper operation of the shield bell slide gates and the port slide gates. While the gate motors are sized to prevent damage to the canister in the event of an inadvertent closure of

the gates, the possibility that the gates would close above the canister during a lift blocking the lift and causing a canister drop was considered.

B4.4.3.5 Basic Event Data

Table B4.4-6 contains a list of basic events used in the drop of object onto canister fault tree. Included are the human failure events and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The object drop probability modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are put into operation. They are consequently evaluated over the interval of time between their actuation, considered to be the duration of a shift, i.e., eight hours. In another example, brakes are also analyzed over a mission time of twenty-four hours. This duration is deemed sufficient to encompass the time required to revert to normal transfer operations, after a malfunction that would have caused a safety system of the CTM to cease transfer activities.

Table B4.4-6. Basic Event Probabilities for the Drop of Object onto Canister Fault Tree

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	3	6.740E-07	—	6.740E-07	1
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	3	5.784E-05	—	7.230E-06	8
51A-CTM-#ZSH0112-ZS-FOH	Shield Skirt Position Switch Fails	3	5.784E-05	—	7.230E-06	8
51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	C	1.377E-05	—	—	1
51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	—	—
51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	1	2.930E-04	2.930E-04	—	—
51A-CTM--CBL0001-WNE-BRK	Wire rope Breaks	1	2.000E-06	2.000E-06	—	—
51A-CTM--CBL0002-WNE-BRK	Wire Rope Breaks	1	2.000E-06	2.000E-06	—	—
51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	C	9.400E-08	—	—	—
51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	1	4.000E-08	4.000E-08	—	—
51A-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	—	—
51A-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure to Hold	3	2.011E-04	—	8.380E-06	24
51A-CTM--EQL-SHV-BLK-FOD	Equalizer sheaves structural failure	1	1.150E-06	1.150E-06	—	—
51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1	1.150E-06	1.150E-06	—	—
51A-CTM--HOLDBRK-BRK-FOD	Brake Failure on Demand	1	1.460E-06	1.460E-06	—	—
51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3	3.520E-05	—	4.400E-06	8
51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	1	2.750E-05	2.750E-05	—	—
51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1	1.150E-06	1.150E-06	—	—
51A-CTM--MISSPOOL-DM-MSP	CTM Mis-spool event	3	6.860E-07	—	6.860E-07	1
51A-CTM--OVERSP--ZS-FOD	Hoist Motor Speed Limit Switch Fails	1	2.930E-04	2.930E-04	—	—
51A-CTM--PORTGT1-MOE-SPO	Spurious port gate1 motor operation	3	6.740E-07	—	6.740E-07	1.
51A-CTM--PORTGT1-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	—	3.650E-07	1
51A-CTM--PORTGT2-MOE-SPO	Spurious port gate 2 motor operation	3	6.740E-07	—	6.740E-07	1

Table B4.4-6. Basic Event Probability for the CTM Drop of Objects onto Canister Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	—	3.650E-07	1
51A-CTM--UPPERBL-BLK-FOD	Upper sheaves structural failure	1	1.150E-06	1.150E-06	—	—
51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	—	—
51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	1	2.930E-04	2.930E-04	—	360
51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	3	1.280E-06	—	1.280E-06	1
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	—	—
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-DRTRN-CT-FOD	CTM Drive Train Protection and Fail Det. Ctl Failure	1	4.000E-06	4.000E-06	—	—
51A-CTM-DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Fails on Demand	1	5.020E-05	5.020E-05	—	—
51A-CTM-HOISTMT-MOE-FTR	CTM hoist Motor (Electric) Fails to Run	3	6.500E-06	—	6.500E-06	1
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.350E-08	—	1.350E-08	1
51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	3	6.740E-07	—	6.740E-07	1
51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	—	4.700E-06	1
51A-CTM-PLC0101-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1
51A-CTM-PLC01021-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operations	3	3.650E-07	—	3.650E-07	1
51A-CTM-PLC0103-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	3	6.740E-07	—	6.740E-07	1
51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) spurious Operation	3	6.740E-07	—	6.740E-07	1
51A-CTM-SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1

Table B4.4-6. Basic Event Probability for the CTM Drop of Objects onto Canister Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CTM-SLIDEGT1-IEL-FOD	CTM Slide Gate Interlock Fails	1	2.750E-05	2.750E-05	—	—
51A-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	—	—
51A-CTM-YS01129-ZS-FOD	CTM Drum Brake Ctl Circuit Limit Switch 1129 Fails	1	2.930E-04	2.930E-04	—	—
51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	3	1.280E-06	—	1.280E-06	1
51A-LOSS-OFFSITE-PWR	Loss of offsite power	1	2.990E-03	2.990E-03	—	—
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1	1.000E-03	1.000E-03	—	—
51A-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block	1	1.000E+00	1.000E+00	—	—
51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	1	4.000E-07	4.000E-07	—	—
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	—	—

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

CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

B4.4.3.5.1 Human Failure Events

Four basic events are associated with human error (Table B4.4-7). These are for drops initiated by operator actions, drops caused by the operator initiating a two-block event, a failure to restore interlocks allowing movement of the crane when the shield skirt is raised and the slide gates are open and the operator closing the slide or port gates during a lift. The quantification of these events includes operator actions and the failures of interlocks intended to prevent such operator action.

Table B4.4-7. Human Failure Events

Name	Description
51A-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block
51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor

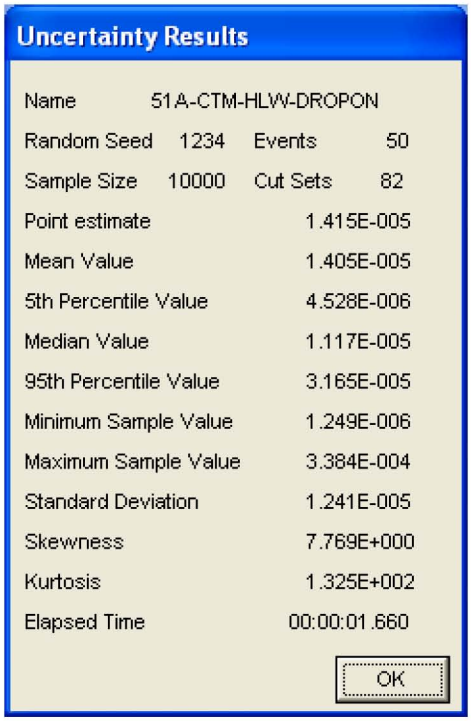
Source: Original

B4.4.3.5.2 Common-Cause Failures

Two common-cause events were considered in the evaluation of this fault tree. One is associated with pairs of sensors used to limit CTM movement. The two upper limit sensors on the hoist are used to prevent a two-block event. The second common-cause event considered is the common-cause failure of the hoist cables.

B4.4.3.6 Uncertainty and Cut Set Generation

Figure B4.4-20 contains the uncertainty results obtaining from running the fault trees for the "Drop of Object onto Canister." Figure B4.4-21 provides the cut set generation results for the "Drop of Object onto Canister" fault tree.



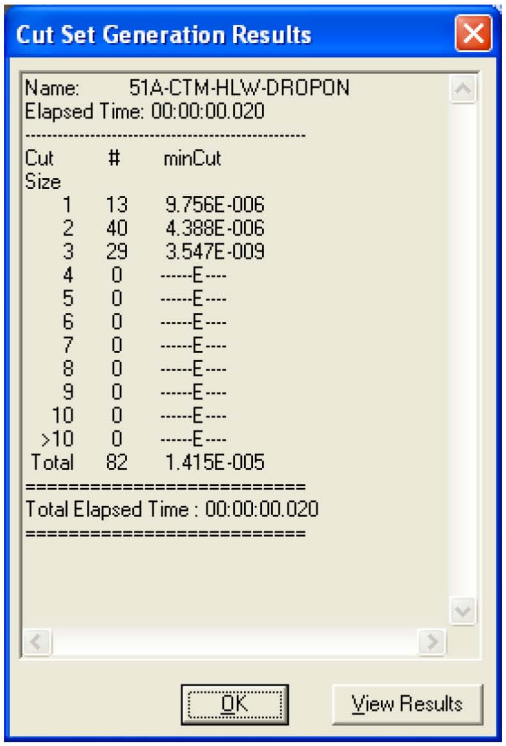
Uncertainty Results

Name	51A-CTM-HLW-DROPON		
Random Seed	1234	Events	50
Sample Size	10000	Cut Sets	82
Point estimate			1.415E-005
Mean Value			1.405E-005
5th Percentile Value			4.528E-006
Median Value			1.117E-005
95th Percentile Value			3.165E-005
Minimum Sample Value			1.249E-006
Maximum Sample Value			3.384E-004
Standard Deviation			1.241E-005
Skewness			7.769E+000
Kurtosis			1.325E+002
Elapsed Time			00:00:01.660

OK

Source: Original

Figure B4.4-20 Uncertainty Results of the Drop of Object onto Canister Fault Tree



Cut Set Generation Results

```
Name:        51A-CTM-HLW-DROPON
Elapsed Time: 00:00:00.020
-------------------------------------------
Cut      #      minCut
Size
   1    13     9.756E-006
   2    40     4.388E-006
   3    29     3.547E-009
   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    82     1.415E-005
==========================
Total Elapsed Time : 00:00:00.020
==========================
```

OK View Results

Source: Original

Figure B4.4-21. Cut Set Generation Results for the Drop of Object onto Canister Fault Tree

B4.4.3.7 Cut Sets

Table B4.4-8 contains the top 20 cut sets for the "Drop of Object onto Canister" fault tree.

Table B4.4-8. Dominant Cut Sets for the "Drop of Object onto Canister Fault" Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Probability
28.20	28.20	3.990E-006	51A-CTM--WT0125--SRP-FOD	Load Cell Pressure Sensor Fails	4.0E-003
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-003
37.25	9.05	1.280E-006	51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	1.3E-006
46.30	9.05	1.280E-006	51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	1.3E-006
54.43	8.13	1.150E-006	51A-CTM--EQL-SHV-BLK-FOD	Equalizer sheaves structural failure	1.2E-006
62.56	8.13	1.150E-006	51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1.2E-006
70.69	8.13	1.150E-006	51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1.2E-006
78.82	8.13	1.150E-006	51A-CTM--UPPERBL-BLK-FOD	Upper sheaves structural failure	1.2E-006
83.58	4.76	6.740E-007	51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	6.7E-007
88.34	4.76	6.740E-007	51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	6.7E-007
93.10	4.76	6.740E-007	51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	6.7E-007
95.93	2.83	4.000E-007	51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	4.0E-007
98.00	2.07	2.930E-007	51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	2.9E-004
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-003
98.66	0.66	9.400E-008	51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.4E-008
98.94	0.28	4.000E-008	51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	4.0E-008
99.22	0.28	4.000E-008	51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
99.47	0.25	3.520E-008	51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3.5E-005
	(continued)	(continued)	51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-003
99.67	0.20	2.796E-008	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.4E-005
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.0E-003

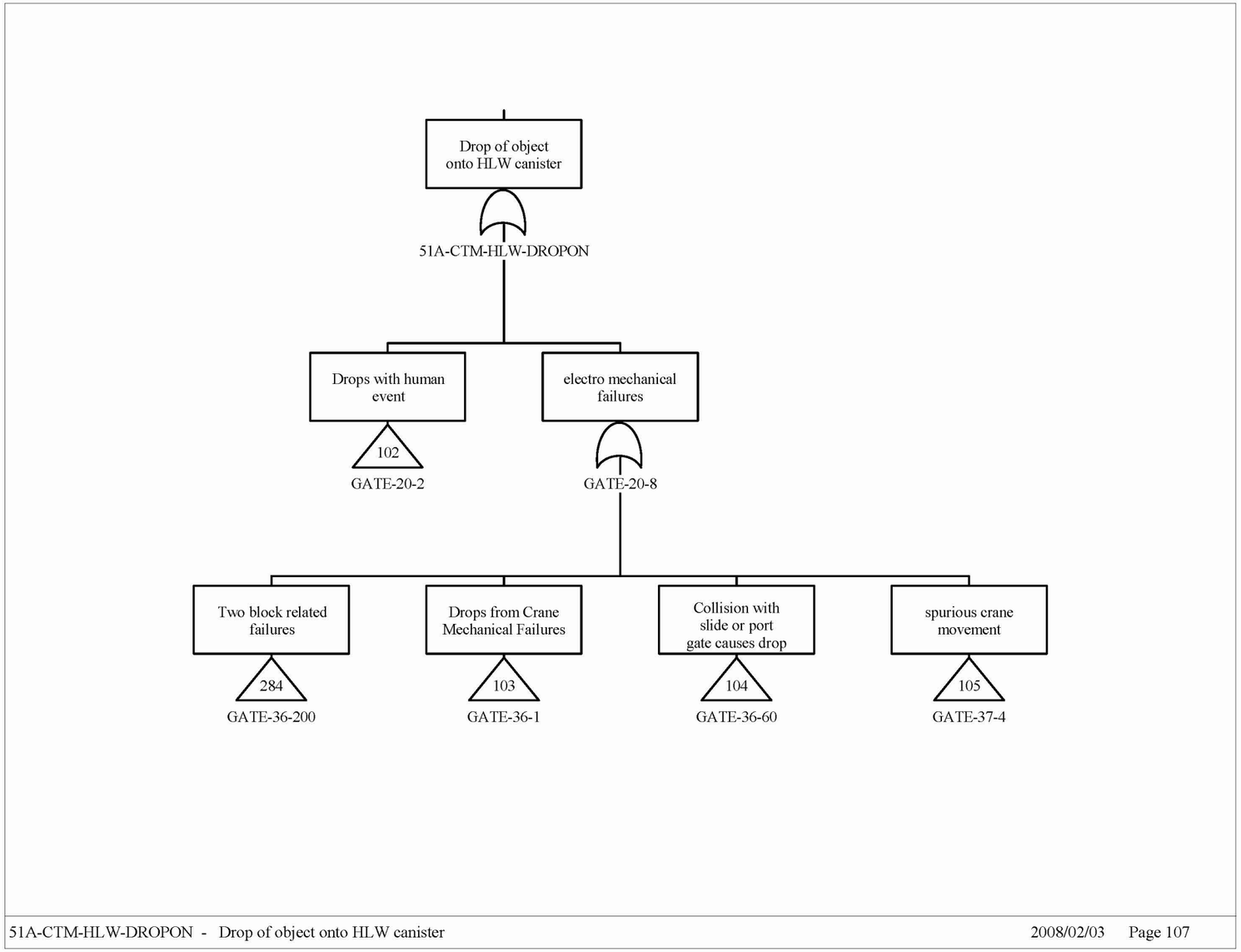
Table B4.4-8. Dominant Cut Sets for the CTM Drop onto Canister Fault Tree (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Probability
99.86	0.19	2.750E-008	51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	2.8E-005
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-003
99.88	0.02	2.689E-009	51A-CTM--PORTGT1-MOE-SPO	Spurious port gate 1 motor operation	6.7E-007
			51A-CTM--WT0125--SRP-FOD	Load Cell Pressure Sensor Fails	4.0E-003
99.90	0.02	2.689E-009	51A-CTM--PORTGT2-MOE-SPO	Spurious port gate 2 motor operation	6.7E-007
			51A-CTM--WT0125--SRP-FOD	Load cell pressure sensor fails	4.0E-003

NOTE: CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

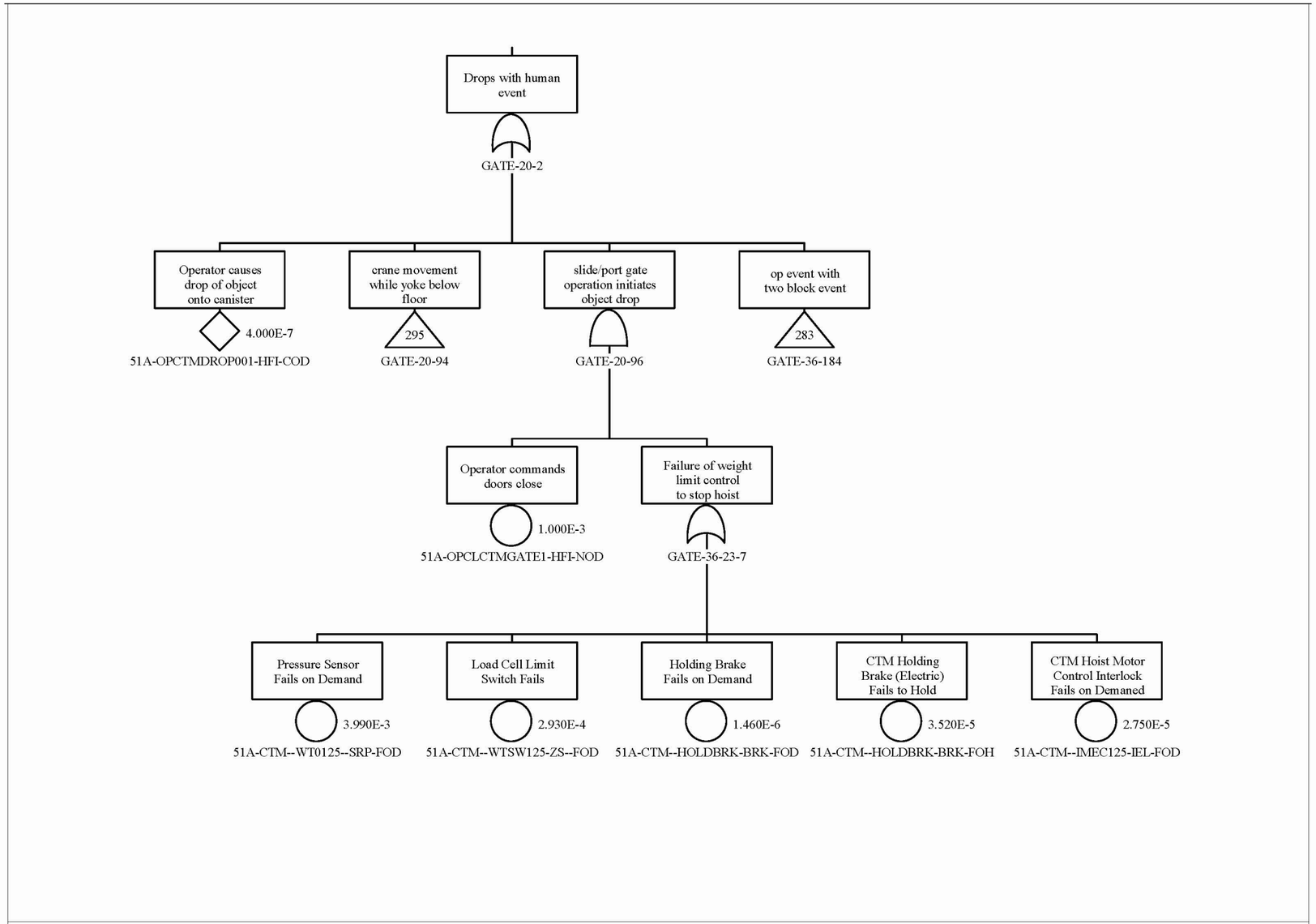
B4.4.3.8 Fault Trees



Source: Original

Figure B4.4-22. Drop of Object onto Cask
Sheet 1

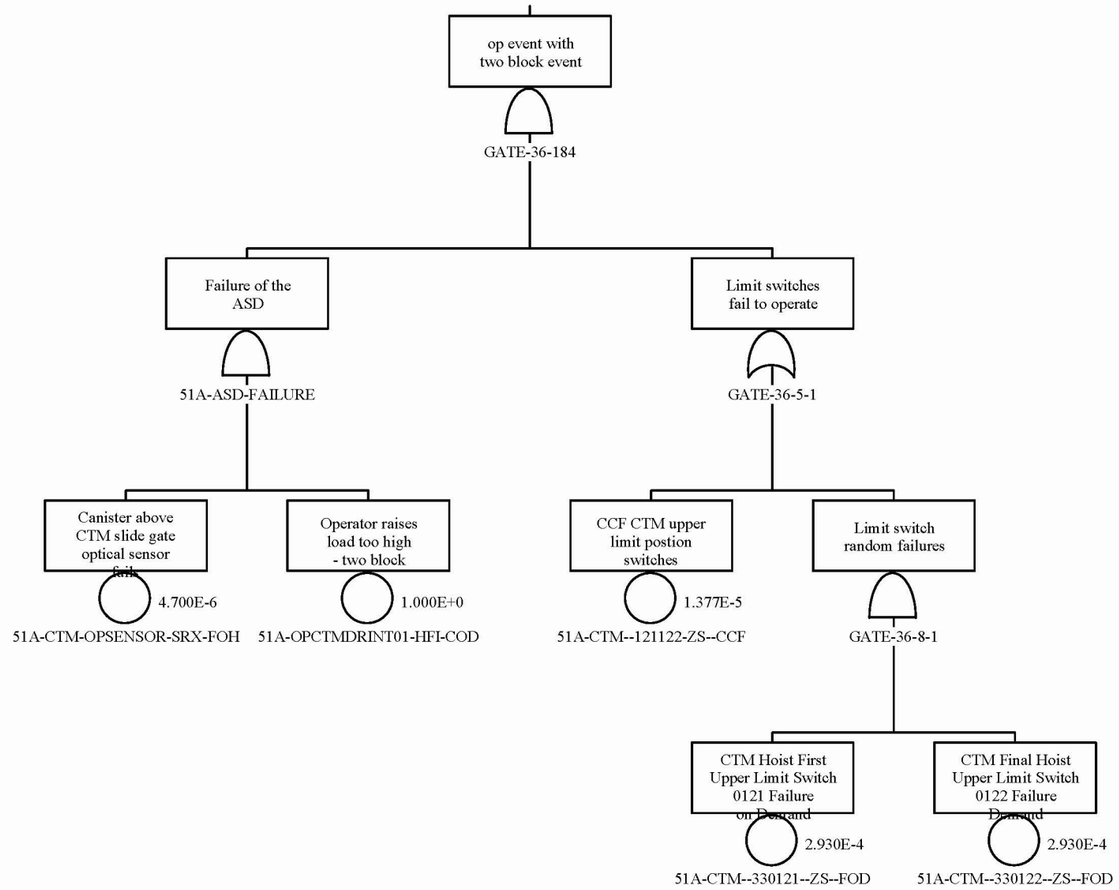
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-23. Drop of Object onto Cask
Sheet 2

INTENTIONALLY LEFT BLANK

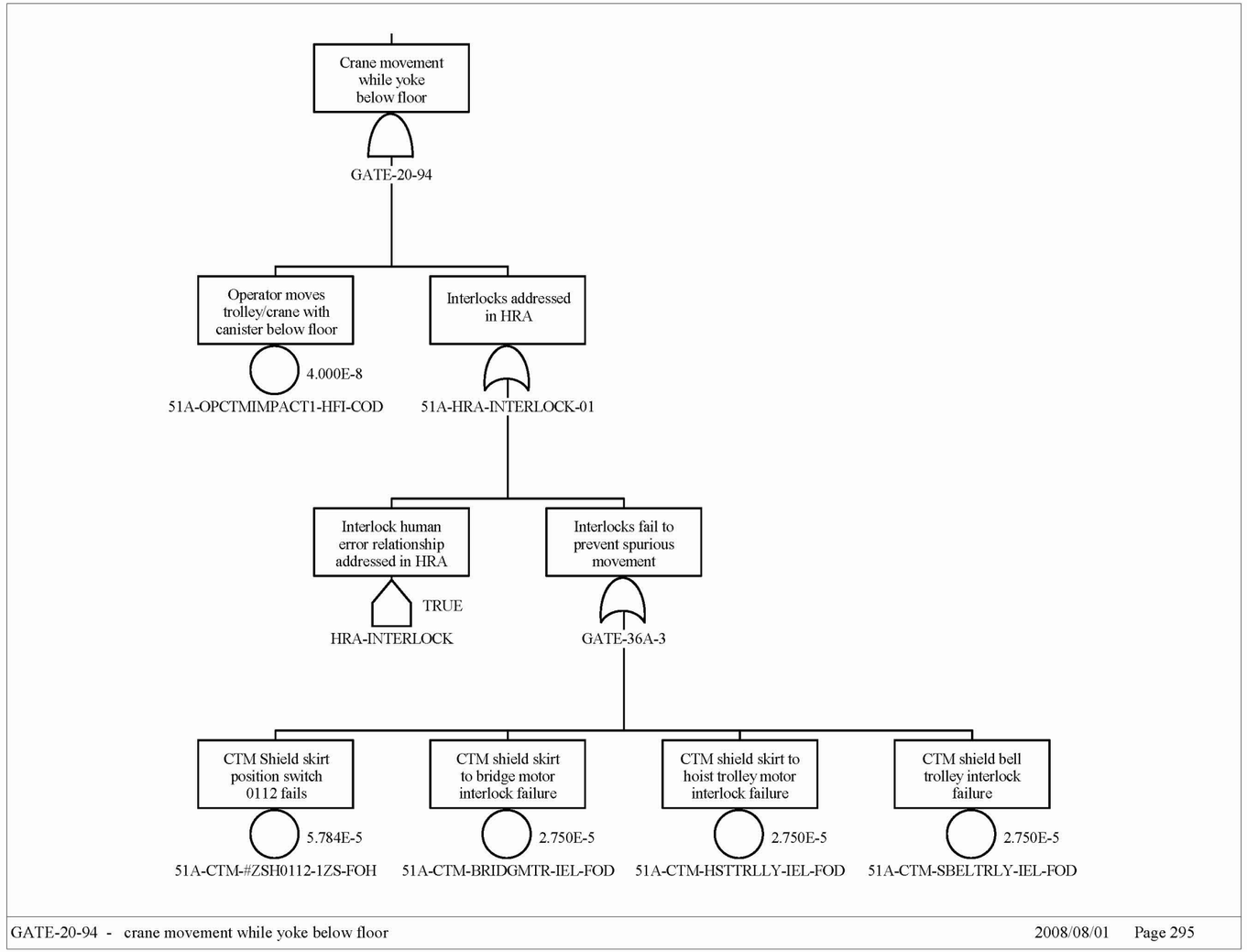


GATE-36-184 - op event with two block event 2008/02/03 Page 283

Source: Original

Figure B4.4-24. Drop of Object onto Cask
Sheet 3

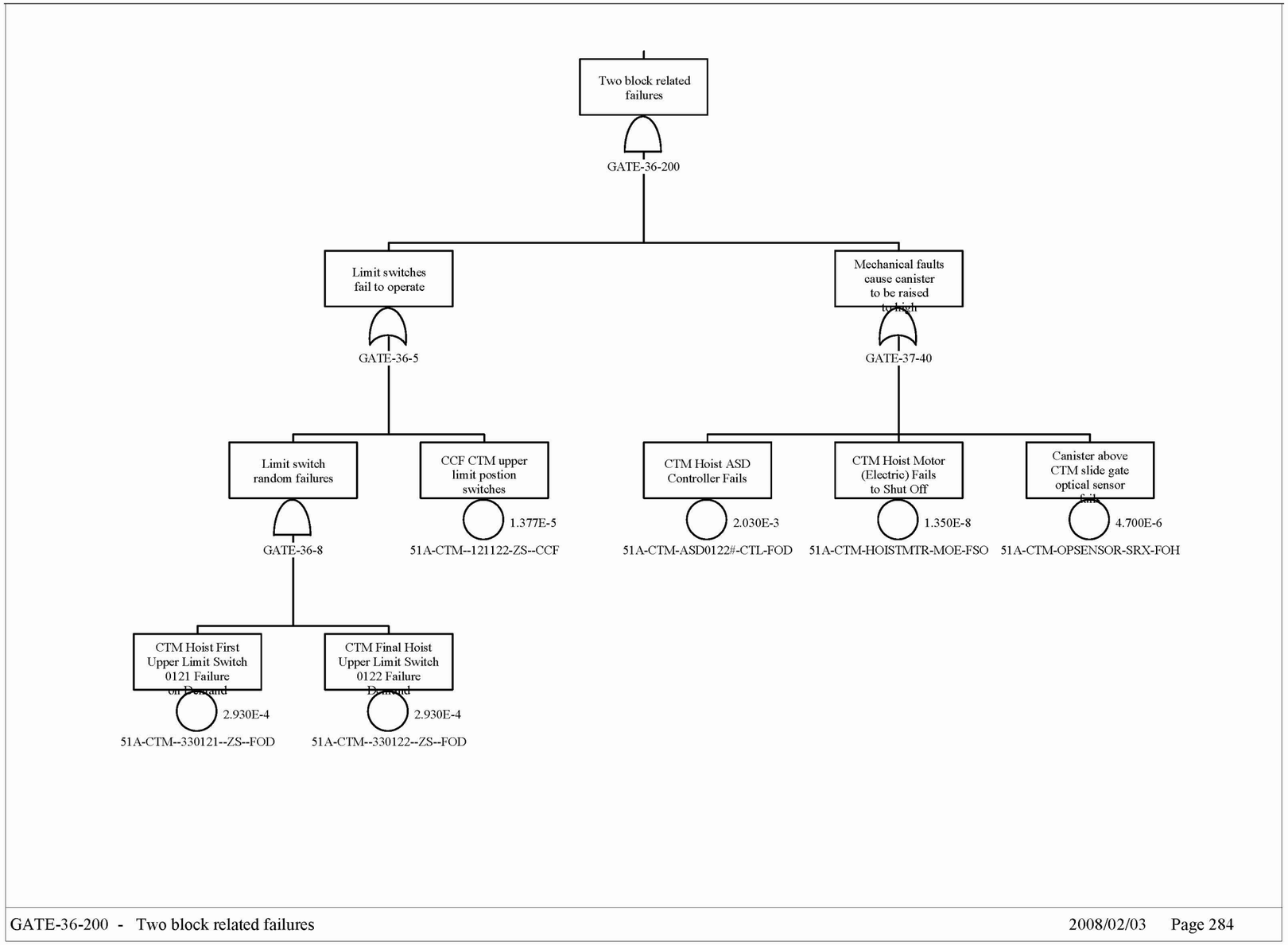
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-25. Drop of Object onto Cask
Sheet 4

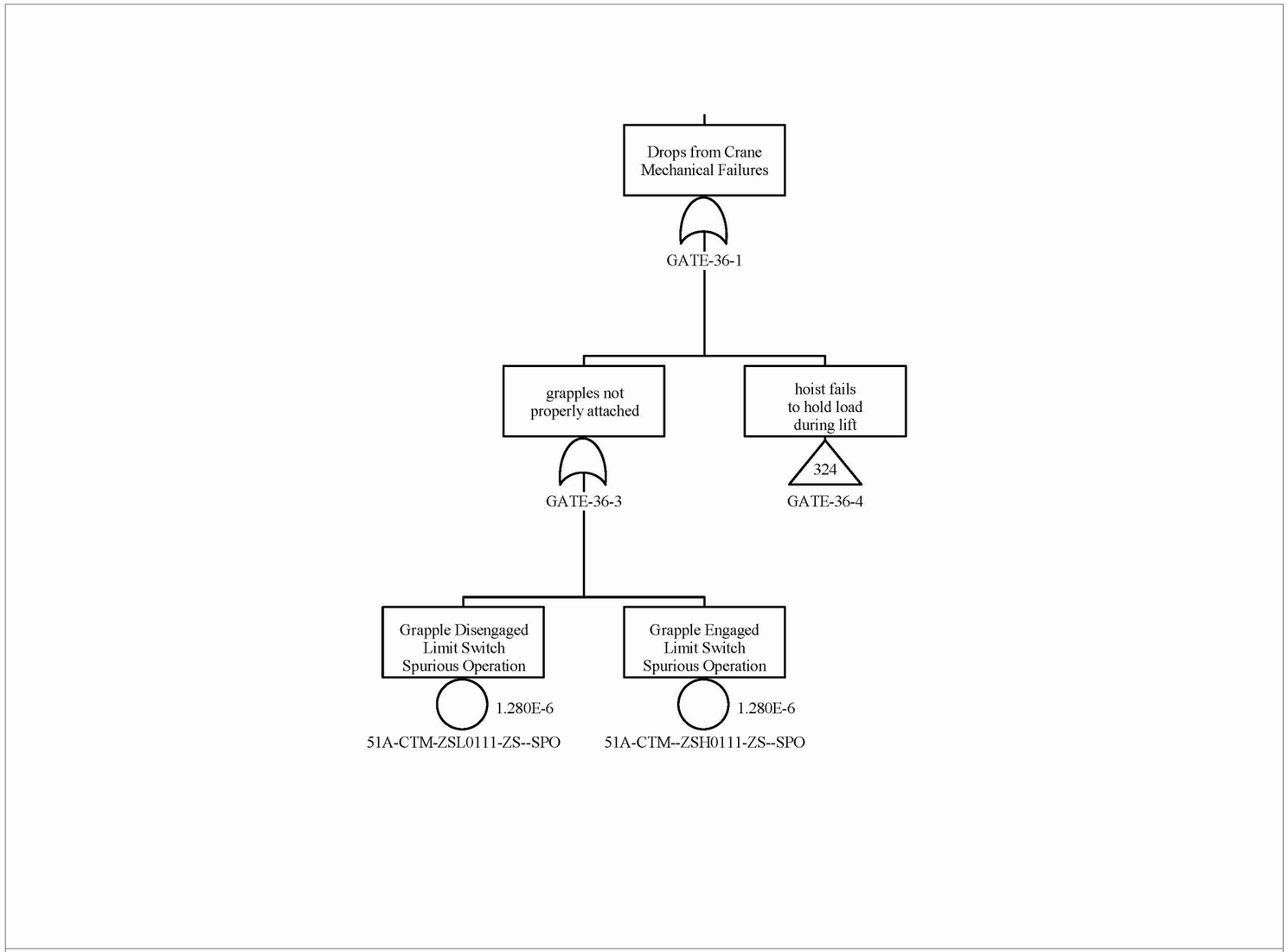
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-26. Drop of Object onto Cask
Sheet 5

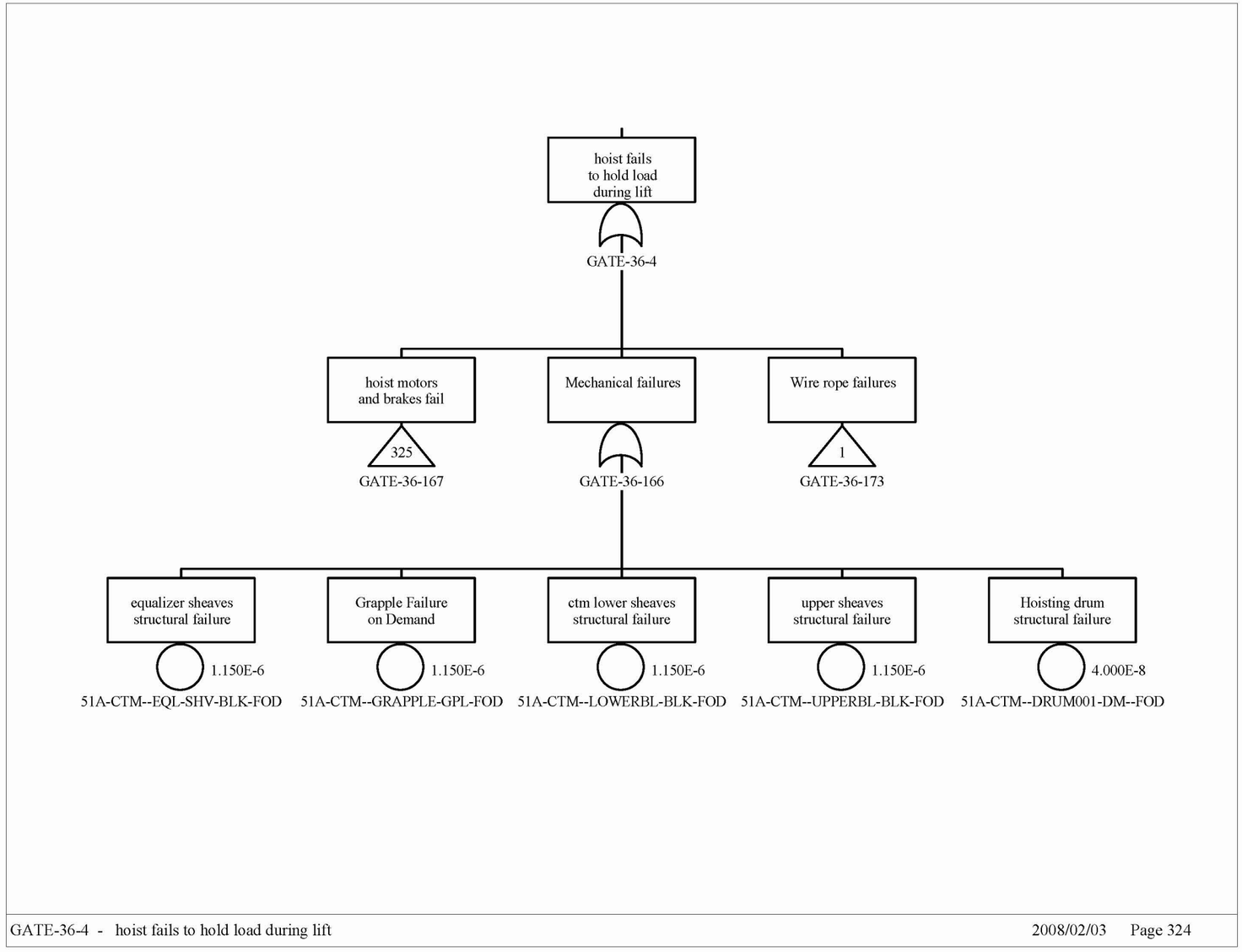
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-27. Drop of Object onto Cask
Sheet 6

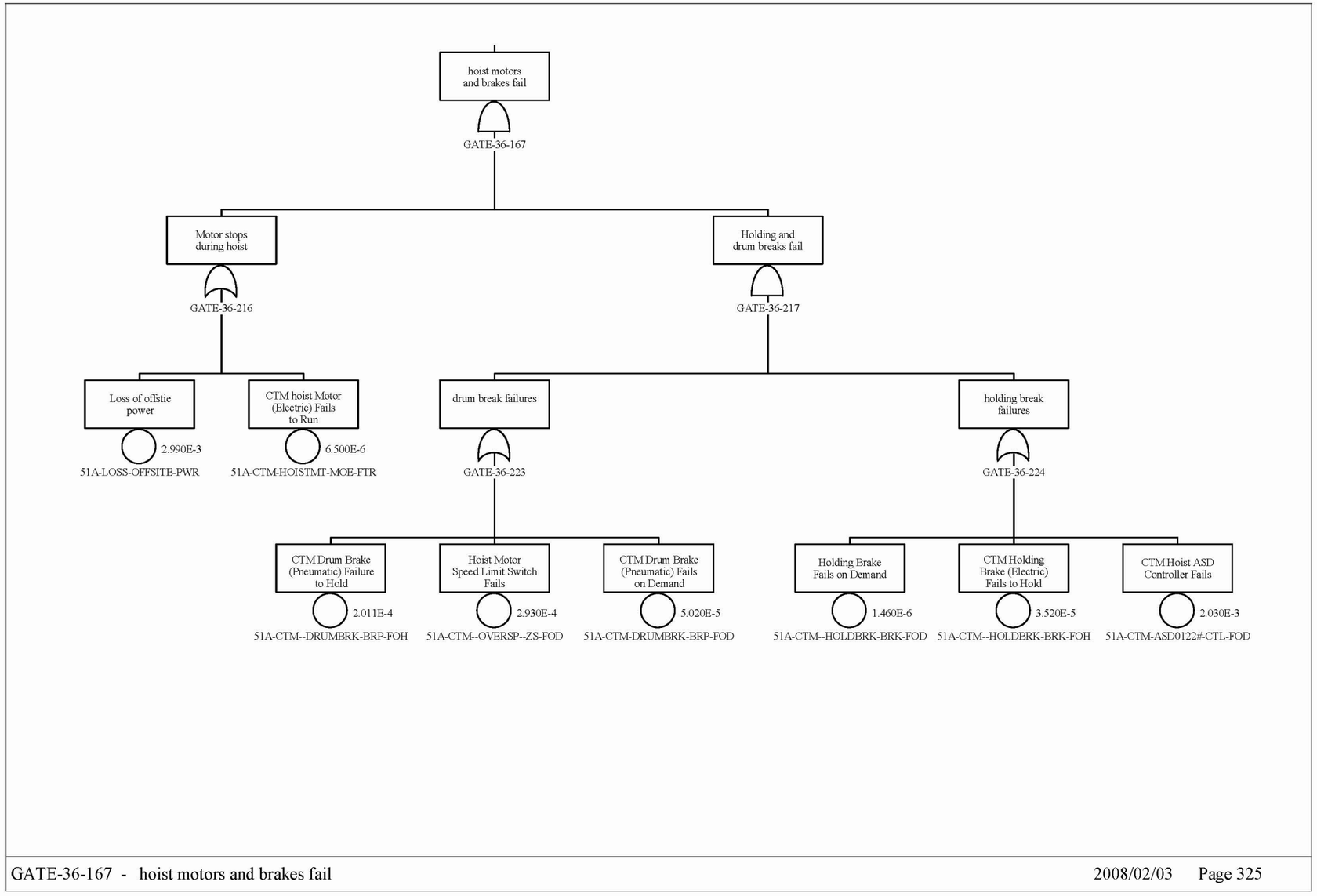
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-28. Drop of Object onto Cask
Sheet 7

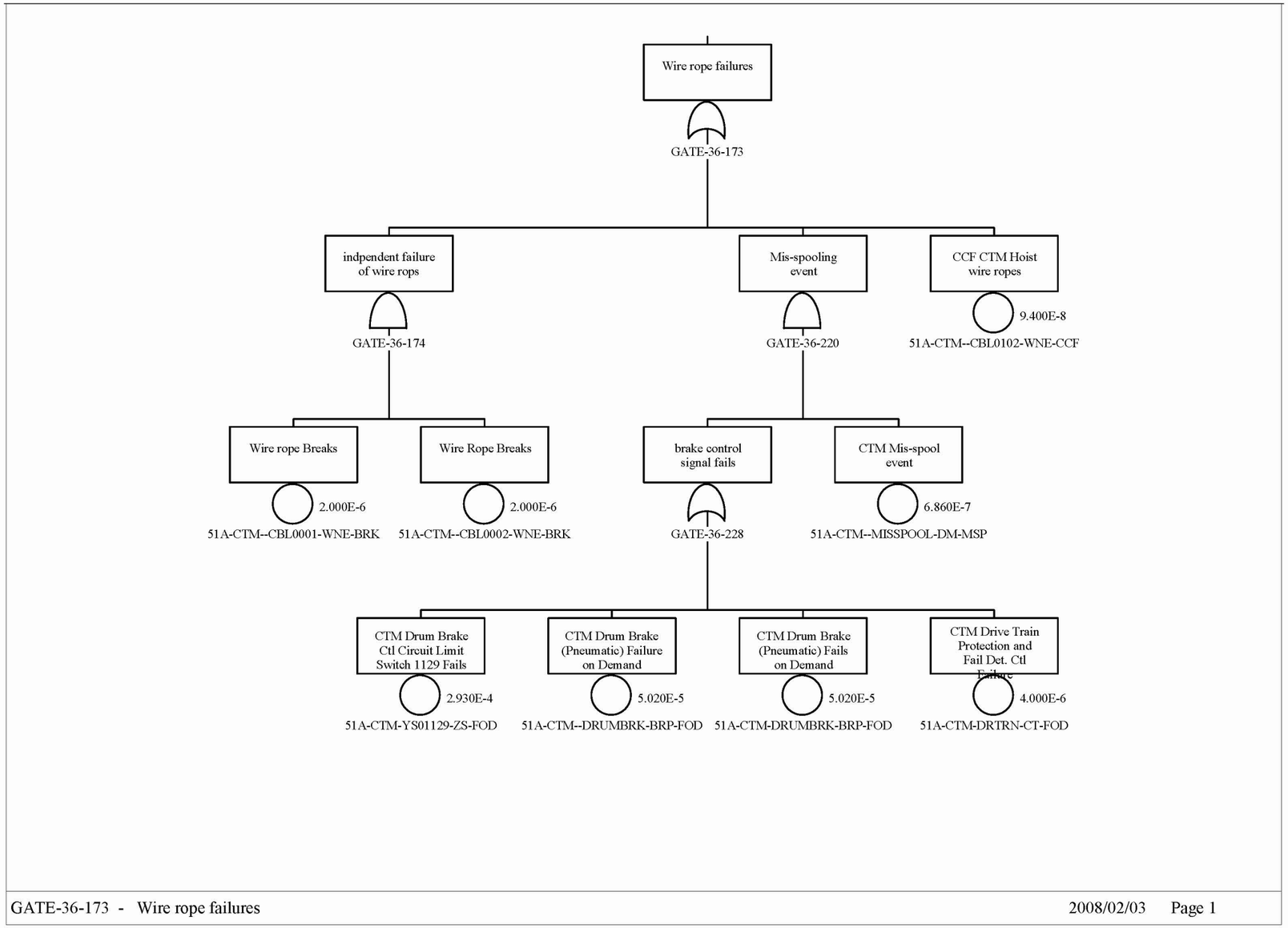
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-29. Drop of Object onto Cask
Sheet 8

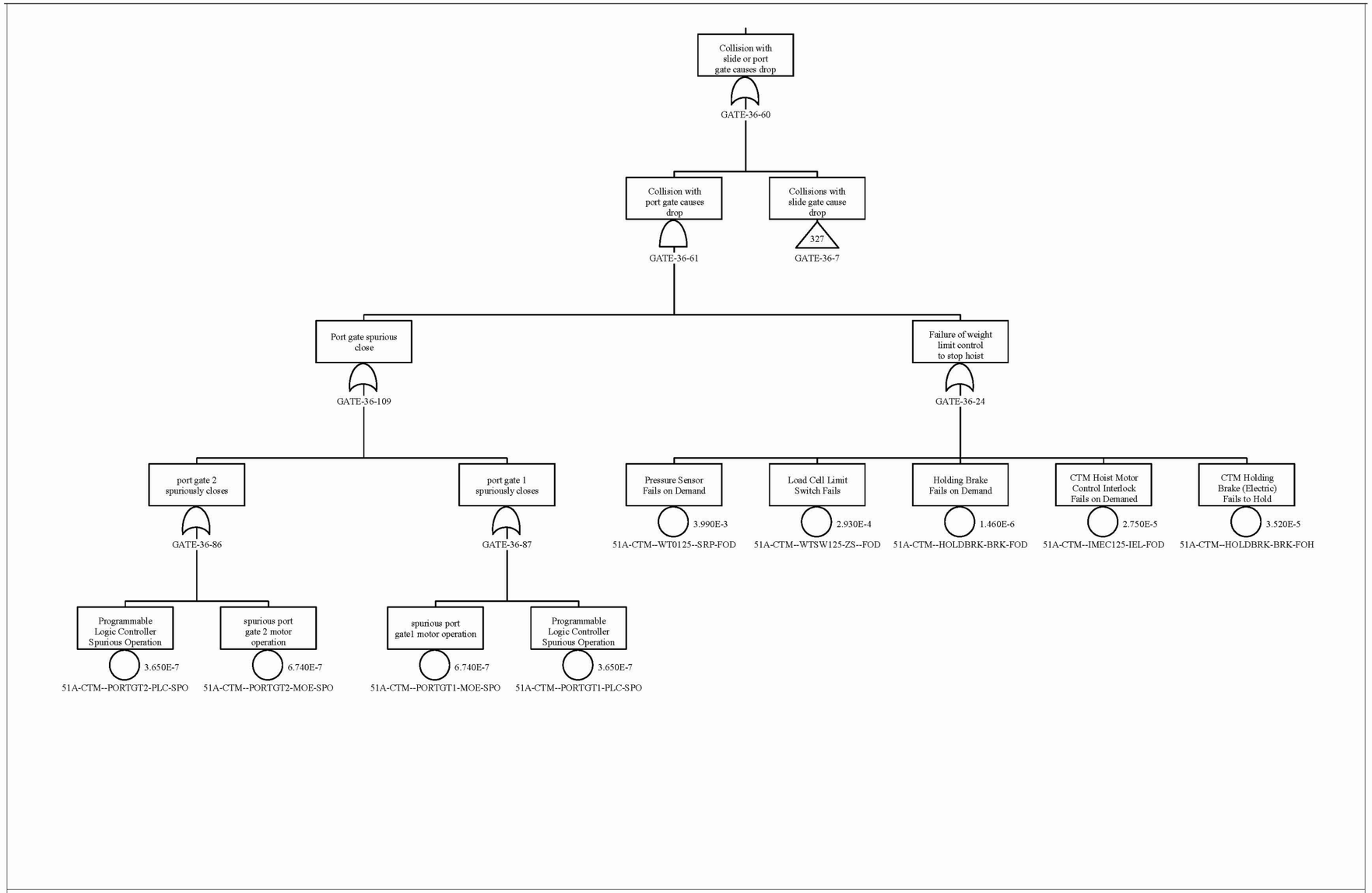
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-30. Drop of Object onto Cask
Sheet 9

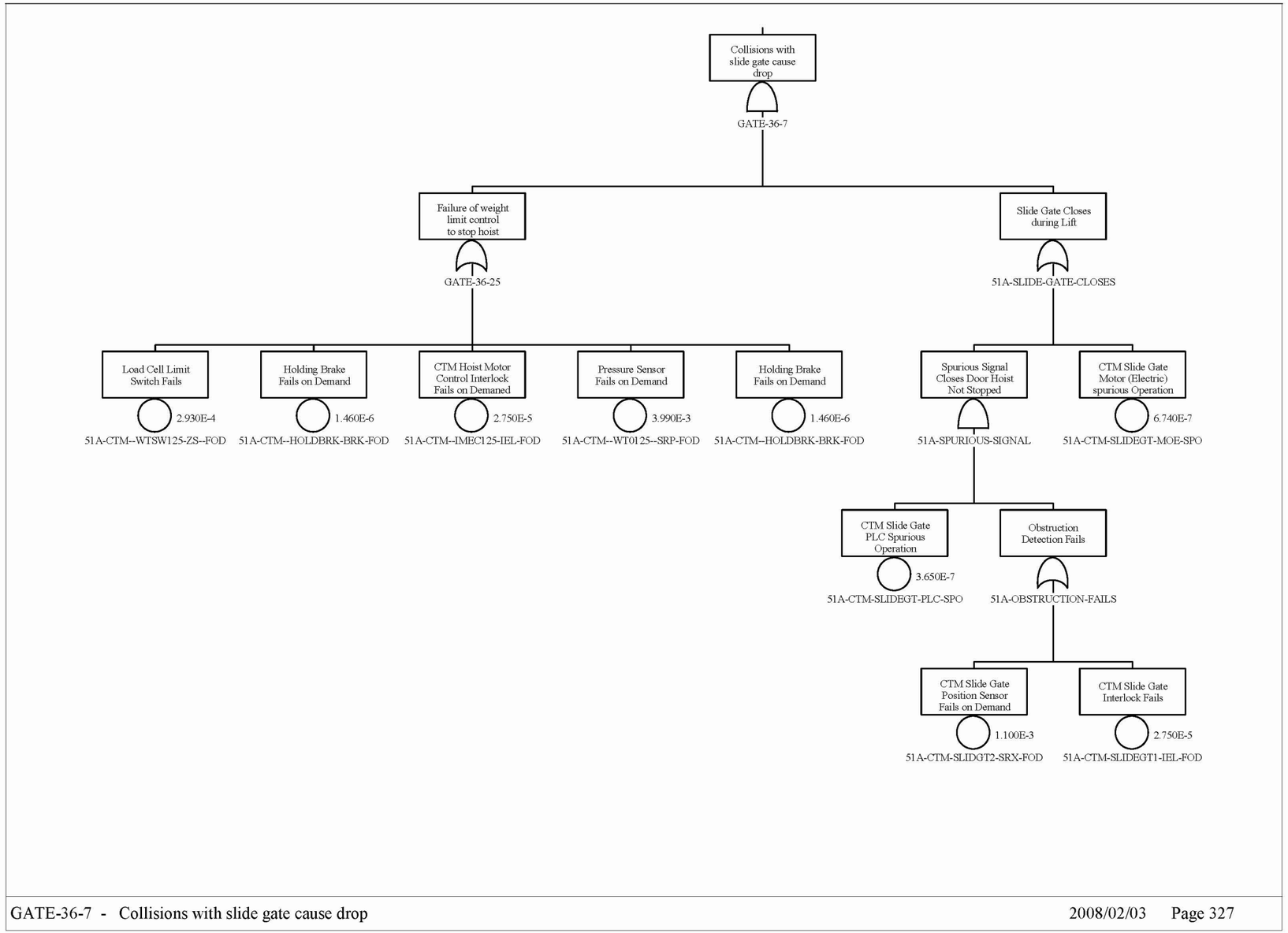
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-31. Drop of Object onto Cask
Sheet 10

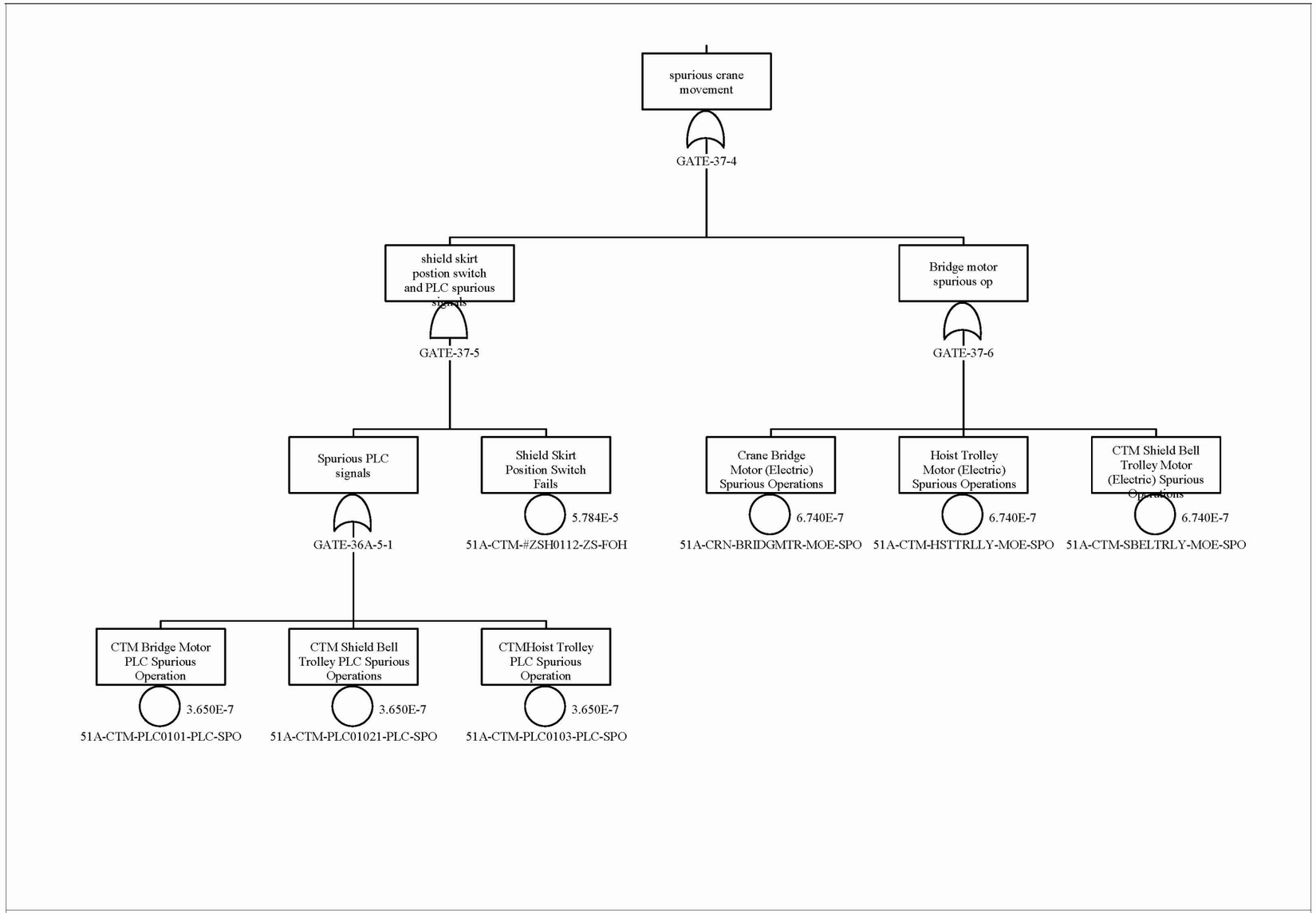
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-32. Drop of Object onto Cask
Sheet 11

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-33. Drop of Object onto Cask
Sheet 12

INTENTIONALLY LEFT BLANK

B4.4.4 Canister Impact

B4.4.4.1 Description

A fault tree was developed to address the potential for impacts to the canister. Collisions between the CTM, shield bell, floor, and a permanent structure were considered.

B4.4.4.2 Success Criteria

Success criteria for the "Canister Impact" is the prevention of a collision between the canister and the shield bell or Canister Transfer Area floor from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.4.3 Design Requirements and Features

Requirements

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

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

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

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

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

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

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

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

Design Features

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

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

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

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

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

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

B4.4.4.4 Fault Tree Model

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

B4.4.4.5 Basic Event Data

Table B4.4-9 contains a list of basic events used in the "Canister Impact" fault tree. Included are the human failure events and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

Table B4.4-9. Basic Event Probabilities for the Canister Impact Fault Tree

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	3	1.949E-06	—	4.450E-10	4380
51A-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	3	1.949E-06	—	4.450E-10	4380
51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.350E-08	—	1.350E-08	1.00E+00
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge Motor Controller Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-BRIDTR-CT-FOD	CTM Bridge Motor Controller Failure	1	4.000E-06	4.000E-06	—	—
51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.750E-05	2.750E-05	—	—
51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	1	3.990E-03	3.990E-03	—	—
51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	3	1.080E-07	—	1.350E-08	8
51A-CTM-TROLLYTR--PR-FOH	CTM Trolley & Run Stop Failure	3	1.949E-06	—	4.450E-10	4380
51A-CTM-TROLT1-HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	1	1.740E-03	1.740E-03	—	—
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	—	—
51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into End stop	1	1.000E+00	1.000E+00	—	—

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

CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

The canister impact modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are tested. They are consequently evaluated over the interval of time between their test (mission time set to the average fault exposure time, one-half the test interval).

B4.4.4.5.1 Human Failure Events

Two basic events are associated with human error (Table B4.4-10). One addresses the movement of the CTM during a lift and the second addresses the potential overrun of the CTM (either the bridge trolley or the hoist/shield skirt trolley). The quantification of these events includes the probability of operator actions and the failure of ITS related interlocks intended to prevent such operator actions.

Table B4.4-10. Human Failure Events

Name	Description
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor
51A-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into end stop

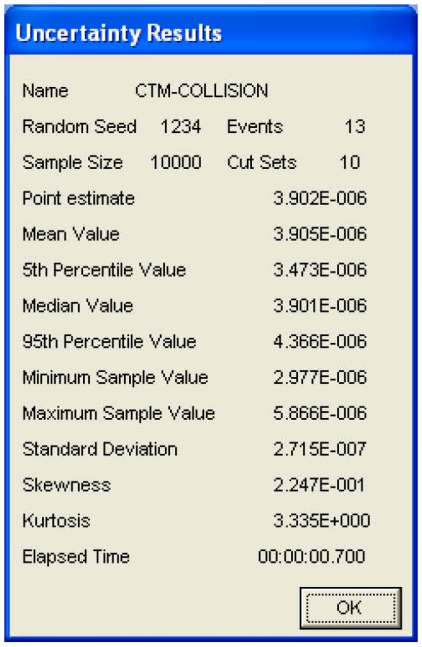
Source: Original

B4.4.4.5.2 Common-Cause Failures

There are no CCFs modeled in the “Canister Impact” fault tree.

B4.4.4.6 Uncertainty and Cut Set Generation

Figures B4.4-34 contains the uncertainty results obtained from running the fault tree for “Canister Impact.” B4.4-35 contains the cut set generation results obtained from running the fault trees for “Canister Impact”.



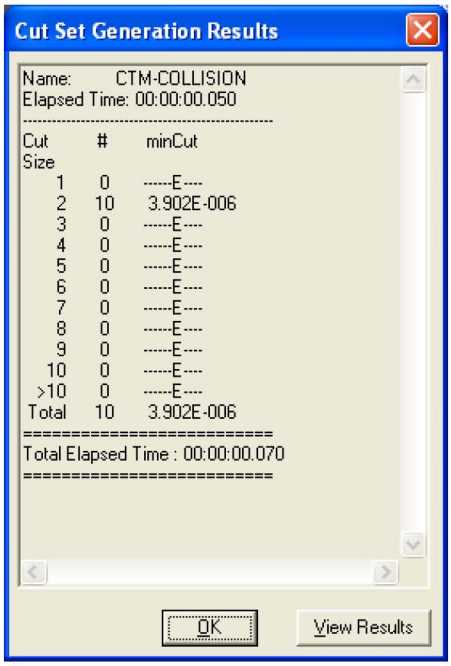
Uncertainty Results

Name	CTM-COLLISION		
Random Seed	1234	Events	13
Sample Size	10000	Cut Sets	10
Point estimate			3.902E-006
Mean Value			3.905E-006
5th Percentile Value			3.473E-006
Median Value			3.901E-006
95th Percentile Value			4.366E-006
Minimum Sample Value			2.977E-006
Maximum Sample Value			5.866E-006
Standard Deviation			2.715E-007
Skewness			2.247E-001
Kurtosis			3.335E+000
Elapsed Time			00:00:00.700

OK

Source: Original

Figure B4.4-34 Uncertainty Results of the Canister Impact Fault Tree



Cut Set Generation Results

```
Name:        CTM-COLLISION
Elapsed Time: 00:00:00.050
-----------------------------------------------
Cut      #      minCut
Size
   1     0      ------E----
   2    10       3.902E-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    10      3.902E-006
==========================
Total Elapsed Time : 00:00:00.070
==========================
```

OK View Results

Source: Original

Figure B4.4-35. Cut Set Generation Results for the Canister Impact Fault Tree

B4.4.4.7 Cut Sets

Table B4.4-11 contains the cut sets for the “Canister Impact” fault tree.

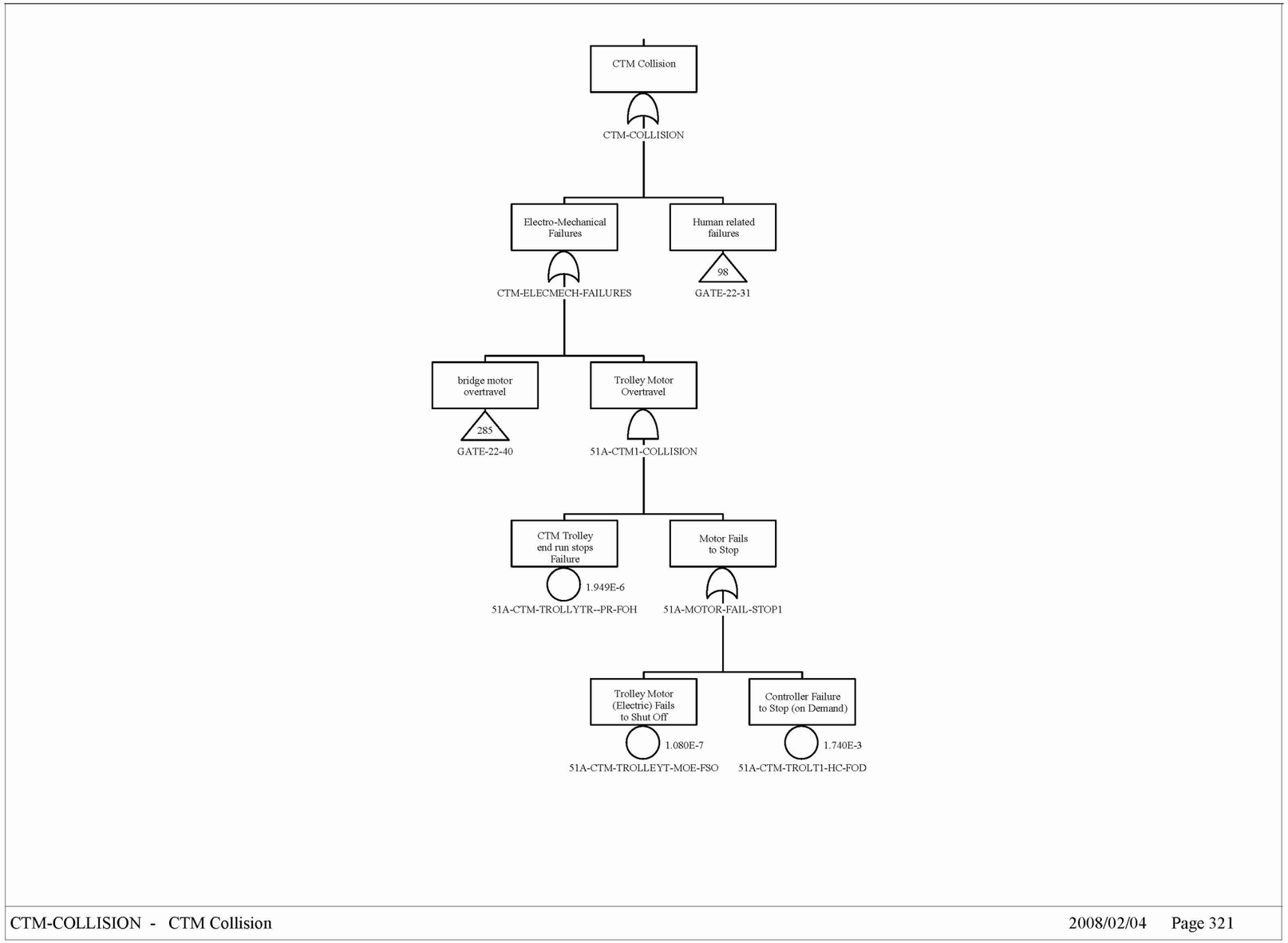
Table B4.4-11. Cut Sets for the Canister Impact Fault Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
49.95	49.95	1.949E-06	51A-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) failure	1.9E-006
			51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into Endstop	1.0E+000
99.90	49.95	1.949E-06	51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.9E-006
			51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into Endstop	1.0E+000
99.99	0.09	3.391E-09	51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.9E-006
			51 A-CTM-TROLT1-HC-FOD	Controller Failure to Stop (on Demand)	1.7E-003
99.99	0.00	1.596E-10	51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	4.0E-003
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
99.99	0.00	7.796E-12	51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	1.9E-006
			51A-CTM-BRIDTR-CT-FOD	CTM Bridge Motor Controller Failure	4.0E-006
99.99	0.00	1.100E-12	51A-CM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	2.8E-005
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
99.99	0.00	1.100E-12	51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	2.8E-005
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
99.99	0.00	1.100E-12	51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.8E-005
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
99.99	0.00	2.105E-13	51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	1.1E-007
			51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.9E-006
99.99	0.00	2.631E-14	51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	1.9E-006
			51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	1.4E-008
99.99		3.902E-06	= Total		

NOTE: CCF =common-cause failure; Ctl =control; CTM =canister transfer machine; PLC =programmable logic controller.

Source: Original

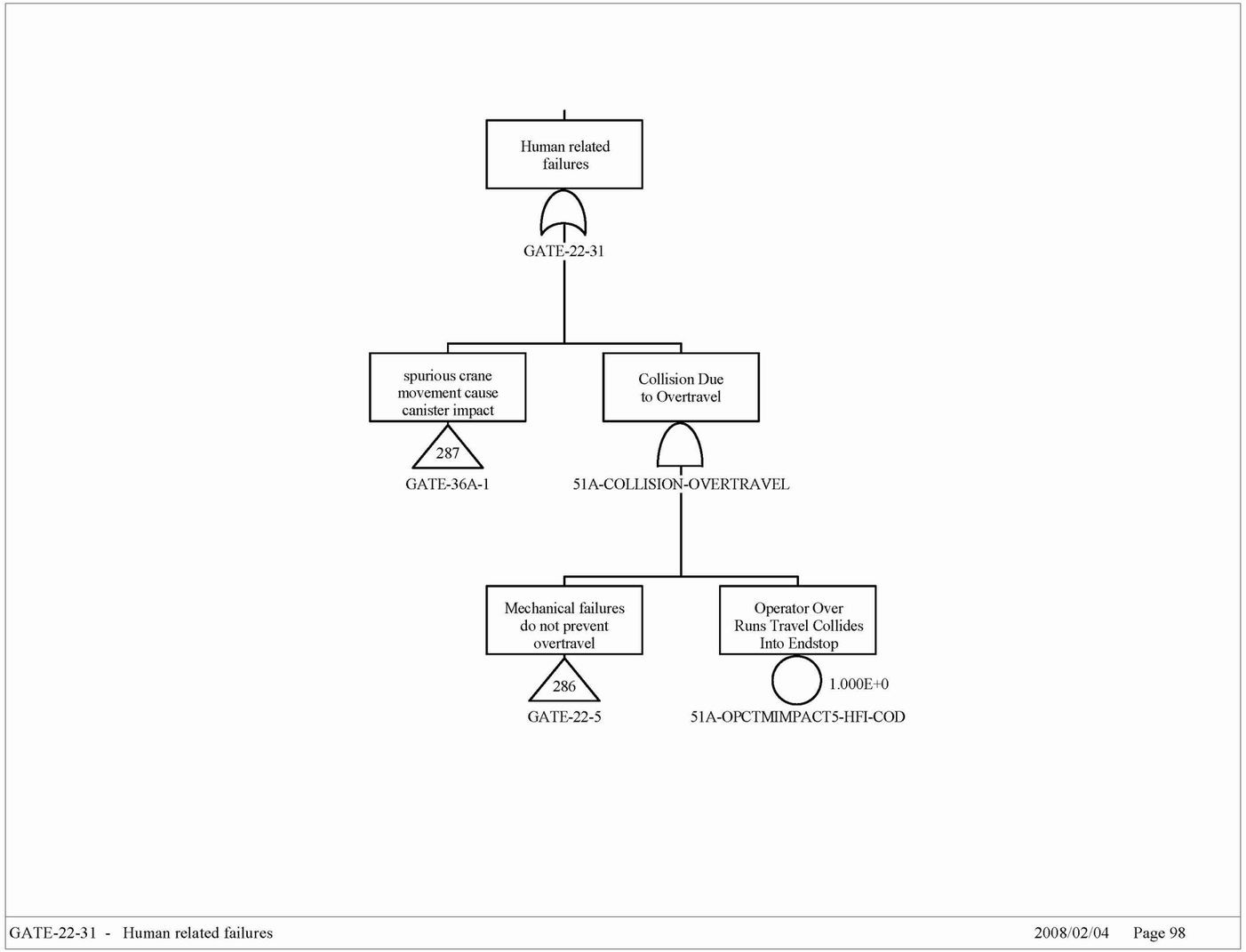
B4.4.4.8 Fault Trees



Source: Original

Figure B4.4-36. CTM Collision Sheet 1

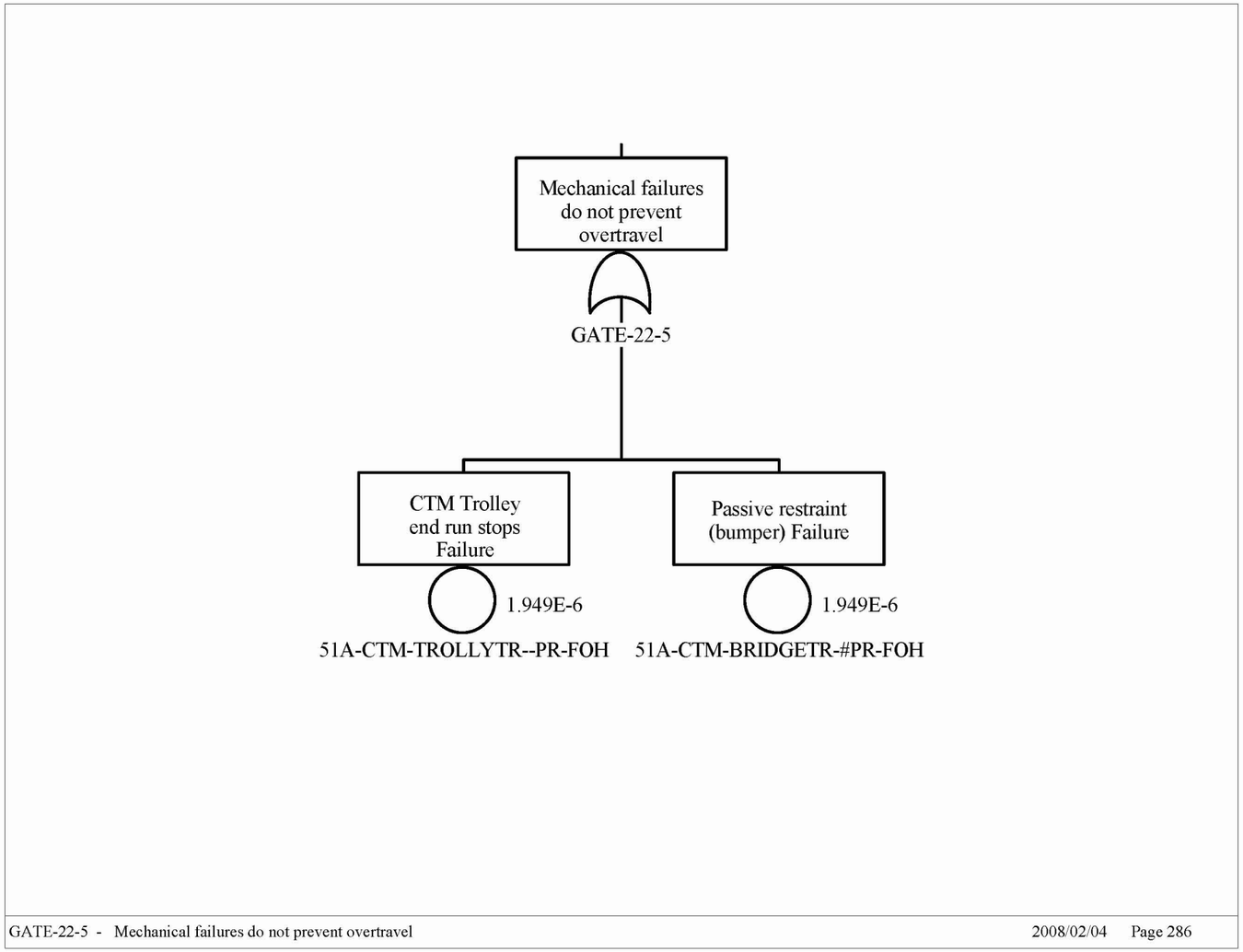
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-37. CTM Collision Sheet 2

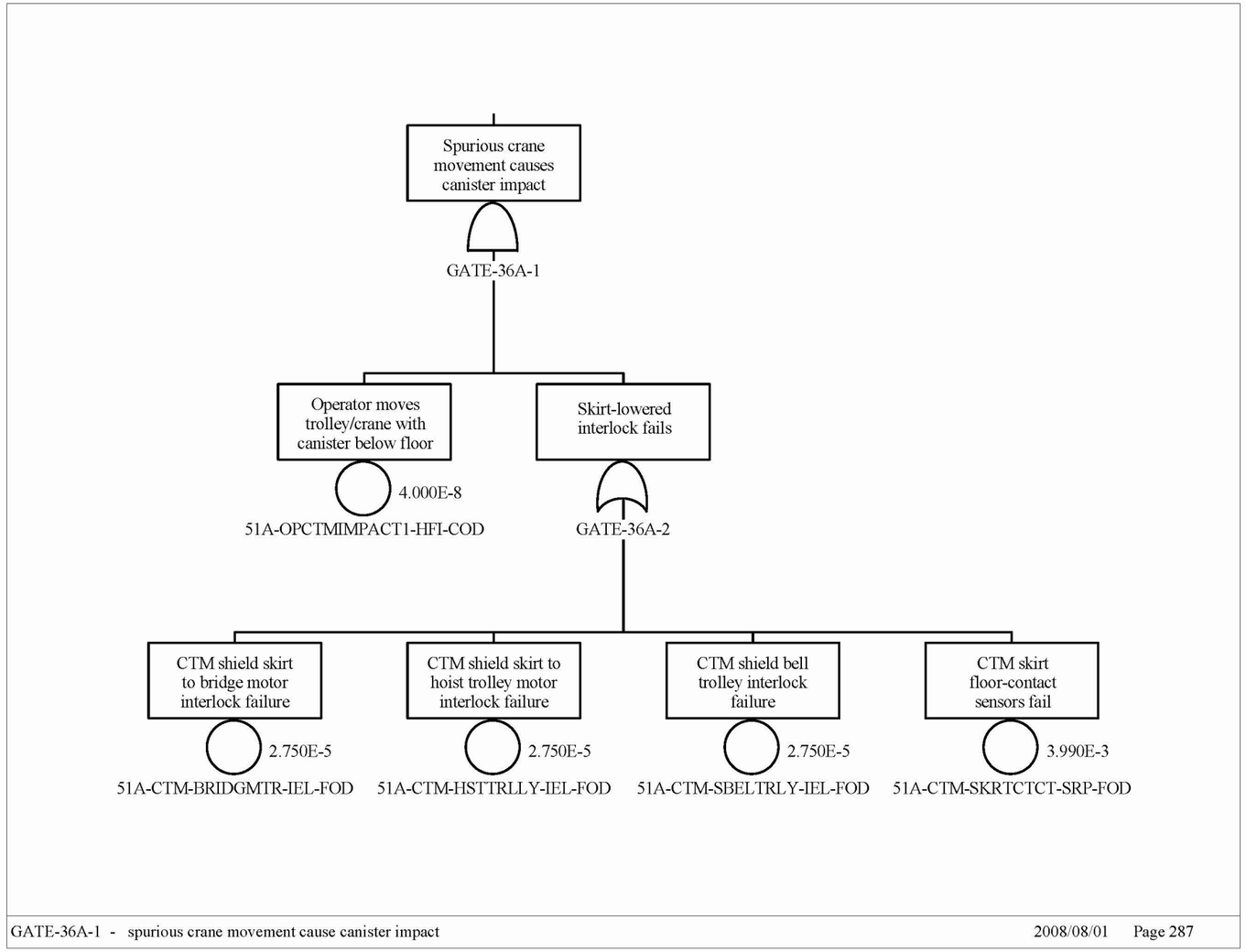
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-38. CTM Collision Sheet 3

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-39. CTM Collision Sheet 4

INTENTIONALLY LEFT BLANK