B4.2.1 CTM Bridge

The bridge design meets the requirements of ASME NOG-1-2004 (Ref. B4.1.1) for a type I crane. The girder design resists the compression, bending, shear, torsion, and buckling loads induced by the fully-loaded trolley, crane dead weight, and impact loads due to seismic events. The end trucks are box section and of high strength design, minimizing deflection and constraining horizontal crane skewing. The flame hardened wheels are attached to the end truck using wheel bearing capsules. Four seismic restraints are provided to prevent excessive horizontal and vertical uplifts.

Hoist, trolley, and bridge drive gearing are enclosed in sealed gear boxes and lubricated with oil of a high flash point, which will not support a flame and fire.

The electric power to the bridge is provided by a crane cable track system along the runway length and supported by the facility wall as shown in Figure B4.2-1.

B4.2.2 Shield Bell Trolley

The shield bell trolley design meets the requirements of ASME NOG-1-2004 (Ref. B4.1.1) for a type I crane. During a seismic event, seismic restraints prevent the trolley from coming off the rails by limiting the amount of uplift. Electrical power to the trolley is provided through hard-wired connections using a cable track system.

B4.2.3 Canister Hoist Trolley

The hoist trolley design meets the requirements of ASME NOG-1-2004 (Ref. B4.1.1) for a type I crane and is also equipped with seismic restraints. The electrical power to the trolley is provided through hard-wired connections using a festoon system. The trolley incorporates a 70-ton hoist system that uses single-failure-proof technology. A canister grapple is supported by the lower block of the 70-ton hoist. The remotely operated grappling system utilizes limit switches to verify grapple engagement. The grapple utilizes a mechanism that includes a mechanical fail-safe drive that does not allow the grapple to disengage when a load is suspended from the canister grapple.

Additional grapples are required for handling high-level radioactive waste (HLW) canisters. The additional canister grapples are manually attached to the CTM canister grapple and limit switches ensure that a proper and complete connection is made.

The hoist motor is designed to lift and lower the load at a nominal speed of 5 ft/min. The hoist motor is controlled by an adjustable speed drive (ASD).

B4.2.4 ITS CTM Normal Operations

A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to a waste package. For this operation a loaded transportation cask, secured in the cask transfer trolley, is positioned below the transfer port in the Cask Unloading Room. The cask lid is in place but unbolted. Similarly, an empty waste package secured by the waste package

transfer trolley is positioned under the adjacent transfer port in the Waste Package Loading Room.

The CTM is moved to a position over the port above the loaded cask. The shield skirt is lowered to rest on the floor, and the port slide gate is opened. The CTM slide gate is opened and the canister grapple is lowered through the shield bell. For HLW casks, the grapple engages a lift fixture on the cask lid. The cask lid is raised into the larger chamber of the CTM. The port slide gate is closed and the shield skirt is raised. The CTM is moved to a cask lid staging area, which is a recess in the floor of the Canister Transfer Area. The cask lid is lowered and placed in the staging area and the grapple is raised.

The CTM is moved over the port above the loaded cask, the CTM grapple is positioned and aligned for the canister pickup, and the shield skirt is lowered. The port slide gate is opened and the grapple is lowered to engage the canister lifting feature. The canister is raised into the shield bell and the hoist stops when a sensor detects that the bottom of the canister has cleared the CTM slide gate. The CTM slide gate and the port slide gate are closed, and the shield skirt is raised.

The CTM is moved to the port above the empty waste package and positioned for canister loading. The shield skirt is lowered and the port slide gate and CTM slide gate are opened. The canister is lowered and placed into the waste package and the grapple is disengaged from the canister.

For HLW waste packages, a waste package inner lid (shield plug) is also placed using the CTM after the waste package is loaded.

The CTM canister grapple is used for handling naval canisters. Other grapples are needed to access the smaller diameter HLW canisters. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Area floor. The CTM hoist is lowered through the shield bell until the CTM grapple is accessible in the room below for canister grapple attachment.

A transportation cask containing one or more HLW canisters is positioned in the Cask Unloading Room. A waste package shield plug (inner lid) with a spreader ring is placed in a lid staging area. An empty waste package is positioned in the loading station of the Waste Package Positioning Room prior to starting the canister transfer operation.

The CTM machine with the correct grapple is used to transfer a HLW canister from the transportation cask to the waste package. After placement of all canisters in the waste package the last step is to place a shield plug in the waste package. This completes a typical loading operation for a HLW type waste package.

The CTM is normally controlled from the facility operations room, but a local control station is also provided.

B4.2.5 ITS CTM Off-Normal Operations

Generally, under off-normal conditions, the CTM is not in operation. Following a loss of AC offsite power, all power to the CTM motors (hoist, bridge, trolley, and bell trolley) is lost. If a transfer is underway when power is lost, all of the CTM motors would stop and the hoist holding brake engages. Operations would be suspended until power is restored and the load can be safely moved. Under other off-normal conditions, transfer operations would be suspended and the CTM would remain idle.

B4.2.6 ITS CTM Testing and Maintenance

The CTM is operated, if not on a continual basis, regularly (e.g., once a shift). Most component functionality is verified during CTM operation. For those components that are not exercised during routine operations (e.g., bridge and trolley end-of-travel end stops, hoist upper limit position switches) routine verification of functionality is required.

B4.2.7 Testing and Maintenance

B4.2.7.1 Requirements

Testing of components not exercised during routine operation of the CTM is tested annually at a minimum.

B4.2.7.2 Design Feature

Normal maintenance is performed in accordance with manufacturer's recommendations; maintenance is performed only when the CTM is not in use.

B4.2.8 Fault Trees

B4.2.8.1 Requirements

The fault tree model for the CTM only includes those components that have been declared as ITS. There is an exception: the spurious operation of PLCs is included in the fault tree model. Spurious operation can result in inadvertent CTM movements.

The mission time for the ITS CTM is set to one hour. Most lifts/transfers require less than one hour. When a transfer consists of several separate activities (e.g., auxiliary equipment movements, lifts, and transfers) each of these activities require less than an hour, but all have been assigned a one-hour mission time.

B4.2.8.2 Design Features

Common-cause failures have been included for three events. Two are associated with position indication sensors: the two upper limit switches on the CTM hoist used to prevent raising a load too high (a two blocking event) and the port gate position sensors (two gates one sensor for each gate). Common-cause failure of the hoist cables is also considered.

Seven human error conditions are incorporated into the model. These are for drops initiated by the operator actions, inadvertent crane movements resulting in impacts, and a failure to restore interlocks allowing movement of the crane when the shield skirt is raised and the slide gates are open.

B4.3 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 B4.3-1 with the following dependencies:

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

Table B4.3-1. Dependencies and Interactions Analysis

Structures, Systems, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
ASDs	Position sensors	—	—	—	—
	CTM hoist, bridge, and trolley motors control	—	—	—	—
CTM Bridge	—	—	CTM bridge	—	—
CTM Motors	ASDs, non-ITS power	—	—	Operational control	Off-site power
Port/Slide Gate Position Switches	ASDs	—	—	—	—
Grapple Position (Engaged/ Disengaged)	ASDs	—	—	—	—
Shied Skirt Position	ASDs	—	—	—	—
Non ITS Power	CTM motors	—	—	—	—
Obstruction sensor	Hoist motor ASD	—	—	—	—

NOTE: ASD = adjustable speed drive; CTM = canister transfer machine; ITS = important to safety.

Source: Original

B4.4 CTM-RELATED FAILURE SCENARIOS

The CTM has five credible failure scenarios:

1. Canister drop from below the canister design-limit drop height. The CTM drops a canister from a height below the design basis height for canister damage (this includes canister drops within the shield bell once the bell slide gate has been closed and drops

through the Canister Transfer Area ports to the loading/unloading areas that can occur before the bell slide gate is closed).

2. Canister drop from above the canister design-limit drop height

3. Drop of object onto canister

4. Canister impact. 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

5. CTM movement subjects canister to shearing forces. The CTM, while carrying a canister, moves in such a manner (e.g., spurious movements, exceeding bridge or trolley end of travel limits) as to cause an impact of the canister with the shield bell.

B4.4.1 Canister Drop from Below the Canister Design-Limit Drop Height

B4.4.1.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of the canisters. These drops have been divided into two classes: drops from heights below the design basis drop height of the canister and drops from heights above the design basis drop height of the canister. The fault tree for canister drops addresses the first of these two scenarios.

B4.4.1.2 Success Criteria

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

B4.4.1.3 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 engagement (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 engagement and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.1.4 Fault Tree Model

The top event in this fault tree is "CTM Drop All Heights." This is defined as a drop of 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.

Failures specifically considered are:

- Electro-mechanical failures that occur as a result of the random catastrophic failure of hoisting components, such as the grapple of the canister transfer machine, or the redundant wire ropes failing independently or by common cause.

- Electro-mechanical failures that occur as a result of the conveyance, from which the canister is being extracted, moving spuriously during the transfer. In response, a misalignment can develop that may result in the canister getting caught on the edge of the shield bell; tension can develop in the wire ropes, conceivably leading to their failure. A load control safety system is capable of detecting such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister.

- Electro-mechanical failures that occur as a result of a slide gate spuriously closing during transfer of a canister. There are two types of slide gates: one that closes the port between the lower and the upper floor in the Canister Transfer Area, and another that closes the bottom part of the shield transfer bell. When the canister is lifted from its container, a spurious slide gate closure can result in the canister getting caught up against the gate; tension can develop in the wire ropes, conceivably leading to their failure. The load control safety system detects such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister.

- Electro-mechanical failures that occur as a result of a spurious movement of the canister transfer machine. The CTM has several trolleys that govern lateral movements, one controls the movement of the CTM bridge, one controls the movement of the shield bell, while another one controls the movement of the load being transferred inside the shield bell (these last two are physically locked together during transfer operations). Spurious actuation of a trolley motor after the grapple is attached to a canister and before the load is lifted above the Canister Transfer Room floor can result in tension developing in the wire ropes, conceivably leading to their failure. Because the load control safety system

does not control lateral movements of the canister transfer machine, it is not capable of stopping operations in this case.

- Human-related actions associated with the operator inappropriately closing a slide gate during vertical canister movement. As for the spurious electro-mechanical slide gate closure discussed previously, tension in the wire ropes can develop as a result of this event, conceivably leading to their failure. The load control safety system detects such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister. The human error probability assigned to this human failure event is a screening value of 0.001, i.e., it is a conservative estimate based upon predetermined characteristics of the human failure event (Table 6.4-1).

- Human-related actions associated with the operator causing a drop of a canister, from a low height, during its extraction from its container. The human error probability for this event required a detailed analysis, entailing an examination of human failure scenarios that account for interactions and error-forcing context resulting from the combination of equipment conditions and human factor. The result of this analysis was condensed into a single basic event whose probability embeds the combination of both human and equipment failures necessary to cause a drop, which explains its relatively low value (5×10^{-7}) (Table 6.4-1).

B4.4.1.5 Basic Event Data

Table B4.4-1 contains a list of basic events used in the "Canister Drop from Below the Canister Design-Limit Drop Height" fault trees. Included are the HFEs and the common-cause failure events identified in those 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 canister 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 canister transfer machine. 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 B4.4-1. Basic Event Probabilities for the Canister Drop from Below Canister Drop Height Limit 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-ZS-FOH	Shield Skirt Position Switch Fails	3	5.784E-05	—	7.230E-06	8
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
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	—	3.650E-07	1
51A-CTM--TROLLY-MOE-SPO	Trolley Motor Spurious Operation	3	6.740E-07	—	6.740E-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	—	—
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-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	—	—

Table B4.4-1. Basic Event Probability for the Canister Drop from Below Canister Drop Height Limit Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CTM-HOISTMT-MOE-FTR	CTM hoist Motor (Electric) Fails to Run	3	6.500E-06	—	6.500E-06	1
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	3	6.740E-07	—	6.740E-07	1
51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Ctl Interlock Fails on Demand	1	2.750E-05	2.750E-05	—	—
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-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
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-WT0125-SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	—	—
51A-CTM-WTSW125-ZS-FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	—	—
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 off site power	1	2.990E-03	2.990E-03	—	—
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1	1.000E-03	1.000E-03	—	—
51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	1	2.000E-04	2.000E-04	—	—

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.

Calc. =calculation; CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

B4.4.1.5.1 Human Failure Events

Two basic events are associated with human error (Table B4.4-2). These are for drops initiated by the operator actions and an operator action to close the shield or slide gate doors while a CTM lift is being performed.

Table B4.4-2. Human Failure Events

Name	Description
51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close

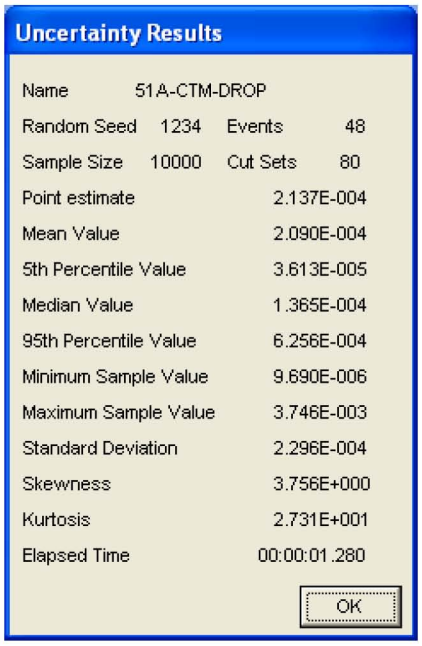
Source: Original

B4.4.1.5.2 Common-Cause Failures

One common-cause event was considered in the evaluation of this top event. The common-cause failure considered is the common-cause failure of the hoist cables.

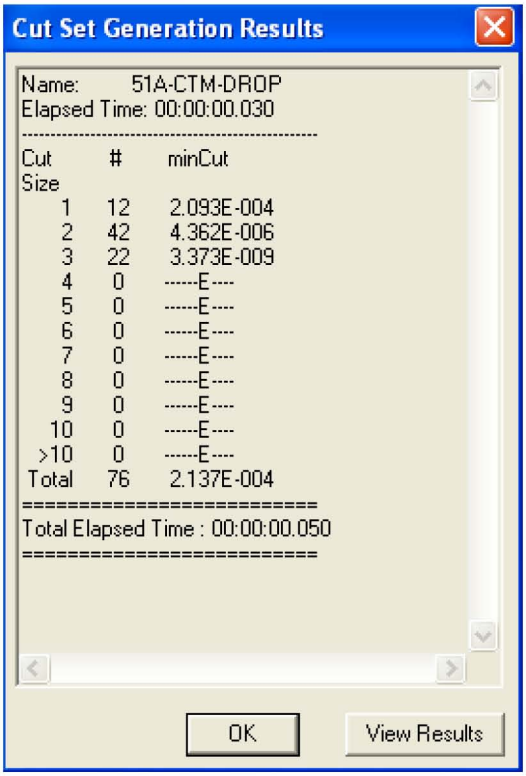
B4.4.1.6 Uncertainty and Cut Set Generation

Figure B4.4-1 contains the uncertainty results obtaining from running the fault trees for the "Canister Drop from Below the Canister Design-Limit Drop Height." Figure B4.4-2 provides the cut set generation results for "Canister Drop from Below the Canister Design-Limit Drop Height".



Source: Original

Figure B4.4-1. Uncertainty Results of the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree

B4.4.1.7 Cut Sets

Table B4.4-3 contains the cut sets for the "Canister Drop from Below the Canister Design-Limit Drop Height" with frequencies above 1E-08.

Table B4.4-3. Dominant Cut Sets for Canister Drop from Below the Canister Design-Limit Drop Height

Fault Tree	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
51A-CTM-DROP	93.60	2.000E-04	51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	2.0E-04
	1.87	3.990E-06	51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	4.0E-03
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-03
	0.60	1.280E-06	51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	1.3E-06
	0.60	1.280E-06	51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	1.3E-06

Table B4.4-3 Dominant Cut Sets for the CTM Canister Drop (Continued)

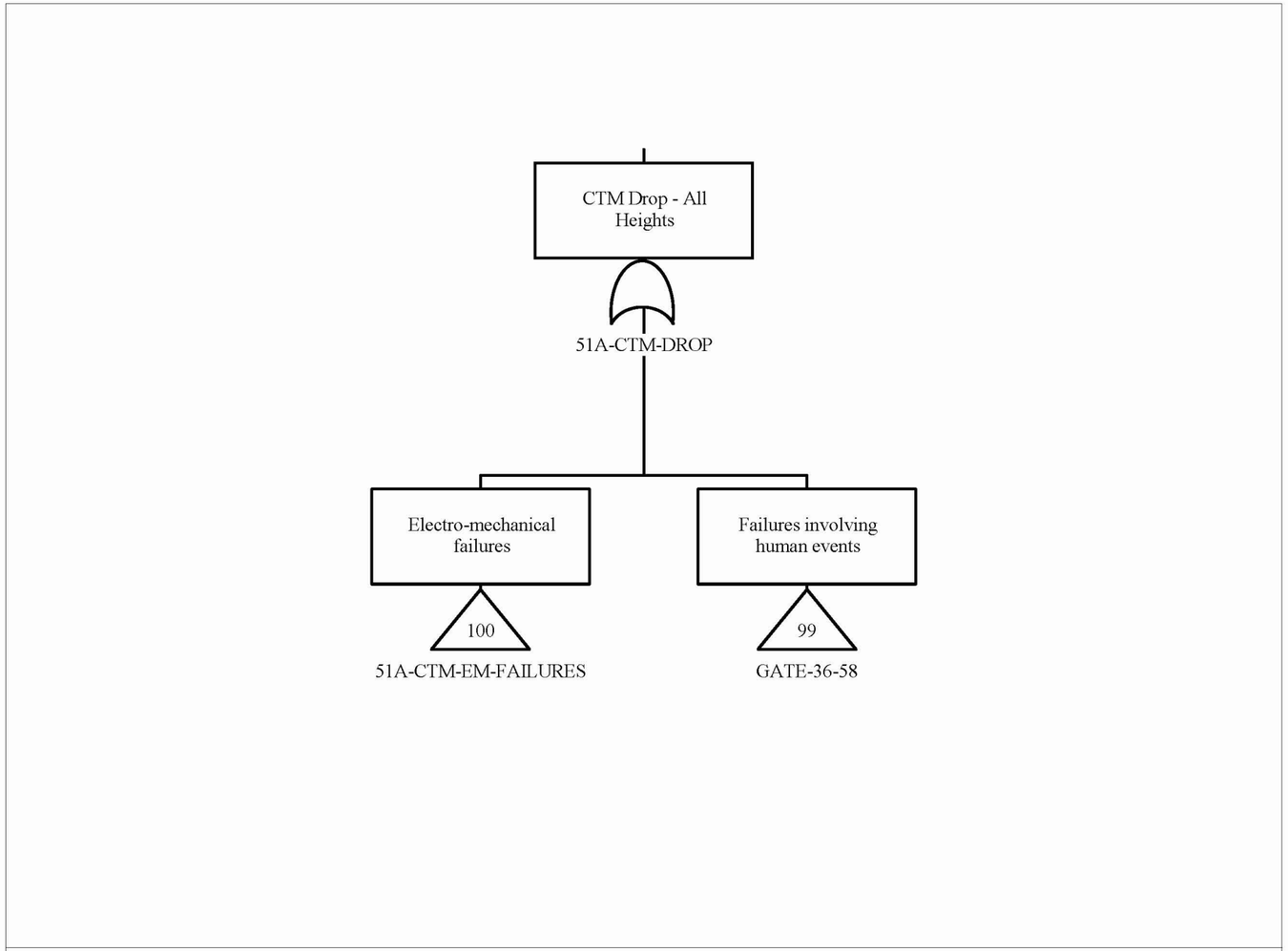
Fault Tree	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
51A-CTM-DROP (continued)	0.54	1.150E-06	51A-CTM--EQL-SHV-BLK-FOD	equalizer sheaves structural failure	1.2E-06
	0.54	1.150E-06	51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1.2E-06
	0.54	1.150E-06	51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1.2E-06
	0.54	1.150E-06	51A-CTM--UPPERBL-BLK-FOD	upper sheaves structural failure	1.2E-06
	0.32	6.740E-07	51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	6.7E-07
	0.32	6.740E-07	51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	6.7E-07
	0.32	6.740E-07	51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	6.7E-07
	0.14	2.930E-07	51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	2.9E-04
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-03
	0.04	9.400E-08	51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.4E-08
	0.02	4.000E-08	51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	4.0E-08
	0.02	3.520E-08	51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3.5E-05
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.0E-03
	0.01	2.750E-08	51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Ctl Interlock Fails on Demand	2.8E-05
		2.137E-004	= Total		

NOTE: CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller; Prob. = probability. Cut sets with frequencies less than 1E-08 are not shown.

Source: Original

B4.4.1.8 Fault Trees

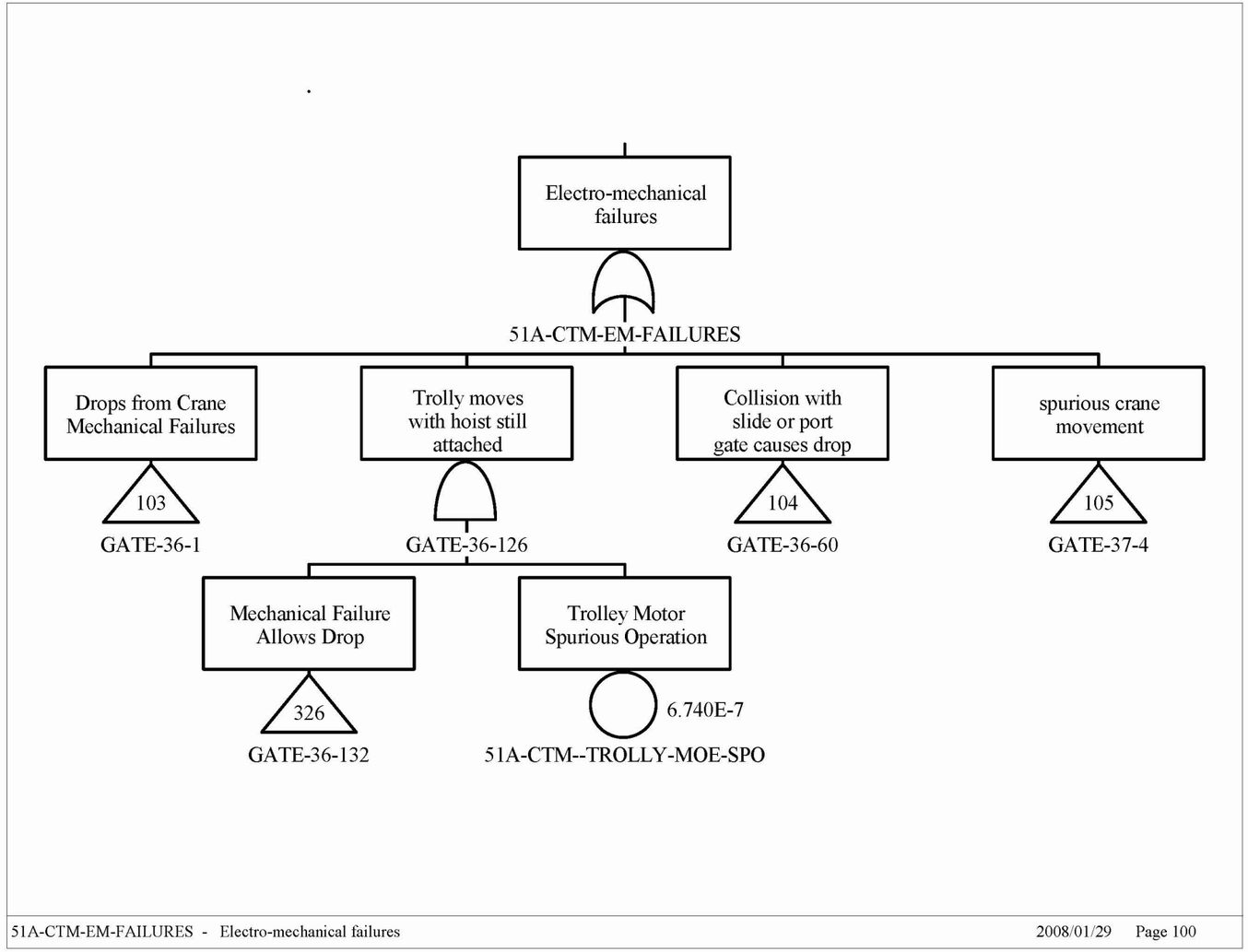
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-3. CTM Drop Fault Tree Sheet 1

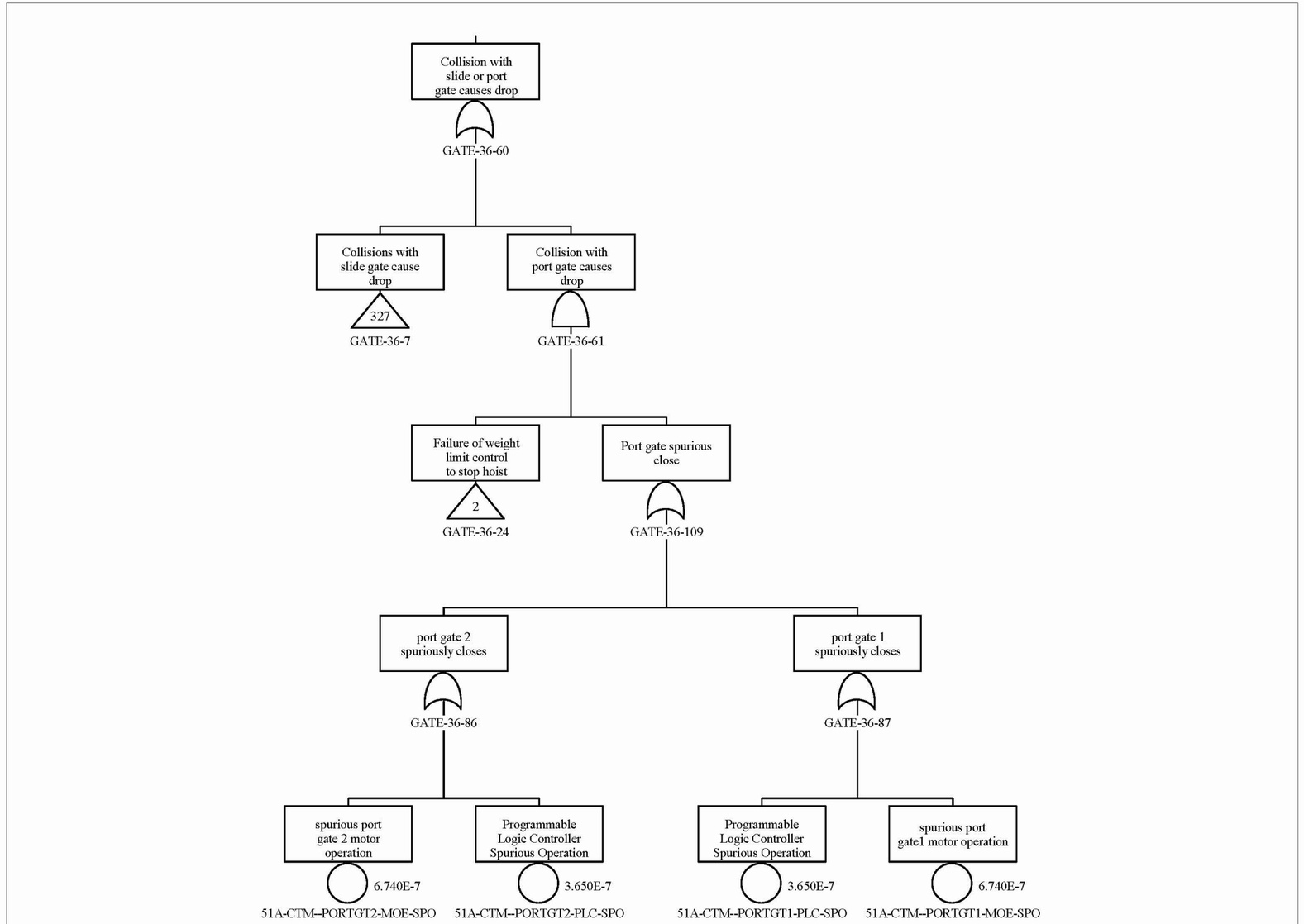
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-4. CTM Drop Fault Tree Sheet 2

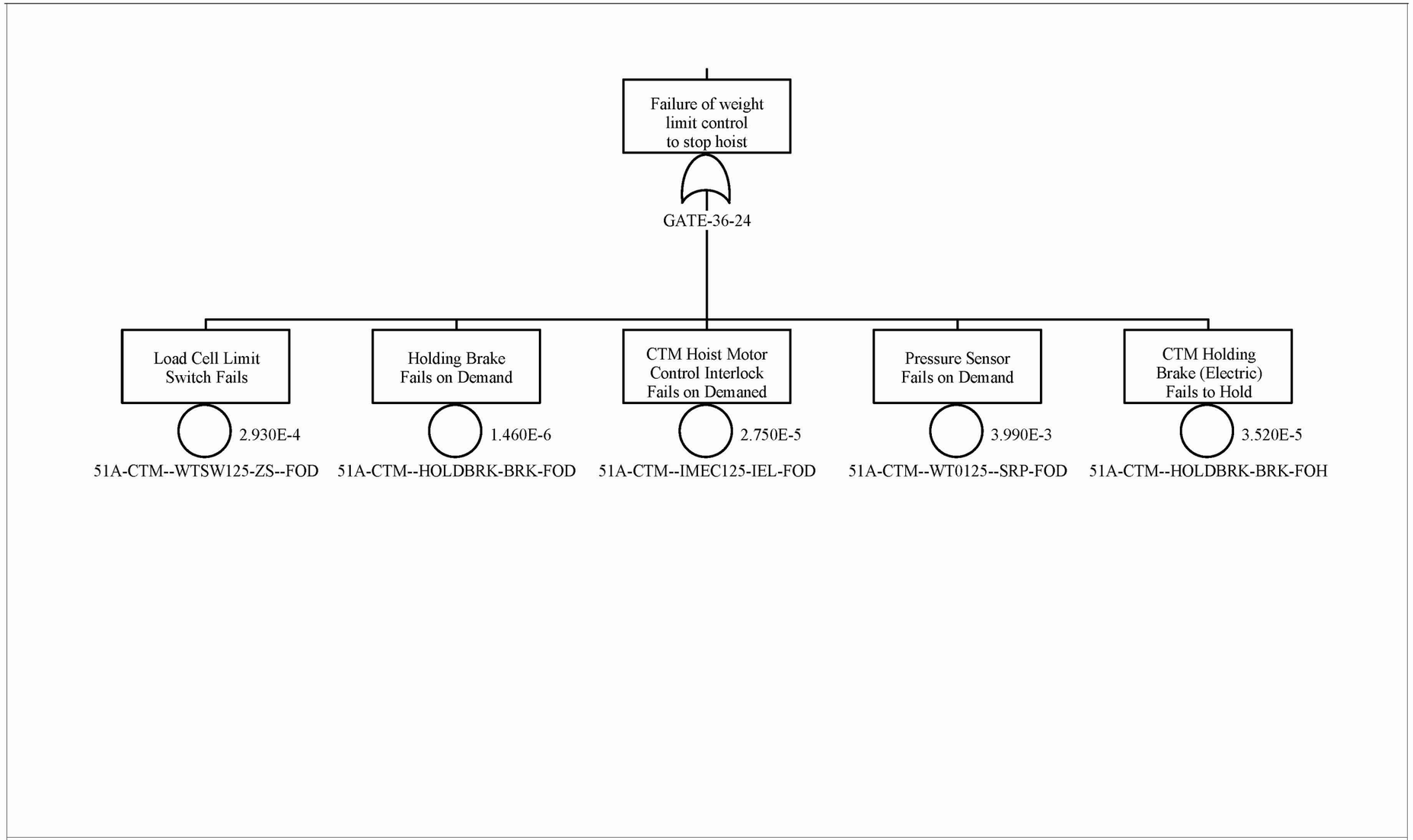
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-5 CTM Drop Fault Tree Sheet 3

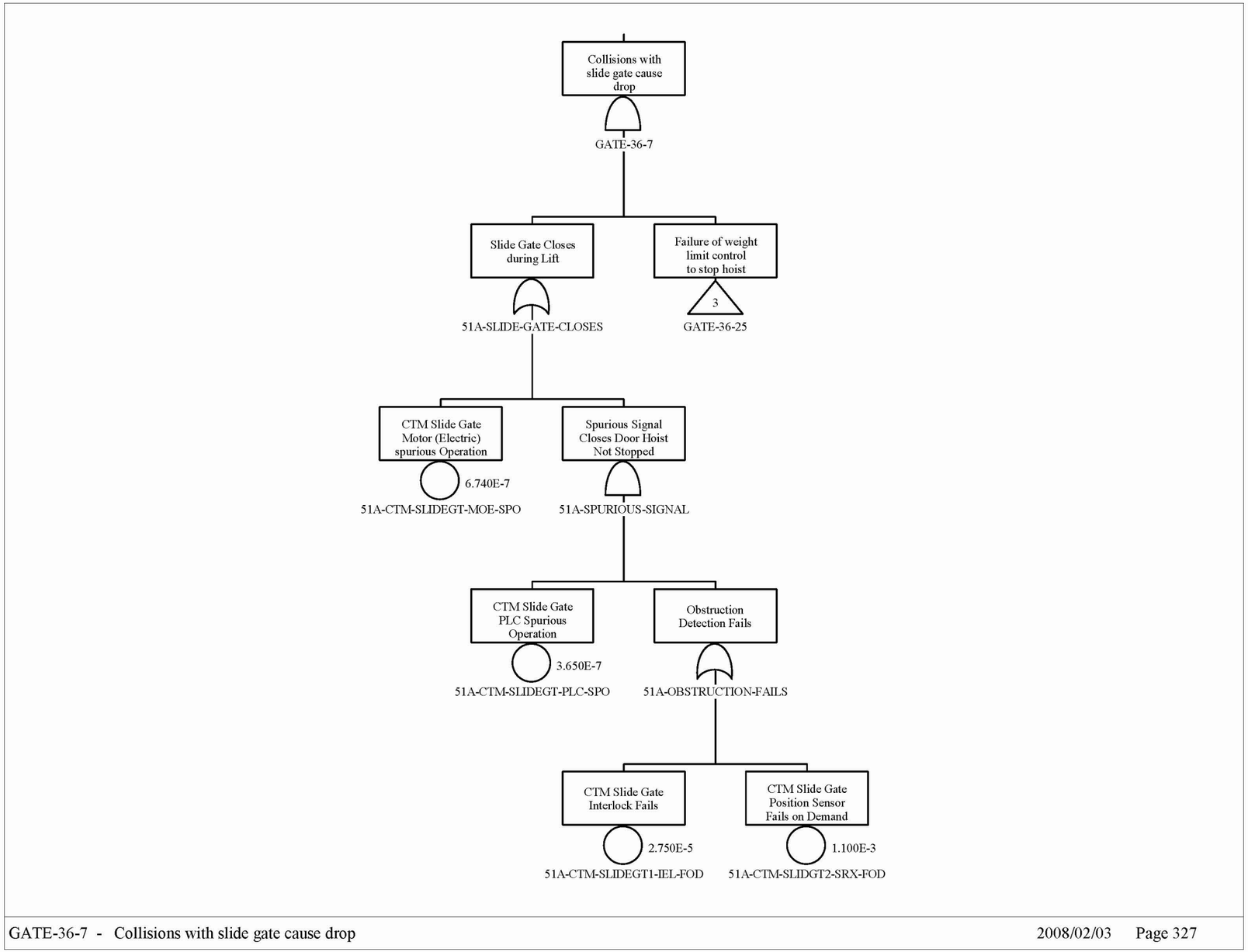
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-6. CTM Drop Fault Tree Sheet 4

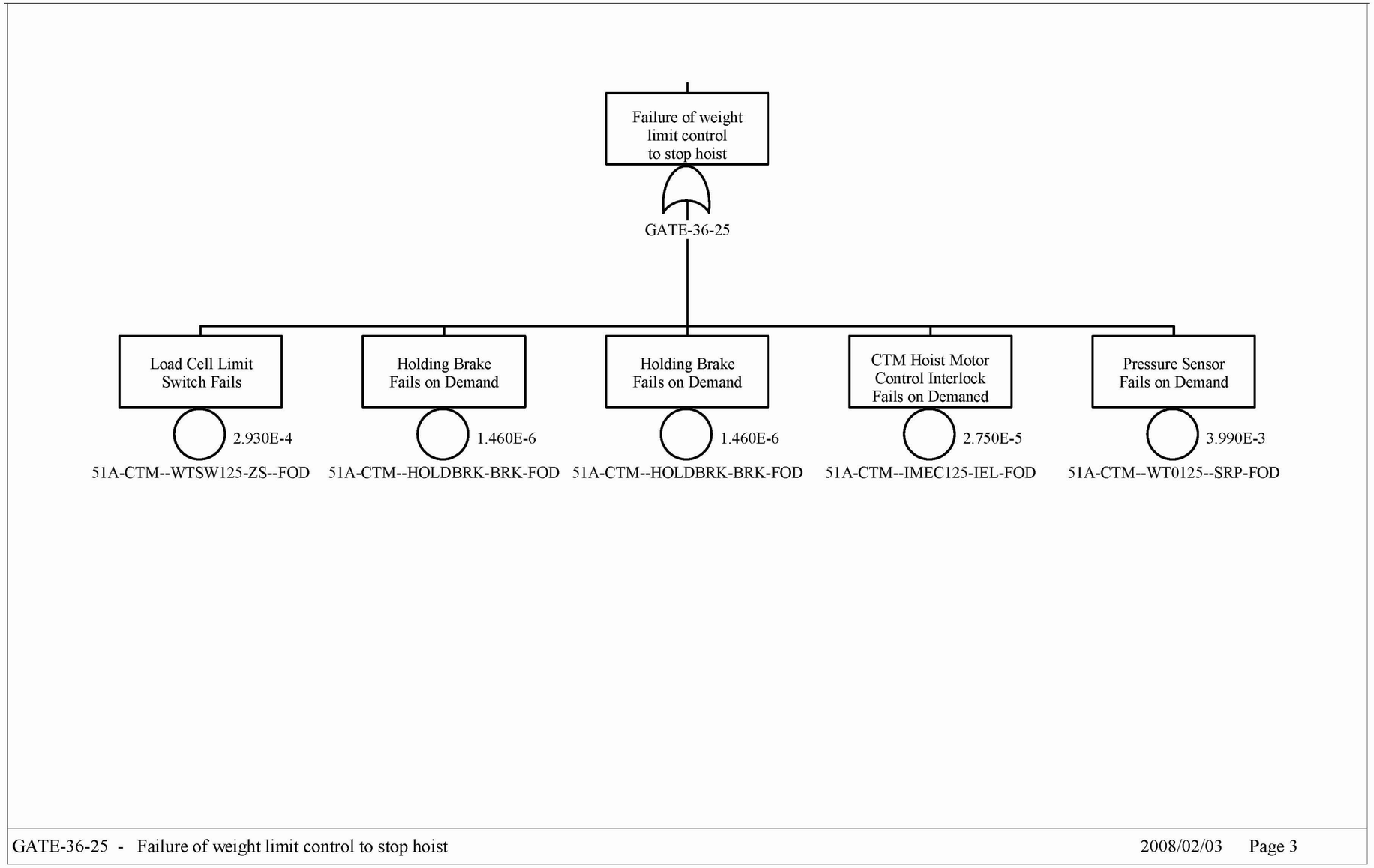
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-7. CTM Drop Fault Tree Sheet 5

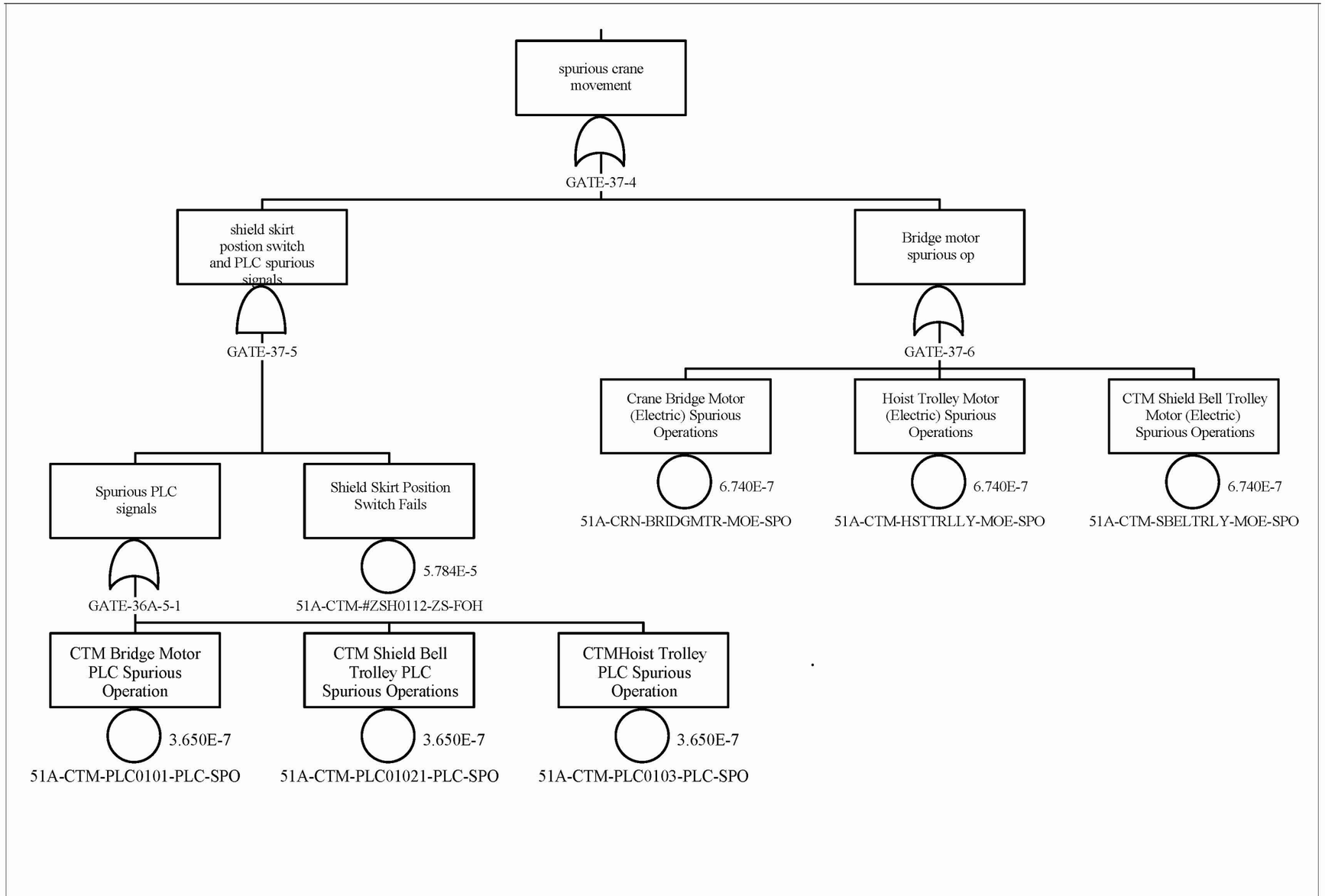
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-8. CTM Drop Fault Tree Sheet 6

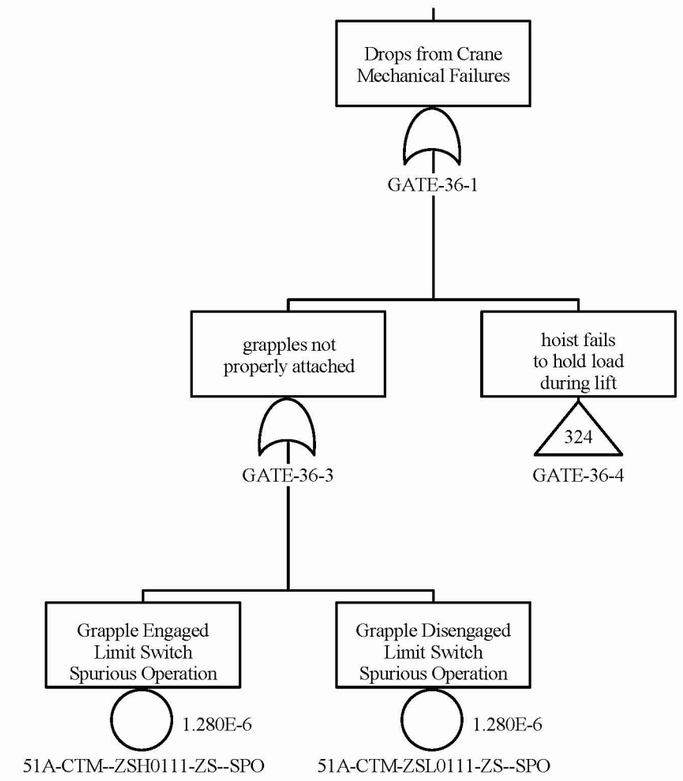
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-9. CTM Drop Fault Tree Sheet 7

INTENTIONALLY LEFT BLANK

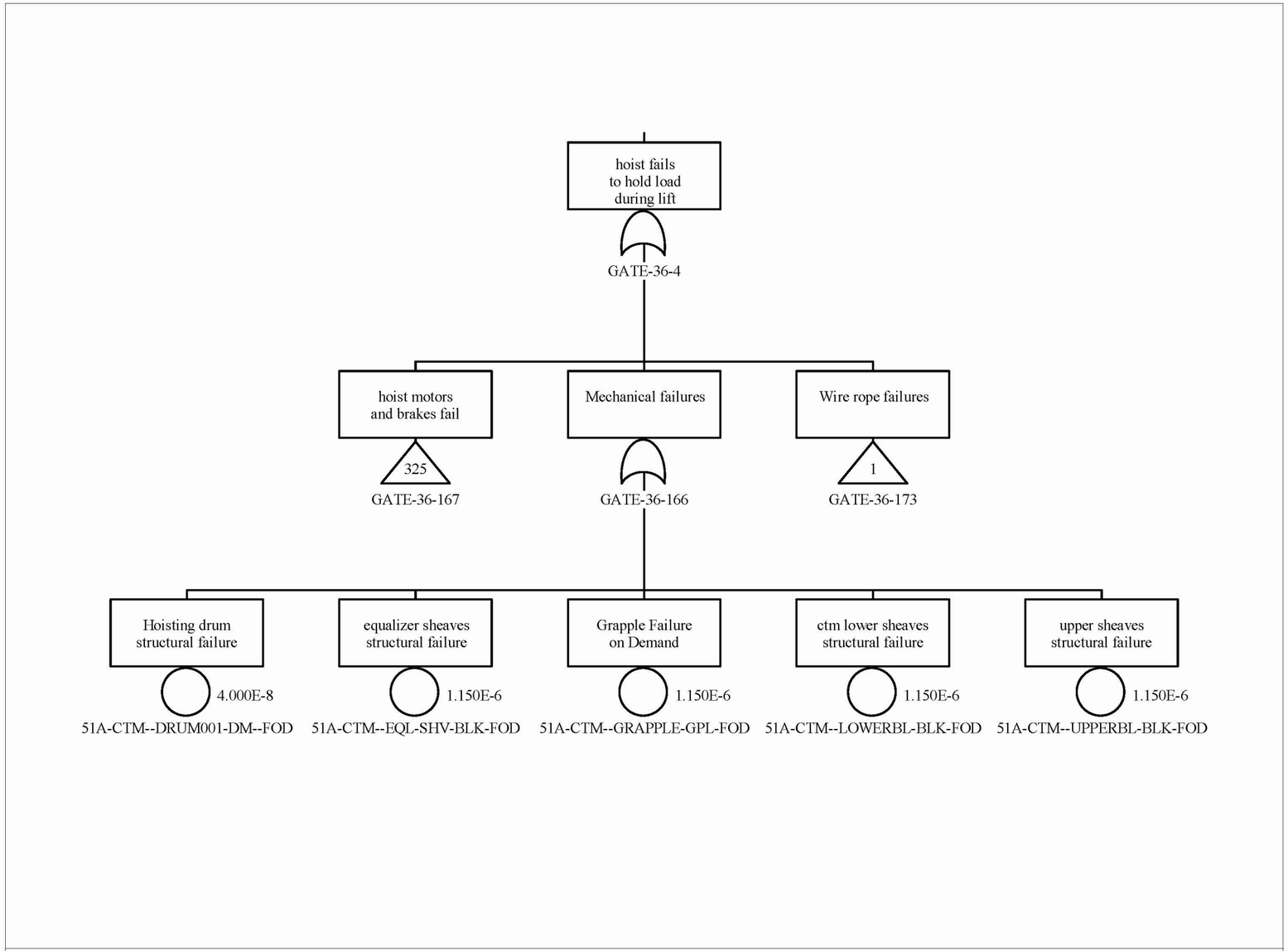


GATE-36-1 - Drops from Crane Mechanical Failures 2008/01/29 Page 103

Source: Original

Figure B4.4-10. CTM Drop Fault Tree Sheet 8

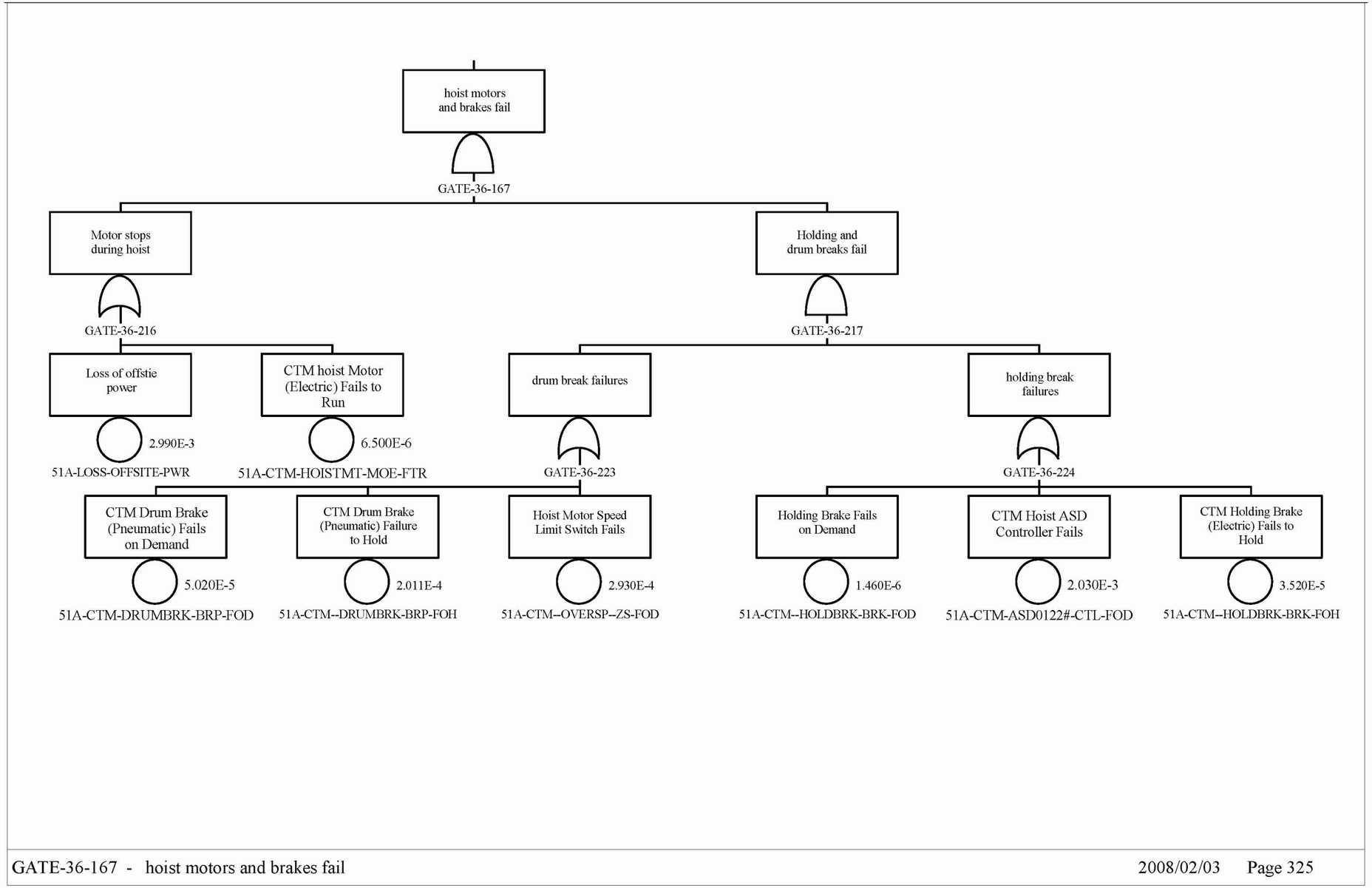
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-11. CTM Drop Fault Tree Sheet 9

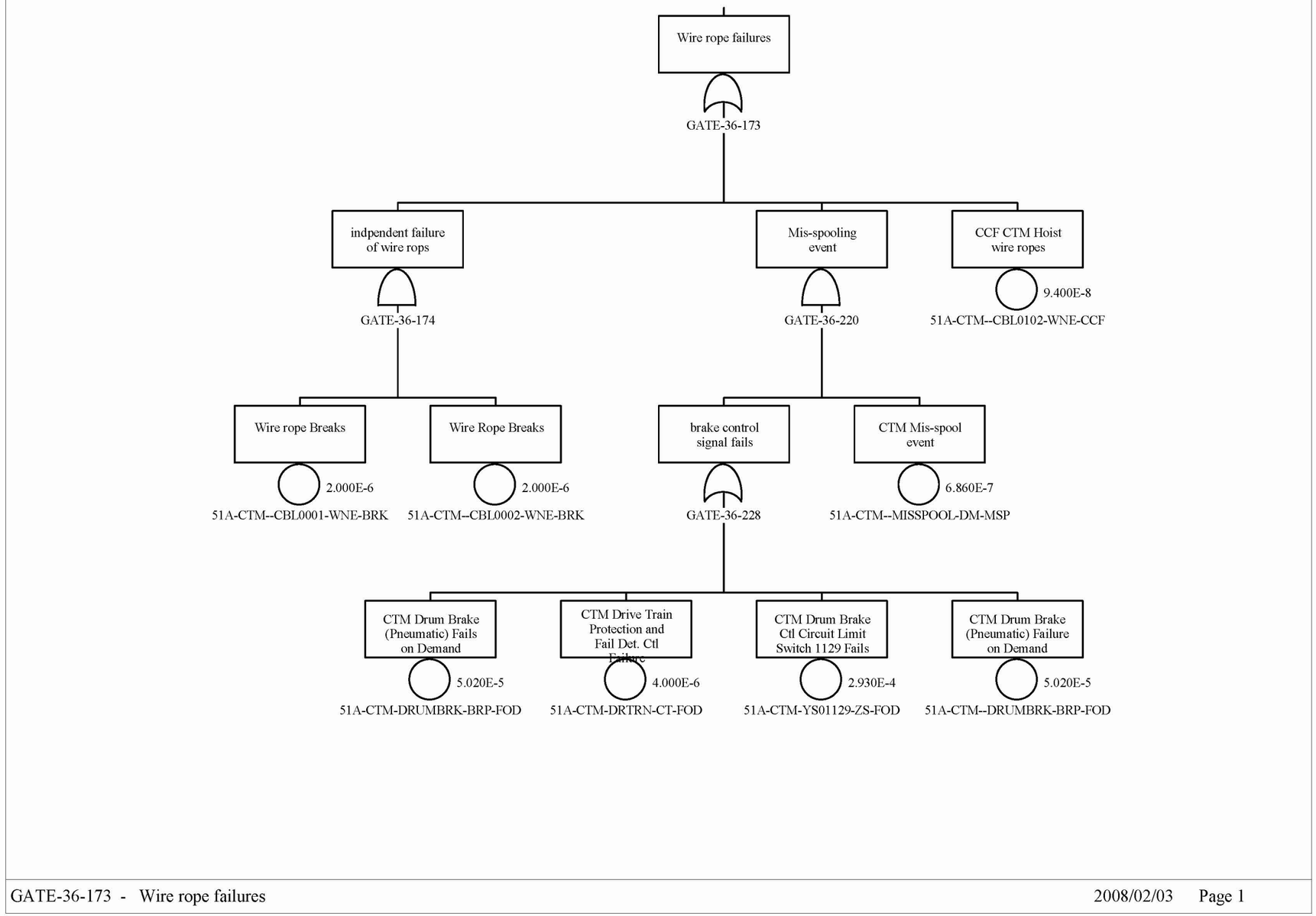
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-12. CTM Drop Fault Tree Sheet 10

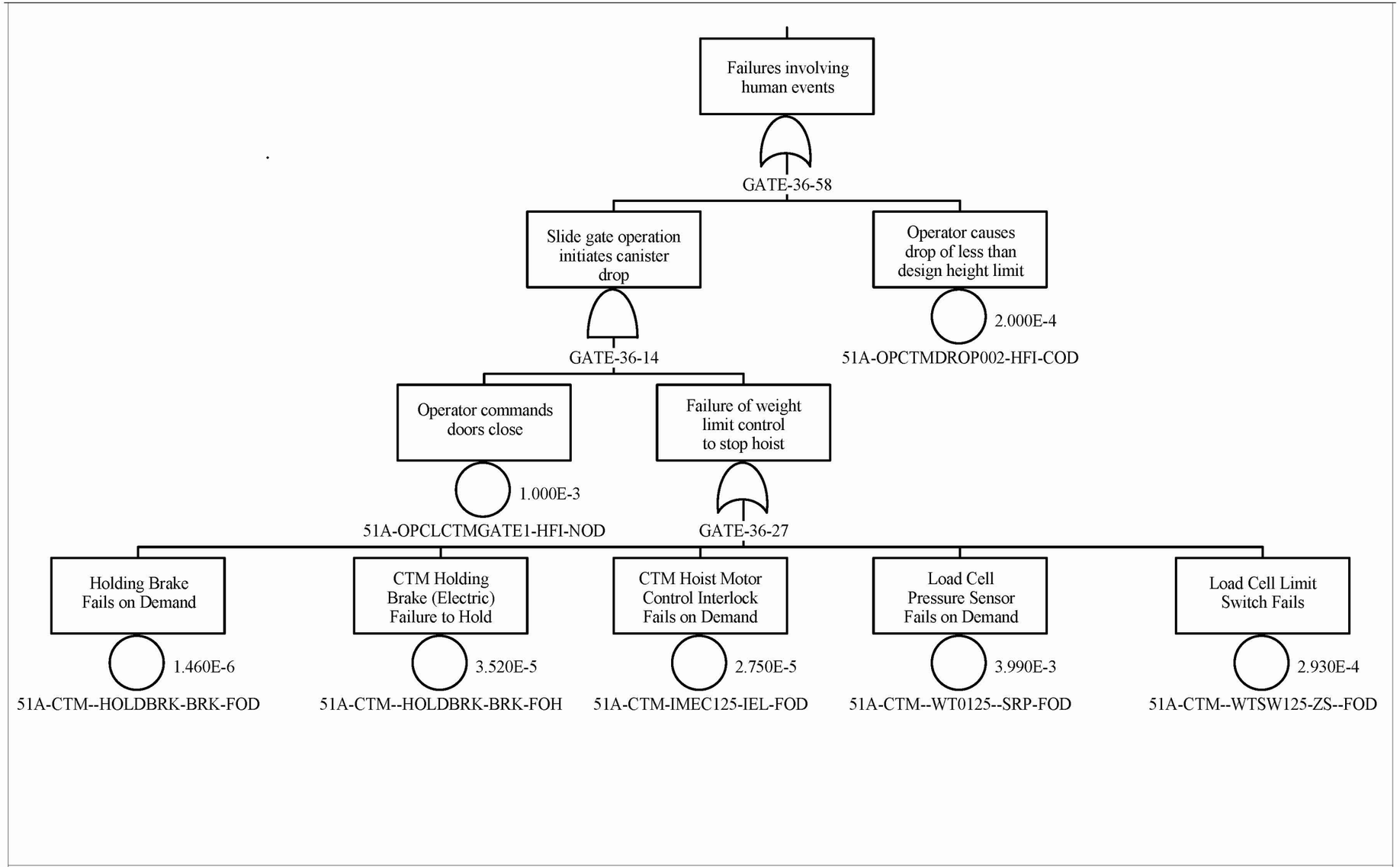
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-13. CTM Drop Fault Tree Sheet 11

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-14. CTM Drop Fault Tree Sheet 12

INTENTIONALLY LEFT BLANK

B4.4.2 Canister Drop from Above the Canister Design Limit Drop Height

B4.4.2.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of the canisters. These drops have been divided into two classes: drops from heights below the design basis drop height of the canister and drops from heights above the design basis drop height of the canister. This fault tree for canister drops addresses the second of these two scenarios.

B4.4.2.2 Success Criteria

Success criteria for the CTM is the prevention of a canister drop from above the canister design limit drop height from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.2.3 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.

B4.4.2.4 Fault Tree Model

The top event in this fault tree is "CTM High Drops from Two Blocking Events." This is defined as a drop of a canister from a height above the design limit height for the canister during transfer operations. (The two-block designation refers to the condition where the object being lifted is raised to the point where the upper and lower blocks of the crane come into contact. Attempts to continue to lift the load at this point place additional strains on the CTM components.) For this event to occur the canister must be lifted above the normal heights associated with a lift and the features designed to limit the drop height must fail. During normal operation, once the canister clears the optical sensor in the shield bell, the shield bell slide gate is closed. Provided the gate is closed at this time, the potential drop height for the canister never exceeds the canister design limit drop height. Faults considered in the evaluation of this top event include: component and human events (considered in conjunction with the interlocks intended to prevent the erroneous human action) that contribute to raising the canister too high. The model does not rely on CTM features that could allow the system to withstand a two-block event without dropping the load. That is, the model conservatively treats two-block events as drops.

B4.4.2.5 Basic Event Data

Table B4.4-4 contains a list of basic events used in the "Canister Drop from Above the Canister Design Limit Drop Height" fault tree. Included are the human failure events and the common-cause failure events identified in the following 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 canister 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).

Table B4.4-4. Basic Event Probabilities for the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})[a]	Miss. Time (hr)[a]
51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	C	1.377E-05	—	—	—
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 on Demand	1	2.930E-04	2.930E-04	—	—
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	—	—
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.350E-08	—	1.350E-08	1
51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	—	4.700E-06	1
51A-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block	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.

ASD = adjustable speed drive; Calc. = calculation; CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; FAIL. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

B4.4.2.5.1 Human Failure Events

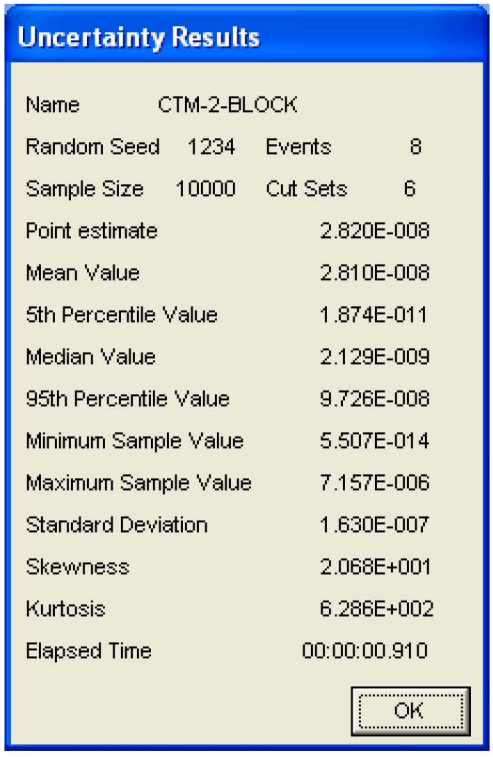
One basic event is associated with human error: 51A-OPCTMDRINT01-HFI-COD (Operator raises load too high - two block). This event models the combination of operator actions and interlock failures required to allow the operator to raise a load above design limits, and action that can lead to a two blocking failure.

B4.4.2.5.2 Common-Cause Failures

One common-cause event was considered in the evaluation of this fault tree. There are two upper limit switches intended to prevent raising a load too high. The common-cause failure of these switches was considered.

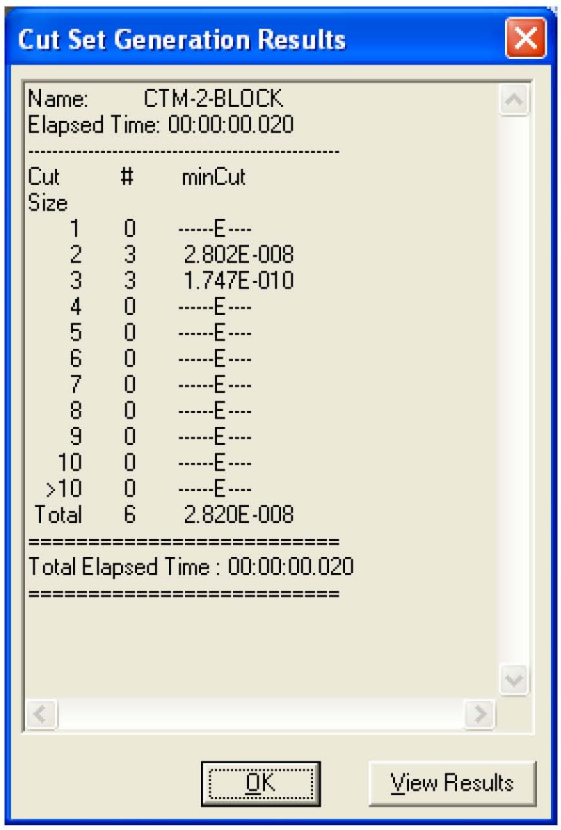
B4.4.2.6 Uncertainty and Cut Set Generation Results

Figure B4.4-15 contains the uncertainty results obtaining from running the fault tree for "Canister Drop from Above the Canister Design Limit Drop Height." Figure B4.4-16 provides the cut set generation results for "Canister Drop from Above the Canister Design Limit Drop Height" fault tree.



Source: Original

Figure B4.4-15. Uncertainty Results of the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree



Source: Original

Figure B4.4-16 Cut Set Generation Results for the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree

B4.4.2.7 Cut Sets

Table B4.4-5 contains the six cut sets for the "Canister Drop from Above the Canister Design Limit Drop Height" fault tree.

Table B4.4-5. Cut Sets for the Canister Drop from Above the Canister Design Limit Drop Height

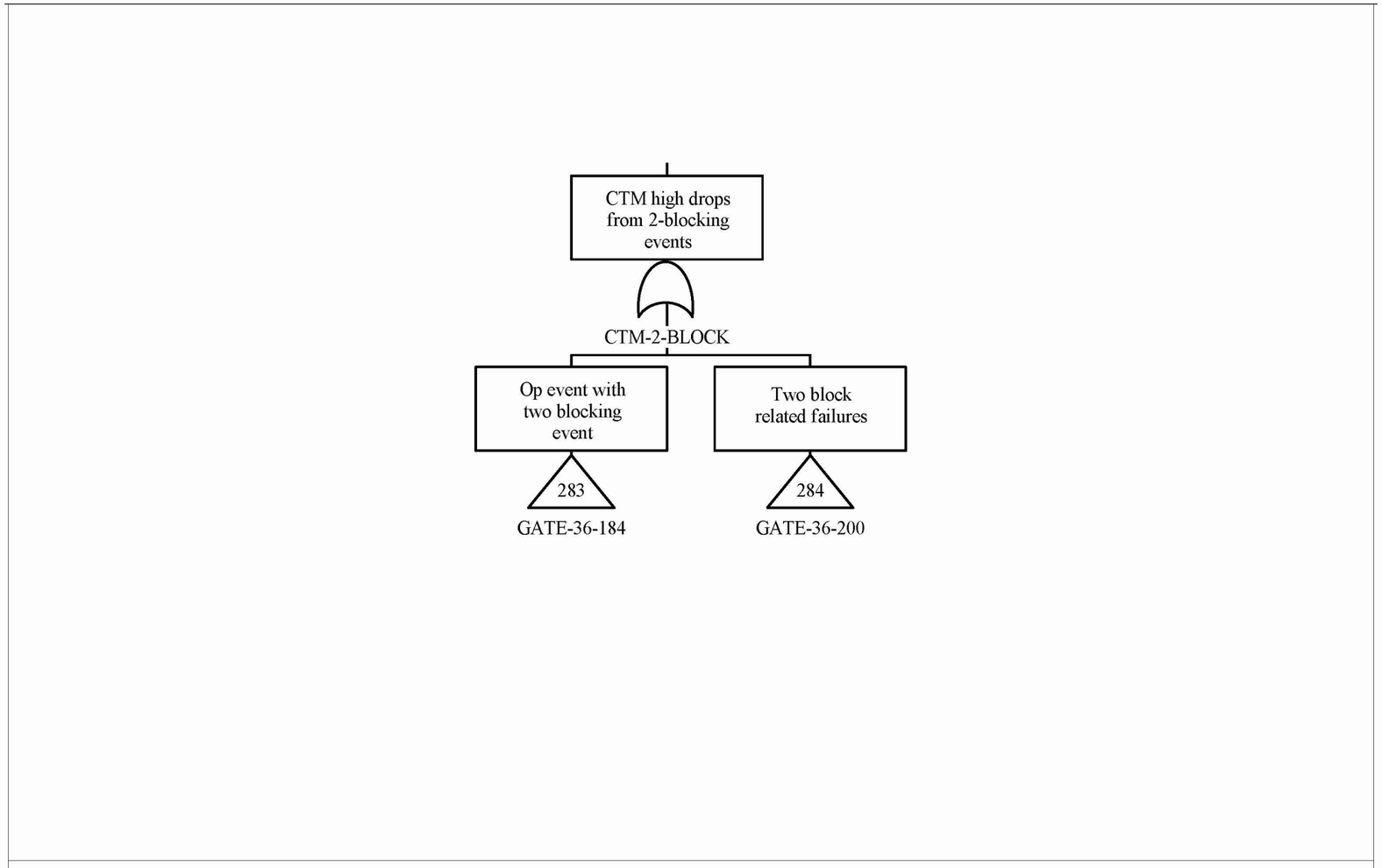
Fault Tree	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
CTM-2-BLOCK	99.15	2.796E-08	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.4E-05
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.0E-03
	0.62	1.743E-10	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.9E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.9E-04
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.0E-03
	0.23	6.472E-11	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.4E-05
			51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.7E-06
	0.00	4.035E-13	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.9E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.9E-04
			51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.7E-06
	0.00	1.859E-13	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.4E-05
			51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.4E-08
	0.00	1.159E-15	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.9E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.9E-04
			51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.4E-08

NOTE: ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine.

Source: Original

B4.4.2.8 Fault Trees

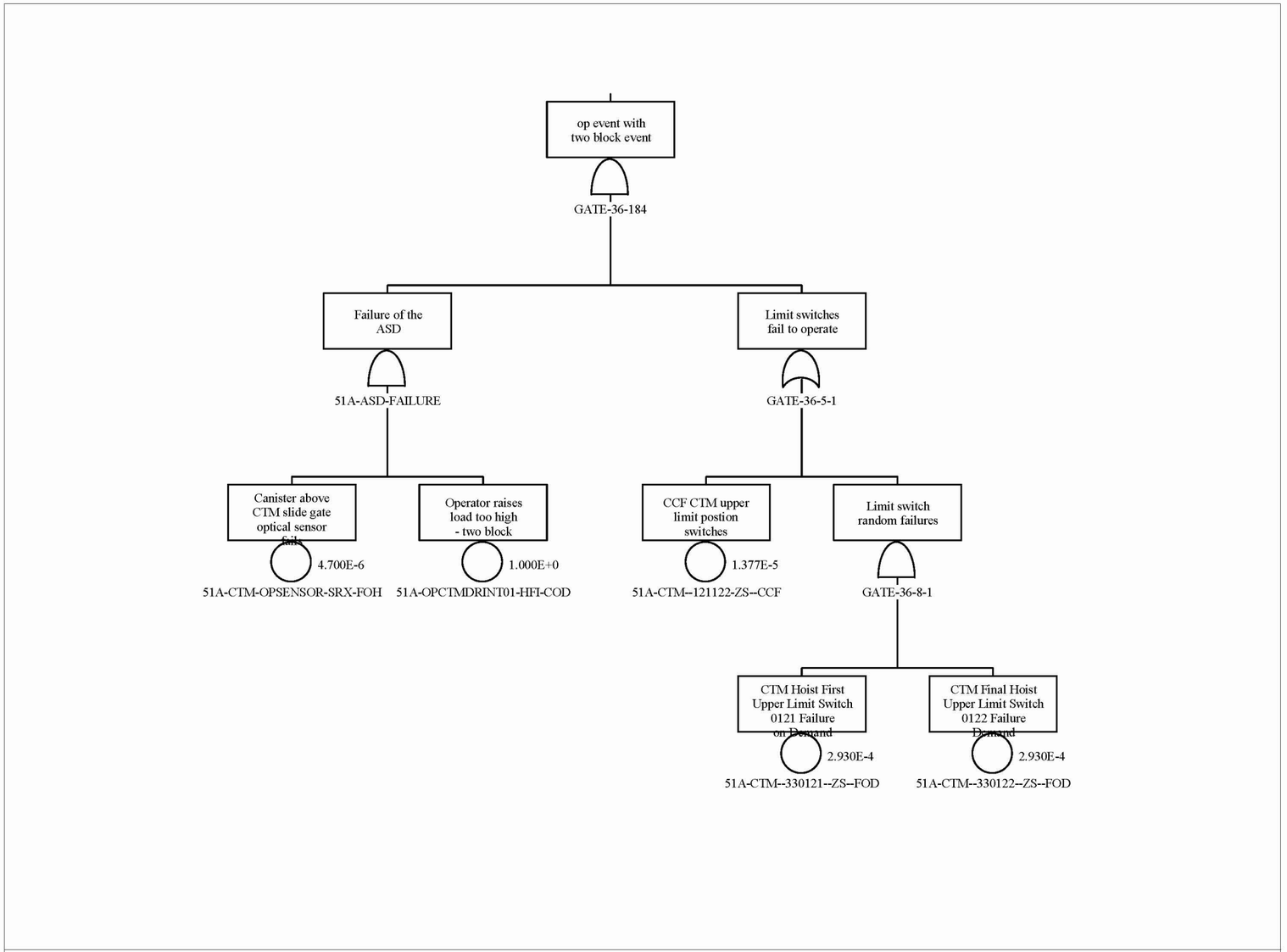
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-17. CTM High Drops from Two Blocking Event Sheet 1

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-18. CTM High Drops from Two Blocking Event Sheet 2

INTENTIONALLY LEFT BLANK