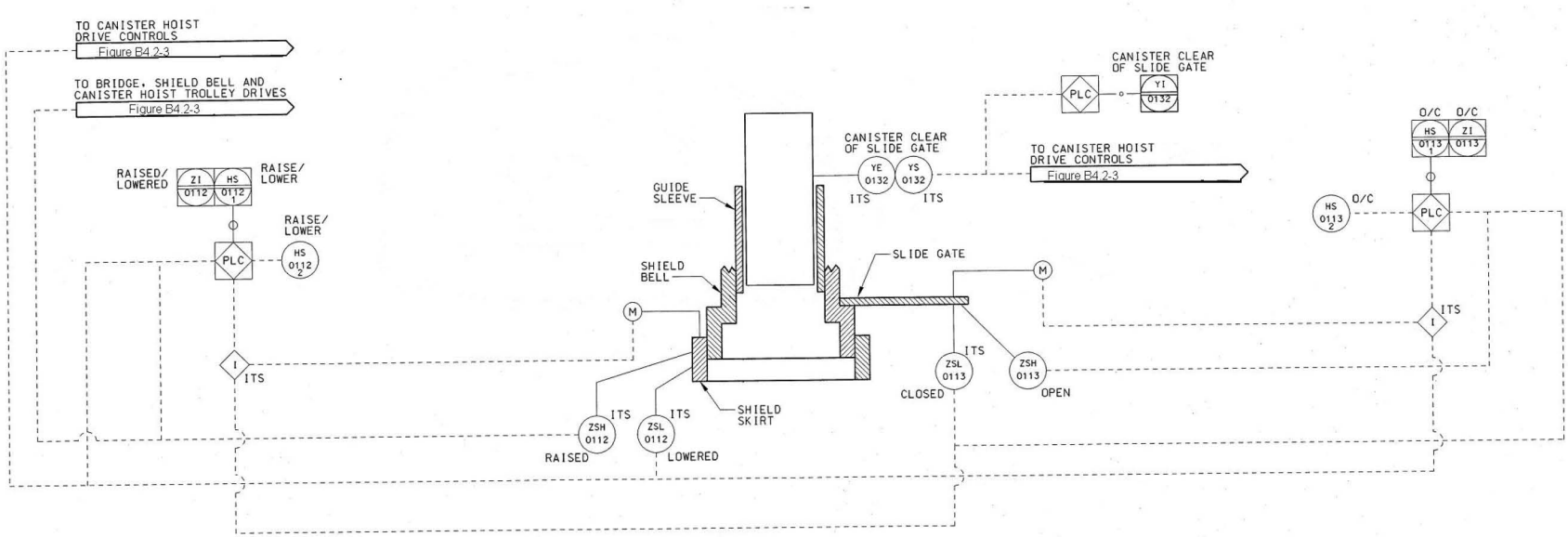
INTENTIONALLY LEFT BLANK

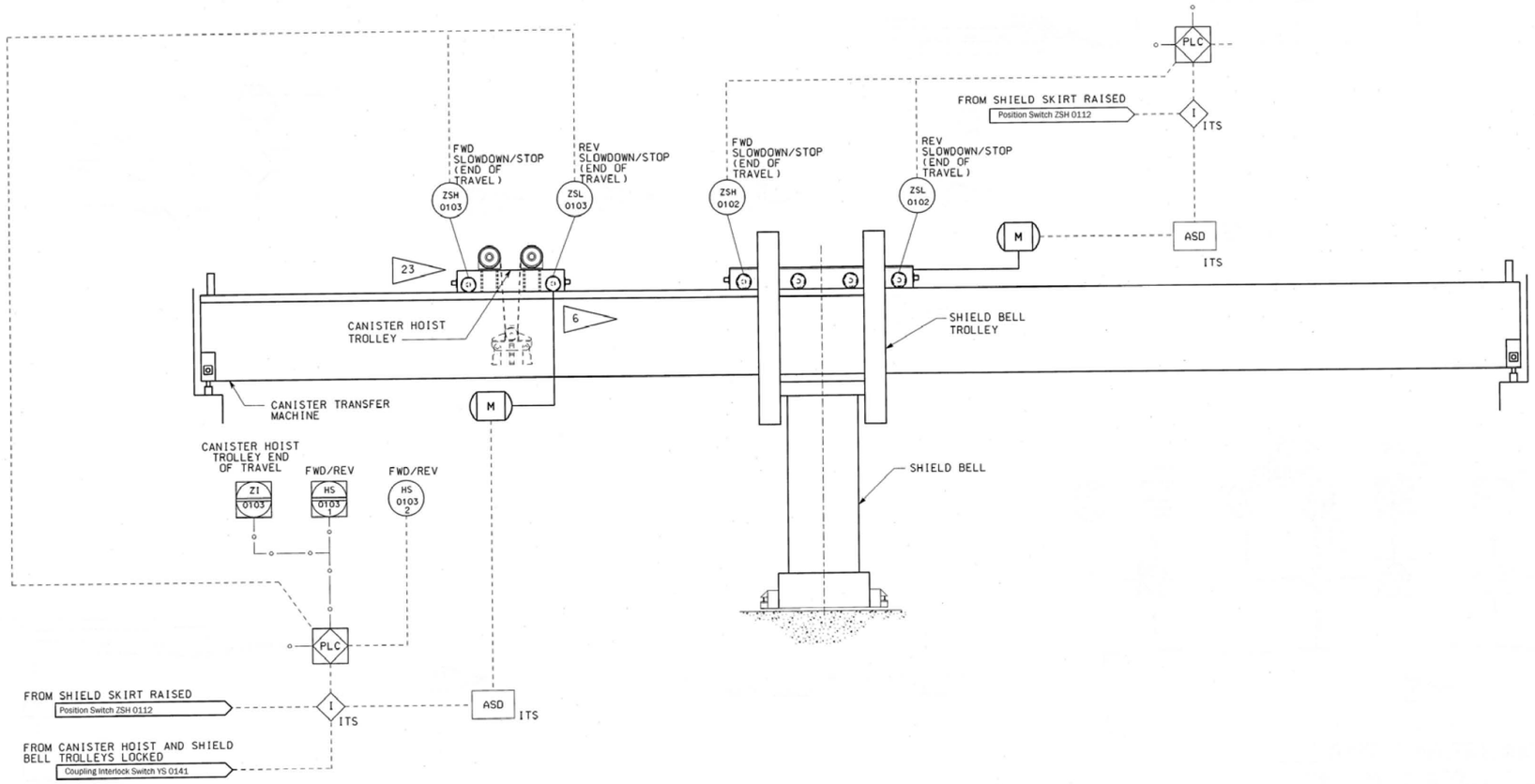


NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: Ref. B4.1.6

Figure B4.2-4. Shield Skirt and Slide Gate Instrumentation

INTENTIONALLY LEFT BLANK

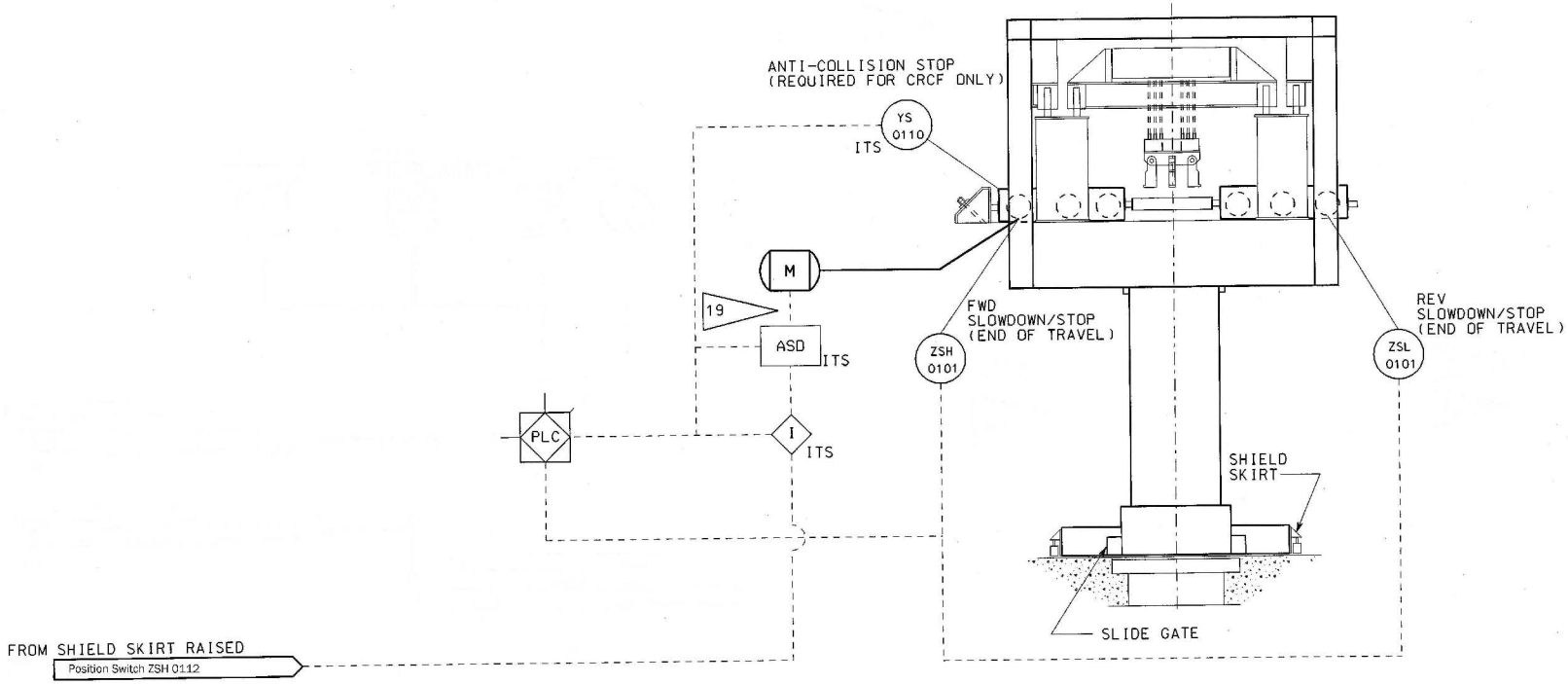


NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: Ref. B4.1.3

Figure B4.2-5. Trolley Instrumentation

INTENTIONALLY LEFT BLANK



Source: Ref. B4.1.3

Figure B4.2-6. Bridge Instrumentation

INTENTIONALLY LEFT BLANK

B4.2.2 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 a 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.

B4.2.3 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.

B4.2.4 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 will not allow the grapple to disengage when a load is suspended from the canister grapple.

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).

B4.2.5 ITS CTM Nominal Operations

The WHF canister transfer system handles DPCs and transportation, aging, and disposal (TAD) canisters. A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to an aging overpack. For this operation a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. The cask lid is in place but unbolted. Similarly, an empty aging overpack is positioned under the adjacent transfer port.

The CTM is moved to a position over the center of 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. 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 transfer room. 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 aging overpack 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 aging overpack and the grapple is disengaged from the canister.

The CTM canister grapple is used for handling large diameter canisters such as TAD canisters and DPCs. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the transfer room floor. The CTM hoist is lowered through the shield bell until the CTM grapple is accessible in the room below for canister grapple attachment.

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

B4.2.6 ITS CTM Off Nominal 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.

B4.2.7 ITS CTM Testing and Maintenance

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

B4.2.8 Testing and Maintenance

Requirements

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

Feature

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

B4.2.9 Fault Trees

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 1 hour. Most lifts/transfers will require less than one hour. When a transfer consists of several separate activities (e.g., auxiliary equipment movements, lifts, transfers, etc.) each of these activities require less than an hour, but all have been assigned a one-hour mission time.

Features

Common-cause failures have been included for four events. Three 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), the grapple engage/disengage position indication sensors, 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 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 dependence
3. Spatial dependence
4. Human dependence
5. Failures based on external events.

Table B4.3-1. Dependencies and Interactions Analysis

Structures, Systems, and 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. 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 room ports to the loading/unloading areas that can occur before the bell slide gate is closed).

2. The CTM drops a canister from a height above the design basis height for canister damage.

3. The CTM drops an object onto a 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 Drops 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

Success criteria for the CTM is the prevention of a canister drop from any cause, during the lift, lateral movement, and lowering 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, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

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

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

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

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

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

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 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 are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

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

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

B4.4.1.4 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 CTM, 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 Machine Room 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 CTM. The CTM has several trolleys that govern lateral movements; one controls the CTM bridge movement, 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 interlocked during canister transfer operations). Spurious actuation of a trolley motor after the grapple has been attached to the canister but before the canister is raised above the Canister Transfer Area 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 CTM, 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 HFE is a screening value of 0.001 (i.e., it is a conservative estimate based upon predetermined characteristics of the human failure event (HFE) (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 CTM fault trees. Included are the HFEs and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

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 which is considered to be the duration of a shift (i.e., eight hours). In another example, brakes are analyzed over a mission time of twenty-four hours. This duration is deemed 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 Probability for the CTM Canister Drop from Below Canister Drop Height Limit Fault Tree

Name	Description	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	1	2.930E-04	2.930E-04	—	—
050-CTM--CBL0001-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	—	—
050-CTM--CBL0002-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	—	—
050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	C	9.400E-08	—	—	—
050-CTM--DRTRN-CT--FOD	Controller Failure	1	4.000E-06	4.000E-06	—	—
050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	1	4.000E-08	4.000E-08	—	—
050-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	—	—
050-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure	3	2.011E-04	—	8.380E-06	2.400E+01
050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1	1.150E-06	1.150E-06	—	—
050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1	1.150E-06	1.150E-06	—	—
050-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	3	6.500E-06	—	6.500E-06	1.000E+00
050-CTM--HOLDBRK-BRK-FOD	CTM Holding Brake Failure on Demand	1	1.460E-06	1.460E-06	—	1.000E+00
050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3	3.520E-05	—	4.400E-06	8.000E+00
050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	1	2.750E-05	2.750E-05	—	—
050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1	1.150E-06	1.150E-06	—	—
050-CTM--OVERSP--ZS--FOD	CTM Hoist motor speed Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	—	—
050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM--PORTGT1-PLC-SPO	Port Gage 1 PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM--PORTGT2-PLC-SPO	Port Gage 2 PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM--SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM--SLIDGT2-IEL-FOD	CTM Slide Gate Interlock Failure	1	2.750E-05	2.750E-05	—	—
050-CTM--TROLLY-MOE-SPO	Motor (Electric) Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1	1.150E-06	1.150E-06	—	—

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

Name	Description	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	—	—
050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	—	—
050-CTM--YS01129-ZS--FOD	CTM Drum Brake Control Circuit Switch Fail	1	2.930E-04	2.930E-04	—	—
050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	—	1.280E-06	1.000E+00
050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	—	—
050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM-MISSPOOL--DM-MSP	CTM mis-spool event	3	6.860E-07	—	6.860E-07	1.000E+00
050-CTM-PLC0101--PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM-PLC0102--PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM-PLC0103--PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	—	3.650E-07	1.000E+00
050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	3	6.740E-07	—	6.740E-07	1.000E+00
050-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	—	—
050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	—	1.280E-06	1.000E+00
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1	1.000E-03	1.000E-03	—	—
050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	1	5.000E-07	5.000E-07	—	—

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.

ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller.

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 operator actions and for 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
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close
050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit

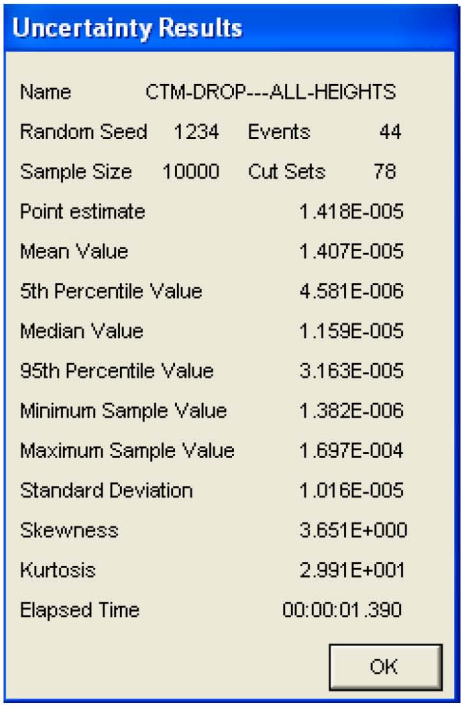
Source: Original

B4.4.1.5.2 Common-Cause Failures

One CCF event is considered in the evaluation of this top event. It is the common-cause failure of the hoist cables. An alpha factor of 0.047 was used to determine the CCF value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

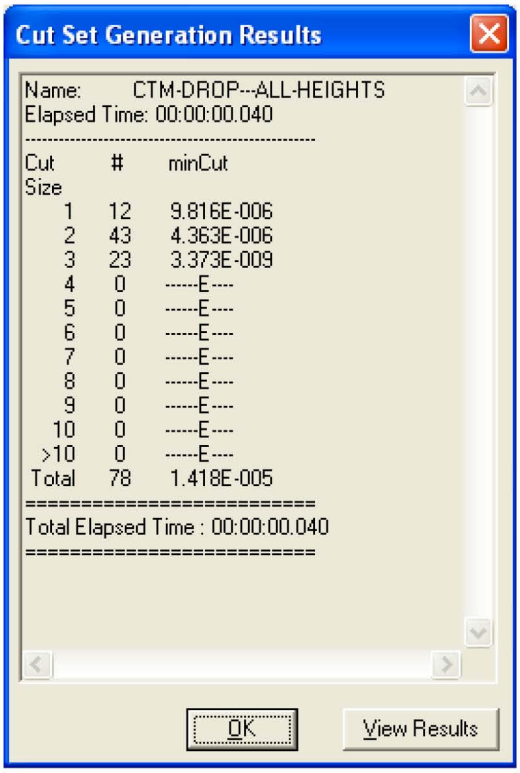
B4.4.1.6 Uncertainty and Cut Set Generation

Figure B4.4-1 contains the uncertainty results obtaining from running the fault trees for the CTM canister drop using a cutoff at 1E-15. Figure B4.4-2 provides the cut set generation results for the CTM canister drop fault tree.



Source: Original

Figure B4.4-1. Uncertainty Results of the “CTM Canister Drop” Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the "CTM Canister Drop" Fault Tree

B4.4.1.7 Cut Sets

Table B4.4-3 contains the top 20 cut sets for the "CTM Canister Drop" Fault Tree.

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

% Total	%Cut Set	Probability /Frequency	Basic Event	Description	Event Probability
28.13	28.13	3.990E-06	050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
37.16	9.03	1.280E-06	050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
46.19	9.03	1.280E-06	050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
54.30	8.11	1.150E-06	050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1.150E-06
62.41	8.11	1.150E-06	050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1.150E-06
70.52	8.11	1.150E-06	050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1.150E-06
78.63	8.11	1.150E-06	050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1.150E-06

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

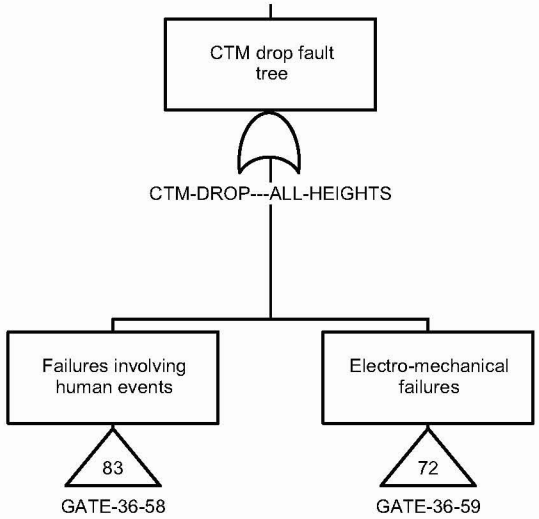
% Total	%Cut Set	Probability /Frequency	Basic Event	Description	Event Probability
83.38	4.75	6.740E-07	050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	6.740E-07
88.13	4.75	6.740E-07	050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	6.740E-07
92.88	4.75	6.740E-07	050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	6.740E-07
96.41	3.53	5.000E-07	050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	5.000E-07
98.48	2.07	2.930E-07	050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	2.930E-04
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.14	0.66	9.400E-08	050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.400E-08
99.42	0.28	4.000E-08	050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	4.000E-08
99.67	0.25	3.520E-08	050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3.520E-05
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.86	0.19	2.750E-08	050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	2.750E-05
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.88	0.02	2.689E-09	050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.90	0.02	2.689E-09	050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.92	0.02	2.689E-09	050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.94	0.02	2.689E-09	050-CTM--TROLLY-MOE-SPO	Motor (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03

NOTE: CCF = common-cause failure; CTM = canister transfer machine.

Source: Original

B4.4.1.8 Fault Trees

INTENTIONALLY LEFT BLANK

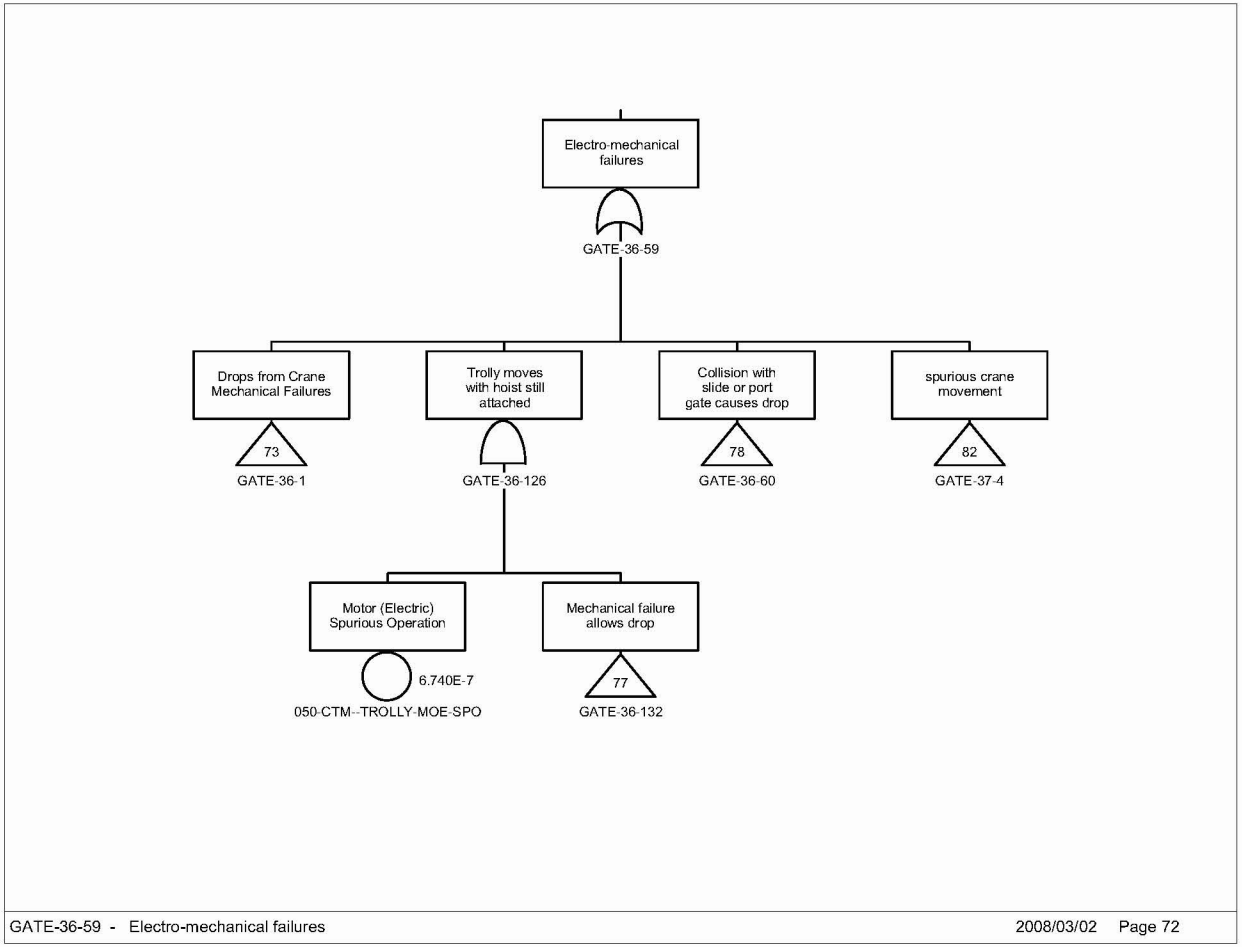


CTM-DROP---ALL-HEIGHTS - CTM Drop fault tree 2008/03/02 Page 71

Source: Original

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

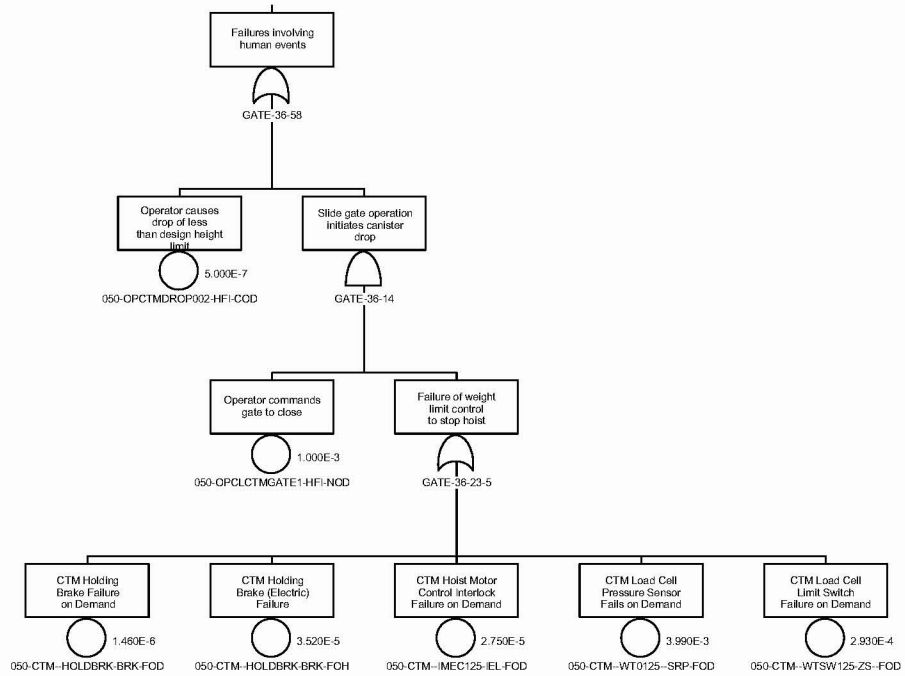
INTENTIONALLY LEFT BLANK



Source: Original

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

INTENTIONALLY LEFT BLANK

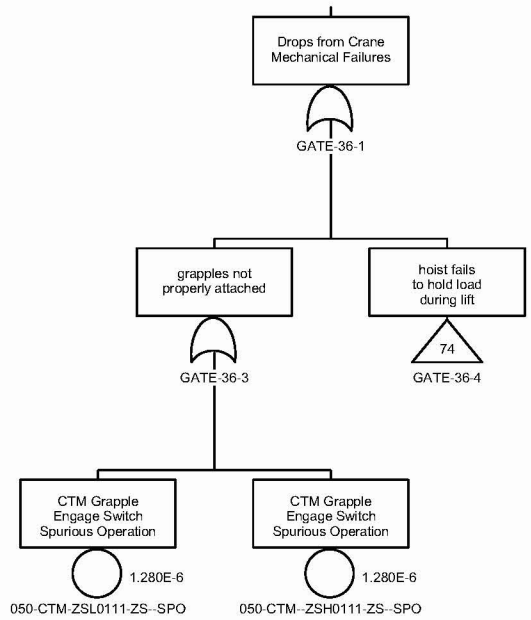


GATE-36-58 - Failures involving human events 2008/03/02 Page 83

Source: Original

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

INTENTIONALLY LEFT BLANK

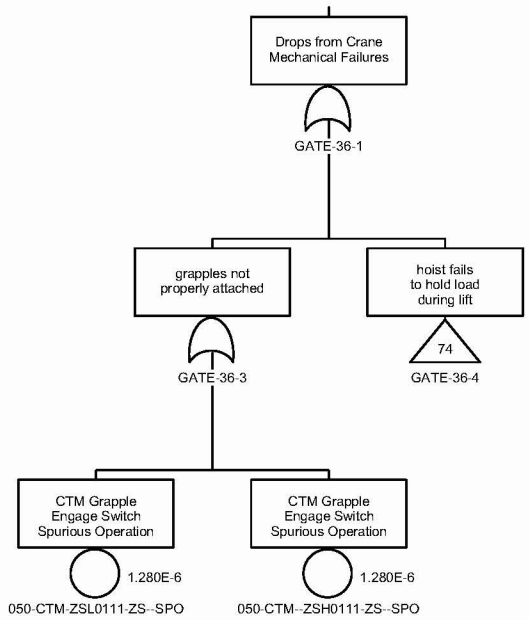


GATE-36-1 - Drops from Crane Mechanical Failures 2008/03/02 Page 73

Source: Original

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

INTENTIONALLY LEFT BLANK

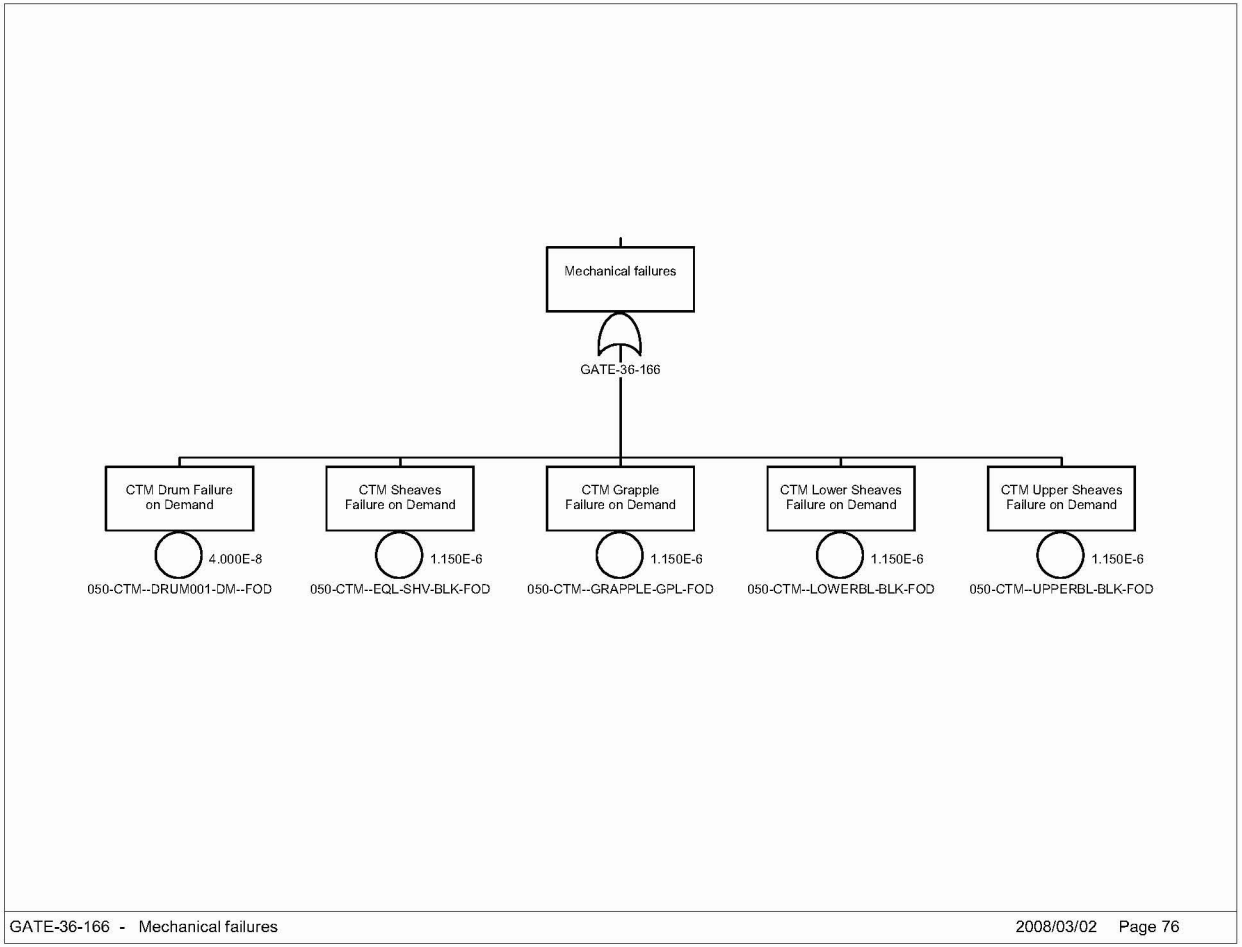


GATE-36-1 - Drops from Crane Mechanical Failures 2008/03/02 Page 73

Source: Original

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

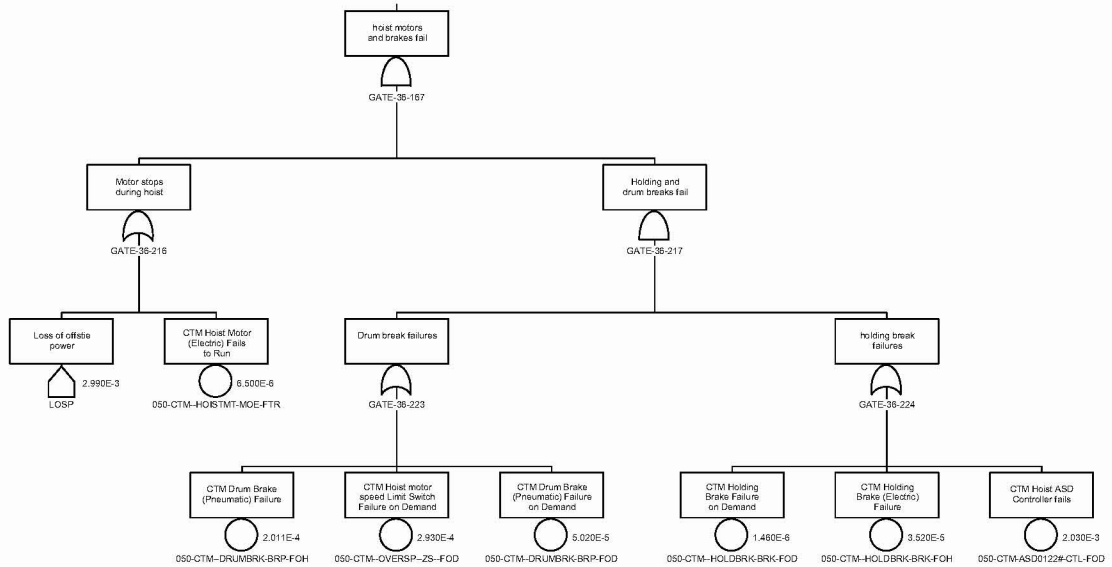
INTENTIONALLY LEFT BLANK



Source: Original

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

INTENTIONALLY LEFT BLANK

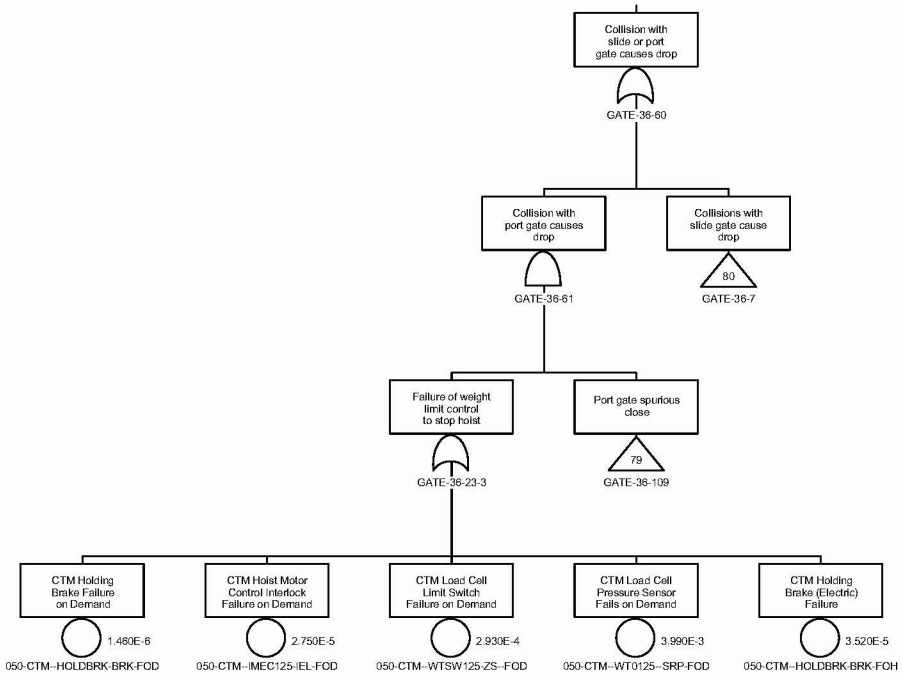


GATE-36-167 - Hoist motors and brakes fail 2008/03/02 Page 75

Source: Original

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

INTENTIONALLY LEFT BLANK

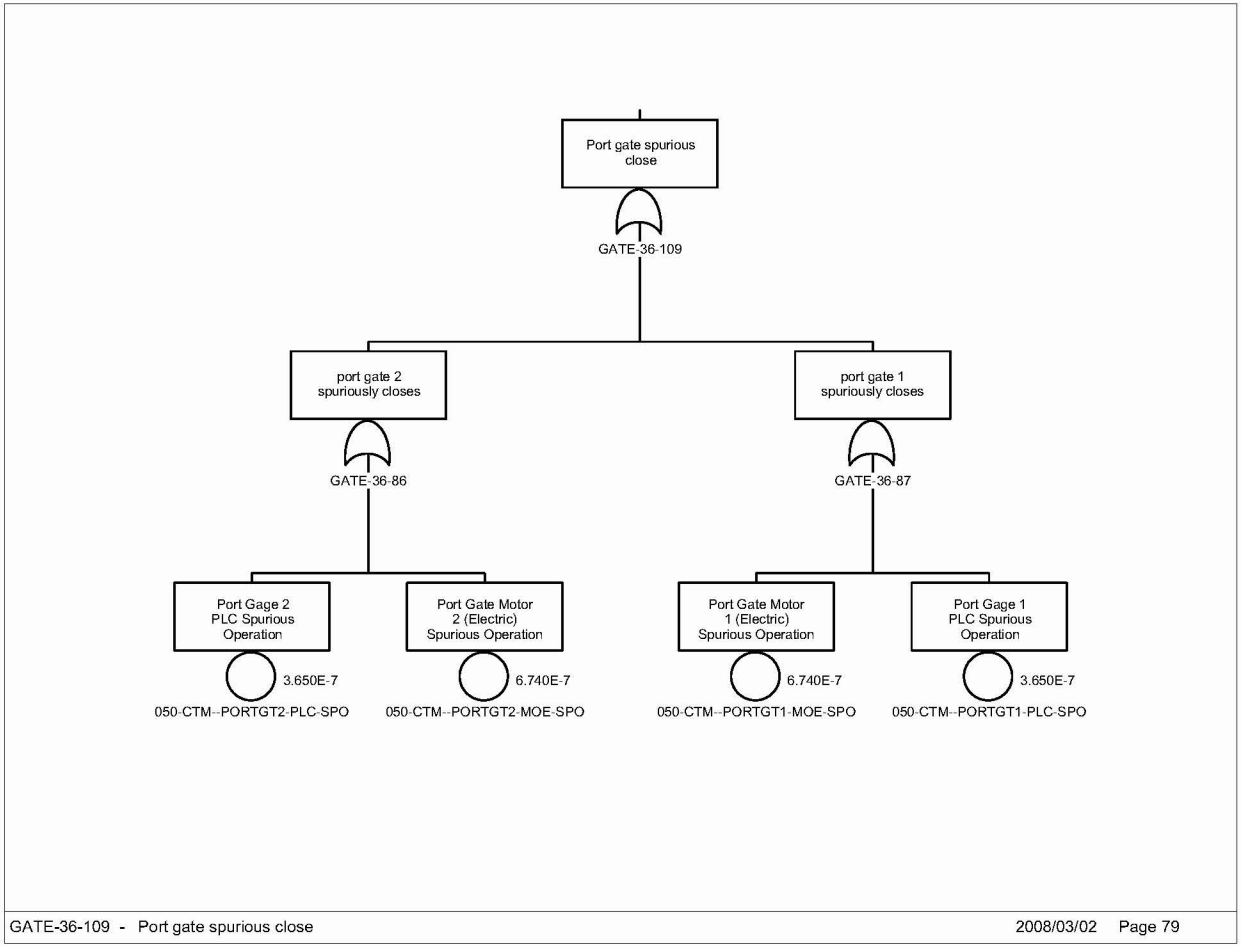


GATE-36-60 - Collision with slide or port gate causes drop 2008/03/02 Page 78

Source: Original

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

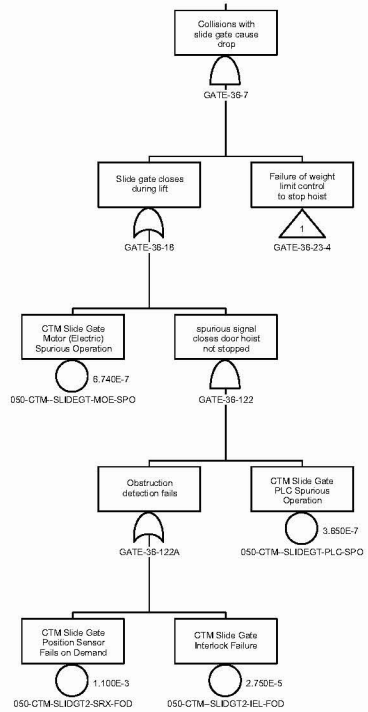
INTENTIONALLY LEFT BLANK



Source: Original

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

INTENTIONALLY LEFT BLANK

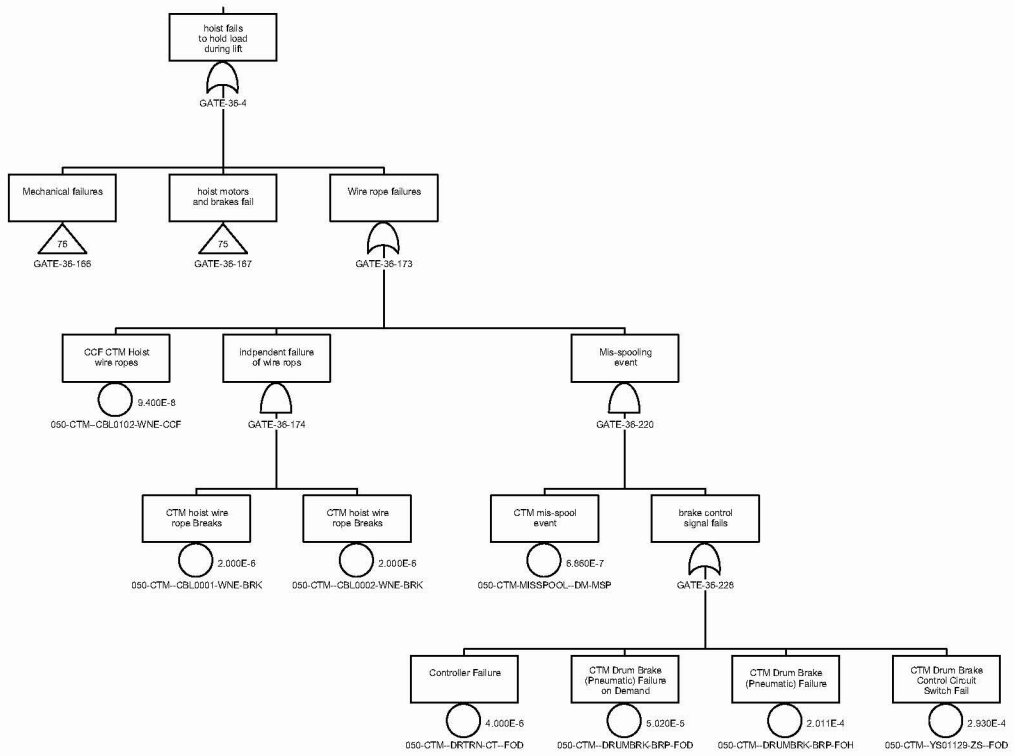


GATE-36-7 - Collisions with slide gate cause drop 2008/03/02 Page 80

Source: Original

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

INTENTIONALLY LEFT BLANK

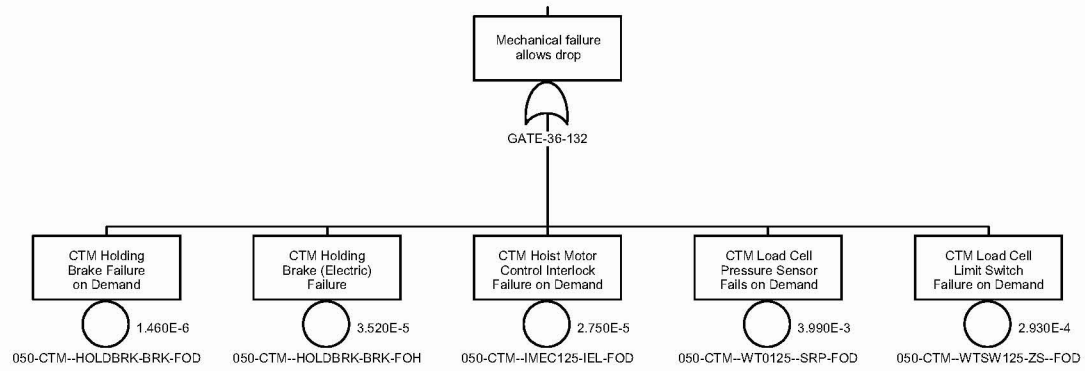


GATE-36-4 - hoist fails to hold load during lift 2008/08/14 Page 74

Source: Original

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

INTENTIONALLY LEFT BLANK

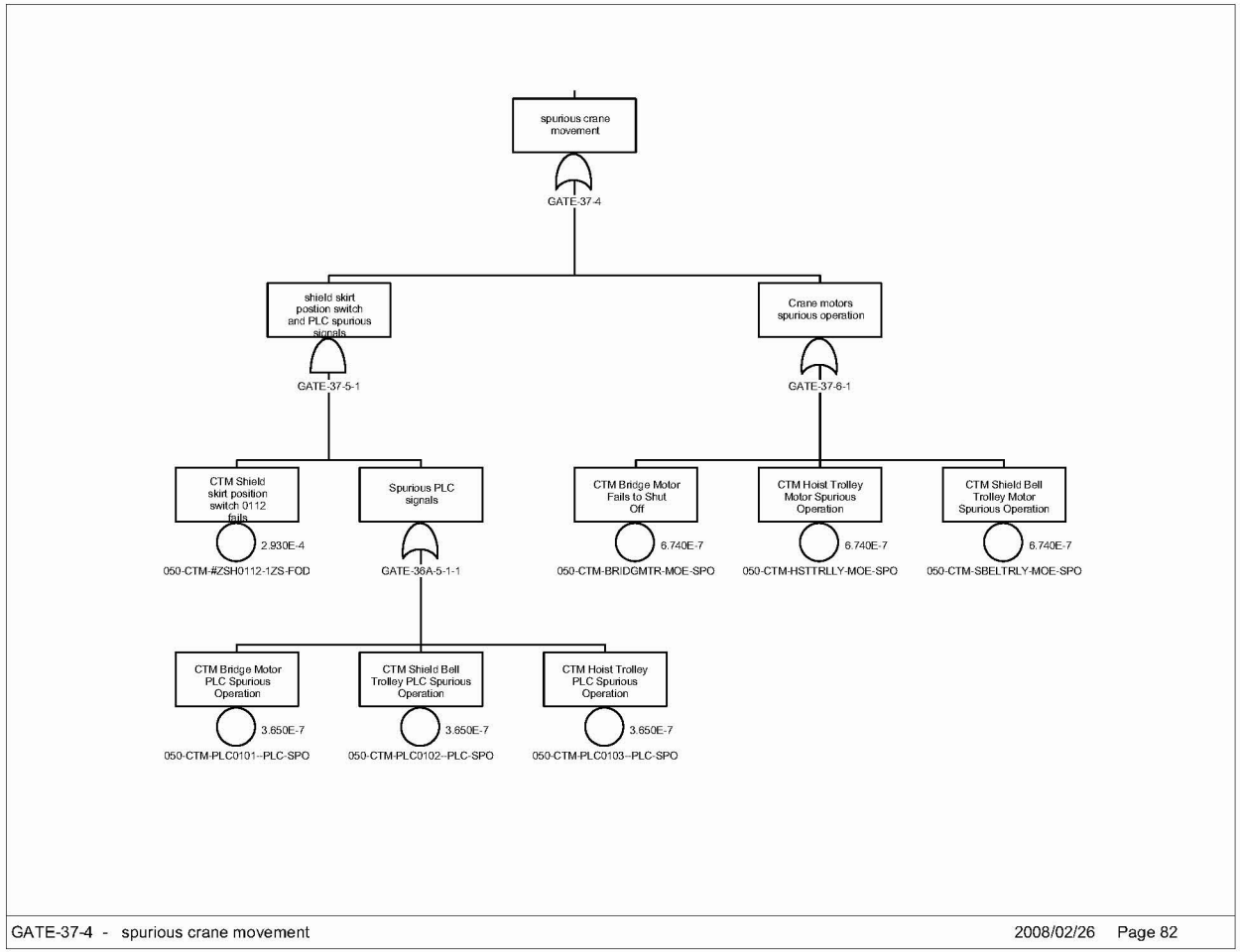


GATE-36-132 - Interlock failures allow movement I 2008/03/02 Page 77

Source: Original

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

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-15. CTM Drop Fault Tree Sheet 13

INTENTIONALLY LEFT BLANK

B4.4.2 Canister Drops 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 simply 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, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

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

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

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

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

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

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

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

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

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

B4.4.2.4 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 places 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 credit CTM features that could mitigate the consequences of a two-block event. It was assumed that all two-block events result in a drop.

B4.4.2.5 Basic Event Data

Table B4.4-4 contains a list of basic events used in the CTM High Drops from Two Blocking Events fault tree. Included are the HFEs and the CCF events identified in the following two

sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The 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).