

INTENTIONALLY LEFT BLANK

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
060-OpCTMdrop001-HFI-COD	<i>Operator Drops Object onto Canister during CTM Operations:</i> Some variations of CTM activities require heavy objects to be moved over the canister; some TC and all AO lids are removed, and WP inner lids are also installed. It is possible that these objects can be dropped onto the canister while being lifted with the CTM.	9	2E-03	<p>In this step, the operator can potentially drop the cask lid, waste package inner lid, or waste package spread ring onto the canister. There are several ways for this failure to occur, including the following:</p> <ul style="list-style-type: none"> Operator fails to fully engage or disengage the grapple before lifting the hoist (i.e., resulting in partial engagement of the grapple). There is an indicator and camera view by which the operator is required to verify engagement. There is also an interlock that does not allow the hoist to move unless the grapple is fully engaged or fully disengaged. This interlock does not have a bypass. Operator fails to properly connect the grapple to the CTM when switching grapples. Operator lifts the lid with the CTT significantly misaligned with the cask port. This misalignment can cause part of the lid to be caught under the second floor. If the CTM keeps pulling, the cable can snap and the lid can drop. There are several electromechanical safeguards preventing this, including load cell interlock, motor temperature interlock, and the cable design. (A similar failure can occur if the CTM is moved with an object below the floor; however, this event is treated separately in <i>060-OpCTMImpact1-HFI-COD</i>.) Operator lifts the object too high. The only object that is lifted over a canister is the lid. The bell is flared at the bottom to accommodate the cask lid; if the operator puts the ASD in maintenance mode or sets it in canister mode, then the lid can be lifted until it hits the inside of the bell. If the CTM operator continues trying to lift, the cable can snap, causing the lid to drop onto the canister. There are several electromechanical safeguards preventing this, including load cell interlock, motor temperature interlock, and the cable design. <p>The preliminary value was chosen based on the determination that this failure is "highly unlikely" (0.001) and was adjusted because there are several ways for a drop to occur and, because the operation is performed remotely, this is a somewhat complex process (×2) as opposed to an extremely complex process (which would be ×3). This HFE was assessed to be less likely than a cask impact or an RC/TT collision, and the preliminary value reflects this.</p>
060-OpCTMdrop002-HFI-COD	<i>Operator Drops Canister during CTM Operations:</i> All variations of CTM activities require the canister to be lifted and transferred to the staging area, to a WP, or to an AO. During this lift, the operator can drop the canister (e.g., by improper grapple engagement).	9	2E-03	Moving a canister with the CTM is very similar to moving an object with the CTM during cask transfer (060-OpCTMdrop001-HFI-COD) and has the same failure modes. The only difference between moving a canister and moving an object (specifically, the lid) is that a canister drop due to lifting too high results in a high drop (e.g., a two-block) as opposed to a design-limit drop, which is analyzed separately. Therefore, it was considered conservative to assign the same preliminary value to this HFE.
060-OpCTMDrInt01-HFI-COD	<i>Operator Lifts Object or Canister too High with CTM:</i> It is possible that, while lifting objects such as the canister or WP inner lid, the operator can cause a two-block by lifting the object too high.	9	1.0	When lifting the canister, the operator can lift it too high, resulting in a two-block event and drop of the canister. In order to accomplish this failure, the interlocks (e.g., optical sensor) and other anti-two-block equipment (e.g., limit switches) must also fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
060-OpNoUnBolt00-HFI-NOD	<i>Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tip Over:</i> If the operators failed to remove all or some of the lid bolts from the cask, when they attempted to remove the cask lid with the CTM, the load would be significantly heavier than the CTM is rated for, and result could be a drop of the cask.	9	1E-03	If the lid bolts were not all removed during preparation activities and the CTM operator does not notice, one of two things may happen: the operator may attempt to lift the cask and the bolts may break, or the CTM operator may attempt to lift the cask and the bolts may hold. If the bolts hold, the load cell stops the CTM from lifting before the cask can be lifted. This failure was not assigned a 1.0 like other failures, which are ANDed with mechanical failures because the load cell is never bypassed and the HFE requires several independent human failures. For this failure to occur, the preparation crew must fail to remove all the bolts and must fail to verify on the checklist that all the bolts have been removed. Independently, the CTM operator would also have to fail to notice that the entire cask is lifting as the lid is lifted into the CTM. This failure was assessed to be "highly unlikely" (0.001) because it involves two human failures by different teams and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator, "failure to properly conduct an operation performed on a daily basis," which also has a default probability of 0.001.
060-OpNoUnBoltDP-HFI-NOD	<i>Operator Fails to Remove Lid Bolts, Resulting in Impact, Drop, or Tip Over (DPCs)</i>	9	N/A	There is no lid on casks containing a DPC; therefore, this failure mode was omitted from analysis.

INTENTIONALLY LEFT BLANK

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
060-OpCTMImpact1-HFI-COD	<i>Operator Moves the CTM while Canister or Object is below or between Levels:</i> If the operator moves the trolley before the canister has cleared the port gate, then the canister can impact the floor if the canister is between levels. If the canister or the lid is completely below the floor, this failure can result in the cable snapping and the canister or object dropping. For canisters, the shear event (movement while the canister is between floors) is the bounding event.	9	1E-03	The operator can inappropriately move the CTM while the canister or lid is below the port gate or while the canister is between levels. If this inadvertent movement occurs while the canister is between levels, it can result in an impact and shear force to the canister. If the movement occurs while the canister is below the port gate, then the cable can snap, resulting in a drop. In order to accomplish this inadvertent movement, the operator would have to fail to follow proper lifting procedures and operate the ASD in manual or lid lift mode. If the lift is done in manual mode, then the CTM operator can fail to lift the canister or object high enough to clear the floor before horizontal movement. If it is in lid lift mode, it would automatically stop too soon, but the operator would have to fail to notice that the canister is not high enough when closing the port and CTM slide gates on the canister. For a canister, the operator would also have to fail to rely on the optical sensor and must also fail to close the slide gate to accomplish this HFE. There are interlocks, such as the load cell interlock, that prevent the CTM from exerting enough force to snap the cable and drop the canister or object. There is also an interlock that prevents horizontal motion if the slide gate is not closed, but this interlock can be bypassed during normal maintenance. Due to the complicated nature of this failure, the interlock was not separately modeled for this HFE. Rather, it was included in the preliminary value. This failure was considered highly unlikely and accordingly assigned a preliminary value of 0.001.
060-OpCICTMGate1-HFI-NOD	<i>Operator Inappropriately Closes Slide or Port Gate during Vertical Canister Movement and Continues Lifting:</i> If the operator signals the CTM slide gate or port gate to close while the canister is being raised, it can result in a canister impact if the door closes on the canister, or it can result in a canister drop if the door closes on the hoist, severing the cables. The NSDB requires the gate motors to be sized such that they cannot damage the canisters; the gate cannot sever the cables either. This failure can, however, result in a drop if the operator closes the slide gate on the cables and continues hoisting such that the canister is stuck and the cable snaps.	9	1E-03	In this operation, the CTM operator is lifting and lowering the canister. The slide gate cannot damage the canister or sever the hoist cables, so the failure required here is for the operator to prematurely close the slide gate and keep hoisting such that the canister catches on the slide gate and the hoist cable snaps. There are two slide gates for each motion—the CTM slide gate and the cask and waste package port slide gate. The operator performs CTM operations daily and has a camera view of the operations. There is no interlock to prevent this error, but if the canister is lifted per the procedure, the operator would use the ASD and not close the gate until the ASD has stopped. It is unlikely the operator would try to close the slide gate while lifting the canister; the most likely scenario is for the operator to fail to lift the canister high enough, close the slide gate as if to move the CTM, and then notice that the canister is too low and try to lift the canister without first opening the slide gate. In order for the operator to fail to lift the canister high enough, the ASD has to have a mechanical failure, or the ASD has to be in the wrong mode. The manual mode is only accessible by entering a password. Because lifting is a slow procedure, it is unlikely that the operator would, if it is even possible, put the ASD in manual mode. If the ASD is in manual mode, it is unlikely that the operator would stop the canister too soon because, independent of the ASD, the optical sensor in the bell stops the canister once it has cleared the bell. The more likely case is that the operator would fail to restore the ASD to canister lift mode after moving the lid. For all waste forms except the DPC, the lid is removed in the previous step. In addition to failing to change ASD mode, the operator must also fail to visually verify the height of the canister before closing the slide gate. In either case, if the operator does stop the canister too soon and closes the slide gate, the operator would still have to forget to reopen the slide gate before resuming the lift in an attempt to correct the error. This failure was assessed to be “highly unlikely” (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001.
060-OpCTMImpact2-HFI-COD	<i>Operator Causes Canister Impact with Lid during CTM Operations (non-DPC):</i> The cask or AO lid, when removed by the CTM, is staged such that the canister must travel over it to move across the Cask Transfer Room. If the lid is improperly stowed, the CTM can collide with the lid. This failure mode is not applicable to DPCs because the cask lid is removed in the Cask Preparation Room.	9	N/A	The lid staging area is in the pathway of the CTM; if the lid is improperly stored, the CTM, carrying a canister, can potentially impact the lid. This failure was omitted from analysis because, if the lid was stored such that it was an obstruction to the CTM, the CTM would run into the lid as it returns to the cask from lid staging. At that point, the error would have to be corrected before operations continued.
060-OpCTMImpact5-HFI-COD	<i>Operator Causes Canister Impact with SSC during CTM Operations (All):</i> If the CTM is moved too far while transferring a canister, it can collide into an end stop and impact the inside of the CTM bell or hit an SSC.	9	1.0	In this step, the operator can potentially impact the canister in several ways: CTM bridge impacts end stops while moving canister CTM trolley impacts end stops while moving canister Bridge used to move canister impacts other bridge. In order to accomplish any of these, however, additional equipment failures must also occur. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.

INTENTIONALLY LEFT BLANK

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
060-OpCTMImpact3-HFI-COD	<i>Operator Causes Two CTMs to Collide:</i> In the CRCF, there are two CTMs and two parallel lines for canister transfer. If two canisters are processed simultaneously and one operator moves the CTM bridge too far, the other CTM can potentially be impacted. There is an anti-collision interlock on the CTM to prevent this failure.	9	1E-01	In the CRCF, it is possible for two CTMs to run into each other during canister transfer. Both CTMs are equipped with an anti-collision interlock that must also fail for an initiating event to occur. Both CTM operators are in one control room, both are aware of the other's operations, and any simultaneous CTM movement is pre-coordinated. This failure was assessed as a likely (0.1) failure because of the potential complexity of dual operations and the potential for poor communication. There are anti-collision interlocks on the CTM to prevent this error.
060-OpDirExpose1-HFI-NOD	<i>Operator Causes Direct Exposure during CTM Activities (First Floor, All CTM Movements):</i> If an operator inadvertently opens the shield door and enters the Cask Unloading Room while the canister is being lifted out of the cask, that operator would get a direct exposure. Likewise, if the operator inadvertently opens the port gate when the CTM is not over the cask or WP with its shield skirt lowered, then an operator on the second floor (Canister Transfer Room) can get a direct exposure.	18	1E-01	Direct exposure during CTM activities can happen if an operator inadvertently opens the shield door to the Canister Transfer Room while the canister is being lifted, or if an operator opens the port gate (with a cask under it) while the shield skirt is not lowered over the port. In order to accomplish either of these scenarios, an interlock must also fail. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. As was previously discussed, the HRA team has generally assigned unsafe actions that are combined with interlocks an HEP of 1.0. As was also discussed, if this very conservative approach did not demonstrate compliance with the performance objectives of 10 CFR 63.111(Ref. E8.2.1) then the HRA team would consider whether a lower preliminary value was justified. That is the case here. In further considering this event, it would be very difficult to make it happen. An extraordinary bypass of the interlock or a random failure of the interlock would be required. Then, a worker would have to violate all administrative controls and training and attempt to enter the room without appropriate clearance from the control room. The operator would also have to conduct the operation improperly since failure of the interlock does not directly result in exposure potential if the operator still conducts the operation correctly (i.e., the interlock would not be challenged unless an additional error was made). To a large extent, all of these things are independent because they are unsafe actions by different individuals doing different things at different times. Therefore, the HRA team feels justified in assigning a lower preliminary value of 0.1 to the unsafe action (still believed to be quite conservative), which, in combination with the interlock failure value, results in an overall value of 3E-6/demand for an exposure.
060-OPCTMDirExp1-HFI-NOD	<i>Operator Causes Direct Exposure during CTM Activities (Second Floor, All CTM Movements):</i> If the CTM operator fails to close the port gate before lifting the shield skirt after placing a canister in a receptacle (e.g., staging rack, AO, or WP) and a worker violates the procedural control by entering the Cask Transfer Room during canister transfer activities, that worker would be exposed.	18	1E-04	Closure of the port gate is a simple action that is performed multiple times in a day. This action is performed every time the CTM is moved without deviation, and the operator is trained on the consequences associated with this failure. In addition to these failures, a completely independent failure, involving violation of a strict procedural control by inappropriately entering a radiation controlled area, by a person of a separate "team" must also occur. This HFE was considered extremely unlikely and assigned a preliminary value of 0.0001.
060-OpDirExpose2-HFI-NOD	<i>Operator Causes Direct Exposure during CTM Activities (Movement into AO):</i> For canister loading in an AO, if the AO is not pre-staged in the Cask Unloading Room, the operator can lower the canister to the floor of the Cask Unloading Room and then place the AO lid directly on the canister. The next step in operations is movement of the AO to the Cask Preparation Room. The ST operator would be exposed as part of the normal operations of this step (i.e., entering the Cask Unloading Room to retrieve the AO). There is an interlock that prevents the port gate from opening if a receptacle (AO) is not below the port.	18	1E-4	Operators can also cause direct exposure during CTM operations by failing to stage an aging overpack in the Cask Unloading Room and then placing the canister on the floor of the Cask Unloading Room and opening the shield door. Placing the aging overpack beneath the cask port is part of the staging activities before CRCF operations for aging overpack loading. Aging overpack staging is checked off by the staging crew and is also checked off by the operations crew directly before operations begin as part of the prejob plan. If the aging overpack is not staged, the CTM operator has the chance to notice when emplacing the canister inside the aging overpack (via a camera view looking down on the aging overpack). If the canister is emplaced on the floor, then the operator has an additional chance to notice that the aging overpack is missing when trying to put the aging overpack lid on the aging overpack with the CTM. This failure received a preliminary value of 0.01 for failure to pre-stage the aging overpack and 0.01 for failure to notice before a direct exposure occurs, resulting in a total preliminary value of 0.0001. This preliminary value is consistent with the preliminary value for failure to install a waste package shield ring (Section E6.7, HFE Group#7: Waste Package Export; 060-OpShieldRing-HFI-NOD), which has a very similar failure mode. There is an interlock that prevents this failure, but because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in HFE 060-OpFailRstInt-HFI-NOM.
060-OpStageRack1-HFI-NOD	<i>Operator Causes Direct Exposure during Canister Staging:</i> For the canister staging, if the CTM operator fails to close the port gate and the supervisor fails to follow the procedural control and check that the port gates are closed before the end of canister transfer activities, when a worker enters the Transfer Room during normal activities, the worker would be exposed.	18	1E-03	Closure of the port gate is a simple action that is performed multiple times in a day. This action is performed every time the CTM is moved without deviation, and the operator is trained on the consequences associated with this failure. The supervisor has to double check the work of the CTM operator; however, the supervisor is part of the same "team" as the CTM operator. A preliminary value of 0.001 was assigned to this failure because it corresponds to the default probability of a "highly unlikely" error and also the default probability of a simple failure of an operation that is performed daily.

INTENTIONALLY LEFT BLANK

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
060-OpFailRstInt-HFI-NOM	<i>Operator Fails to Restore Interlock after Maintenance:</i> There are several interlocks that may be bypassed during normal maintenance. Failure to restore the interlock which prevents the port gate from opening before a receptacle is placed underneath the port is explicitly modeled here. If the bypass is not restored, this could result in a direct exposure due to the HFE above (HFE 060-OpDirExpose2-HFI-NOD)	18	1E-02	If the maintenance bypass for the interlock which prevents the cask port gate from opening before a waste package is placed underneath the port bypass is not restored, it could result in a direct exposure due to HFE 060-OpDirExpose2-HFI-NOD. This interlock would be bypassed during CTM maintenance. This failure would require the crew member to fail to reset the bypass and the crew member to fail to properly perform the prejob check of the CTM equipment. These failures were assigned a preliminary value of 0.01, which corresponds to the generic preliminary value for the pre-initiator "failure to properly restore an operating system to service when the degraded state is not easily detectable."
060-OpFailSG-HFI-NOD	<i>Operator Fails to Close the CTM Slide Gate before Moving the CTM with the Canister inside the Bell:</i> If the canister is inside the CTM with the shield skirt raised and the slide gate open, then personnel on the Canister Transfer Room floor may get a direct exposure. This configuration is achieved if the operator fails to close the CTM slide gate and then raises the shield skirt to move the canister to a new receptacle. There is an interlock that does not allow the shield skirt to rise if the slide gate is open.	18	1E-03	Direct exposure during CTM activities can happen if there is a canister in the bell and the CTM slide gate is open while the shield skirt is raised. The most likely way to get this configuration is for the operator to forget to close the slide gate and then raise the shield skirt to move the CTM as per normal operations. There is an interlock that prevents this failure, but because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in HFE 060-OpFailRstInt-HFI-NOM. This operation is performed multiple times a day and, for every CTM lift, the operator closes the slide gate before lifting the shield skirt. This operation is performed by a highly trained operator and also corresponds closely to the generic human-induced initiator "failure to properly conduct an operation performed on a daily basis," which also has a default probability of 0.001. No adverse PSFs were identified in this operation that would merit adjusting this preliminary value.
060-OpNoUnplugST-HFI-NOD	<i>Operator Fails to Disconnect Power Supply from ST in the Cask Unloading Room:</i> When the ST is moved to the Cask Unloading Room and positioned under the cask port, the operator is supposed to lower and turn off the ST. If the ST operator fails to disconnect the ST from the power source, the ST can get a spurious signal during canister lifting that can cause a collision of the ST into the canister.	9	1E-03	While in the Canister Transfer Room, the site transporter is off with the load lowered. The site transporter is controlled locally (i.e., via pendant), and there are no operators in the Canister Transfer Room during CTM operations. In order to cause a spurious movement of the site transporter, the operators must fail to disconnect the site transporter from the power source, and the controller must send a spurious signal to the site transporter. The connection point for the site transporter is outside of the Cask Unloading Room, in the Cask Preparation Room. In order for this failure to occur, when exiting the Cask Unloading Room and closing the shield door, the personnel would have to fail to notice the cord going in through the shield door. If the shield door does not sever the power cord, then there is an interlock that prevents this error: the interlock prevents the port gate from opening (and thus CTM activities commencing) if the shield door is not completely closed. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. This failure was assessed to be "highly unlikely" (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator "failure to properly conduct an operation performed on a daily basis," which also has a default probability of 0.001.
060-OpNoDiscoAir-HFI-NOD	<i>Operator Fails to Disconnect Air Supply from CTT in the Cask Unloading Room:</i> When the CTT is moved to the Cask Unloading Room and positioned under the cask port, the operator is supposed to disconnect the air supply from the CTT. If the operator fails to do so, the CTT can get a spurious signal during canister lifting that can cause a collision of the CTT into the canister.	9	1E-03	While in the Canister Transfer Room, the CTT is parked with the air supply disconnected. The CTT is controlled locally (i.e., via pendant), and there are no operators in the Canister Transfer Room during CTM operations. In order to cause a spurious movement of the CTT, the operators must fail to disconnect the CTT from the air source, and the controller must send a spurious signal to the CTT. The connection point for the CTT is outside of the Cask Unloading Room in the Cask Preparation Room. In order for this failure to occur, when exiting the Cask Unloading Room and closing the shield door, the personnel would have to fail to notice the hose going in through the shield door. If the shield door does not sever the air hose, then there is an interlock that prevents this error: the interlock prevents the port gate from opening (and thus CTM activities commencing) if the shield door is not completely closed. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. This failure was assessed to be "highly unlikely" (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator "failure to properly conduct an operation performed on a daily basis," which also has a default probability of 0.001.
Spurious movement of CTT or ST during CTM activities	<i>Operator Causes Spurious Movement of CTT or ST while Canister is Being Loaded</i>	9	N/A	The CTT is locally controlled and sitting in the Unloading Room deflated. The ST is locally controlled and sitting in the Unloading Room disconnected from a power source. There are no personnel in the Unloading Room during this operation, and there is an interlock on the shield door that prevents access to the room while the canister is being removed from the cask. This failure was omitted from analysis because it involves several mechanical and human failures, including violation of the procedural control which restricts access to the Unloading Room. Furthermore, if a person enters the Unloading Room during canister removal, they would receive a direct exposure; this failure is captured in 51A-OpDirExpose1-HFI-NOD.

INTENTIONALLY LEFT BLANK

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
060-OpWPTTSpur01-HFI-NOD	<i>Operator Causes Spurious Movement of WPTT while Canister is Being Loaded:</i> The WPTT is controlled remotely. If the operator sends a signal for the WPTT to move during canister lowering, the WPTT would impact the canister.	9	1E-03	While the canister is being lifted with the CTM, an operator can inadvertently signal the WPTT to move. The controls for the WPTT are on a separate control board, and the WPTT operator is not involved in the CTM operations. The WPTT operator does not begin work until after the CTM operator is done and hands off the checklist to the WPTT operator. This failure would require a significant departure from normal operations; the analysts could not identify any contexts in which the WPTT or CTM operator would believe it was appropriate to move the WPTT during this operation. In order for the WPTT to move while a canister is being loaded, an interlock must also fail. This failure was assessed to be "highly unlikely" (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator "failure to properly conduct an operation performed on a daily basis," which also has a default probability of 0.001.
060-OpTiltDown01-HFI-NOD	<i>Operator Initiates Premature Tilt-Down during Transfer to Closure Area:</i> The WPTT is controlled remotely. If the operator sends a signal for the WPTT to tilt-down during canister lowering, the WPTT would impact the canister.	9	1.0	The operator can cause the WPTT to prematurely tilt down. The WPTT operator is not supposed to be operating or near the controls for the WPTT during CTM operations. The WPTT operator has no reason to be near the controllers, much less to begin tilt-down. Tilt-down only occurs during waste package loadout in the Waste Package Loadout Room, and the controller for the WPTT tilt-down is distinct from other WPTT controls. In order to accomplish this failure, several interlocks must also fail. These interlocks, including an interlock taking power away from the WPTT when the port gate is open and an interlock between the tilt-down mechanism and the docking station, have no bypass. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
060-OpDSNFLoad-HFI-NOD	<i>Operator Misloads DSNF:</i> Due to potential criticality implications, no more than four DSNF canisters can be put together in a single WP or in a staging rack. The only way to get into this configuration is if the operator loads five or more DSNF canisters into a TAD canister WP or places them in a TAD canister staging rack.	N/A	1E-03	Due to potential criticality implications, no more than four DSNF canisters can be put together in a single WP or in a staging rack. The only way to get into this configuration is if the DSNF canisters are loaded into a TAD canister, loaded into a waste package, or placed in a TAD canister staging rack. Misloading a TAD requires the setup crew to prepare and stage the wrong waste package, the operating crew to fail to notice it is the wrong WP during their preoperational check, and the CTM operator to fail to notice it is the wrong waste package while loading the waste package. In addition to that set of failures, the CTM operator would also have to violate procedures and try to fit more than the standard four DSNF canisters in the waste package. For misstaging a DSNF canister in a TAD canister staging rack, the CTM operator must fail to pick the appropriate staging rack. The TAD canister and DSNF staging racks are sufficiently different in size and location that this failure would require significant inattention, particularly because the DSNF racks are expected to be used frequently, but the TAD canister staging racks have no expected use during normal operations. In addition to this failure, to cause a potential criticality problem, the CTM operator would have to repeat the same failure four times, each time putting the DSNF canister in the same TAD canister staging rack. This event was considered highly unlikely and given the default preliminary value of 0.001.

NOTE: AO = aging overpack; ASD = adjustable speed drive; CRCF = Canister Receipt and Closure Facility; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; DSNF = U.S. Department of Energy spent nuclear fuel; ESD = event sequence diagram; HFE = human failure event; HRA = human reliability analysis; ID = identification; NSDB = nuclear safety design basis; PSF = performance shaping factor; RC = railcar; SSC = structure, system, or component; ST = site transporter; TAD = transportation, aging, and disposal (canister); TC = transportation cask; TT = truck trailer; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

INTENTIONALLY LEFT BLANK

E6.5.3 Detailed Analysis

After the preliminary screening analysis and initial quantification are completed, those HFES that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives are subjected to a detailed analysis. The overall framework for the HRA is based upon the process guidance provided in ATHEANA (Ref. E8.1.22). Consistent with that framework, the following four steps from the methodology described in Section E3.2 provide the structure for the detailed analysis portion of the HRA.

Step 5: Identify Potential Vulnerabilities

Prior to defining specific scenarios that can lead to the HFES of interest (Step 6), information is collected to define the context in which the failures are most likely to occur. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in HFES or unsafe actions. This information collection step is discussed in Section E6.5.3.2.

Step 6: Search for HFE Scenarios (Scenarios of Concern)

An HFE scenario is a specific progression of actions with a specific context that leads to the failure of concern; each HFE is made up of one or more HFE scenarios. In this step, documented in Sections E6.5.3.3 and E6.5.3.4, the analyst identifies deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These unsafe actions make up an HFE scenario. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions.

Step 7: Quantify Probabilities of HFES

Detailed HRA quantification methods are selected as appropriate for the characteristics of each HFE and are applied as explained in Section E6.5.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)
- ATHEANA expert judgment (Ref. E8.1.22).

There is no implication of preference in the order of listing these methods. They are jointly referred to as the "preferred methods" and are applied either individually or in combination as best suited for the unsafe action quantified. The ATHEANA (Ref. E8.1.22) expert judgment method (as opposed to the overall ATHEANA (Ref. E8.1.22) methodology that forms the framework and steps for the performance of this HRA) is used when the other methods are deemed to be inappropriate to the unsafe action, as is often the case for cognitive EOCs.

Appendix E.IV of this analysis explains why these specific methods were selected for quantification and gives some background on when a given method is applicable based on the focus and characteristic of the method.

All judgments used in the quantification effort are determined by the HRA team and are based on their own experience, augmented by facility-specific information and the experience of subject matter experts, as discussed in Section E4. If consensus can be reached by the HRA team on an HEP for an unsafe action, that value is used as the mean. If consensus cannot be reached, the highest opinion is used as the mean.

Step 8: Incorporate HFEs into the PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. The summary table of HFEs by group that lists the final HEP by basic event name provides the link between the HRA and the rest of the PCSA. This table can be found in Section E6.5.4.

E6.5.3.1 HFEs Requiring Detailed Analysis

The detailed analysis methodology, Sections E3.2.5 through E3.2.9, states that HFEs of concern are identified for detailed quantification through the preliminary analysis (Section E3.2.4). An initial quantification of the CRCF PCSA model determined that there were five HFEs in this group whose preliminary values were too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111. These HFEs are presented in Table E6.5-2.

Table E6.5-2. Group #5 HFEs Requiring Detailed Analysis

HFE	Description	Preliminary Value
060-OpCTMdrop001-HFI-COD	Operator causes drop of object onto canister during CTM operations	2E-03
060-OpCTMdrop002-HFI-COD	Operator causes drop of canister during CTM operations (low-level drop).	2E-03
060-OpCTMImpact1-HFI-COD	Operator moves the CTM while canister or object is below or between levels	1E-03
060-OPCTMDirExp1-HFI-NOD	Operator Causes Direct Exposure during CTM Activities (Second Floor)	1E-04
060-OpStageRack1-HFI-NOD	Operator Causes Direct Exposure during Canister Staging	1E-03

NOTE: CTM = canister transfer machine; HEP = human error probability.

Source: Original

E6.5.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the ATHEANA approach to detailed quantification is to identify and characterize factors that could create potential vulnerabilities in the crew’s ability to respond to the scenarios of interest and might result in HFEs or unsafe actions. In this sense, the “vulnerabilities” are the context and factors that influence human performance and constitute the characteristics, conditions, rules and tendencies that pertain to all the scenarios analyzed in detail.

These vulnerabilities are identified through activities including but not limited to the following:

1. The facility familiarization and information collection process discussed in Section E4.1, such as the review of design drawings and concept of operations documents
2. Discussions with subject matter experts from a wide range of areas, as described in Section E4.2
3. Insights gained during the performance of the other PCSA tasks (e.g., initiating event analysis, system analysis, and event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the CTM operation that relate to potential human failure scenarios relevant to the three HFEs listed above. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during CTM operations, but these have no bearing on this analysis.

E6.5.3.2.1 Operating Team Characteristics

The operating team consists of the following personnel:

CTM operator—The CTM operator is located in the CRCF Control Room. The CTM operator receives standard training for crane operations and observes operations prior to being allowed to operate the CTM on a dry run. After training, the CTM operator is signed off to operate the CTM based on an evaluation of proficiency in a dry run. The CTM operator is observed on initial operations until signed off for solo operation. A single operator is assigned to the CTM operation.

Crew members (two)—Maintenance crew members are trained in tasks required for preparing the CTM for canister transfer, including affixing the appropriate grapple for the canister. Training consists of observation and “hands-on” instruction for the CTM preparation process. The CTM is prepared by a team of two workers.

Supervisor—The supervisor, or some other personnel with comparable training and certification, is in the CRCF control room watching CTM operations. This person is in charge of completing an end-of-operations checklist and independently verifying that the Canister Transfer Room is in a safe configuration after canister transfer activities have been completed.

E6.5.3.2.2 Operation and Design Characteristics

Control Panel—The panel consists of a joystick controller for two-dimensional movements of the bridge and trolley. Speed in both directions is fully variable within unit capabilities, based on the extent of joystick deflection. Buttons for the up–down movement of the hoist are spring returned and must be held in for hoist movement. The height of the hoist yoke is displayed digitally on the panel. There is a joystick for fine motion alignment of grapple (e.g., it can move the hoist within the bell). A flat screen display shows view from the camera mounted on the boom above the yoke. A control interface for the ASD is incorporated into the panel.

ASD—The ASD is equipped with a semi-automated system for lifts. The ASD has two normal modes and one maintenance (i.e., manual) mode. Normal modes have two settings: canister lift and lid lift. In the canister lift mode, the operator sets the mode and pushes/holds the lift button; the ASD lifts to the proper height and stops. The maintenance mode allows for full manual operation. The maintenance mode can be engaged only by entering a password.

Interlocks/Alarms—Only hardwired (non-PLC) interlocks are considered.

Hoist Operational Upper Limit—A light curtain located just above (~2 in.) the CTM slide gate. The interlock removes the power from the hoist lift circuit if nothing is sensed within the bell at this height (i.e., when the hoist cables, load cell, grapple, and any load have cleared this height). Indicators on the control panel (red/green lights) indicate whether the limit is cleared or blocked. The upper limit can be bypassed.

Grapple Engagement/Disengagement Interlock—The grapple interlock provides indication to the operator that the grapple is either fully engaged with the load or fully disengaged. Red and green lights indicate position. When both lights are on, this indicates that the grapple is between positions, and the interlock prevents hoist movement under this condition.

Grapple Interlock—The grapple interlock also prevents hoist movement if the secondary grapple is not properly attached to the primary grapple on the hoist. There is an interlock which prevents operation of the CTM canister grapple (primary grapple) if it is not properly attached to the hoist.

Load Cell Overlimit—The load cell overlimit stops hoist movement when excessive force is applied to the hoist. This could shut down the hoist if the lid is pulled up against the bottom of the bell, but would not provide any protection against two-blocking because it is located below the lower block (i.e., between the block and the grapple).

Inadvertent Grapple Disengagement—The grapples are mechanically designed such that they cannot disengage while under a load; therefore, inadvertent grapple disengagement is precluded. However, to be conservative, this is modeled as an electric interlock.

Shield Skirt/Slide Gate Interlock—Prevents the shield skirt from lifting if the CTM slide gate is not closed. The failure mode of failing to reset the bypass for this interlock has not been modeled because there is no bypass for this interlock.

E6.4.3.2.3 Operational Conditions

There is no direct view of the CTM operation by any individual. Visual cues are hampered because all observations are made through cameras and observed on screens. The precise locations of the cameras have not been specified in the design, but the intent is to provide cameras that can view the grapple and canister (and move with the hoist) on the hoist trolley (that can see into the bell) and at other locations that can provide views of the outside of the bell and the Canister Transfer Room.

Control panel indications provide positive indication that the grapple has been deployed in the locked position (a red light) or the unlocked position (a green light), but the ability to provide a

direct (as opposed to indirect or inferred) confirmation of full engagement in the lift fixture is not proven.

The total operation of the CTM for a canister takes about two hours. The operator has a number of specific tasks to perform during that time, so the overall process can be considered reasonably active. However, the lifting task (relevant to drops) is one of the longest periods of inactivity for the operator (i.e., 10 minutes, of which only the last 30 seconds or so can be considered potentially active). The potential for the onset of boredom, complacency, or distraction is higher than normal during this task.

E6.5.3.2.4 Formal Rules and Procedures

Procedural Controls—Procedural controls ensure that the operators and maintenance personnel do not enter the Canister Transfer Room during CTM activities. Procedural controls also include a checklist that must be filled out at the end of transfer activities to ensure that all the port slide gates (including staging racks) are closed.

E6.5.3.2.5 Operator Tendencies and Informal Rules

Dependency on Hoist Interlocks and Alarms—The CTM operator should actively observe and confirm proper operation of the CTM and not depend on either alarms to be informed that limits are being reached or interlocks to stop or prevent improper motion. However, there can be a tendency for the operator to count on these devices to prevent human failure, in particular because the visual information received from the cameras is distorted.

Dependency on Grapple Engagement/Disengagement Indicator—In a similar fashion, the operator should confirm positive engagement of the grapple through the camera, but the lack of clarity expected in the camera view can create a tendency to depend solely on the indicator.

E6.5.3.2.6 Operator Expectations

Consequences of Failure—The CTM operations are performed remotely. No personnel are in the vicinity of the operation, and so the threat of physical injury is absent. Operators expect that failures are mitigated by design features without serious consequences, which promotes complacency in the operations.

Anticipatory Actions—The lifting process is simple, the goal is clear, and problems are not expected. There is a tendency for the CTM operator to focus on future tasks while the hoist is in motion rather than concentrate on the ongoing task. The operator expects that no one attempts to enter the Canister Transfer Room during CTM activities.

Expectation of Grappling Success—The grapple is a simple device. The operator can expect that once the grapple is actuated, it properly engages or disengages. The operator does not expect a failure or expect the engagement indicator to show a failure. The operator can also not expect that the grapple is not properly attached to the hoist (i.e., the operator can expect and trust that the crew members have properly prepared the CTM).

E6.5.3.3 HFE Scenarios and Expected Human Failures (Step 6)

Given that the vulnerabilities that provide the operational environment and features that could influence human performance have been specified, then the HFE scenarios within this environment are identified. An HFE scenario is a specific progression of actions during normal operations (with a specific context) leading to the failure of concern. Each HFE is made up of one or more HFE scenarios. In accordance with the methodology, each scenario integrates the unsafe actions with the relevant equipment failures to provide the complete context for understanding and quantification of the HFE.

The HAZOP is instrumental in initially scoping out the HFE scenarios, but they are then refined through discussions with subject matter experts from a wide range of areas, as described in Section E4.2.

Table E6.5-3 summarizes all of the HFE scenarios developed for the HFEs in HFE Group #5.

Table E6.5-3. HFE Scenarios and Expected Human Failures for HFE Group #5

HFE	HFE Scenarios
<p>060-OpCTMdrop001-HFI-COD <i>Operator causes drop of object onto canister during CTM operations</i></p>	<p>HFE Scenario 1(a): (1) A crew member improperly installs the grapple, (2) the preoperational check fails to note the improper installation, (3) the primary grapple interlock gives a false positive signal, (4) the operator fails to notice the bad connection between the hoist and the grapple through the camera, and (5) the grapple/lid drops from the hoist and strikes the canister.</p> <p>HFE Scenario 1(b): (1) The operator fails to fully engage the grapple, (2) the grapple engagement interlock gives a false positive signal, (3) the operator fails to notice that the grapple is not fully engaged through camera, and (4) the lid drops from the grapple and strikes the canister.</p> <p>HFE Scenario 1(c)^{a, b}: (1) The operator leaves the ASD in maintenance mode OR the operator places the ASD in canister mode OR the ASD height control fails, (2) the operator fails to notice that the lift is taking too long OR the operator “locks” the lift button into position, (3) the load cell overload interlock fails, and (4) mechanical failure of the hoist under overload causes the lid to drop.</p> <p>HFE Scenario 1(d)^{a, c}: (1) The CTT is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice the lid tilt and continues the lift OR the operator “locks” the lift button into position, (4) the lid catches and jams in port, (5) the load cell overload interlock fails, and (6) mechanical failure of the hoist under overload causes the lid to drop.</p> <p>HFE Scenario 1(e): (1) The operator activates the grapple disengagement switch prematurely, (2) the load cell disengagement interlock fails, and (3) the lid drops from the grapple and strikes the canister.</p>

Table E6.5-3. HFE Scenarios and Expected Human Failures for HFE Group #5 (Continued)

HFE	HFE Scenarios
<p>060-OpCTMdrop002-HFI-COD <i>Operator causes drop of canister during CTM operations (low-level drop)</i></p>	<p>HFE Scenario 2(a): (1) A crew member improperly installs the grapple, (2) a primary grapple interlock gives a false positive signal, (3) the operator fails to notice the bad connection between the hoist and the grapple through the camera, and (4) the grapple/canister drops from the hoist.</p> <p>HFE Scenario 2(b): (1) The operator fails to fully engage the grapple, (2) the grapple engagement interlock gives a false positive signal, (3) the operator fails to notice that the grapple is not fully engaged through camera, and (4) the canister drops from the grapple.</p> <p>HFE Scenario 2(c)^d: (1) The CTT is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice that the DPC contacting the ceiling and continues the lift OR the operator “locks” the lift button into position, (4) the load cell overload interlock fails, and (5) mechanical failure of the hoist under overload causes the DPC to drop.</p>
<p>060-OpCTMImpact1-HFI-COD <i>Operator moves the CTM while canister or object is below or between levels</i></p>	<p>HFE Scenario 3(a): (1) The operator leaves the CTM in the lid lift mode (for non-DPCs), (2) the operator fails to notice that the lift stops too soon, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, and (5) the CTM slide gate interlock fails.</p> <p>HFE Scenario 3(b): (1) The operator puts the CTM in the lid lift mode (for DPCs), (2) the operator fails to notice that the lift stops too soon, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, and (5) the CTM slide gate interlock fails.</p> <p>HFE Scenario 3(c): (1) The operator puts the CTM in the maintenance mode (for non-DPCs), (2) the operator terminates the lift prior to the automatic stop, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, and (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, (5) the CTM slide gate interlock fails.</p> <p>HFE Scenario 3(d)^e: (1) The operator leaves the CTM in the maintenance mode (for DPCs), (2) the operator terminates the lift prior to the automatic stop, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, and (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, (5) the CTM slide gate interlock fails.</p>
<p>060-OPCTMDirExp1-HFI-NOD <i>Operator Causes Direct Exposure during CTM Activities (Second Floor)</i></p>	<p>HFE Scenario 4(a): (1) A worker violates administrative control by entering the Canister Transfer Room during canister transfer, and (2) the operator fails to close port gate before raising the shield skirt.</p>
<p>060-OpStageRack1-HFI-NOD <i>Operator Causes Direct Exposure during Canister Staging</i></p>	<p>HFE Scenario 5(a): (1) The operator fails to close staging rack port gate, and (2) the supervisor fails to verify that the staging rack port gate is closed as part of end-of-operations check.</p>

NOTE: ^a Scenarios (1c) and (1d) in this event do not apply to DPCs since DPC lids are not removed in the CTM.
^b This scenario does not apply to placing the waste package inner lid since it can only occur over the canister when lifting a transportation cask/aging overpack lid.
^c This scenario does not apply to placing the waste package inner lid or the aging overpack lid since it can only occur over the canister when lifting a transportation cask/aging overpack lid.
^d This scenario only applies to DPCs because the transportation cask lid was removed in the preparation area.
^e Only scenario 3(d) is applicable for lids.

ASD = adjustable speed drive; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure events.

Source: Original

Since there are five HFEs identified for detailed analysis in this group, the scenarios are organized under these three HFE categories, with the scenarios under the first HFE category numbered as 1(a), 1(b), etc.; those under the second category numbered 2(a), etc.; and similarly those under the third category numbered 3(a), 3(b), etc.

Each HFE scenario is in turn characterized by several unsafe actions, numbered sequentially as (1), (2), (3), etc. The Boolean logic of the HFE scenarios is expressed with an implicit AND connecting the subsequent unsafe actions and OR notation wherever two unsafe action paths are possible, as shown in Table E6.5-3.

The HFE scenarios summarized in Table E6.5-3 are discussed and quantified in detail in the following sections.

E6.5.3.4 Quantitative Analysis (Step 7)

Once the HFE scenarios and the unsafe actions within them are scoped out, it is then possible to review them in detail and apply the appropriate quantification methodology in each case that permits an HEP to be calculated for each HFE. Stated another way, each HFE is quantified through the quantification and combination of the contributing HFE scenarios. Dependencies between the unsafe actions and equipment responses within each scenario and across the scenarios are carefully considered in the quantification process.

This section provides a description of the quantitative analysis performed, structured hierarchically by each HFE category (identified by a basic event name), the HFE scenario, and the unsafe actions under each scenario, as previously documented in Table E6.5-3.

Prior to the scenario-specific quantification descriptions, a listing is provided of the values used in the quantification that are common across many of the HFE scenarios.

In generating the final HEP values, the use of more than a single significant figure is not justified given the extensive use of judgment required for the quantification of the individual unsafe actions within a given HFE. For this reason, all calculated final HEP values are reduced to one significant figure. When doing this, the value is always rounded upwards to the next highest single significant figure.

E6.5.3.4.1 Common Values Used in the HFE Detailed Quantification

There are some mechanical failures that combine with unsafe actions to form HFEs. In general, these mechanical failures are independent of the specific HFE scenario, and so they can be quantified independently. These values are presented in this section.

Interlock Failures—There are a number of interlock failures in the HFE scenarios. While the status of these events can affect subsequent events in the scenarios in different ways, the likelihood of this event occurring is independent of the scenario. This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for an interlock, from Attachment C, Table C4-1, is approximately $2.7E-05$ per demand.

$$\text{Interlock fails to perform function} = 2.7E-05$$

ASD Height Control Fails—This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for the ASD, from the Attachment C, Table C4-1, is approximately $3.4E-05$ per demand.

$$\text{ASD height control fails} = 3.4E-5$$

Load Drops from Hoist—This is the last event in a drop scenario. This event accounts for the safety margins built into the hoist system to accept overload without failure resulting in severed cables, failed clutches, and partially engaged grapples. The various events need to be quantified in relation to each other, using engineering judgment to account for the load being applied to the system versus its capacity to bear the load.

The first drop considered is where a canister (DPC) is being lifted and it catches the ceiling of the Cask Unloading Room. In this case, an overload of the system is created by adding the additional force of the hoist motor straining to lift the unmoving canister (over and above the force created by the canister) to the system. The extent to which this exceeds the ultimate load-bearing capacity of the system is a function of the total force that can be generated by the motor and the amount of time that the motor can exert this force while not turning before the motor overheats. Typical design requirements for NOG-1 cranes (Ref. E8.1.2) provide a significant safety margin against overload failures. The probability of this event is based on analyst judgment in accordance with the PCSA approach to the use analyst judgment for probability estimation. There is limited analysis of this condition. Lacking or inconclusive analysis would argue for assignment of even odds (0.5) for this event. The weight of evidence for the inherent margin in a single failure-proof design could form an argument that the failure is unlikely (0.1). The HRA team is convinced that the best estimate from the available information (given the current state of knowledge) is somewhere in between. The HRA team assigns 0.5 as the 95% confidence level and 0.1 as the 5% confidence level. Using a lognormal distribution, the mean associated with these confidence limits follows:

$$\text{Mechanical failure of hoist under overload causes DPC drop} = 0.25$$

The other drops are evaluated relative to this. First considered is the similar case where the lid is jammed in the port and the hoist is straining to lift the jammed lid. In this case, the force generated by the hoist is the same, but the weight of the lid is less. The HRA team judges that it is reasonable to reduce the failure probability by a factor of two to account for this difference:

$$\text{Mechanical failure of hoist under overload causes lid drop} = 0.1$$

Considered next is the condition where the grapple is either not properly connected to the hoist or the grapple itself is only partially engaged with the canister or lid. This failure (i.e., drop of canister or lid from an improperly engaged grapple) is judged to be comparable to mechanical failure of the hoist under overload because in both cases the load-bearing capacity of the system is reduced. Therefore the resulting probability is as follows:

$$\text{Grapple/canister drops from hoist} = 0.25$$

$$\text{Canister drops from grapple} = 0.25$$

Regarding the case of a lid, again the force is lower than the canister case and also lower than the jammed lid case, with a similar situation in that the load-bearing capacity of the system is reduced. Using the logic above, this would argue for using the 0.1 value. However, in the case of the lid, there is always the possibility that the drop would occur when the lid was not over the canister, or it would occur in a manner that the lid would not impact the canister (i.e., it would only strike the structure of the transportation cask, aging overpack, or waste package). In the absence of analysis, the HRA team has applied a 50-50 chance of this occurring, which reduces the probability by a factor of two. Therefore:

$$\text{Grapple/lid drops from hoist and strikes canister} = 0.05$$

$$\text{Lid drops from grapple and strikes canister} = 0.05$$

Given the information available about the design, the analyses in existence, and the knowledge of the requirements of NOG-1 (Ref. E8.1.2) and other applicable standards to be applied to the CTM, the HRA team believes this to be both a reasonable assessment and at as fine a level of detail and differentiation as can be justified.

E6.5.3.4.2 Quantification of HFE Scenarios for 060-OpCTMdrop001-HFI-COD: Operator Causes Drop of Object onto Canister during CTM Operations

E6.5.3.4.2.1 HFE Group #5 Scenario 1(a) for 060-OpCTMdrop001-HFI-COD

1. Maintenance crew member improperly installs grapple.
2. Preoperational check fails to note improper installation.
3. Primary interlock gives false positive signal.
4. Operator fails to notice bad connection between hoist and grapple through camera.
5. Grapple/lid drops from hoist and strikes canister.

Crew Member Improperly Installs Grapple—Prior to a lift operation, a crew member prepares the CTM for the operation by installing the appropriate grapple for the type of cask lid to be processed. While it is possible that this operation need not be performed (it may be the cask lid grapple is the same grapple used for previous waste package and no other work on or with the CTM may have been performed), it is uncertain how often this can occur, so this analysis considers that this action needs to be performed each time. To install the grapple, the primary CTM grapple lowers and engages the secondary grapple. If the primary grapple is only partially engaged, the secondary grapple appears to be secured in place, but it is not.

The operator aligns the grapple visually using the camera view and then engages the grapple. If it is not aligned properly, the grapple does not fully engage. The crew members locally verify engagement and connect the appropriate wire connections from the secondary grapple to the primary grapple. This is a straightforward matter of task execution. The task is simple and routine and can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well designed, highly practiced routine task performed to the highest possible standards by highly motivated, highly trained, and experienced person, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 3: Time pressure. The full affect EPC would be $\times 11$, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.
- EPC 8: Poor environment. This EPC is applied not so much because the environment is poor, but rather that it is simply not optimal. The full affect EPC would be $\times 8$, but this applies when working in the plant with suit and breathing apparatus, possible access problems, and for more than 45 minutes so that fatigue sets in. The APOA anchor for 0.1 is for work in the plant with suit and breathing apparatus but none of the other environmental stressors. In this task no breathing apparatus is required, but the task is somewhat physically demanding. Given the tradeoffs, the APOA is set at 0.1.
- EPC 13: Operator under load/boredom. The full affect EPC would be $\times 3$, which applies to a routine task of low importance carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Crew member improperly installs grapple} = 0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006 \quad (\text{Eq. E-7})$$

Preoperational Check Fails to Notice Improper Installation—There are two crew members responsible for preparing the CTM for each operation. Each crew member has a distinct set of assignments, although they collaborate when needed and are expected to check each other's work. The second crew member checks the first crew member's installation of the grapple, which provides an opportunity for the error to be detected. The second crew member also has a set of activities to perform, and so checking the first crew member is a secondary function. In addition, the existence of the grapple/hoist interlock provides an expectation that any error can be detected.

The second crew member would have helped initially with the connection of the grapple to line it up but would then move on to other things. At best, the second crew member performs a cursory check at the end of the job. Since the crew member was involved in the early stages, there is a bias that the job was done correctly. It is concluded that the level of dependence is high. The baseline HEP for the checking, for checking routine tasks without a checklist, is best determined from THERP (Ref. E8.1.26), Table 20-22, item (2), which is 0.2. The HEP for high dependence is from THERP (Ref. E8.1.26), Table 20-21, item (4)(e), which is 0.6.

$$\text{Preoperational check fails to note improper installation} = 0.6$$

Primary Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the primary grapple engagement interlock.

The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

Primary grapple interlock gives false positive signal = $2.7E-5$

Operator Fails to Notice Improper Connection between Hoist and Grapple through Camera—When the CTM operator is in the process of lifting the canister, the camera shows the operator the secondary grapple and its connection to the primary grapple. The operator is not focused on that connection but is focused on lining up the secondary grapple with the lifting device. However, as the lift begins, the operator is supposed to watch through the cameras. This gives the operator the opportunity to note that the grapple is not properly connected (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not expecting any problems in this simple operation, and the operator tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

This action is best represented by the CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made. The baseline HEP is 0.003.
- CPC “Adequacy of Man–Machine Interface”: For this particular observation, the use of a camera view (while the only practical means) is somewhere between tolerable and inappropriate. The CPC for an observation task with tolerable man–machine interface is 1.0, and for inappropriate is 5.0. With regard to being able to actually observe the condition of the grapple lock pin, the CPC is set as 4.0.
- CPC “Number of Simultaneous Goals”: The operator is primarily focusing on properly aligning the bell and hoist, opening the ports, and grappling the lid. While it could be argued that this is not “more than capacity,” it certainly relegates looking at the grapple/hoist connection to a secondary action. It is therefore deemed appropriate to apply the more than capacity CPC, which is 2.0.
- CPC “Adequacy of Training/Preparation”: Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

The resulting value follows:

$$\begin{aligned} &\text{Operator fails to notice bad connection between hoist and grapple through camera} \\ &= 0.003 \times 4 \times 2 \times 0.8 = 0.02 \end{aligned}$$

Grapple/Lid Drops from Hoist and Strikes Canister—Just because the lift is occurring with an improper grapple installation does not mean that the lid and grapple fall. The safety margins

build into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation, especially given that it is sized for a canister, and the lid is much lighter. Additionally, even if the lid and grapple do fall, they could fall early (a weak connection) or later (sufficient connection that they need time and motion to cause them to break loose). These two cases can result in the lid and grapple breaking loose when they are not above the canister. In addition, it is not a certainty that the lid and grapple, once dropped, would fall in an orientation that would impact the canister in the transportation cask, aging overpack, or waste package, even if they are above the canister at the time of the drop (the orientation of the falling lid and grapple may cause them to only impact the transportation cask, aging overpack, or waste package structure).

This event is quantified in Section E6.5.3.4.1.

$$\text{Grapple/lid drops from hoist} = 0.05$$

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.5-4.

Table E6.5-4. HEP Model for HFE Group #5 Scenario 1(a) for 060-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Crew member improperly installs grapple	0.0006
B	Preoperational check fails to note improper installation	0.6
C	Primary grapple interlock gives false positive signal	2.7E-5
D	Operator fails to notice bad connection between hoist and grapple through camera	0.02
E	Grapple/lid drops from hoist and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E-5 \times 0.02 \times 0.05 = 1E-11 \quad (\text{Eq. E-8})$$

According to NARA, the lower limit of credibility for an HFE accomplished by a single operator or team is 1E-5 per demand. Using this truncated value for the set of unsafe actions, the probability of this scenario is:

$$1E-5 \times 2.7E-5 < 1E-8 \quad (\text{Eq. E-9})$$

E6.5.3.4.2.2 HFE Group #5 Scenario 1(b) for 060-OpCTMdrop001-HFI-COD

1. Operator fails to fully engage grapple.
2. Grapple engagement interlock gives false positive signal.
3. Operator fails to notice grapple not fully engaged through camera.
4. Lid drops from grapple and strikes canister.

Operator Fails to Fully Engage Grapple—The operator engages the grapple from the control panel. The grapple can be roughly positioned using the alignment guides for the CTM and the hoist height indicator on the control panel, but final alignment must be done visually using the view from the cameras provided on the grapple. Once the operator believes the grapple is aligned, the operator engages the grapple with the lift fixture and confirms through the camera that the grapple has engaged. If the operator sees that the grapple has not properly engaged (generally by checking the interlock condition if it looks engaged visually), then the operator disengages it, repositions the grapple, and tries again to engage.

The operator aligns the grapple visually using the view from the camera and engages the grapple. If it is not aligned properly, it does not fully engage. This unsafe action can be best represented by the task execution error NARA GTT A1, adjusted by the following CPCs:

- NARA GTT A1: Carry out a simple manual task with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005
- EPC 3: Time pressure. The full affect EPC would be $\times 11$, but this applies only in cases where there is barely enough time to complete a task and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.
- EPC 11: Poor, ambiguous, or ill-matched system feedback. This EPC is applied to account for the need to observe the operation through cameras. The full affect EPC would be $\times 4$. The full effect is applicable when legibility is poor or label is obscured or where the layout of controls makes visual access and physical access difficult. The use of the camera view is deemed to represent full effect. The APOA is set at 1.0.
- EPC 13: Operator underload/boredom. The full affect EPC would be $\times 3$, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\begin{aligned} &\text{Operator fails to fully engage grapple} = \\ &0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad (\text{Eq. E-10}) \end{aligned}$$

Grapple Engagement Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

Grapple engagement interlock gives false positive signal = $2.7E-5$

Operator Fails to Notice Grapple Not Fully Engaged through Camera—As the lift begins, the operator is supposed to watch through the cameras. This allows the opportunity to note that the grapple is not properly engaged (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not expecting any problems in this simple operation, and the tendency is to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

In this task, the operator is checking the actions taken through the camera. The operator believe that the action was initially performed correctly (because the action was performed by the operator), and this belief is confirmed by the false positive from the interlock, this last observation is deemed completely dependent on the prior actions. Using THERP (Ref. E8.1.26) Table 20-21 to assess dependency, item (5) for complete dependency:

Operator fails to notice grapple not fully engaged through camera = 1.0

Lid Drops from Grapple and Strikes Canister—Just because the lift is occurring with an incomplete engagement of the grapple does not mean that the grapple would fall. The safety margins build into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation, especially given that it is sized for a canister, and the lid is much lighter. Additionally, even if the lid does fall, it could fall early (a weak connection) or later (sufficient connection that they need time and motion to cause them to break loose). These two cases can result in the lid breaking loose when it is not above the canister. In addition, it is not a certainty that the lid, once dropped, would fall in an orientation that would impact the canister in the transportation cask, aging overpack, or waste package even if it is above the canister at the time of the drop (the orientation of the falling lid may cause it to only impact the transportation cask, aging overpack, or waste package structure).

This event is quantified in Section E6.5.3.4.1.

Lid drops from grapple = 0.05

HEP Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.5-5.

Table E6.5-5. HEP Model for HFE Group #5 Scenario 1(b) for 060-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator fails to fully engage grapple	0.07
B	Grapple engagement interlock gives false positive signal	2.7E-5
C	Operator fails to notice grapple not fully engaged through camera	1.0
D	Lid drops from grapple and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D = 0.07 \times 2.7E-5 \times 1.0 \times 0.05 = 1E-7 \quad (\text{Eq. E-11})$$

E6.5.3.4.2.3 HFE Group #5 Scenario 1(c) for 060-OpCTMdrop001-HFI-COD

1. Operator leaves ASD in maintenance mode OR operator places ASD in canister mode OR ASD height control fails.
2. Operator fails to notice lift is taking too long OR operator “locks” lift button into position.
3. Load cell overload interlock fails.
4. Mechanical failure of hoist under overload causes lid drop.

Operator Leaves ASD in Maintenance Mode—The ASD controls the height of the lift. Before beginning the lifting process, the operator should ensure that the ASD is in the lid lift mode. It could be in maintenance mode because of activities performed in the days between canister transfers. It is not clear how often this would occur, so for the purpose of this analysis, the bounding case is that the ASD is always in maintenance mode between canister transfers. Therefore, the operator must change the mode prior to the lid lift. In doing this, the operator could either fail to change the mode (miss this step in the process) or erroneously place it in the canister lift mode, either of which results in the ASD trying to lift the lid too high and impacting the bottom of the bell. The third way this could occur is simply a mechanical failure of the height control set point of the ASD.

The CTM operator is supposed to set the CTM system to the appropriate lift mode prior to performing a lift. This is fundamental to the operation, not simply a step in a procedure that can be missed. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in maintenance mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3, and adjusted by the following EPCs:

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves ASD in maintenance mode = 0.0007

Operator Places ASD in Canister Lift Mode—Given that a CTM operator has correctly decided to set the CTM system status prior to operations, the appropriate operating mode also needs to be selected. There are only two modes to choose from: lid lift and canister lift. The ASD control is a screen where the operator can scroll between the choices to pick the appropriate lift mode. The act of selecting the wrong mode from these two can be best represented by task execution error NARA GTT A1, and adjusted by the following EPCs:

- NARA GTT A1: Carry out a simple single manual action with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005.
- This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The ASD control system requests confirmation from the operator (e.g., “You have selected canister lift. Confirm Y/N”). The baseline HEP is used without adjustment.

Operator places ASD in canister lift mode = 0.005

ASD Height Control Fails—This is a mechanical failure of the ASD controller. This event is quantified in Section E6.5.3.4.1.

ASD height control fails = $3.4E-5$

Operator Fails to Notice Lift is Taking Too Long—Lifting the lid takes on the order of a few minutes, whereas lifting the canister takes on the order of ten minutes. Because the operator holds the lift button or the lift stops, there is an opportunity to notice that the hoist has not stopped when expected and to release the button and stop the hoist, either before the lid contacts the interior of the bell or before it begins to overload the system. Realistically, the operator would have on the order of 30 seconds between when it should stop and when it would be too late. The hoist position indicator and camera view are in front of the operator on the control panel.

The operator is supposed to hold the lift button until the lift automatically stops. This operation has been performed many times in the past by the operator, and the operator has an instinctive feel for how long the lift takes. If an operator feels it is taking too long, the operator need only look at the camera and the indicators on the control panel for verification. Failing to recognize this situation can be represented by CREAM CFF I3, adjusted by the following CPCs with values not equal to 1.0:

- CFF I3: Delayed interpretation (not made in time). The baseline HEP is 0.01.

- CPC “Working Conditions”: The operator has optimal working conditions in the CRCF Control Room. The CPC for an interpretation task with advantageous working conditions is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to notice lift is taking too long} = 0.01 \times 0.8 = 0.008$$

Operator “Locks” Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to “lock” the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without an ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the operator would not believe that the deviation is unsafe, and it would free up time to prepare for subsequent steps or to perform other duties.

The operator is supposed to hold the lift button until the lift automatically stops. However, it is always possible to rig something up that would hold the button in place, relieving the operator of the “inconvenience” of holding it. The HRA team believes that the preferred methods do not provide baseline HEPs for such unsafe actions. Therefore, the ATHEANA expert judgment approach is used. In considering the judgment, HEART and NARA do provide some insight into the existence of EPCs that can affect this unsafe action, such as the following:

- A mismatch between an operator’s model of the world and that imagined by a designer—The designer considers the “push-and-hold” as a safety feature that keeps the operator’s attention on the operation. The operator considers it as an unnecessary inconvenience in what should be an automated function.
- A mismatch between real and perceived risk—Locking the button removes a layer of safety provided by the operator monitoring operations, but the operator perceives the reliability of the limits and interlocks as such that there is no additional risk involved (HEART EPC 12).
- Little or no independent checking or testing of output—A single operator is operating the CTM from a remote location. No one is looking over the operator’s shoulder (HEART EPC 17).
- An incentive to use other, more dangerous procedures—Holding the button means that the operator’s ability to accomplish other work is limited. The operator can be more efficient (e.g., planning for future activities, completing paperwork) by trusting the control system to complete the task (HEART EPC 21, NARA EPC 15).
- Operator under load, boredom—Holding a button when one fully expects that the system automatically controls the operation is not very challenging (NARA EPC 13).

- Little or no intrinsic meaning in a task—The operator really has to wonder why the system wasn't designed to simply perform the operation on its own. The operator could come to consider the “push-and-hold” feature as a poorly thought out design flaw (HEART EPC 28).

Taking this as a whole, the HRA team judges that the operator locks the button in place about 10% of the time (which can be interpreted as some operators doing it quite frequently and other operators less or not at all, depending on their compunction to do so). However, this action is not unrelated to prior failures in this scenario. An operator who fails to set the CTM system status (leaves the ASD in maintenance mode) has already demonstrated a predilection towards rushing and perhaps a bias towards short-cuts for the particular lift. Therefore, the HRA team judges that the success or failure of this task is related to the way in which the ASD failure occurs. It is judged that if the failure occurs as a result of leaving the ASD in maintenance mode, the HEP for locking the button in place is twice the baseline (0.2). If it occurs for either of the other two reasons, the HEP is one-half the baseline (0.05).

Operator “locks” lift button into place (ASD left in maintenance) = 0.2

Operator “locks” lift button into place (ASD placed in canister mode or fails mechanically) = 0.05

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the lid in contact with the bell (which would put the full load of the bell on the hoist) would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

Load cell interlock fails = $2.7E-5$

Mechanical Failure of Hoist under Overload Causes Lid Drop—There are three potential failure modes that could cause the lid to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the grapple or lid. However, just because the hoist keeps pulling does not mean that the lid falls (the hoist motor could overload and fail before the lid becomes detached from the hoist) or that the lid, once dropped, falls in an orientation that would impact the canister in the transportation cask or aging overpack (the orientation of the falling lid may cause it to only impact the transportation cask or aging overpack structure).

This event is quantified in Section E6.5.3.4.1.

Mechanical failure of hoist under overload causes lid drop = 0.1

HEP Calculation for Scenario 1(c)—The events in the HEP model for Scenario 1(c) are presented in Table E6.5-6.

Table E6.5-6. HEP Model for HFE Group #5 Scenario 1(c) for 060-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator leaves ASD in maintenance mode	0.0007
B	Operator places ASD in canister mode	0.005
C	ASD height control fails	3.4E-5
D	Operator fails to notice lift is taking too long	0.008
E1	Operator “locks” lift button into position (ASD left in maintenance)	0.2
E2	Operator “locks” lift button into position (ASD placed in canister mode or fails mechanically)	0.05
F	Load cell overload interlock fails	2.7E-5
G	Mechanical failure of hoist under overload causes lid drop	0.1

NOTE: ASD = allowable stress design; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$\{A \times (D + E1) + [(B + C) \times (D + E2)]\} \times F \times G = \{0.0007 \times (0.008 + 0.2) + [(0.005 + 3.4E-5) \times (0.008 + 0.05)]\} \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-12})$$

E6.5.3.4.2.4 HFE Group #5 Scenario 1(d) for 060-OpCTMdrop001-HFI-COD

1. CTT is not sufficiently centered under port.
2. Operator fails to notice CTT not sufficiently centered.
3. Operator fails to notice lid tilt and continues lift OR operator “locks” lift button into position.
4. Lid catches and jams in port.
5. Load cell overload interlock fails.
6. Mechanical failure of hoist under overload causes lid drop.

CTT Is Not Sufficiently Centered Under Port—This unsafe action actually occurs prior to this operation, during movement of the CTT (or site transporter) into the Cask Unloading Room. The CTT (or site transporter) operator brings the unit into the Cask Unloading Room and centers it directly under the cask port by aligning it against end stops that properly locate it and by using markings on the floor. If the cask is not properly centered, it is possible that the lid could strike the ceiling around the cask port rather than rising smoothly through the cask port. The cask would have to be off-center by more than a foot.

The unsafe action results from stopping the CTT prematurely and leaving it at least a foot short of the proper location. This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.
- CPC “Available Time”: There is adequate time to perform this task. The only time pressure is the desire to keep the process moving, but the consequences are insignificant. The CPC for an execution task with adequate time is 0.5.
- CPC “Adequacy of Training/Preparation”: This routine task is well trained and practiced and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{CTT is not sufficiently centered under port} = \\ 0.003 \times 0.5 \times 0.8 = 0.002$$

Operator Fails to Notice that CTT Is Not Sufficiently Centered—The CTM operator centers the CTM grapple over the cask lid lift fixture using a two-step process. First, the CTM operator does a rough alignment using the bridge and trolley position indicators and sets the bell and shield skirt in place. Then the operator opens the cask port and performs a fine alignment using a camera alignment system. The operator is not looking for perfect alignment but would expect it to be close. At this point, the operator would have the opportunity to question the amount of distance needed to move the hoist into position. Possible responses include: (1) the position is not off by much, (2) the initial placement of the bell is in question and it is repositioned (which may be easier to accomplish than asking another crew member to move the CTT), or (3) a belief that the position of the CTT is not off center by enough to make a difference.

In this task, the CTM operator roughly centers the CTM over the cask port, lowers the shield, and opens the port and CTM gates. The operator needs to more accurately locate the grapple over the lid by moving the hoist within the bell. At this point, the operator has an opportunity to judge if the amount of movement required to align the grapple is too much for the lid to clear the edges of the port during the lift. In this case, it is not so much an observation error (the operator can't help but observe the relative locations of the grapple and lid) or a diagnosis error (the operator knows the canister is not perfectly centered), but rather a decision error, where the operator decides that it doesn't matter that the cask is not centered (it's “close enough”). This can be represented by CREAM CFF I2, adjusted by the following CPCs with values not equal to 1.0:

- CFF I2: Decision error (either not making a decision or making a wrong or incomplete decision). The baseline HEP is 0.01.
- CPC “Available Time”: With regard to the general level of time pressure for the task and the situation type, it would be easy to believe that there is adequate time since the consequences of taking more time are (from a safety perspective) insignificant. However, from a production perspective, this would be a significant setback since the CTM operator would have to get the CTT crew back to move the CTT, a time-consuming process. This time pressure could bias the operator towards a decision

that “it’s close enough.” The CPC for an interpretation task with continuously inadequate available time is 5.0.

Applying these factors yields the following:

Operator fails to notice that CTT is not sufficiently centered = $0.01 \times 5 = 0.05$

Operator Fails to Notice Lid Tilt—The CTM operator is able to see the lid through the camera display. When the lid strikes the ceiling, it begins to tilt as the hoist continues to rise. The operator has the opportunity to notice the lid tilting before it potentially jams and has the opportunity to stop the lift. The prior unsafe action of failing to notice that the cask is too far off center could still lead the operator to be somewhat more careful and observant during the lift than if it had been closer to center (e.g., like the extra care a driver might show while pulling into a narrower than normal parking space).

If the operator is looking at the camera view during the lift, then the operator has the opportunity to observe the lid contacting the ceiling of the Cask Unloading Room and tilting into the port rather than rising straight through. The most likely failure would be that the operator is not looking at the screen at the time that this occurs, which can be represented by CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made (omission). The baseline HEP is 0.003.
- CPC “Adequacy of Man–Machine Interface”: There are two vulnerabilities in the man-machine interface for this observation. First, there is no alarm or indicator to alert the operator. Second, the camera view is not perfect. These are inherent to this type of operation, but would make it more likely that the operator would not be looking at the screen at the time. Thus, the man–machine interface should be considered inappropriate with regard to success of this observation. The CPC for an observation task with inappropriate man–machine interface is 5.0.

Applying these factors yields the following:

Operator fails to notice lid tilt = $0.003 \times 5 = 0.02$

Operator “Locks” Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to “lock” the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without an ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the action would not be perceived as unsafe but rather as a clever way to free time to get ready for subsequent steps or perform other duties. Again, the operator might be less likely to do this if there are doubts about the positioning of the cask.

The quantification of this event is discussed in detail under Scenario 1(c). In this scenario, it is judged that there is no bias dependency towards this failure that results from prior failures in the scenario. Therefore, the value used for the non-bias case is applied here:

Operator “locks” lift button into place = 0.05

Lid Catches and Jams in Port—Given the size of the lid in relation to the port, it is entirely possible that when it strikes the ceiling and tilts sideways, it still goes through the port at an angle without jamming.

The lid is smaller than the port, and a round object passing through a large round hole would generally be expected not to jam (unlike, for example, a square lid and a square hole where there are a number of orientations where jamming could occur). Nevertheless, for the purpose of this analysis this is assessed as having “even-odds” of jamming versus not jamming.

Lid catches and jams in port = 0.5

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the lid jammed in the port would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

Load cell interlock fails = $2.7E-5$

Mechanical Failure of Hoist under Overload Causes Lid Drop—There are three potential failure modes that could cause the lid to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the grapple or lid. However, just because the hoist keeps pulling does not mean that the lid falls (the hoist motor could overload and fail before the lid becomes detached from the hoist) or that the lid, once dropped, falls in an orientation that impacts the canister in the transportation cask or aging overpack (the orientation of the falling lid may cause it to only impact the transportation cask or aging overpack structure).

This event is quantified in Section E6.5.3.4.1.

Mechanical failure of hoist under overload causes lid drop = 0.1

HEP Calculation for Scenario 1(d)—The events in the HEP model for Scenario 1(d) are presented in Table E6.5-7.

Table E6.5-7. HEP Model for HFE Group #5 Scenario 1(d) for 060-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	CTT is not sufficiently centered under port	0.002
B	Operator fails to notice CTT not sufficiently centered	0.05
C	Operator fails to notice lid tilt and continues lift	0.02
D	Operator "locks" lift button into position	0.05
E	Lid catches and jams in port	0.5
F	Load cell overload interlock fails	2.7E-5
G	Mechanical failure of hoist under overload causes lid drop	0.1

NOTE: CTT = cask transfer trolley; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times (C + D) \times E \times F \times G = 0.002 \times 0.05 \times (0.02 + 0.05) \times 0.5 \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-13})$$

E6.5.3.4.2.5 HFE Group #5 Scenario 1(e) for 060-OpCTMdrop001-HFI-COD

1. Operator activates grapple disengagement switch prematurely.
2. Load cell disengagement interlock fails.
3. Lid drops from grapple and strikes canister.

Operator Activates Grapple Disengagement Switch Prematurely—Once engaged with the lid, the grapple is supposed to remain engaged until the lid is placed in its staging area. The operator could prematurely activate grapple disengagement for one of two reasons. Either the wrong control could be activated (e.g., while closing the port slide gate), or a number of operational steps could be skipped and the operator could actuate the control.

This is a straightforward case of taking an action out of sequence. This can be represented by CREAM CFF E4, adjusted by the following CPCs with values not equal to 1.0:

- CFF E4: Action performed out of sequence (e.g., repetitions, jumps, reversals). The baseline HEP is 0.003.
- CPC “Working Conditions”: With regard to this potential unsafe action, the working conditions for the CTM operator are deemed to be advantageous. The CPC for an execution task with advantageous working conditions is 0.8.
- CPC “Adequacy of Training/Preparation”: This routine action is well trained and performed often. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

Operator activates grapple disengagement switch prematurely

$$=0.003 \times 0.8 \times 0.8 = 0.002$$

Load Cell Disengagement Interlock Fails—One of the load cell interlocks is designed to disable the grapple disengagement circuit if a load is sensed. This interlock would have to fail in order for the operator’s action to trigger the disengagement mechanism.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

$$\text{Load cell disengagement interlock fails} = 2.7E-5$$

Lid Drops from Grapple and Strikes Canister—In order for the lid to actually drop, the grapple disengagement mechanism would need to overcome the dead weight friction caused by the weight of the lid. In the case of the canister, this is clearly expected to be true, but the lid weighs much less than the canister; thus, the same expectation is not clear. However, there is still a chance that the grapple would not disengage or would not disengage while the lid is over the open cask port.

There are a number of factors that affect the likelihood of this event. First, in order to strike the canister the disengagement must occur over the canister, including that the slide gates are open. Second, the design of the grapple is such that it may not have the force to disengage when it is loaded (this is certainly true when lifting a canister, but perhaps less so when lifting a lid). Finally, the lid has to fall in an orientation such that it strikes the canister. Taking this all into consideration, the HRA team judges that it is justifiable to assign a 10% chance that this event would occur.

$$\text{Lid drops from grapple and strikes canister} = 0.1$$

HEP Calculation for Scenario 1(e)—The events in the HEP model for Scenario 1(e) are presented in Table E6.5-8.

Table E6.5-8. HEP Model for HFE Group #5 Scenario 1(e) for 060-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator activates grapple disengagement switch prematurely	0.002
B	Load cell disengagement interlock fails	2.7E-5
C	Lid drops from grapple and strikes canister	0.1

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.002 \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-14})$$

E6.5.3.4.2.6 HEP for HFE 060-OpCTMdrop001-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for lifting a lid off a transportation cask or aging overpack follows:

$$\begin{aligned} &060\text{-OpCTMdrop001-HFI-COD (lid lift)} = \\ &\text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(c)} + \text{HFE 1(d)} + \text{HFE 1(e)} = \\ &(<1\text{E-8}) + 1\text{E-7} + (<1\text{E-8}) + (<1\text{E-8}) + (<1\text{E-8}) = 2\text{E-7} \end{aligned} \quad (\text{Eq. E-15})$$

The Boolean expression for the overall HFE (all scenarios) for placing an inner lid on a waste package or a lid on an aging overpack follows:

$$\begin{aligned} &060\text{-OpCTMdrop001-HFI-COD (lid placement)} = \\ &\text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(e)} = \\ &2\text{E-8} + 1\text{E-7} + (<1\text{E-8}) = 2\text{E-7} \end{aligned} \quad (\text{Eq. E-16})$$

Except for DPCs, which only have a lid placement, all canisters have one lid lift and one lid placement as part of their processing. For simplicity, DPCs were conservatively modeled the same as other canisters, and the Boolean expression for the overall HFE for a lid lift and a lid placement follows:

$$\begin{aligned} &060\text{-OpCTMdrop001-HFI-COD (total)} = 060\text{-OpCTMdrop001-HFI-COD (lid lift)} \\ &+ 060\text{-OpCTMdrop001-HFI-COD (lid placement)} = 2\text{E-7} + 2\text{E-7} = 4\text{E-7} \end{aligned} \quad (\text{Eq. E-17})$$

E6.5.3.4.3 Quantification of HFE Scenarios for 060-OpCTMdrop002-HFI-COD: Operator Causes Drop of Canister during CTM Operations

E6.5.3.4.3.1 HFE Group #5 Scenario 2(a) for 060-OpCTMdrop002-HFI-COD

1. Crew member improperly installs grapple.
2. Primary grapple interlock gives false positive signal.
3. Operator fails to notice bad connection between hoist and grapple through camera.
4. Grapple/canister drops from hoist.

Crew Member Improperly Installs Grapple—Prior to a lift operation, a crew member prepares the CTM for the operation by installing the appropriate grapple for the type of canister to be processed. While it is possible that this operation does not need to be performed (it may be the same grapple as for the cask lid), it is uncertain how often this occurs, so this analysis considers that this action needs to be performed each time. The crew member can improperly secure the grapple to the hoist. This makes the grapple appear to be secured in place when it is not.

This is a straightforward matter of task execution. The task is simple and routine and can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well-designed, highly practiced routine task performed to the highest possible standards by highly motivated, highly trained, and experienced

person, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 3: Time pressure. The full affect EPC would be $\times 11$, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure, so the APOA is set at 0.2.
- EPC 8: Poor environment. This EPC is applied not so much that the environment is poor, but rather that it is simply not optimal. The full affect EPC would be $\times 8$, but this applies when working on the plant, with suit and breathing apparatus, possible access problems, and for more than 45 minutes so that fatigue sets in. The APOA anchor for 0.1 is for work in the plant with suit and breathing apparatus, but none of the other environmental stressors. In this task no breathing apparatus is required, but it is somewhat physically demanding. Given the tradeoffs, the APOA is set at 0.1.
- EPC 13: Operator underload/boredom. The full affect EPC would be $\times 3$, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\begin{aligned} &\text{Crew member improperly installs grapple} = \\ &0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006 \quad (\text{Eq. E-18}) \end{aligned}$$

Preoperational Check Fails to Note Improper Installation—There are two crew members responsible for preparing the CTM for each operation. The second crew member checks the first crew member’s installation of the grapple, which provides an opportunity for the error to be detected. The second crew member also has activities to perform, and so checking the first crew member is a secondary function. In addition, the existence of the grapple/hoist interlock provides an expectation that any error can be detected.

For the action being analyzed, the second crew member has helped initially with the connection of the grapple to line it up but then moves on to other things. At best, the second crew member performs a cursory check at the end of the job. Since the crew member was involved in the early stages, there is a bias that the job was done correctly. It is concluded that the level of dependence is high. The baseline HEP for the checking, for checking routine tasks without a checklist is best determined from THERP (Ref. E8.1.26), Table 20-22, item (2), which is 0.2 (Ref. E8.1.26). The HEP adjusted for high dependence is from THERP (Table 20-21, item (4)(e)), which is 0.6.

$$\text{Preoperational check fails to note improper installation} = 0.6$$

Grapple Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the primary grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

$$\text{Grapple interlock gives false positive signal} = 2.7E-5$$

Operator Fails to Notice Bad Connection between Hoist and Grapple through Camera—When the CTM operator is in the process of lifting the canister, the view through the camera shows the grapple and its connection to the hoist. The operator is not focused on that connection while lining up the grapple with the lifting device. However, as the lift begins, the operator is supposed to watch through the cameras. This gives the operator the opportunity to note that the grapple is not properly connected (e.g., unexpected canister movement to one side or tilting of the grapple). This is an opportunity to question the stability of the connection and to lower the canister back down to recheck the connection. However, the operator does not expect any problems in this operation and tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

This action is best represented by the CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made. The baseline HEP is 0.003.
- CPC “Adequacy of Man–Machine Interface”: For this particular observation, the use of a camera view (while the only practical means) is somewhere between tolerable and inappropriate. The CPC for an observation task with tolerable man–machine interface is 1.0, and for inappropriate is 5.0. With regard to being able to actually observe the condition of the grapple lock pin, the CPC is set as 4.0.
- CPC “Number of Simultaneous Goals”: The operator is primarily focusing on properly aligning the bell and hoist, opening the ports, and grappling the lid. While it could be argued that this is not “more than capacity,” it certainly relegates looking at the grapple/hoist connection to a secondary action. It is therefore deemed appropriate to apply the more than capacity CPC, which is 2.0.
- CPC “Adequacy of Training/Preparation”: Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

$$\begin{aligned} \text{Operator fails to notice bad connection between hoist and grapple through} &= \\ 0.003 \times 4 \times 2 \times 0.8 &= 0.02 \end{aligned}$$

Grapple/Canister Drops from Hoist—Just because the lift is occurring with an improper grapple installation does not mean that the lid and grapple fall. The design safety margins built

into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation.

This event is quantified in Section E6.5.3.4.1.

$$\text{Grapple/canister drops from hoist} = 0.25$$

HEP Calculation for Scenario 2(a)—The events in the HEP model for Scenario 2(a) are presented in Table E6.5-9.

Table E6.5-9. HEP Model for HFE Group #5 Scenario 2(a) for 060-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	Crew member improperly installs grapple	0.0006
B	Preoperational check fails to note improper installation	0.6
C	Grapple interlock gives false positive signal	2.7E-5
D	Operator fails to notice bad connection between hoist and grapple through camera	0.02
E	Grapple/canister drops from hoist	0.25

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E-5 \times 0.02 \times 0.25 < 1E-8 \quad (\text{Eq. E-19})$$

E6.5.3.4.3.2 HFE Group #5 Scenario 2(b) for 060-OpCTMdrop002-HFI-COD

1. Operator fails to fully engage grapple.
2. Grapple engagement interlock gives false positive signal.
3. Operator fails to notice grapple not fully engaged through camera.
4. Canister drops from grapple.

CTM Operator Fails to Fully Engage Grapple—The operator engages the grapple from the control panel. The grapple can be roughly positioned using the alignment guides for the CTM and the hoist height indicator on the control panel, but final alignment must be done visually using the view from the cameras provided on the grapple. Once the operator believes the grapple is aligned, the operator engages the grapple with the lift fixture and confirms through the camera. If the operator sees that the grapple has not properly engaged, then the operator disengages and repositions the grapple and tries again to engage.

In this task, the operator aligns the grapple visually using the camera view and then engages the grapple. If it is not aligned properly, it does not fully engage. This unsafe action can be best represented by the task execution error NARA GTT A1, adjusted by the following CPCs:

- NARA GTT A1: Carry out a simple manual task with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005

- EPC 3: Time pressure. The full affect EPC would be $\times 11$, but this applies only in cases where there is barely enough time to complete a task and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.
- EPC 11: Poor, ambiguous or ill-matched system feedback. This EPC is applied to account for the need to observe the operation through cameras. The full affect EPC would be $\times 4$. The full effect is applicable when legibility is poor or label is obscured, or where the layout of controls makes visual access and physical access difficult. The use of camera view is deemed to represent full effect. The APOA is set at 1.0.
- EPC 13: Operator underload/boredom. The full affect EPC would be $\times 3$, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\begin{aligned} &\text{Operator fails to fully engage grapple} = \\ &0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad (\text{Eq. E-20}) \end{aligned}$$

Grapple Engagement Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

$$\text{Grapple engagement interlock gives false positive signal} = 2.7\text{E-}5$$

CTM Operator Fails to Notice Grapple Not Fully Engaged through Camera—As the lift begins, the operator is supposed to watch through the cameras. This gives the operator the opportunity to note that the grapple is not properly engaged (e.g., unexpected canister movement to one side or tilting of the grapple), which allows the operator the opportunity to question the stability of the connection and to lower the canister back down to recheck the connection. However, the operator does not expect any problems in this operation and tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

In this case, the operator's check is a self-check, again through the camera. The CTM operator believes that the correct action was performed initially, and this was confirmed by the false positive from the interlock, so this observation is deemed completely dependent on the prior

actions. Using THERP (Ref. E8.1.26) Table 20-21 (Ref. E8.1.26) to assess dependency, item (5) for complete dependency:

Operator fails to notice grapple not fully engaged through camera = 1.0

Canister Drops from Grapple—Just because the lift is occurring with an improper grapple engagement does not mean that the canister falls. The safety margins built into these systems mean that it is possible that the lift and place are completed successfully even with improper installation.

This event is quantified in Section E6.5.3.4.1.

Canister drops from grapple = 0.25

HEP Calculation for Scenario 2(b)—The events in the HEP model for Scenario 2(b) are presented in Table E6.5-10.

Table E6.5-10. HEP Model for HFE Group #5 Scenario 2(b) for 060-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	Operator fails to fully engage grapple	0.07
B	Grapple engagement interlock gives false positive signal	2.7E-5
C	Operator fails to notice grapple not fully engaged through camera	1.0
D	Canister drops from grapple	0.25

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D = 0.07 \times 2.7E-5 \times 1.0 \times 0.25 = 5E-7 \quad (\text{Eq. E-21})$$

E6.5.3.4.3.3 HFE Group #5 Scenario 2(c) for 060-OpCTMdrop002-HFI-COD (Applies to DPC/Transportation Cask Only)

1. CTT is not sufficiently centered under port.
2. Operator fails to notice CTT not sufficiently centered.
3. Operator fails to notice DPC contacting ceiling and continues lift OR operator “locks” lift button into position.
4. Load cell overload interlock fails.
5. Mechanical failure of hoist under overload causes DPC drop. (NOTE: This scenario only applies to DPCs because the transportation cask lid was removed in the preparation area).

CTT Is Not Sufficiently Centered under Port—This unsafe action actually occurs prior to this operation, during movement of the CTT into the Cask Unloading Room. The CTT operator brings the unit into the Cask Unloading Room and locates it centered directly under the cask port by aligning it against end stops that properly locate it and by using markings on the floor. If the cask is not properly centered, it is possible that the DPC could strike the ceiling around the cask port rather than rising smoothly through the cask port. This only applies to DPCs because their transportation cask lids are removed in the preparation area. For all other waste forms any misalignment would be discovered during the lid lift by the CTM. In order for the DPC to hit the Cask Unloading Room ceiling during lift, the cask would have to be off-center by more at least a few feet.

The unsafe action results from stopping the CTT prematurely and leaving it at least a number of feet short of the proper location. This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.
- CPC “Available Time”: There is adequate time to perform this task. The only time pressure is the desire to keep the process moving, but the consequences are insignificant. The CPC for an execution task with adequate time is 0.5.
- CPC “Adequacy of Training/Preparation”: This routine task is well trained and practiced and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.

The above parameters were the same as those applied to failure to properly center the CTT for a lid, where only being about a foot or two out of position could cause a problem. For the case of a canister, the miss must be by at least a few feet in order for the canister to strike the ceiling on the way up. The HRA team believes it is inappropriate to apply the same number to both unsafe actions, and deems it reasonable to further reduce the HEP for the unsafe action by a factor of two to account for this (a multiplier of 0.5).

Applying these factors yields the following:

$$\begin{aligned} \text{CTT is not sufficiently centered under port (DPC/transportation cask)} = \\ 0.003 \times 0.5 \times 0.8 \times 0.5 = 0.001 \end{aligned}$$

Operator Fails to Notice that CTT Is Not Sufficiently Centered—The CTM operator centers the CTM grapple over the cask lid lift fixture using a two-step process. First the CTM operator does a rough alignment using the bridge and trolley position indicators and sets the bell and shield skirt in place. Then the operator opens the cask port and performs a fine alignment using a camera alignment system. The operator is not looking for perfect alignment but would expect it to be close. At this point, the operator would have the opportunity to question the amount of distance needed to move the hoist into position. Possible responses include: (1) the position is not off by much, (2) the initial placement of the bell is in question and it is repositioned (which

may be easier to accomplish than asking another crew member to move the CTT), or (3) a belief that the position of the CTT is not off center by enough to make a difference.

In this task, the CTM operator roughly centers the CTM over the cask port, lowers the shield, and opens the port and CTM gates. The operator needs to more accurately locate the grapple over the lid by moving the hoist within the bell. At this point, the operator has an opportunity to judge if the amount of movement required to align the grapple is too much for the lid to clear the edges of the port during the lift. In this case, it is not so much an observation error (the operator can't help but observe the relative locations of the grapple and lid) or a diagnosis error (the operator knows the canister is not perfectly centered), but rather a decision error, where the operator decides that it doesn't matter that the cask is not centered (it's "close enough"). This can be represented by CREAM CFF I2, adjusted by the following CPCs with values not equal to 1.0.

- CFF I2: Decision error (either not making a decision or making a wrong or incomplete decision). The baseline HEP is 0.01.
- CPC "Available Time": With regard to the general level of time pressure for the task and the situation type, it would be easy to believe that there is adequate time since the consequences of taking more time are (from a safety perspective) insignificant. However, from a production perspective, this would be a significant setback since the CTM operator would have to get the CTT crew back to move the CTT, a time-consuming process. This time pressure could bias the operator towards a decision that "it's close enough." The CPC for an interpretation task with continuously inadequate available time is 5.0.

Applying these factors yields the following:

Operator fails to notice that CTT is not sufficiently centered = $0.01 \times 5 = 0.05$

Operator Fails to Notice DPC Contacting Ceiling and Continues Lift—The CTM operator is able to see the DPC through the camera display. When the DPC strikes the ceiling, it will stop as the hoist continues to try to rise. The operator has an opportunity to notice the stopped CTM before it stops the lift. The prior unsafe action of failing to notice that the cask is too far off center could lead the operator to be somewhat more careful and observant during the lift than if it had been closer to center (e.g., like the extra care a driver might show while pulling into a narrower than normal parking space).

If the operator is looking at the camera view during the lift, there is an opportunity to observe the DPC contacting the ceiling of the Cask Unloading Room and stopping rather than rising straight through. The most likely failure is not looking at the screen at the time this occurs, which can be represented by CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made (omission). The baseline HEP is 0.003.
- CPC "Adequacy of Man-Machine Interface": There are two vulnerabilities in the man-machine interface for this observation. First, there is no alarm or indicator to alert

the operator. Second, the camera view is not perfect. These are inherent to this type of operation, but would make it more likely that the operator would not be looking at the screen at the time. Thus, the man-machine interface could be considered inappropriate with regard to success of this observation (as it was for scenario 1(e)). However, the fact that the magnitude of the CTT offset required to cause a problem is so much greater in this case argues for a somewhat lesser adjustment. That is, the man-machine interface is somewhat better with regard to this failure, and it is more likely that the operator is looking and sees the contact. The CPC for an observation task with inappropriate man-machine interface is 5.0. The HRA team has determined that a CPC of 3.0 is more appropriate in this case.

Applying these factors yields the following:

$$\text{Operator fails to notice DPC contacting ceiling and continues lift} = 0.003 \times 3 = 0.01$$

Operator “Locks” Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to “lock” the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the action would not be perceived as unsafe but rather as a clever way to free time to get ready for subsequent steps or perform other duties. Again, the operator might be less likely to do this if there are doubts about the positioning of the cask.

The quantification of this event is discussed in detail under Scenario 1(c). In this scenario, it is judged that there is no bias dependency towards this failure that results from prior failures in the scenario. Therefore, the value used for the non-bias case (0.05) could be applied here. However, similar to the previous discussion, the HRA team believes that the magnitude of the CTT offset required to cause a problem actually creates a bias in the operator against taking any shortcuts (as opposed to no bias), so that a further reduction of 0.5 should be applied.

$$\text{Operator “locks” lift button into place} = 0.05 \times 0.5 = 0.03$$

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the DPC in contact with the ceiling would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

$$\text{Load cell interlock fails} = 2.7E-5$$

Mechanical Failure of Hoist under Overload Causes DPC Drop—There are three potential failure modes that could cause the canister to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the

grapple or DPC. However, just because the hoist keeps pulling does not mean that the DPC falls (the hoist motor could overload and fail before the DPC becomes detached from the hoist).

This event is quantified in Section E6.5.3.4.1.

Mechanical failure of hoist under overload causes DPC drop = 0.25

HEP Calculation for Scenario 2(c)—The events in the HEP model for Scenario 2(c) are presented in Table E6.5-11.

Table E6.5-11. HEP Model for HFE Group #5 Scenario 2(c) for 060-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	CTT is not sufficiently centered under port	0.001
B	Operator fails to notice CTT not sufficiently centered	0.05
C	Operator fails to notice DPC contacting ceiling and continues lift	0.01
D	Operator "locks" lift button into position	0.03
E	Load cell overload interlock fails	2.7E-5
F	Mechanical failure of hoist under overload causes DPC drop	0.25

NOTE: CTT = cask transfer trolley; DPC = dual-purpose canister; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times (C + D) \times E \times F = 0.001 \times 0.05 \times (0.01 + 0.03) \times 2.7E-5 \times 0.25 < 1E-8 \quad (\text{Eq. E-22})$$

E6.5.3.4.3.4 HEP for HFE 060-OpCTMdrop002-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for lifting a DPC/transportation cask follows:

$$060\text{-OpCTMdrop002-HFI-COD (DPC/TC)} = \text{HFE 2(a)} + \text{HFE 2(b)} + \text{HFE 2(c)} = (<1E-8) + 5E-7 + (<1E-8) = 5E-7 \quad (\text{Eq. E-23})$$

The Boolean expression for the overall HFE (all scenarios) for lifting all other canisters follows:

$$060\text{-OpCTMdrop002-HFI-COD (non-DPC/TC)} = \text{HFE 2(a)} + \text{HFE 2(b)} = (<1E-8) + 5E-7 + (<1E-8) = 5E-7 \quad (\text{Eq. E-24})$$

E6.5.3.4.4 Quantification of HFE Scenarios for 060-OpCTMImpact1-HFI-COD: Operator Moves the CTM while Canister or Object Is Below or Between Levels

E6.5.3.4.4.1 HFE Group #5 Scenario 3(a) for 060-OpCTMImpact1-HFI-COD

1. Operator leaves CTM in lid lift mode (non-DPCs).
2. Operator fails to notice that lift stops too soon.

3. Operator fails to close port slide gate OR fails to notice that it does not fully close.
4. Operator fails to close CTM slide gate OR fails to notice it does not fully close.
5. CTM slide gate interlock fails.

Operator Leaves CTM in Lid Lift Mode (Non-DPCs)—The operator is supposed to set the ASD to canister lift mode prior to lifting the canister. It should be in lid lift mode because the lid was lifted right before the canister. Failing to reset for a canister lift would result in the canister stopping part way through the port.

Setting the CTM system to the appropriate lift mode prior to performing a lift is fundamental to the operation, not simply a step in a procedure that can be missed. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in lid lift mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3, adjusted by the following EPCs.

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves CTM in lid lift mode = 0.0007

Operator Fails to Notice that Lift Stops too Soon—Lifting the canister takes on the order of ten minutes, whereas lifting the lid takes only on the order of three minutes. Since the operator has to hold the lift button in or the lift stops, there is an opportunity to notice that the hoist has stopped sooner than expected. On the control panel the operator would have the camera view and also the hoist position indication, either of which can confirm that the canister has not been fully lifted. Failure to do so would result in continuing the operations with the canister between floors.

The operator is supposed to hold the lift button until the lift automatically stops. The operator has performed this operation many times in the past and has an instinctive feel for how long the lift takes. A canister lift should take around three times as long as a lid lift. If the operator feels it has not taken long enough, the camera and the indicators on the control panel can provide confirmation that the lift was prematurely terminated. Failing to recognize the short lift (and thus an implied failure to question the result of the action) could be an observation error (CREAM CFF O2, wrong identification made, or O3, observation not made). But the more conservative and more applicable approach is represented by the interpretation error CREAM CFF I1, adjusted by the following CPCs with values not equal to 1.0:

- CFF I1: Faulty diagnosis (either a wrong diagnosis or an incomplete diagnosis). The baseline HEP is 0.2.
- CPC “Working Conditions”: The operator has optimal working conditions in the control room. The CPC for an interpretation task with advantageous working conditions is 0.8.

- CPC “Available Time”: The operator clearly has adequate time before beginning the next steps in the process to realize that the amount of time spent in the lift is not reasonable for a canister lift. The CPC for an interpretation task with adequate available time is 0.5.
- CPC “Adequacy of Training/Preparation”: Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to notice lift is taking too long} = 0.2 \times 0.8 \times 0.5 \times 0.8 = 0.07$$

Operator Fails to Close Port Slide Gate—The operator is supposed to close the port slide gate as soon as the lift is completed. This gives the operator an opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the canister). In the latter case, the slide gate open/close indicator lights are in an incorrect state (either both on or both off, depending on design).

The operator is supposed to close the port slide gate prior as a part of the lift and transfer process. This is an EOO that can most closely be represented by CREAM CFF E5, adjusted by the following CPCs with values not equal to 1.0:

- CFF E5: Action missed, not performed (omission), including the omission of the last actions in a series. The baseline HEP is 0.03.
- CPC “Available Time”: There is adequate time available. The CPC for an execution task with adequate time is 0.5.
- CPC “Adequacy of Training/Preparation”: Training is adequate with high experience. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to close port slide gate} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—The action of closing the port slide gate is simple. In this scenario, the gate does not close all the way because the canister is in the way. The operator has visible feedback on the failure of the gate to close because the “open” (or “green”) light on the control panel stays on and the “closed” (or “red”) light also comes on and stays on. Both lights on at the same time signifies that the port is neither fully open nor fully closed. The problem can be easily confirmed by looking at the camera or checking the status of the light curtain at the bottom of the bell. This unsafe action can be represented by NARA GTT C1, adjusted by the following EPCs.

- GTT C1: Simple response to a range of alarms/indications providing clear indication of situation (simple diagnosis required). The baseline HEP is 0.0004.

- EPC 3: Time pressure. The full affect EPC would be $\times 11$, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. This appears reasonable for this task, so the APOA is set at 0.1.
- EPC 13: Operator underload/boredom. The full affect EPC would be $\times 3$, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\begin{aligned} &\text{Operator fails to notice that port slide gate does not fully close} \\ &= 0.0004 \times [(11-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.001 \quad (\text{Eq. E-25}) \end{aligned}$$

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the CTM slide gate as soon as the port slide gate is closed. This gives the operator another opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the hoist cables or load cell). In the latter case, the slide gate open/close indicator lights would be an incorrect state (either both on or both off, depending on design).

The baseline HEP for failure to close this gate would be the same as for the similar unsafe action for the port slide gate.

$$\text{Operator fails to close CTM slide gate (independent)} = 0.01$$

However, this would only apply in the case where the earlier unsafe action was failure to notice that the port slide gate had failed to close. In the case where the earlier unsafe action was failure to close the port slide gate, there is a dependence on the failure to perform a similar task next in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP (Ref. E8.1.26) Table 20-21, the HEP follows:

$$\text{Operator fails to close CTM slide gate (given failure to close the port slide gate)} = 0.5$$

Operator Fails to Notice CTM Slide Gate Does Not Fully Close—The baseline HEP for failure to notice that this gate did not fully close would be the same as for the similar unsafe action for the port slide gate.

$$\text{Operator fails to notice CTM slide gate does not fully close (independent)} = 0.001$$

However, this would only apply in the case where the earlier unsafe action was failure to close the port slide gate. In the case where the earlier unsafe action was failure to notice that the port slide gate did not fully close, there is a dependence on the failure to perform a similar task next

in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP (Ref. E8.1.26) Table 20-21, the HEP follows:

Operator fails to notice CTM slide gate does not fully close
(given failure notice that port slide gate did not fully close) = 0.5

CTM Slide Gate Interlock Fails—The CTM slide gate interlock prevents CTM movement with the slide gate open (the shield skirt cannot be raised). If the interlock itself fails, the operator can move the CTM with the canister between levels.

This is a mechanical failure of the interlock. This event is quantified in Section E6.5.3.4.1.

CTM slide gate interlock fails = $2.7E-5$

HEP Calculation for Scenario 3(a)—The events in the HEP model for Scenario 3(a) are presented in Table E6.5-12.