

- Determine what equipment is impacted by test and maintenance activities.

For human-induced initiator and post-initiator HFEs, such information is needed to:

- Identify important operator tasks
- Identify the specific actions required for each operator task
- Identify the procedures (e.g., normal operating and emergency operating procedures) and procedure steps associated with each operator task
- Identify the cues (e.g., procedure steps, alarms) for operator tasks
- Assess the procedures that support operator tasks as PSFs
- Assess the training that supports operator tasks as PSFs.

#### **E4.1.2 Industry Data Reviewed by the HRA Team**

Due to the unique nature of the activities and equipment associated with subsurface operations, no industry data was available for review. Rather, the HRA team had to rely upon extensive discussion with subject matter experts to gain insights into failure modes and important contexts for subsurface operations (Section E4.2.2).

### **E4.2 USE OF EXPERTS AND ENGINEERING JUDGMENT IN THE HRA**

Subject matter experts were employed in the identification, verification, preliminary analysis, and detailed analysis of HFEs. Identification of HFEs, of which a HAZOP evaluation was a part, was performed as a combined effort by experts from a wide range of areas. This identification was not specifically a part of the HRA task, but it was used by the HRA team in the process of identifying HFEs. A description of the HAZOP evaluation process and a list of experts who specifically participated in the HAZOP evaluation are provided in the *Subsurface Operations Event Sequence Development Analysis* (Ref. E8.1.6).

#### **E4.2.1 Role of HRA Team Judgment**

The preliminary analysis primarily performed by the HRA team in a consensus-based process follows:

- Each HFE that was identified during the HAZOP evaluation and the operational experience review was characterized with input from the Engineering and Operations departments, including the context under which the HFE would occur.
- Once the individual members of the HRA team were confident that they understood the HFE and the context, they each independently assigned an HEP to the HFE and briefly documented the rationale relative to a set of anchor points established for the HRA (the basic anchor points can be found in Appendix E.III of this analysis).

- The values and rationales were combined into a single spreadsheet, and the HRA team then met to discuss their values.
- The HRA team used their knowledge of the preclosure process and design to develop a consensus on the factors affecting the HFE and a resulting conservative estimate of the HEP. In most cases, the HRA team ultimately reached a consensus on a value and a rationale. In a few cases a consensus could not be reached, and the most conservative value and rationale from that team member was used. The value and rationale applied was then documented.

This process is explained in much greater detail in Appendix E.III of this analysis.

As shown in Section E6, no HFEs requiring detailed analysis have been identified for subsurface operations event sequence and categorization analysis. Therefore, the judgment process associated with detailed quantification is not relevant in this case.

#### **E4.2.1.1 HRA Team**

**Paul J. Amico**—Mr. Amico is a nuclear engineer with 30 years of experience in risk, safety, regulation, and operation of NPPs, nuclear material production reactors, nuclear weapons research, production and storage facilities, nuclear fuel cycle facilities, chemical demilitarization facilities, and industrial chemical plants. He has been involved in the conduct and review of HRA since 1979. His experience includes the use of THERP, Time-Reliability Correlation (TRC), Systematic Human Action Reliability Procedure, Human Cognitive Reliability (HCR), HEART, ATHEANA, CREAM and NARA, and he has been involved in projects related to methodology enhancements to some of these techniques. Prior to joining the YMP, he was involved in HRA for a number of NPP PRAs in the United States and overseas; for chemical process plants; and for SNF handling and storage at NPPs, including the development of project procedures for HRA. He developed a phased approach to the use of HRA during the design process of advanced NPPs and supported a project to expand HRA techniques for SNF handling operations.

**Erin P. Collins**—Ms. Collins is a risk analyst with over 20 years of experience in safety, reliability, and risk analysis for the U.S. Army chemical weapons destruction program, National Aeronautics and Space Administration, the Federal Aviation Administration, NPPs, and the chemical process industry. Her specialties are equipment reliability database development and HRA. Ms. Collins was a prime participant in a safety hazard analysis of an acrylic fiber spinning facility in northeastern Italy. This analysis evaluated worker risk in various areas of the facility through the use of hazard analysis techniques, including a HAZOP evaluation, and resulted in the recommendation of economical risk reduction measures. Her project experience in Spain includes technical review and support of the HRAs for the Ascó and the Santa Maria de Garoña nuclear plant PRAs. She also supported the review of the Kola and Novovoronezh Russian nuclear reactor HRAs for the U.S. Department of Energy. In the United States, Ms. Collins has participated in PRA-related HRAs of the Hanford N Reactor and the Robinson (using simulator exercises), Crystal River 3, and Catawba NPPs. Throughout these efforts, she has applied the HEART, CREAM, THERP, and TRC methods of quantification.

**Douglas D. Orvis, Ph.D.**—Dr. Orvis is a registered professional engineer (California, Nuclear No. 0925) with over 35 years of experience in nuclear engineering, regulation, and risk analysis of NPPs, alternative concepts for interim storage of SNF, and aerospace applications. Dr. Orvis has participated in the development of HRA techniques (e.g., Systematic Human Action Reliability Procedure for Electric Power Research Institute (EPRI), effects of organizational factors for the NRC) and has measured and analyzed data for evaluating the reliability of NPP control room operators during simulated accidents. These data-based analyses included the EPRI-sponsored operator reliability experiments (e.g., measurements performed at the Diablo Canyon, Kewaunee, and LaSalle simulators) and the follow-on programs performed at the Maanshan (Taiwan) simulator. Data collection and analysis included observing operator behavior, variability between crews, developing time-response correlations for key operator actions, and evaluating the numbers and kinds of errors and deviations committed. Postsimulation interviews with crew members and trainers were conducted to elicit information on conditions and factors that contributed to crew performance. The data analysis included comparisons of data to the HCR model and a statistical evaluation of the types and causes of errors and deviations. A similar data collection evaluated the efficacy of an expert system called the Emergency Operating Procedures Tracking System.

Dr. Orvis participated in a comprehensive review of HRA methods for a Swiss agency and was a consultant to the International Atomic Energy Agency to incorporate concepts of HRA and organizational factors into (Assessment of the Safety Culture in Organizations Team) guidelines for plant self-assessment of safety culture. Dr. Orvis has performed event tree and fault tree analyses of hazardous systems for both internal events and seismic initiators that included consideration of HRA. Dr. Orvis has participated in HAZOP evaluation sessions for repository operations.

**Mary R. Presley**—Ms. Presley is an engineer with 3 years of experience in risk analysis for NPPs, specializing in human reliability. Ms. Presley graduated in 2006 from the Massachusetts Institute of Technology with her M.S. in nuclear engineering, where she wrote her thesis *On the Assessment of Human Error Probabilities for Post Initiating Events*, which included an extensive review of current HRA methods. While her work focused on the EPRI HRA calculator and the NRC ATHEANA framework, she is also familiar with other HRA methods, including THERP, Accident Sequence Evaluation Program, HEART, NARA, Failure Likelihood Index Methodology, Success Likelihood Index Method/Multi-Attribute Utility Decomposition, Standardized Plant Analysis Risk Human Reliability Analysis, CREAM, Methode d’Evaluation de la Relisation des Missions Operateur pour la Surete, Cause-Based Decision Tree, and HCR/operator reliability experiments.

#### **E4.2.2 Role of Subject Matter Expert Judgment**

Subject matter experts were also consulted during the compilation of the base case scenarios. The outline of the base case scenarios came from the mechanical handling block flow diagram. The details of human interaction with the mechanical systems were derived from expected operations inferred directly from the design by the subject matter experts. Where a detailed design was not available, the experts extrapolated these details from common industry practice for similar operations. These experts come from the YMP Engineering, Operations, and PCSA groups, as well as from outside the YMP project.

In addition to the development of base case scenarios, subject matter experts were regularly consulted during the analysis to provide clarification of design, clarification of expected operations, and insight into expected operating conditions and failure modes. These experts provided details about the design of systems that were relevant to human performance, such as the presence of job aids and interlocks and the intended design of control system interfaces. They also provided details regarding the concept of operations for the processes, such as the role of the humans versus the use of automatic systems, the operational controls, and the use of procedures. These experts would also review specific parts of the analysis for technical accuracy.

Following is a list of some areas where subject matter experts were consulted during the HRA for their expertise:

- PCSA models (i.e., facility or system fault trees)
- Radiation protection (e.g., cask shielding/shield rings; locks, interlocks, and procedural controls for entering high radiation areas and drifts)
- General facility (including aging pad and emplacement drifts) layout and time line of operations
- Interlocks (general)
- TEV design and operations
- Drip shield gantry design and operations
- Emplacement drift and portal gate security equipment (e.g., cameras), procedures and staffing
- Safety features of rail crossings with site roadways
- Emplacement procedures, calculations, and accountability
- Other systems.

## **E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES**

Over the history of performance of HRAs, certain terminology has become commonplace and different classification schemes for human error has been developed. This section provides a background of this terminology and associates it to the YMP PCSA HRA. In addition, the description of operations includes references to different types of personnel. The functions of each classification of personnel are described in this section. Finally, a discussion is provided of the specific issues that relate to human performance at the YMP.

## **E5.1 TERMINOLOGY**

### **E5.1.1 Classification of HFEs**

As noted in the methodology (Section E3.2), HFEs are classified to support the HRA preliminary analysis, selection of HRA quantification methods, and detailed quantification. A combination of four classification schemes is used in the YMP HRA. The first three schemes are familiar standards in HRA. The fourth scheme has its basis in behavioral science and has been used in some second-generation HRA methods.<sup>5</sup>

The four classification schemes are based on the following:

1. The three temporal phases used in PRA modeling:
  - A. Pre-initiator
  - B. Human-induced initiator
  - C. Post-initiator.
2. Error modes:
  - A. EOOs
  - B. EOCs.
3. Human failure types:
  - A. Slips/lapses
  - B. Mistakes.
4. Informational processing failures:
  - A. Monitoring and detection
  - B. Situation awareness
  - C. Response planning
  - D. Response implementation.

The following sections define these classification methods.

#### **E5.1.1.1 Temporal Phases of HFEs**

There are three temporal phases of HFEs:

---

<sup>5</sup>There is another classification not included here that has been often used in nuclear power plant PRAs: the behavior type taxonomy. This category classifies HFEs into skill-, rule-, or knowledge-type behavior. While this taxonomy has limited usefulness in addressing HFEs that take place in an NPP control room under time constraints, this distinction is not particularly useful for other types of actions. As a result, it is generally not used for HRAs in such applications as chemical process facilities, chemical demilitarization facilities, or NASA manned-mission risk assessments. Given the type of human actions and HFEs that are important at the YMP, use of this approach for the YMP PCSA HRA is not recommended.

- Pre-Initiator HFE—An HFE that represents actions taken before the initiating event that causes systems or equipment to be unavailable. Examples of such HFEs are miscalibration of equipment or failure to restore equipment to an operable state after testing or maintenance activities.
- Human-Induced Initiator—An HFE that represents actions that cause or lead to an initiating event.
- Post-Initiator HFE<sup>6</sup>—A post-initiator HFE represents those operator failures to manually actuate or manipulate systems or equipment, as required for accident response. Post-initiator HFEs can be further divided into recovery and non-recovery events.
  - A non-recovery post-initiator HFE (i.e., failure during response to an initiator) is when an operator does not operate frontline equipment in accordance with required procedural actions due to errors in diagnosis or implementation. For quantification purposes, these HFEs are usually decomposed into cognitive and implementation parts, as shown in Appendix E.II of this analysis. In general, post-initiator HFEs associated with such actions are incorporated directly in the model prior to initial PRA quantification using preliminary values. The results of the initial event sequence quantification are used to determine if detailed modeling of these HFEs is needed.
  - A recovery post-initiator HFE represents operator failure to manually actuate or manipulate frontline equipment (or alternatives to frontline equipment<sup>7</sup>) that has failed to automatically actuate as required. In general, post-initiator HFEs associated with correction or recovery of failed frontline systems from either equipment or human failures are not modeled until after initial PRA quantification. The results of initial event sequence quantification are used to determine if modeling of such recovery HFEs is needed.

#### **E5.1.1.2 Error Modes**

HFEs can be classified by error mode as either an EOO or EOC. EOOs and EOCs can occur in any temporal phase (i.e., pre-initiator, initiator, or post-initiator). This classification is highly dependent upon the specific event tree or fault tree model. In other words, the same operator action could be modeled as either an EOO (e.g., failed to actuate system x) or an EOC (e.g., actuated system y instead of x). The error mode model is chosen based on consistency with the PCSA model and at the discretion of the HRA analyst. In early PRAs, EOCs were often excluded. Current PRAs, however, address both EOOs and EOCs, although there are still few methods for identifying and quantifying EOCs. In the current analysis, EOO and EOC are defined as follows:

---

<sup>6</sup> The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

<sup>7</sup> Alternatives to frontline equipment, include equipment that operators can use for performing the functions of frontline equipment in case of an impossibility to recover the failed frontline equipment in a timely manner.

- EOO—An HFE that represents the failure to perform one or more actions that should have been taken and that then leads to an unchanged or inappropriately changed configuration with the consequences of a degraded state. Examples include the failure of a radiation protection worker to perform the radiologic survey before a cask is released from the facility.
- EOC—An HFE that represents one or more actions that are performed incorrectly or some other action(s) that is performed instead. It results from an overt, unsafe action that, when taken, leads to a change in configuration with the consequence of a degraded state. Examples include commanding a crane to lift when it should be lowered.

### **E5.1.1.3 Human Failure Type**

Human failure types include the following:

- Slip/lapses—An action performed where the outcome of the action was not as intended due to some failure in execution. Slips are errors that result from attention failures, while lapses are errors that result from failures in memory recall.
- Mistake—An action performed as intended, but the intention is wrong. Mistakes are typically failures associated with monitoring (especially deciding what to monitor and how frequently to monitor), situation awareness, and response planning. Section E5.1.1.4 provides definitions of these terms.

### **E5.1.1.4 Informational Processing Failures**

Assessment of HFES can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is recommended for the YMP HRA is based on the discussion in Chapter 4 of ATHEANA (Ref. E8.1.14) and consists of the following elements:

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.
- Situation awareness—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents operators' understanding of the present situation and their expectations for future conditions and consequences.
- Response planning—This term is defined as the process operators use to decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.

- **Response implementation**—This term is defined as the activities involved with physically carrying out the actions identified in response planning.

When there are short time frames for response and the possibility of severely challenging operating conditions (e.g., environmental conditions) exists, then failures in all information processing stages must be considered. Also, slips/lapses and mistakes are considered for each information processing stage. Response implementation failures are expected to dominate the pre-initiator failures that are modeled. Post-initiator failures and failures that initiate event sequences can occur for all information processing stages, although detection failures are likely to be important only for events requiring response in very short time frames.

### **E5.1.2 Personnel Involved in Subsurface Operations**

A brief description of the duties of personnel involved in subsurface operations is listed below.

**Crew member**—A generic term for personnel (not including TEV operators, radiation protection workers, or supervisors) involved in the facility operations.

**Engineer**—The certified crew member who performs engineering calculations and the verification of programming emplacement locations into the TEV programmable logic controller (PLC).

**Gantry operator**—The person who is designated to operate the drip shield gantry. This person is in charge of ensuring that the gantry is in the appropriate configuration for drip shield emplacement. This person is located in the Central Control Center Facility (CCCF) and controls the gantry remotely.

**Person in charge (PIC)**—The certified crew member who is in charge of coordinating and overseeing the operation. This is the person who is notified when a waste form is ready for transit and who coordinates, according to this information, the appropriate personnel, procedures, and equipment to be used to process this cask type. This person is in charge of communicating this information to all the crew members involved in the emplacement of the waste package and ensuring that the relevant equipment is properly staged and in proper operational condition.

**Quality control**—The certified crew member in charge of quality control. This person is involved in supervising critical operations and tracking the appropriate documentation (i.e., tracking the waste package emplacement position).

**Radiation protection worker**—The certified health physics technician, whose job is to monitor radiation during cask-related activities. This person is responsible for stopping operations if high radiation levels are detected.

**Security guard**—The person responsible for monitoring the activities to ensure that security barriers are maintained and procedures are followed. This person ensures that crew members (or others) do not enter the drifts unless scheduled. The security guard has authorization to halt operations if security is being compromised.

**Supervisor**—The person who is in charge of the given operation and who supervises and checks the critical operations in a given step. For steps requiring independent verification, this analysis uses the term “supervisor” as the person who provides the independent check. This analysis does not rely upon the fact that this check is performed by the actual supervisor, only that an independent check is done by someone with the appropriate training and qualifications (i.e., the supervisor).

**TEV operator**—The person who is designated to operate the TEV. This person is in charge of ensuring that, prior to leaving the facility, the TEV is in the appropriate configuration for movement of a waste package to the drifts. This person is located in the CCCF and controls the TEV remotely.

## **E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES**

This section discusses the general human performance issues that characterize the human interaction with the subsurface operations.

**Communication Difficulties**—There are significant challenges in communication between the local and remote team members performing subsurface operations. TEV operators located in the CCCF must converse with other crew members local to the drifts (e.g., the security guard) using some sort of communication device (e.g., walkie talkies). Garbled communication (due to system interference or background noise) is clearly possible, and in some cases it may not even be possible to clearly determine who is speaking. A belief that a particular individual is speaking, even if they are not, can bias the listeners into hearing what they expect to hear.

**Visual Challenges**—For most of the remote operations, successful completion of the operation requires a certain amount of visual acuity both for the performance of the operation and the confirmation of the status. Safety concerns require that visual observation be performed using cameras that provide images to screens in the control room. In addition, views may be obstructed, such as by some structure or equipment.

**Unchallenging Activities**—The activities involved in subsurface operations are, in general, heavily automated and therefore the human–machine interface is quite simple in nature. In addition, the speed of the movements is quite slow, so each action takes a long time to complete. Basically, this is mostly boring work, with a significant amount of downtime between actions for some individuals. There is ample opportunity for diversion and distraction, and an air of informality and complacency can easily exist within and amongst the crew members. From a psychological perspective, there is insufficient dynamic activity to generate an optimum stress level for performance.

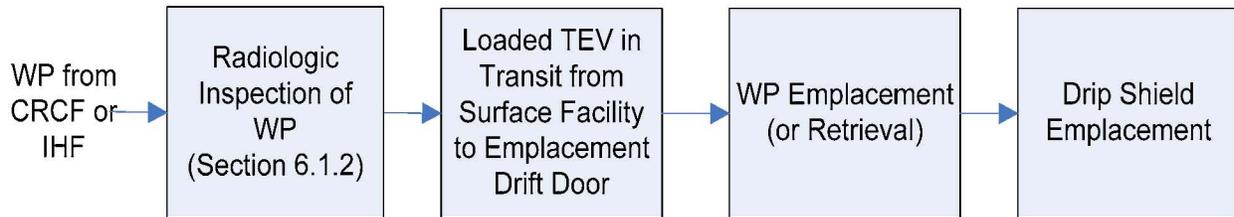
## **E6 ANALYSIS**

### **E6.0 BACKGROUND**

#### **E6.0.1 Reader’s Guide to the HRA Analysis**

Section E3.2 describes nine steps that comprise the HRA process. This section describes the implementation of Steps 2 through 8.

This section documents the qualitative and quantitative analysis of HFEs associated with subsurface operations. Subsurface operations are significantly less complicated than a set of facility operations; therefore, the entire set of subsurface operations was analyzed as one group of operations. Figure E6.0-1 provides an overview of subsurface operations. Each high-level operational activity is described in Section E6.1; Section E6.2 provides a description and quantification for the corresponding HFEs. Table E6.0-1 provides a link between the high-level operational activities described in Section E6.1 and the ESD and HAZOP evaluation nodes. The link between the HFEs and the rest of the PCSA is provided through the ESD cross-references for each HFE in Table E6.2-1.



NOTE: CRCF = Canister Receipt and Closure Facility; IHF = Initial Handling Facility; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Figure E6.0-1. Major Subsurface Operations Steps

Table E6.0-1. Correlation of Subsurface Operations to ESDs and HAZOP Evaluation Nodes

Activity	HAZOP Evaluation Node	ESD
<b>Transit from Surface Facility to Emplacement Drift Door (Section E6.1.3)</b>		
Loaded TEV exits facility (Section E6.1.3)	1	1
Loaded TEV transit from facility to North Portal (Section E6.1.3)	2	2
Loaded TEV transit from North Portal to emplacement drift door (Section E6.1.3)	3	3
<b>Waste Package Emplacement (or Retrieval) (Section E6.1.4)</b>		
Waste package emplacement (Section E6.1.4.1)	4	3
Waste packager (Section E6.1.4.2)	4	3
<b>Drip Shield Emplacement (Section E6.1.5)</b>		
Drip shield emplacement (Section E6.1.5)	5	3

NOTE: ESD = event sequence diagram; HAZOP = hazard and operability; TEV = transport and emplacement vehicle.

Source: Original

ESD 4 (Event Sequence Associated with Loss or Lack of Shielding) and ESD 5 (Event Sequence Associated with Localized Internal Fire) are applicable to all subsurface operations.

## E6.1 DESCRIPTION OF SUBSURFACE OPERATIONS BASE CASE SCENARIOS

Subsurface operations include movement of the loaded TEV to the emplacement drift; emplacement of the waste package; and, once all the waste packages are emplaced, emplacement of the drip shield. While not anticipated to be part of the normal subsurface operations, the subsurface operators have the capability to retrieve an emplaced waste package, as well.

### E6.1.1 Initial Conditions

The following conditions and design considerations provide the background for the base case scenario:

- A TEV is sitting in the appropriate facility, loaded with waste packages and with the facility doors shut. The TEV shield doors are closed, and it is ready to leave the facility to go to the subsurface drifts.
- The facility doors are closed.
- The TEV operators are located in the CCCF and watch TEV operations via camera (there are cameras on the front and back of the TEV). The only PLC override control these operators have is to signal the TEV to stop. There are lights on the front and back of the TEV and in the access mains (but not necessarily in the emplacement drifts).
- In the CCCF there is a display board that has a map of the facility and drifts. This display board has lights to represent movement of the TEV, and the drifts have lights to represent emplaced waste packages. There are also indicators of switch position in the control room.
- There are TEV crossing indicators/lights where the TEV rail intersects site roads.
- For accountability purposes, the drift inventory is verified (by counting the number of waste packages in each drift) every month until the drift is closed. This is done by sending the drip shield gantry with a camera into the drifts to allow the operators to count the number of emplaced waste packages. The gantry can travel the length of the tunnel.
- Safety features of the TEV include an override to stop the shield doors from opening if the operator notices that the TEV is too close to a waste package.
- No construction is permitted in the proximity of the TEV path on the surface; the closest construction to the TEV path is roughly 30 m away.
- The TEV speed is limited to less than 2 mph. The TEV has visual and auditory alarms when loaded and traveling on the surface. Before the TEV leaves a facility, the operators signal all (intersection) crossings to close (including the crossing gate, lights, and the auditory signal).

- There are operational controls that prohibit another TEV from traveling on the surface while a loaded TEV is traveling on the surface. There is a similar restriction for TEV traffic in the drifts.
- The TEV rails are on a concrete pad; the edge of this pad marks the “exclusion zone.” To exceed the 100-mrem dosage, a person must be located approximately one ft from the TEV for approximately one hour.
- There is an electromechanical interlock that physically prevents the TEV shield doors from opening during transit. This interlock is engaged or disengaged at the facility door and the drift door.
- There are front and rear anticollision interlocks. These interlocks, however, are routed through the PLC.
- There are operational controls restricting TEV operation during inclement weather (e.g., thunderstorms); however, water or ice on the tracks does not pose a problem for the TEV.
- There are at least two personnel entrances into the drifts: the North Portal and a (or several) sealed bulkhead(s) on the construction side. Both entrances are monitored by security and clearly marked. Personnel expected to enter the drifts are controlled and their positions monitored. The emplacement drift access door has an emergency escape door (roughly 12 by 16 in.) that only allows traffic to exit the drift. The access door itself has a lock box that must either be physically unlocked, or personnel in the CCCF can remotely activate the access door. The North Portal is the main access point to the drifts.
- The TEV operates off an electrically powered third rail.

The following personnel are involved in these operations:

- Crew member
- Engineer
- Gantry operator
- PIC
- Quality control
- Radiation protection worker
- Security guard
- Supervisor
- TEV operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

### **E6.1.2 Radiologic Inspection of Waste Package**

**Prejob Plan**—Before the TEV is dispatched to the Canister Receipt and Closure Facility (CRCF)/ Initial Handling Facility (IHF), the PIC is notified of the type of waste package that needs to leave the facility. According to this information, the PIC determines the appropriate procedures to be used in emplacement. The PIC also communicates this information to all the crew members involved in the emplacement of this waste package. This prejob plan includes engineering calculations to determine in which drift to emplace the waste package, based on the thermal output of the fuel inside the waste package; these calculations are verified by quality control. This plan also includes programming this emplacement location into the TEV PLC; this program is verified by an engineer, quality control personnel, and the supervisor. All crew members are properly trained in their task and abide by the procedures of the facility.

**Radiologic Inspection of the Waste Package**—The waste package cannot be inspected directly; it is inspected visually via camera during TEV loading (in the CRCF or IHF), and a radiological survey is performed on the loaded TEV as a proxy to direct inspection of the waste package. Once the TEV is loaded and ready for export, a radiation protection worker enters the Waste Package Loadout Room of the facility and visually inspects and conducts radiological surveys of the exterior of the TEV.

### **E6.1.3 TEV in Transit from Surface Facility to Emplacement Drift Door**

**Leaving Surface Facility**—Once the TEV is loaded and closed, a crew member opens the facility doors, and the TEV operator signals the TEV to initiate travel to the North Portal.

Prior to the initiation of this step, the TEV track must be cleared of all objects and debris. The operator ensures that all the switches have been properly thrown and that the proper crossing lights and blockades (e.g., at the rail crossings with site roads) have been activated when the TEV moves across the facility.

Once the TEV has left the facility, the facility crew member closes the facility door.

**TEV to North Portal**—The TEV automatically travels from the facility to the North Portal. There are periodic check points (most probably at the switch points) when the operator has to give a confirmation signal for the TEV to continue. There are 5 to 10 switches along the path from a given facility to the North Portal. There is no requirement for a camera view of the switches; however, the switch position is indicated on a switchboard in the control room. Once the TEV has reached the outer gate of the North Portal, it automatically stops.

**TEV Travels into Subsurface**—When the TEV has reached the North Portal, the security guard opens the outer gate and the TEV operator signals the TEV to proceed. The TEV travels into the gated area and stops after clearing the first gate (prior to reaching the second gate). The security guard closes the outer gate and verifies that there are no personnel in the drift. Once it is clear, the guard opens the second gate and the TEV operator signals the TEV to travel to the proper drift.

**TEV to Turnout and Emplacement Drift**—Once the TEV reaches the proper emplacement drift it automatically stops. As the TEV approaches the drift door, a switch on the track is

tripped. This switch signals the drift door to open and disengages the interlock that prevents an inadvertent opening of the TEV shield door. Once the drift door is open, the operator in the CCCF initiates the movement of the TEV into the drift. The TEV stops and the drift door automatically closes once the TEV has cleared the doorway.

#### **E6.1.4 Waste Package Emplacement (or Retrieval)**

##### **E6.1.4.1 Waste Package Emplacement**

**TEV Shield Doors Opened**—Once the loaded TEV is stopped midway into the drift (at a predetermined distance from the closest waste package), the TEV shield doors automatically open. No human action is necessary for this step.

**Back Shield Lifted**—After the shield doors are opened, the TEV back shield automatically lifts. No human action is necessary for this step.

**Bottom Shield Extended**—When the TEV back shield is lifted, the bottom shield automatically extends. No human action is necessary for this step.

**TEV Continues to Final Waste Package Position**—Once the bottom shield is extended, the TEV automatically moves the waste package into its emplacement position (approximately four inches away from the last waste package in the drift). No human action is necessary for this step.

**Lowering Shielding and Emplacing Waste Package**—The waste package is automatically lowered and emplaced when the TEV is in position. No human action is necessary for this step.

**Confirming Proper Waste Package Location**—The operator in the CCCF uses the camera to confirm proper emplacement of the waste package within the drift. The operator also consults the control board to confirm that the waste package is in the proper drift. Quality control personnel verify the completion of this step.

**Backing TEV away from Waste Package**—Once the waste package is set in position, the TEV automatically backs away from the waste package until the TEV doors have completely cleared the waste package. No human action is necessary for this step.

**Lifting Shielded Compartment**—The TEV stops and then automatically lifts the shielded compartment. No human action is necessary for this step.

**Retracting Bottom Shield**—Once the TEV has cleared the emplaced waste package, it automatically retracts the bottom shield. No human action is necessary for this step.

**Lowering Back Shield and Closing TEV Doors**—With the bottom shield retracted, the back shield automatically lowers and the TEV doors close in preparation for TEV movement. No human action is necessary for this step.

#### **E6.1.4.2 Waste Package Retrieval**

**Moving Empty TEV into Drift**—The operator in the CCCF moves an empty TEV into the drift where the waste package to be retrieved is located.

**TEV Shield Doors Opened**—The TEV shield doors automatically open once the loaded TEV is stopped midway into the drift (a predetermined distance away from the closest waste package). No human action is necessary for this step.

**Back Shield Lifted**—The TEV back shield automatically lifts after the TEV shield doors are opened. No human action is necessary for this step.

**Bottom Shield Extended**—The TEV bottom shield automatically extends after the TEV back shield is lifted. No human action is necessary for this step.

**Lowering Shielded Compartment**—The TEV shielded compartment is automatically lowered when the TEV is in position. No human action is necessary for this step.

**Driving Forward**—The TEV automatically moves forward to the location of waste package to be retrieved. No human action is necessary for this step.

**Locating Waste Package**—The TEV automatically moves over the waste package to be retrieved. No human action is necessary for this step.

**Lifting Shielded Compartment and Waste Package**—The TEV automatically lifts the waste package into the TEV by lifting the shielded compartment.

**Retracting Bottom Shield**—The TEV bottom shield is automatically retracted after the TEV has cleared the emplaced waste package. No human action is necessary for this step.

**Lowering Back Shield and Closing TEV Doors**—With the bottom shield retracted, the back shield automatically lowers and the TEV doors close in preparation for TEV movement. No human action is necessary for this step.

**Leaving Old Drift**—The operator in the CCCF signals the TEV to leave the drift once the TEV has been loaded with the retrieved waste package. The TEV then travels to the drift door and stops. The drift door automatically opens and the operator signals the TEV to travel out of the emplacement drift to the new drift. The drift door then automatically closes and the TEV shield door interlock reengages once the TEV has cleared the doorway.

**Entering New Drift**—The TEV automatically stops after it reaches the proper drift. As the TEV approaches the drift door a switch on the track is tripped; this switch signals the drift door to open and it disengages the interlock that prevents an inadvertent opening of the TEV shield door. After the drift door has opened, the operator signals the TEV to start, and the TEV enters partway into the drift and stop. The drift door automatically closes once the TEV has cleared the doorway.

**Emplace Waste Package in New Drift**—Further information is provided in Section E6.1.4.1.

### **B6.1.5 Drip Shield Emplacement**

**Drip Shield Gantry to North Portal**—The surface and subsurface rail system track must be cleared of all objects and debris prior to the initiation of this step. The proper crossing lights and blockades (e.g., at the rail crossings with site roads) activate as the gantry moves across the facility.

The gantry automatically travels to the North Portal without human interaction.

**Drip Shield Gantry Continues to Subsurface**—The gantry stops upon arrival at the North Portal gate. A security guard then opens the outer gate. The gantry operator signals the gantry to travel into the gated area and stop after clearing the first gate (prior to reaching the second gate). The security guard closes the outer gate and verifies that there are no personnel in the drift. Once the area is verified to be clear, the guard opens the second gate and the gantry operator signals the gantry to travel to the proper drift.

**Drip Shield Gantry to Turnout and Selected Drift**—The gantry automatically stops at the entrance to the proper drift. As the gantry approaches the drift door, it activates a switch on the track that signals the drift door to open. The operator signals the gantry to commence movement once the drift door is open; the gantry enters the drift. The drift door automatically closes after the gantry has cleared the doorway.

**Continuing to Final Drip Shield Position**—The gantry automatically continues to move until it is in position. It stops at this position.

**Lowering Drip Shield**—The gantry is automatically lowered into place and released.

**Confirming Proper Drip Shield Location and Interlock**—The gantry operator in the CCCF uses the camera to confirm proper placement of the drip shield within the drift. Quality control personnel acknowledge that this step has been accomplished. The drip shield is lowered onto the part of the previous segment of drip shield and mechanically locks into place.

**TEV to Drift Entrance and Turnout**—The gantry operator in the CCCF signals the gantry to leave the drift after the gantry has installed the drip shield in the proper location. The gantry moves to the drift door and stops. The drift door automatically opens and the operator in the CCCF signals the gantry to travel out of the emplacement drift. The drift door automatically closes once the gantry has cleared the doorway. The gantry then exits the subsurface.

## **E6.2 ANALYSIS OF SUBSURFACE HUMAN FAILURE EVENTS**

This section documents the qualitative analysis of HFEs associated with the operations described in Section E6.1. The qualitative analysis includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis.

### E6.2.1 HFEs Common to Multiple Operations

Before beginning the analysis of the individual failure events, there are a number of generic HFEs that were evaluated across operations and determined to be conducive to establishing ground rules for use throughout the analysis. These are discussed in this section.

**Interlocks**—For the HRA, interlocks were generally modeled explicitly in the fault tree instead of being embedded in the HRA for the preliminary analysis. The approach chosen by the HRA team to assign preliminary HEPs when interlocks were present was simplified. Since the interlock would prevent the operator from completing an unsafe action (even if the operator tried to) it was conservatively analyzed as if the operator would always take the unsafe action (i.e., the HEP for the HFE containing the unsafe action was conservatively set to 1.0 as a first approximation of the HEP). Unless otherwise specified, this was done for all cases where the human cannot easily defeat the interlock that protects against the associated unsafe action and HFE. Therefore, the analysis is relying entirely upon the interlock to prevent the failure. The interlock failure probability is taken from the active component failure database, which gives a value of  $2.7E-5$  per demand (approximately  $3E-5/\text{demand}$ ). It is recognized in using this approach that, despite the interlock not being easy to defeat, there is always a possibility that it could be defeated (either by the operator or by the maintenance crew and then not restored). However, if this were the case then it would still be necessary for the operator to erroneously conduct the unsafe action. The HRA team considered that it was very unlikely that the screening combination of the bypass error and the unsafe action would approach or exceed the  $3E-5$  value for the random failure of the interlock. The HRA team judged that this preliminary value would implicitly account for the failure to restore an interlock after maintenance if that interlock is difficult to bypass and is not bypassed during normal maintenance. If this conservative approach was not adequate to demonstrate compliance with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1), a more realistic preliminary value was applied and justified. That is, the HRA team went back and took a further look at the unsafe action and its associated interlock, and determined whether a lower preliminary HEP for the unsafe action could be justified. If so, this is clearly discussed and documented in the preliminary analysis. Interlocks that humans can reasonably defeat were generally not explicitly modeled in the fault tree, but rather included in the HEP for the HFE since they are not independent of operator actions. Regardless of this approach, in any case where the preliminary HEP was not sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1) and a detailed analysis was needed, all interlocks and other mechanical failures or physical phenomena that contribute to the overall HFE were integrated into the HRA along with the contributing unsafe actions and evaluated within the overall HFE quantification as part of the context of the HFE and fully discussed and documented in the detailed analysis. In all cases, interlocks that rely on PLCs were not credited in this analysis since they won't be declared important to safety.

**HVAC System**— For subsurface operations that occur in the CRCF Loadout Room, the CRCF heating, ventilation, and air conditioning (HVAC) system is an integral part of the system modeled. It should be noted that the analysis of this system is not applicable to waste packages exported from the IHF since the HVAC system in the IHF has not been classified as important to safety. In addition, the subsurface ventilation system has not been classified as important to safety. The following pre-initiating HFEs were identified and assigned preliminary values:

060-VCTO-DR00001-HFI-NOD: Operators Open Two or More Vestibule Doors in CRCF

**Preliminary Value:** 1E-02

**Justification:** Used general guidance for pre-initiator HFE preliminary values in Table E.III-2 for failure to properly restore an operating system to service when the degraded state is not easily detectable.

060-VCTO-HFIA000-HFI-NOM: Human Error: Exhaust Fan Switch Wrong Position

**Preliminary Value:** 1E-01

**Justification:** Used general guidance for pre-initiator HFE preliminary values in Table E.III-2 for failure to properly restore a standby system to service.

060-VCTO-HEPALK-HFI-NOD: Operator Fails to Notice HEPA Filter Leak in Train A

**Preliminary Value:** 1.0

**Justification:** To be conservative, credit was not given for the operator noticing HEPA filter leaks.

**Electrical System**— The CRCF electrical system is an integral part of the system modeled because it affects the CRCF HAVC system reliability. The following pre- and post-initiating HFEs were identified and assigned preliminary values:

060-#EEE-LDCNTRA-BUA-ROE and 060-#EEE-LDCNTRB-BUA-ROE: Operator Fails to Restore ITS Load Center Post Maintenance

26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS: Operator Fails to Restore Diesel Generator to Service

**Preliminary Values and Justification:** For electrical systems, the HFE assigned to operator failure to restore a system (i.e., motor control center or diesel generator) to service was assigned a conservative value of 0.1. The overall failure probability for load centers (060-#EEE-LDCNTRA-BUA-ROE and 060-#EEE-LDCNTRB-BUA-ROE) is 1.03E-05 and for diesel generators (26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS) is 1.95E-04. These failure probabilities reflect the probability that the motor control center or diesel generator requires service, and they are further discussed in Attachment B. Table E6.2-1 summarizes the preliminary values for the cross-operation generic HFEs.

Table E6.2-1. Summary of Preliminary Values for the Generic HFEs

HFE ID	HFE Brief Description	Preliminary Value
060-VCTO-DR00001-HFI-NOD	Operators open two or more vestibule doors in CRCF	1E-02
060-VCTO-HFIA000-HFI-NOM	Human error: exhaust fan switch wrong position	1E-01
060-VCTO-HEPALK-HFI-NOD	Operator fails to notice HEPA filter leak in train A	1.0
060-#EEE-LDCNTRA-BUA-ROE 060-#EEE-LDCNTRB-BUA-ROE	Operator fails to restore ITS load center post maintenance	1.03E-05
26D-#EEY-ITSDG-A-#DG-RSS 26D-#EEY-ITSDG-B-#DG-RSS	Operator fails to restore diesel generator to service	1.95E-04

NOTE: CRCF = Canister Receipt and Closure Facility; HEPA = high-efficiency particulate air; HFE = human failure event; ID = identification; ITS = important to safety.

Source: Original

### E6.2.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during subsurface operations are summarized in Table E6.2-2. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

INTENTIONALLY LEFT BLANK

Table E6.2-2. HFE Group #1 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
TEV derailment	<i>Operator Causes TEV to Derail as it Travels between the Facility and the Drifts</i>	2, 3	N/A <sup>a</sup>	Throughout subsurface operations the TEV travels on rail to and from various locations. A human-induced derailment HFE was not explicitly quantified because the probability of derailment due to human failure is incorporated in the historical data used to provide a general failure probability for derailment. Documentation for this failure can be found in Attachment C.
800-HEE0-WKRDRFT-HFI-NOD	<i>Worker Enters Drift from Access Main:</i> If a worker enters an active drift, purposefully or accidentally, then that worker would get a direct exposure.	4	N/A	If a worker enters an active drift for a prolonged period of time, purposefully or accidentally, then the worker would get a direct exposure. This failure event was screened from consideration and is not part of this HRA. Section 6.0 of the main report provides the justification for screening this event from consideration.
800-HEE0-WKRPROX-HFI-NOD	<i>Worker Stands too Close to TEV for an Extended Period of Time:</i> If a worker stands too close to a loaded TEV for a prolonged period of time (~1 hour), purposefully or accidentally, then that worker would get a direct exposure.	4	N/A	If a worker stands too close to a loaded TEV for a prolonged period of time, purposefully or accidentally, then the worker gets a direct exposure. This failure event was screened from consideration and is not part of this HRA. Section 6.0 of the main report provides the justification for screening this event from consideration.
800-HEE0-WKRFACD-HFI-NOD	<i>Operator Causes Collision of TEV with Facility Doors:</i> While exiting the CRCF or IHF, the operator can signal the TEV to move before the facility doors are completely open, or the facility doors can be closed on the TEV before the TEV has cleared the doorway.	1	2.0E-03	The facility doors are normally in the safe load path of the TEV and, during export, the doors can be partially opened such that the operator thinks that there is enough clearance to pass through the door, but instead collides with the doors. Alternatively, the operator can inadvertently close the doors on the TEV. There are no hardwired interlocks that would prevent this failure; the anticollision interlock on the TEV is not sufficient because the doors are considered to be open. The TEV is a large vehicle with operators watching the operations via camera, and it would go against operator training to begin moving the TEV before the doors are completely open or for the operator to begin closing the door before the TEV is completely through. This failure was considered highly unlikely (0.001, which also corresponds to the default probability for a simple action performed daily) and was adjusted to account for the fact that TEV operations are viewed via camera (×2).
800-HEE0-SIDEIMP-HFI-NOW	<i>Operator Causes Collision of TEV with SSC:</i> While the TEV is in transit between the facility and the emplacement drift, it can collide with an object on the tracks or with a site vehicle.	2	3.0E-04	In this step, the TEV is impacted by a site vehicle, most likely at an intersection or crossing. Aboveground, during TEV travel, all intersections have special crossing barricades and/or signals (like railroad crossing signals). All traffic in the subsurface is operationally restricted from being in the same area as a loaded TEV. The TEV also has an operator watching the TEV via camera, and the TEV moves very slowly, roughly 2 mph. Because of the special operational restrictions, the training that the operations personnel have regarding the TEV, and the slow speed of the TEV, this failure mode was determined to be roughly an order of magnitude lower than a collision of a vehicle while exiting the facility (800-HEE0-WKRFACD-HFI-NOD).
800-HEE0-TEVDOOR-HFI-NOD	<i>Human Error Causes TEV Doors to Open during Transit:</i> If the TEV operator prematurely signals the TEV shield doors to open, and the doors indeed open, any personnel present would receive a direct exposure.	4	1.0E-03	The TEV is controlled remotely by highly trained operators. The TEV shield doors are only opened in the facility and in the drifts, where they do so semi-automatically. There are interlocks to prevent inadvertent TEV door opening during transit. In order to commit this unsafe action, the operator would have to be careless as it is expected that the control, which would allow the operator to open the TEV doors, is distinct from the other TEV controls. Therefore, this action was considered highly unlikely and assigned the default preliminary value of 0.001.
800-HEE0-AXSDR00-HFI-NOD	<i>Operator Causes Collision of TEV with Access Doors:</i> While entering the North Portal or a drift, the operator can signal the TEV to move before the portal gate or drift door is completely open, or the gate/door can be closed on the TEV before the TEV has cleared the doorway.	2, 3	2.0E-03	The TEV automatically stops in front of the North Portal/drift doors, and the operator, watching via camera, has to give a "go" signal to the TEV for it to continue its operations. If the operator prematurely signals the TEV to enter through the North Portal or drift door before the door/gate is open, doing so would result in a collision of the TEV. The chance that the operator would fail to look closely at the gate/door before giving the "go" signal is highly unlikely (0.001) but was adjusted (×2) to account for the fact that this is a camera operation that could potentially involve visibility issues. This failure is similar to 800-HEE0-WKRFACD-HFI-NOD; it is consistent for these two failures to have the same preliminary values.
800-HEE0-IMPACTF-HFI-NOD	<i>Human Error Causes TEV to Impact WP in the Drift:</i> While emplacing the WP in a drift, the TEV is under manual control. The TEV operator could collide into an emplaced WP. The TEV operator can also impact an emplaced WP with the TEV shield doors if the TEV is too close to the WP when the operator signals the shield doors to be opened.	3	1.0E-03	Once inside the drift, the operators manually control the TEV for waste package emplacement. There are two ways the operator can damage a waste package in the drift during this step: collide the TEV directly into a waste package or open the shield doors into the waste package. The TEV can only move very slowly (2 mph or less) and there are guide marks to aid in positioning the TEV. TEV operations, however, are done via camera and in the drift the only available lighting is provided by the TEV itself. It is expected that the operator would be attentive during this step as it requires active control. This error was assessed to be highly unlikely and thus assigned the default value of 0.001.

INTENTIONALLY LEFT BLANK

Table E6.2-2. HFE Group #1 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
HFE-RUNAWAY-RESPONSE	<i>Operator Fails to Stop TEV Using Manual Override during a Runaway Event:</i> If speed control for the TEV malfunctions and the TEV begins to overspeed, the TEV operator must use the manual override to stop the TEV before a high-speed collision occurs.	1, 2, 3	N/A	No credit is given for recovery actions; therefore, this HFE is not modeled.
OP-FAILS-ENDOFRAIL	<i>Operator Error Causes TEV to Run over End of Rail:</i> TEV movement across the surface and into the drifts is highly automated. If the operator misprograms the TEV such that it overtravels a segment of path, the TEV can collide into an SSC or overrun the rails.	2, 3	1.0E-03	A TEV can potentially overtravel the rail and collide into the end stop if the operator improperly programs the TEV route. This failure is separate from a collision with a waste package during emplacement because emplacement is performed manually. For the portions of travel for which this failure is relevant, there is a consistent set of coordinates that do not change. The exception is the selection of the coordinates of the surface facility from which the waste package will originate. This event is similar to the pre-initiator "calibration error," which has a default preliminary value of 0.01. This value was adjusted by an order of magnitude ( $\times 0.1$ ) to account for the fact that the programming process, including an independent check, is designed to be more rigorous than the average calibration process during routine maintenance. Also, the TEV operator closely monitors the TEV during this operation and would have the opportunity to stop the TEV if it does not seem to be properly programmed.
Drip shield emplacement	<i>Operator Error Causes Impact to WP during Drip Shield Emplacement:</i> During drip shield emplacement, the operator moves a drip shield into the drift and installs it over the WPs. If an operator improperly performs this operation, the operator can potentially impact a WP with the drip shield or the drip shield gantry.	3	N/A	The drip shield gantry travels on rails that cause its travel to be wider and higher than the emplacement path of the waste packages. No plausible scenarios by which humans could impact a waste package during drip shield emplacement were identified. Therefore, this failure mode was screened from analysis.

NOTE: <sup>a</sup>Historical data was used to produce the probability; this historical data is not included as part of the HRA but is addressed in Attachment C on active component failure data.  
 CRCF = Canister Receipt and Closure Facility; ESD = event sequence diagram; HFE = human failure event; HRA = human reliability analysis; ID = identification;  
 IHF = Initial Handling Facility; N/A = not applicable; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

INTENTIONALLY LEFT BLANK

### E6.3 DETAILED ANALYSIS

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives. Therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

### E7 HUMAN RELIABILITY ANALYSIS DATABASE

Table E7-1 presents a summary of all of the human failures identified in this analysis. It also provides a link between the HFE and the ESD in which the human failure is modeled.

Table E7-1. HFE Data Summary

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
060-#EEE-LDCNTRA-BUA-ROE	Operator fails to restore load center A post maintenance	1	1.03E-05	10	Preliminary
060-#EEE-LDCNTRB-BUA-ROE	Operator fails to restore load center B post maintenance	1	1.03E-05	10	Preliminary
060-VCTO-DR00001-HFI-NOD	Operators open two or more vestibule doors in CRCF	1	1E-02	3	Preliminary
060-VCTO-HFIA000-HFI-NOM	Human error: exhaust fan switch in wrong position	1	1E-01	3	Preliminary
060-VCTO-HEPALK-HFI-NOD	Operator fails to notice HEPA filter leak in train A	1	1.0	N/A	Preliminary
26D-#EEY-ITSDG-A-#DG-RSS	Operator fails to restore diesel generator A to service	1	1.95E-04	10	Preliminary
26D-#EEY-ITSDG-B-#DG-RSS	Operator fails to restore diesel generator B to service	1	1.95E-04	10	Preliminary
800-HEE0-WKRDRFT-HFI-NOD	Worker enters drift from access main	4	N/A <sup>b</sup>	N/A	Screened from analysis
800-HEE0-WKRPROX-HFI-NOD	Worker stands too close to TEV for an extended period of time	4	N/A <sup>b</sup>	N/A	Screened from analysis
800-HEE0-WKRFACD-HFI-NOD	Operator causes collision of TEV with facility doors	1	2.0E-03	5	Preliminary
800-HEE0-SIDEIMP-HFI-NOW	Operator causes collision of TEV with SSC	2	3.0E-04	10	Preliminary
800-HEE0-TEVDOOR-HFI-NOD	Human error causes TEV doors to open during transit	4	1.0E-03	5	Preliminary
800-HEE0-AXSDR00-HFI-NOD	Operator causes collision of TEV with access doors	2, 3	2.0E-03	5	Preliminary
800-HEE0-IMPACT-HFI-NOD	Human error causes TEV to impact WP in the drift	3	1.0E-03	5	Preliminary
Drip shield emplacement	Operator error causes impact to WP during drip shield emplacement	3	N/A <sup>b</sup>	N/A	Screened from analysis

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
HFE-RUNAWAY-RESPONSE	Operator fails to stop TEV using manual override during a runaway event	1, 2, 3	N/A <sup>b</sup>	N/A	Screened from analysis
OP-FAILS-ENDOFRAIL	Operator error causes TEV to run over end of rail	2, 3	1.0E-03	5	Preliminary
TEV derailment	Operator causes TEV to derail as it travels between the facility and the drifts	2, 3	N/A <sup>a</sup>	N/A	Historical data

NOTE: <sup>a</sup>HRA value replaced by use of historic data (Attachment C provides further information on active component failure data).

<sup>b</sup>These HFEs were initially identified, but omitted from analysis for various reasons, including a design change precluding the human failure, or the failure would require a series of unsafe actions in combination with mechanical failures, such that the event is no longer credible. See Section E6.2 for a case-by-case justification for these omissions.

CRCF = Canister Receipt and Closure Facility; ESD = event sequence diagram; HEPA = high-efficiency particulate air; HFE = human failure event; N/A = not applicable; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

## E8 REFERENCES

### E8.1 DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of this document. There are no superseded or cancelled documents associated with the modifications that led to the issuance of this revision. Cancelled or superseded documents associated with the portions of this document for which the snapshot has not yet been updated are designated herein with a dagger (†).

The inputs in this section noted with an asterisk (\*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

E8.1.1 \*AIChE (American Institute of Chemical Engineers) 1992. *Guidelines for Hazard Evaluation Procedures*. 2nd Edition with Worked Examples. New York, New York: American Institute of Chemical Engineers. TIC: 239050. ISBN: 0-8169-0491-X.

E8.1.2 \*ASME RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.

- E8.1.3 \*BSC (Bechtel SAIC Company) 2006. *Engineering Standard for Repository Component Function Identifiers*. 000-30X-MGR0-00900-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20060816.0001.
- E8.1.4 \*BSC 2007. *Engineering Standard for Repository Area Codes*. 000-3DS-MGR0-00400-000 REV 004. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070911.0015.
- E8.1.5 †\*BSC 2007. *Repository System Codes*. 000-30X-MGR0-01200-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071101.0022.
- E8.1.6 BSC 2008. *Subsurface Operations Event Sequence Development Analysis*. 000-PSA-MGR0-00400-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080214.0004.
- E8.1.7 \*CRA (Corporate Risk Associates) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique*. CRA-BEGL-POW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.
- E8.1.8 \*Dougherty, E.M., Jr. and Fragola, J.R. 1988. *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. New York, New York: John Wiley & Sons. TIC: 3986. ISBN: 0-471-60614-6.
- E8.1.9 \*Gertman, D.; Blackman, H.; Marble, J.; Byers, J.; and Smith, C. 2005. *The SPAR-H Human Reliability Analysis Method*. NUREG/CR-6883. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0009.
- E8.1.10 \*Hall, R.E.; Fragola, J.R.; and Wreathall, J. 1982. *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlations*. NUREG/CR-3010. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0211.
- E8.1.11 \*Hannaman, G.W. and Spurgin, A.J. 1984. *Systematic Human Action Reliability Procedure (SHARP)*. EPRI-NP-3583. Palo Alto, California: Electric Power Research Institute. TIC: 252015.
- E8.1.12 \*Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.
- E8.1.13 NRC (U.S. Nuclear Regulatory Commission) 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084. )
- E8.1.14 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.

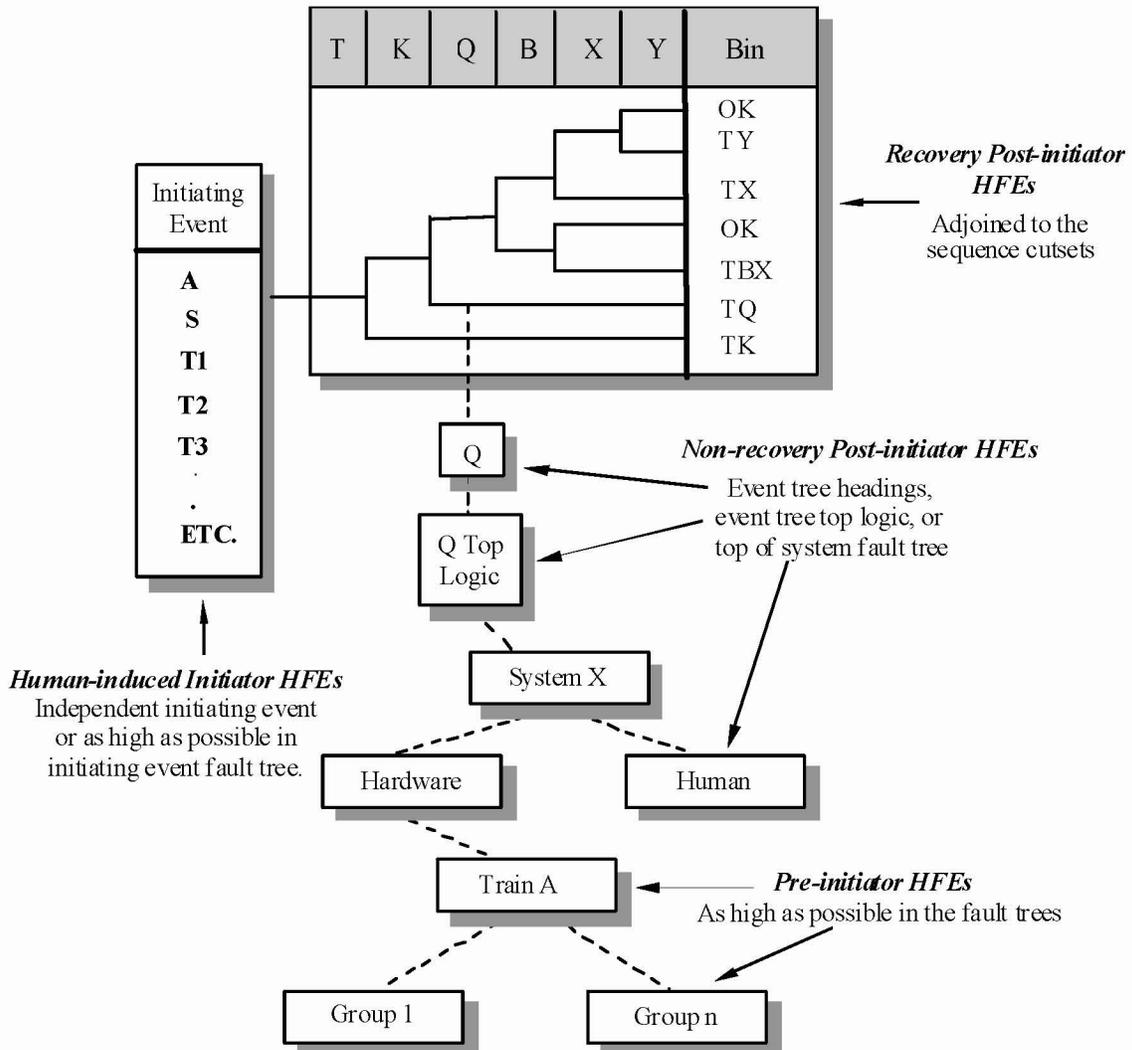
- E8.1.15 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0230.
- E8.1.16 \*Rasmussen, J. 1983. "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models." *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13*, (3), 257–266. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259863.
- E8.1.17 \*Swain, A.D. 1987. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. NUREG/CR-4772. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0026.
- E8.1.18 \*Swain, A.D. and Guttman, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*. NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.
- E8.1.19 \*Williams, J.C. 1986. "HEART - A Proposed Method for Assessing and Reducing Human Error." *9th Advances in Reliability Technology Symposium - 1986*. Bradford, England: University of Bradford. TIC: 259862.
- E8.1.20 \*Williams, J.C. 1988. "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance." [*Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants*]. Pages 436–450. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259864.

## **E8.2 DESIGN CONSTRAINTS**

- E8.2.1 10 CFR 63. 2007. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. U.S. Nuclear Regulatory Commission.

### APPENDIX E.I RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA

Figure E.I-1 provides a graphical illustration of how HFEs are incorporated into the PCSA.

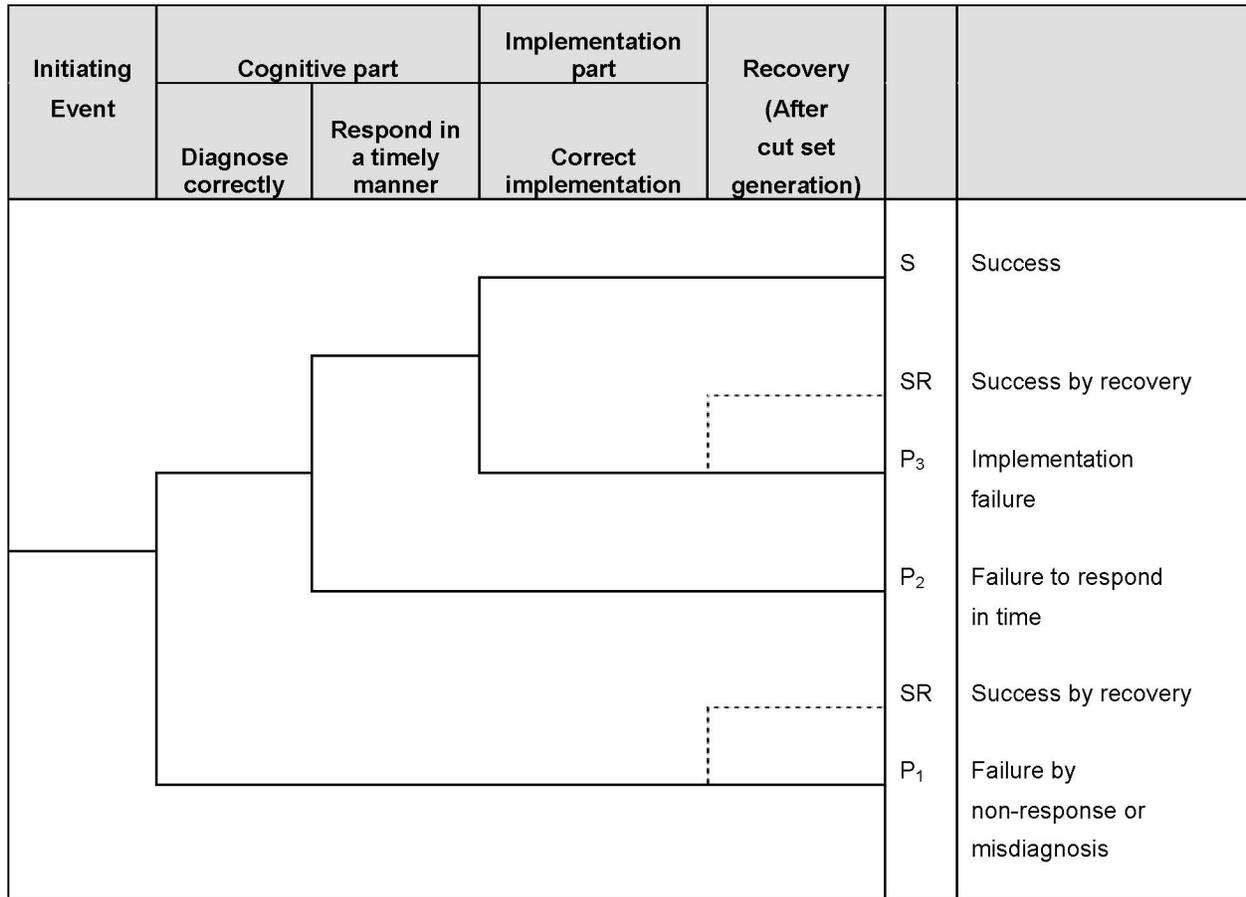


NOTE: HFE = human failure event.

Source: Original

Figure E.I-1. Incorporation of Human Reliability Analysis within the PCSA

**APPENDIX E.II  
GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS**



Source: Original

Figure E.II-1. Post-initiator Operator Action Event Tree

The representation in Figure E.II-1 consists of two elements, corresponding to a cognitive part (detection, diagnosis, and decision making) and an implementation (i.e., action) part.

P<sub>1</sub> represents the probability that operators make an incorrect diagnosis and decision and do not realize that they have done so. Some of the reasons for such mistakes are: incorrect interpretation of the procedures, incorrect knowledge of the plant state owing to communication difficulties, and instrumentation problems.

Given that the crew decides what to do correctly, there is still a possibility of failure to respond in time (represented by P<sub>2</sub>) or making an error in implementation (represented by P<sub>3</sub>).

However, it may be probable in certain scenarios that a recovery action can be taken. This consideration is taken into account after the initial quantification is completed and is applied as appropriate to the dominant cut sets.

**APPENDIX E.III  
PRELIMINARY (SCREENING) QUANTIFICATION  
PROCESS FOR HUMAN FAILURE EVENTS**

The preliminary quantification process consists of the following:

**Step 1—Complete the Initial Conditions Required for Quantification.**

The preliminary quantification process requires the following:

- The baseline scenarios are available.
- The HFEs and their associated context have been defined.
  - Collect any additional information that is not already collected and that is needed to describe and define the HFEs (and associated contexts).
  - Review all information for clarity, completeness, etc.
  - Interpret and prioritize all information with respect to relevance, credibility, and significance.

Table E.III-1 provides examples of information normally identified using the ATHEANA method (*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis* (Ref. E8.1.14) that serves as inputs to the quantification process. The HFE/context descriptions in Table E.III-1 touch briefly on the information that is relevant to the screening-level quantification of the HFE. Since the baseline scenario generally touches on much of this information, the point of including the HFE/context descriptions is to summarize the information that pertains to the specific HFE to minimize the need for the analysts to refer back to the baseline scenario, except to obtain additional detail.

Table E.III-1. Examples of Information Useful to HFE Quantification

Information Type	Examples
Facility, conditions, and behavior for possible deviations of the scenarios	Reasonably possible unusual plant behavior and failures of systems; equipment, and indications, especially those that may be unexpected or difficult to detect by operators. Includes presence of interlocks that would have to fail to promote the deviation.
Operating crew characteristics (i.e., crew characterization)	Crew structure, communication style, emphasis on crew discussion of the “big picture.”
Features of procedures	Structure, how implemented by operating crews, opportunities for “big picture” assessment and monitoring of critical safety functions, emphasis on relevant issue, priorities, any potential mismatches with deviation scenarios.
Relevant informal rules	Experience, training, practice, ways of doing things—especially those that may conflict with informal rules or otherwise lead operators to take inappropriate actions.
Timing	Plant behavior and requirements for operator intervention versus expected timing of operator response in performing procedure steps, etc.

Table E.III-1. Examples of Information Useful to HFE Quantification (Continued)

Information Type	Examples
Relevant vulnerabilities	Any potential mismatches between the scenarios and expected operator performance with respect to timing, formal and informal rules, biases from operator experience, and training, etc.
Error mechanisms	Any that may be particularly relevant by plant context or implied by vulnerabilities; applicable mechanisms depend upon whether HFE is a slip or mistake. Examples include: failures of attention, possible tunnel vision, conflicts in priorities, biases, missing or misleading indications, complex situations, lack of technical knowledge, timing mismatches and delays, workload, and human-machine interface concerns.
Performance-shaping factors	Those deemed associated with, or triggered by, the relevant plant conditions and error mechanisms.

NOTE: HFE = human failure event.

Source: Original

In Step 1, interpreting and prioritizing all information with respect to relevance, credibility, and significance is especially important if:

- Some information is applicable only to certain scenarios, HFEs, or contexts
- There are conflicts among information sources
- Information is ambiguous, confusing, or incomplete
- Information must be extrapolated, interpolated, etc.

Completion of the “lead-in” initial conditions is primarily performed by a single individual, using the results of the YMP HAZOP evaluation process and reviews of other relevant information sources. Discussions are also held with the Operations Department to augment that information, and the resulting write-ups are reviewed by the PCSA facility leads and the HRA team. The initial conditions are refined as part of an open discussion among the experts (in this case, the HRA team for the study) involved in the expert opinion elicitation process. The goal of this discussion is not to achieve a consensus but, rather, to advance the understanding of all the experts through the sharing of distributed knowledge and expertise. In each case, the scenario (or group of similar scenarios) and the HFE in question are described and the vulnerabilities and strong points associated with taking the right action are discussed openly among the HRA team.

**Step 2—Identify the Key or Driving Factors of the Scenario Context.**

The purpose of Step 2 is to identify the key or driving factors on operator behavior/performance for each HFE and associated context. Each expert participating in the elicitation process individually identifies these factors based on the expert’s own judgment. Usually, these factors are not formally documented until Step 4.

Typically, there are multiple factors deemed most important to assessing the probability for the HFE in question. This is due to the focus of the ATHEANA search process on combinations of factors that are more likely to result in an integrated context (Ref. E8.1.14). When there is only a single driving factor, it is usually one that is so overwhelming that it alone can easily drive the estimated probability. For example, if the time available is shorter than the time required to

perform the actions associated with the HFE, quantification becomes much simpler and other factors need not be considered.

### **Step 3—Generalize the Context by Matching it With Generic, Contextually Anchored Rankings, or Ratings.**

In Step 3, each expert participating in the elicitation process must answer the following question for each HFE: based upon the factors identified in Step 2, how difficult or challenging is this context relative to the HFE being analyzed?

Answering this question involves independent assessments by each expert. In order to perform this assessment, the specifics of the context defined for an HFE must be generalized or characterized. These characterizations or generalizations then must be matched to general categories of failures and associated failure probabilities.

To assist the experts in making their judgments regarding the probability of events, some basic guidance is provided. In thinking about what a particular HEP associated with an HFE may be, they are encouraged to think about similar situations or experiences and use that to help estimate how many times out of 10, 100, 1,000, etc., would they expect crews to commit the HFE, given the identified conditions. The following examples of what different probabilities mean are provided to the experts to help them scale their judgments:

“Likely” to fail (extremely difficult/challenging)	~0.5	(5 out of 10 would fail)
“Infrequently” fails (highly difficult/challenging) <sup>8</sup>	~0.1	(1 out of 10 would fail)
“Unlikely” to fail (somewhat difficult/challenging)	~0.01	(1 out of 100 would fail)
“Highly unlikely” to fail (not difficult/challenging)	~0.001	(1 out of 1000 would fail)

The experts are allowed to select any value to represent the probability of the HFE. That is, other values (e.g.,  $3E-2$ ,  $5E-3$ ) can be used. The qualitative descriptions above are provided initially to give analysts a simple notion of what a particular probability means. For exceptional cases, the quantification approach allows an HEP of 1.0 to be used when failure was deemed essentially certain. The following general guidance in Table E.III-2 is also provided to help calibrate the assessment by providing specific examples that fall into each of the above bins, and is based on the elicited judgment and consensus of the HRA team based on their past experience. This guidance applies to contexts where generally optimal conditions exist during performance of the action. Therefore, the experts should modify these values if they believe that the action may be performed under nonoptimal conditions or under extremely favorable conditions. Values may also be adjusted to take credit for design features, controls and interlocks, or procedural safety controls<sup>9,10</sup>. Examples of such adjustments are also provided below; however these values are not taken to be firm in any sense of the word, but rather simply as examples of where in

<sup>8</sup> The default value is 0.1. This value is used if no preliminary assessment is performed.

<sup>9</sup>As an initial preliminary value, unsafe actions that are backed up by interlocks are assigned a human error probability of 1.0 such that no credit for human performance is taken (i.e., only the interlocks are relied upon to demonstrate 10 CFR Part 63 (Ref. E8.2.1) compliance). If this proves insufficient, a more reasonable preliminary value is assigned to the unsafe action in accordance with this Appendix.

<sup>10</sup>Note that if such credit is taken, then it may be necessary (based on the PCSA results) to include these items in the nuclear safety design basis or the procedural safety controls for the YMP facilities.

general terms HEPs may fall and how they may relate to each other. Types of HFEs not listed here can be given values based on being “similar to” HFEs that are listed. Whatever value is selected, the basis is briefly documented.

Table E.III-2. Types of HFEs

<b>PRE-INITIATOR HFEs</b>	
Fail to properly restore a standby system to service	0.1
Failure to properly restore an operating system to service when the degraded state is not easily detectable	0.01
Failure to properly restore an operating system to service when the degraded state is easily detectable	0.001
Calibration error	0.01
<b>HUMAN-INDUCED INITIATOR HFEs</b>	
Failure to properly conduct an operation performed on a daily basis	0.001
Failure to properly conduct an operation performed on a very regular basis (on the order of once/week)	0.01
Failure to properly conduct an operation performed only very infrequently (once/month or less)	0.1
Operation is extremely complex OR conducted under environmental or ergonomic stress	×3
Operation is extremely complex AND conducted under environmental or ergonomic stress	×10
<b>NON-RECOVERY POST-INITIATOR HFEs</b>	
Not trained or proceduralized, time pressure	0.5
Not trained or proceduralized, no time pressure	0.1
Trained and/or proceduralized, time pressure	0.1
Trained and/or proceduralized, no time pressure	0.01

Source: Original

#### **Step 4—Discuss and Justify the Judgments Made in Step 3.**

In Step 3, each expert independently provides an estimate for each HFE. Once all the expert estimates are recorded, each expert describes the reasons why they chose a particular failure probability. In describing their reasons, each expert identifies what factors (positive and negative) are thought to be key for characterizing the context, and how this characterization fits the failure category description and the associated HEP estimate.

After the original elicited estimates are provided, a discussion is held that addresses not only the individual expert estimates but also differences and similarities among the context characterizations, key factors, and failure probability assignments made by all of the experts. This discussion allows the identification of any differences in the technical understanding or interpretation of the HFE versus differences in judgment regarding the assignment of failure probabilities. Examples of factors important to HFE quantification that might be revealed in the discussion include:

- Differences in key factors and their significance, relevance, etc., based upon expert-specific expertise and perspective.
- Differences in interpretations of context descriptions.

- Simplifications made in defining the context.
- Ambiguities and uncertainties in context definitions.

A consensus opinion is not required following the discussion.

**Step 5—Refinement of HFEs, associated contexts, and assigned HEPs (if needed).**

Based upon the discussion in Step 4, the experts form a consensus on whether or not the HFE definition must be refined or modified, based upon its associated context. If the HFE must be refined or redefined, this is done in Step 5. If such modifications are necessary, the experts “reestimate” based upon the newly defined context for the HFE (or new HFEs, each with an associated context).

The experts participating in the elicitation process are also allowed to change their estimate after the discussion in Step 4 based on the discussions during that step, whether or not the HFE definition and context are changed. Once again, a consensus is not required.

**Step 6—Determine final preliminary HEP for HFE and associated context.**

The final preliminary value to be incorporated into the PCSA for each HFE is determined in Step 6.

The failure probabilities assigned in the preliminary HRA quantification are based on the context outlined in the base case scenarios and deemed to be “realistically conservative.” To help ensure this conservatism, if a consensus value could not be reached, the final failure probability that was assigned to each HFE was determined by choosing the highest assigned probability among the final estimates of the experts participating in the expert elicitation process.

## APPENDIX E.IV SELECTION OF METHODS FOR DETAILED QUANTIFICATION

There are a number of methods available for the detailed quantification of HFEs (preliminary quantification is discussed in Appendix E.III of this analysis). Some are more suited for use for the YMP PCSA than others. A number of methods were considered, but many were rejected as inapplicable or insufficient for use in quantification. Several sources were examined as part of the background analysis for selecting a method for detailed quantification ((Ref. E8.1.11), (Ref. E8.1.8), (Ref. E8.1.16), and (Ref. E8.1.13)). As discussed in Section E3.2 the following four were chosen:

- ATHEANA expert judgment (Ref. E8.1.14)
- CREAM (Ref. E8.1.12)
- HEART (Ref. E8.1.19)/NARA (Ref. E8.1.7)
- THERP (Ref. E8.1.18).

This appendix discusses the selection process.

**Basis for Selection**—The selection process was conducted with due consideration of the HRA quantification requirements set forth in the ASME Level 1 PRA standard (Ref. E8.1.2) to the extent that those requirements, which were written for application to NPP PRA, apply to the types of operations conducted at the YMP. Certainly, all of the high level HRA quantification requirements were considered to be applicable. Further, all of the supporting requirements to these high level requirements were considered applicable, at least in regards to their intent. In some cases, the specifics of the supporting requirements are only applicable to NPP HRA and some judgment is needed on how to apply them. This was particularly true of those supporting requirements that judged certain specific quantification methods acceptable. This appendix lays out the specific case for the methods selected for use at the YMP (or, more to the point, the exclusion of certain methods that would normally be considered acceptable under the standard, but are deemed inappropriate for use for the YMP PCSA).

**Differences between NPP and the YMP Relevant to HRA Quantification**—There are a number of contrasts between the operations at the YMP and the operations at an NPP that affect the selection of approaches to performing detailed HRA quantification (Table E.IV-1).

Table E.IV-1. Comparison between NPP and YMP Operations

NPP	YMP
Central control of operations maintained in control room.	Decentralized (local), hands on control for most operations.
Most important human actions are in response to accidents.	Most important human actions are initiating events.
Postaccident response is important and occurs in minutes to hours. Short time response important to model in HRA.	Postaccident response evolves more slowly (hours to days). Short time response not important to model.

Table E.IV-1. Comparison between NPP and YMP Operations (Continued)

NPP	YMP
Multiple standby systems are susceptible to pre-initiator failures.	Standby systems do not play major role in the YMP safeguards, therefore few opportunities for pre-initiator failures.
Auxiliary operators sent by CCCF operators to where needed in the plant.	Local control reduces time to respond.
Most actions are controlled by automatic systems.	Most actions are controlled by operators.
Reliance on instrumentation /gauges as operators' "eyes."	Most actions are local, either hands on or televised. Less reliance on man-machine interface.
High complexity of systems, interactions, and phenomena. Actions may be skill, rule, or knowledge based.	Relatively simple process with simple actions. Actions are largely skill based.
Many in operation for decades; HRA may include walk-downs and consultation with operators.	First of a kind; HRA performed for construction application, therefore walk-downs and consultation with operators not feasible.

NOTE: CCCF = Central Control Center Facility; HRA = human reliability analysis; NPP = nuclear power plant; YMP = Yucca Mountain Project.

Source: Original

**Assessment of Available Methods**—There are essentially four general types of quantification approaches available:

1. Procedure focused methods:
  - A. Basis: These methods concentrate on failures that occur during step-by-step tasks (i.e., during the use of written procedures). They are generally based on observations of human performance in the completion of manipulations without much consideration of the root causes or motivations for the performance (e.g., how often does an operator turn a switch to the left instead of to the right).
  - B. Methods considered: THERP (Ref. E8.1.18).
  - C. Applicability: This method is of limited use for the YMP because important actions are not procedure driven. Many operations are skill based and/or semiautomated (e.g., crane operation, trolley operation, canister transfer machine operation, TEV operation). However, there are some instances where such an approach would be applicable to certain unsafe actions within an HFE. In addition, the THERP dependency model is adopted by NARA as being appropriate to use within a context-based quantification approach.
  - D. Assessment: THERP is retained as an option in the detailed quantification for its dependency model and for limited use when simple, procedure-driven unsafe actions are present within an HFE.
2. Time-response focused methods:
  - A. Basis: These methods focus on the time available to perform a task, versus the time required, as the most dominant factor in the probability of failure. They are,

for the most part, based on NPP control room observations, studies, and simulator exercises. They also tend to be correlated with short duration simulator exercises (i.e., where there is a clear time pressure in the range of a few minutes to an hour to complete a task in response to a given situation).

- B. As discussed in *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications* (Ref. E8.1.8), examples of time-response methods include: HCR (Ref. E8.1.8) and TRC (Ref. E8.1.10).
- C. Applicability: These methods are not applicable to the YMP because most actions do not occur in a control room and, in addition, are generally not subject to time pressure. This is particularly true of the most important HFEs, those that are human-induced initiators. Other than a desire to complete an action in a timely fashion to maintain production schedules, time is irrelevant to these actions, especially in the context of the type of time pressure considered by these methods. Even those actions at the YMP that may take place in a control room in response to an event sequence and have time as a factor would only require response in the range of hours or days, which is outside the credible range for these methods.
- D. Assessment: No use can be identified for these methods within the YMP PCSA. None of them are retained.

3. Context and/or cognition driven methods:

- A. Basis: These methods focus on the context and motivations behind human performance rather than the specifics of the actions, and as such are independent of the specific facility and process. To the extent that some of the methods are data driven (i.e., they collect and use observations of human performance) the data utilized is categorized by generic task type rather than by the type of facility or equipment where the human failure occurred. This makes them more broadly applicable to various industries, tasks, and situations, in large part because they allow context-specific PSFs to be considered. This allows for them to support a variety of contexts, individual performance factors (e.g., via PSFs) and human factor approaches.
- B. Methods considered: HEART (Ref. E8.1.19), “A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance” (Ref. E8.1.20)/NARA (Ref. E8.1.7), CREAM (Ref. E8.1.12), and ATHEANA expert judgment (Ref. E8.1.14).
- C. Applicability: The broad applicability of these methods and their flexibility of application make them most suited for application at the YMP. The use of information from a broad range of facilities and other performance regimes (e.g., driving, flying) support their use as facility-independent methods. The generic tasks considered can be applied to the types of actions of most concern to the YMP (i.e., human-induced initiators) as opposed to the more narrow

definitions used in other approaches that make it difficult to use them for other than post-initiator or pre-initiator actions.

- D. Assessment: Optimally it would be convenient to use only one of the three methods of this type for all the detailed quantification. However, HEART (Ref. E8.1.19)/NARA (Ref. E8.1.7) and CREAM (Ref. E8.1.12) approach their generic task types slightly differently and also use different PSFs and adjustment factors. There are unsafe actions within the YMP HFEs that would best fit the HEART (Ref. E8.1.19)/NARA (Ref. E8.1.7) approach and others that would best fit the CREAM (Ref. E8.1.12) approach. In addition, the union of the two approaches still has some gaps that would not cover a small subset of unsafe actions for the YMP (primarily in the area of unusual acts of commission). One gap relates to dependencies between actions, but in this case NARA (Ref. E8.1.7) specifically endorses the THERP (Ref. E8.1.18) approach and so this is used. However, other gaps exist. For these cases, the ATHEANA (Ref. E8.1.14) expert judgment approach provides a viable and structured framework for the use of judgment to establish the appropriate HEP values in a manner that would meet the requirements of the ASME RA-S-2002 (Ref. E8.1.2) standard. Therefore, all three of these methods are retained for use and the selection of one versus the other is made based on the specific unsafe action being quantified. This is documented as appropriate in the actual detailed quantification of each HFE.

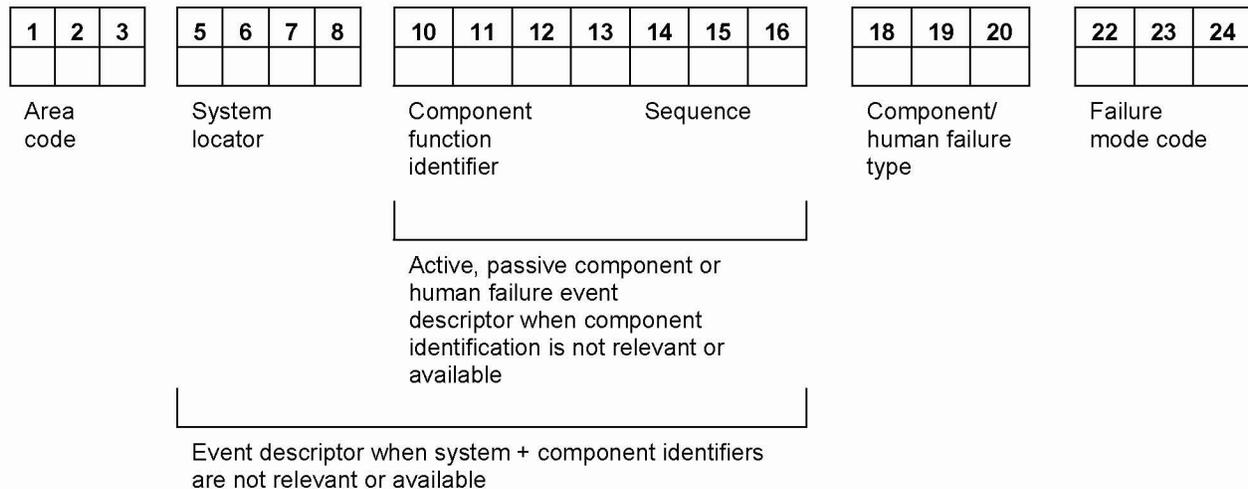
#### 4. Simplified methods:

- A. Basis: These methods use the results of past PRAs to focus attention on those HFEs that have dominated risk. These are essentially PRA results from NPPs. As such, they presuppose NPP situations and actions, and define important PSFs based on these past NPP PRAs. They have very limited (if any) ability to investigate context, individual and human factors that are beyond NPP experience. The HEPs that result from applying these methods are calibrated to other NPP methods.
- B. Methods considered: Accident Sequence Evaluation Program (Ref. E8.1.17) and Standardized Plant Analysis Risk Human Reliability Analysis (Ref. E8.1.9).
- C. Applicability: These methods are clearly biased by their very close dependence on the results of past NPP PRAs. They are too limited for application beyond the NPP environment. They are not simply inappropriate for this application, but it would be extremely difficult to make a sound technical case regarding technical validity.
- D. Assessment: No use can be identified for these methods within the YMP PCSA or any technical case made supporting them for a non-NPP application. None of them are retained.

### APPENDIX E.V HUMAN FAILURE EVENTS NAMING CONVENTION

Event names for HFEs in the YMP PCSA model follow the general structure of the naming convention for fault tree basic events. This is true whether the HFE is modeled in a fault tree, directly on an event tree, or as an initiating event. The convention, as adapted for HFEs, is as follows:

This basic event naming convention in Figure E.V-1 is provided to ensure consistency with project standards and to permit this information to fit into a 24-character SAPHIRE field such that each basic event can be correlated to a unique component or human failure.



Source: Original

Figure E.V-1. Basic Event Naming Convention

The area code defines the physical design or construction areas where a component would be installed. Area codes are listed in *Engineering Standard for Repository Area Codes*, (Ref. E8.1.4). These codes are used rather than the facility acronyms to maintain consistency with Engineering. In this system, the CRCF is designated by area code 060, the Wet Handling Facility is 050, the Receipt Facility is 200, the IHF is 51A, and the Subsurface Facility and subsurface operations are designated as 800. Intra-Site Operations could fall under one of several repository area codes and, therefore, the most appropriate code to use was the repository general area code. However, this code was insufficient for the purposes of this analysis, and a designator of ISO was substituted instead. For the majority of cases, the area coding of HFEs in Attachment E reflects the location of the operations being evaluated, such as ISO for Intra-Site Operations. However, for certain HFEs, the coding corresponds to the location of the systems impacted by the human failure, such as HVAC, which is specific to the CRCF and therefore retains the 060 coding, and AC power, which retains the 26x and 27x coding. For these specific instances, such coding provides better traceability of the HFE back to the affected equipment.

The system locator code identifies operational systems and processes. System locator codes (four characters) are listed in Table 1 of *Repository System Codes* (Ref. E8.1.5). These are generally three or four characters long, such as VCT for tertiary confinement HVAC.

The component function identifiers identify the component function and are listed in the *Engineering Standard for Repository Component Function Identifiers* (Ref. E8.1.3). These are generally three or four characters long. Some Bechtel SAIC Company, LLC, component function identifiers for typical components are shown in Table E.V-1, but in cases where there is not an equivalent match, the most appropriate PCSA type code should be used (also given in Table E.V-1).

The sequence code is a numeric sequence and train assignment (suffix), if appropriate, that uniquely identifies components within the same area, system, and component function.

If an HFE is related to the failure of an individual component with an existing component function identifier and sequence code, the naming scheme should utilize these codes in the event name. If an HFE is such that these codes do not apply, the basic event name can be a free form field for describing the nature of the event, such as HCSKSCF for operator topples cask during scaffold movement or HFCANLIDAJAR for operator leaves canister lid ajar, utilizing either seven characters when there is a relevant system locator code, or 12 characters when no system codes are applicable.

The human failure type and failure mode codes are three characters each, consistent with the coding provided in Table E.V-1.

For HFEs, the type code always begins with HF and continues with a one letter designator for the HFE temporal phase: P for pre-initiator, I for human-induced initiator, N for non-recovery post-initiator, R for recovery post-initiator (this latter code is not used during preliminary analysis).

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes

<b>PRE-INITIATOR HFEs; TYP=HFP</b>		<b>FMC=</b>
Fail to properly restore a standby system to service		RSS
Failure to properly restore an operating system to service when the degraded state is not easily detectable		ROH
Failure to properly restore an operating system to service when the degraded state is easily detectable		ROE
Calibration error		CAL
<b>HUMAN-INDUCED INITIATOR HFEs; TYP=HFI</b>		
Failure to properly conduct an operation	Operation is performed on a daily basis.	NOD
	Operation is performed on a very regular basis (on the order of once per week)	NOW
	Operation is performed only very infrequently (once per month or less)	NOM
Operation is extremely complex OR conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	COD
	Operation is performed on a very regular basis (on the order of once per week)	COW
	Operation is performed only very infrequently (once per month or less)	COM
Operation is extremely complex AND conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	CSD
	Operation is performed on a very regular basis (on the order of once per week)	CSW
	Operation is performed only very infrequently (once per month or less)	CSM
<b>NON-RECOVERY POST-INITIATOR HFEs; TYP=HFN</b>		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN
<b>RECOVERY POST-INITIATOR HFEs; TYP=HFR</b>		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN

NOTE: FMC = failure mode code; HFE = human failure event; HFI = human-induced initiator HFE; HFN = human failure non-recovery post-initiator HFE; HFP = human failure pre-initiator HFE; HFR = human failure recovery post-initiator HFE; TYP = type.

Source: Original

**ATTACHMENT F**  
**FIRE ANALYSIS**

INTENTIONALLY LEFT BLANK

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	F-7
F1 INTRODUCTION .....	F-9
F2 REFERENCES .....	F-9
F3 BOUNDARY CONDITIONS .....	F-10
F3.1 INTRODUCTION .....	F-10
F4 ANALYSIS METHOD .....	F-12
F4.1 INTRODUCTION .....	F-12
F4.2 IDENTIFICATION OF OUTSIDE FIRE INITIATING EVENTS .....	F-12
F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY .....	F-13
F5 ANALYSIS .....	F-17
F5.1 INTRODUCTION .....	F-17
F5.2 INITIATING EVENT FREQUENCIES .....	F-17
F5.3 RESULTS .....	F-19

INTENTIONALLY LEFT BLANK

**TABLES**

	<b>Page</b>
F4.2-1. Outside Fire Area Categories.....	F-13
F4.3-1. Types of Facilities: Cross Reference Between NFPA and NAICS .....	F-15
F4.3-2. Fraction of Fires and Fire Frequency for Outside Areas of a Facility .....	F-16
F5.3-1. Onsite Transport Fire Initiating Event Frequency and Associated Distribution.....	F-20

INTENTIONALLY LEFT BLANK

## ACRONYMS AND ABBREVIATIONS

### Acronyms

FEMA	Federal Emergency Management Agency
NAICS	North American Industry Classification System
NFIRS	National Fire Incident Reporting System
NFPA	National Fire Protection Association
PCSA	preclosure safety analysis
PRA	probabilistic risk assessment
TEV	transport and emplacement vehicle
YMP	Yucca Mountain Project

INTENTIONALLY LEFT BLANK