INTENTIONALLY LEFT BLANK

CONTENTS

CONTENTS (Continued)

Page

FIGURES

Page

INTENTIONALLY LEFT BLANK

TABLES

Page

INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

Acronyms

ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event Analysis
BOP	balance of plant
CRCF	Canister Receipt and Closure Facility
CREAM	Cognitive Reliability and Error Analysis Method
CSNF	commercial spent nuclear fuel
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EFC	error forcing context
EOC	error of commission
EOO	error of omission
EPC	error-producing condition
EPRI	Electric Power Research Institute
ESD	event sequence diagram
GROA	geologic repository operations area
HAM	horizontal aging module
HAZOP	hazard and operability
HCR	Human Cognitive Reliability
HCTT	cask tractor and cask transfer trailer
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HSTC	horizontal shielded transfer cask
HTC	a transportation cask that is never upended
HVAC	heating, ventilation, and air conditioning
ISFSI	independent spent fuel storage installation
LLW	low-level radioactive waste
LLWF	Low-Level Waste Facility
MLD	master logic diagram
NARA	Nuclear Action Reliability Assessment
NPP	nuclear power plant

ACRONYMS AND ABBREVIATIONS (Continued)

NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
PCSA	preclosure safety analysis
PRA	probabilistic risk assessment
PSF	performance-shaping factor
RF	Receipt Facility
SHARP	Systematic Human Action Reliability Procedure
SNF	spent nuclear fuel
SPM	site prime mover
TAD	transportation, aging, and disposal
THERP	Technique for Human Error Rate Prediction
TRC	Time-Reliability Correlation
VTC	a transportation cask that is upended on a railcar
WHF	Wet Handling Facility
YMP	Yucca Mountain Project

E1 INTRODUCTION

This document describes the work scope, definitions, terms, methods, and analysis for the human reliability analysis (HRA) task of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA) reliability assessment.

The HRA task identifies, models, and quantifies human failure events (HFEs) postulated in the PCSA to assess the impact of human actions on event sequences modeled in the PCSA. The HFEs evaluated and quantified by this task are identified during the following activities:

- Initiating event identification and grouping
- Event sequence development and categorization
- System analysis
- Sequence quantification and uncertainty analysis.

The HRA task ensures that the HFEs identified by the other tasks (e.g., hazard and operability (HAZOP) evaluation, event sequence diagram (ESD) development, event tree analysis, and fault tree analysis) are quantified with HRA techniques. The ESD finding is that the human-induced initiating events dominate the HRA. No post-initiator human actions have been credited in this analysis. The HRA task also ensures that modeled HFEs are appropriately incorporated into the PCSA and provides appropriate human error probabilities (HEPs) for all modeled HFEs. It is important to note that YMP operations differ from those of traditional nuclear power plants (NPPs), and the HRA analysis reflects these differences; Appendix E.IV of this analysis provides further discussion on these differences and how they influenced the choice of methodology.

E1.1 SUMMARY

The HRA was carried out using a nine-step process that is derived from *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624 (Ref. E8.1.23):

1. Define the scope of the analysis.
2. Describe the base case progression of actions and responses that constitute successful completion of the operations being evaluated (base case scenarios).
3. Identify and define HFEs of concern.
4. Perform preliminary (screening) analysis and identify HFEs requiring detailed analysis.
5. Identify potential vulnerabilities for the HFEs requiring detailed analysis.
6. Search for HFE scenarios (i.e., scenarios of concern).
7. Quantify probabilities of HFEs.

8. Incorporate HFEs into the PCSA.

9. Evaluate HRA/PCSA results and iterate with design.

After the scope was defined, the activities within the Intra-Site Operations scope were identified and base case scenarios were defined that described in detail the normal operations for each activity. Once the operations were defined and the base cases were documented, HFEs were identified through an iterative process whereby the human reliability analysts, in conjunction other PCSA analysts and Engineering and Operations personnel, met and discussed the design and operations in order to appropriately model the human interface. This process consisted of the HAZOP evaluation, master logic diagram (MLD) and event sequence development, fault tree and event tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the model. The iteration with the event sequence and system reliability analysis also identified HFEs of potential concern. HFEs identified include both errors of omission (EOOs) and errors of commission (EOCs).

Included in this process was an extensive information collection process where the human reliability analysts reviewed industry data and interviewed subject matter experts to identify potential vulnerabilities and HFE scenarios.

The result of this identification process was a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then became the error forcing context (EFC) for a specific HFE. Additions and refinements to these initial EFCs were made during the preliminary and detailed analyses.

A preliminary, or screening-type, analysis was then performed to preserve HRA resources so that detailed analyses can be focused on only the most risk-significant HFEs. The preliminary analysis included verification of the validity of HFEs included in the initial PCSA model, assignment of a conservative screening value to each HFE, and verification of preliminary values. The actual quantification of preliminary values was a six-step process that is described in detail in Appendix E.III of this analysis. Once the preliminary values were assigned, the PCSA model was quantified (initial quantification), and HFEs were identified for detailed analysis if: (1) the HFE was a risk-driver for a dominant sequence, and (2) using the preliminary values, that event sequence was above Category 1 or Category 2 according to the 10 CFR 63.111 (Ref. E8.2.1) performance objectives. The remaining HFEs retained their preliminary values. While most of the activities associated with preliminary analysis were tedious and time-consuming, extra care was taken to perform these tasks conscientiously since the results of the initial quantification were used to identify which HFEs require detailed analysis. For this analysis, preliminary values proved to be sufficient to demonstrate compliance with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1); therefore, no detailed analyses were required for this HRA.

For the preliminary analysis, HFEs were modeled at a high level in order to reduce dependencies that arise from modeling detailed actions. In addition, uncertainties were accounted for by assigning a lognormal distribution and applying an error factor of 3, 5, or 10 to the distribution, depending on the mean value of the final HEP.

To aid the reader in linking the HRA with other parts of the PCSA, Section E6.0.1 provides an overview of the Intra-Site Operations and provides a map which links this analysis back to the MLD, the ESD, and the HAZOP evaluation.

E2 SCOPE AND BOUNDARY CONDITIONS

E2.1 SCOPE

The scope of the HRA is established in order to focus the analysis on the issues pertinent to the goals of the overall PCSA. Thus, the scope is as follows:

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers.

2. Pursuant to the above, the following types of HFEs are excluded:

   A. HFEs resulting in standard industrial injuries (e.g., falls)

   B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount

   C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.

3. The identification of HFEs is restricted to those areas of the site or facility that handle waste forms and only during the times that waste forms are being handled (e.g., HFEs are not identified for site transportation activities during the movement of empty transportation casks).

4. The exception to #3 is that system-level HFEs are considered for support systems when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.

5. Recovery post-initiator actions (as defined in Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.

6. In accordance with Section 1 (boundary conditions of the PCSA), initiating events associated with conditions introduced in structures, systems, and components before they reach the site are not, by definition of 10 CFR 63.2 (Ref. E8.2.1), within the scope of the PCSA nor, by extension, within the scope of the HRA.

E2.2 BOUNDARY CONDITIONS

Unless specifically stated otherwise, the following general conditions and limitations are applied throughout the HRA task. The first two conditions always apply. The remaining conditions apply unless the HRA analyst determines that they are inappropriate. This judgment is made for each individual action considered:

- Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior (i.e., deliberate acts of sabotage and the like) are not considered in this task.

- Facility personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard operating procedures is made because employees believe their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.

- Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include spent nuclear fuel (SNF) handling at reactor sites having independent spent fuel storage installations (ISFSIs), chemical munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the geologic repository operations area facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.

- The facility is initially operating under normal conditions and is designed to the highest quality human factors specifications. The level of operator stress is optimal unless otherwise noted in the analysis.

- In performing the operations, the operator does not need to wear protective clothing unless the operation is similar to those performed in other comparable facilities where protective clothing is required.

- The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are experienced and have functioned in their present positions for a sufficient amount of time to be proficient.

- The environment inside each facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made regarding optimal weather and road conditions. YMP personnel are required to stop work if conditions are perceived to be unsafe.

- Personnel involved with the facility operations are expected to have the proper training commensurate with nuclear industry standards. As appropriate, this training is followed by a period of observation until the operator is proficient.
- While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill-of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

E3 METHODOLOGY

E3.1 METHODOLOGY BASES

The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in the American Society of Mechanical Engineers (Ref. E8.1.3) and incorporates the guidance provided by the U.S. Nuclear Regulatory Commission (NRC) in *Preclosure Safety Analysis – Human Reliability Analysis*. HLWRS-ISG-04 (Ref. E8.1.24).

E3.2 GENERAL APPROACH

The HRA consists of several steps, that follow the intent of American Society of Mechanical Engineers (ASME) RA-S-2002 (Ref. E8.1.3) and the process guidance provided in NUREG-1624 (Ref. E8.1.23). Detailed descriptions of each HRA step are provided in the following subsections to summarize the processes used by the analysts. The step descriptions are based on the ATHEANA (A Technique for Human Event Analysis) documentation, with some passages taken essentially verbatim and others paraphrased to adapt the material based on NPPs to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. 8.1.23). Further discussion on information collection and use of expert judgment in this process can be found in Section E4.

HFE probabilities produced in this analysis are mean values. The HEPs are modeled as a lognormal distribution, where the error factors are defined based on the method presented in Section E3.4.

E3.2.1 Step 1: Define the Scope of the Analysis

The objective of the YMP HRA is to provide a comprehensive quantitative assessment of the HFEs that can contribute to the facility's event sequences resulting in radiological release, criticality, or direct exposure. Any aspects of the work that provide a basis for bounding the analysis are identified in this step. In the case of the YMP, the scope is bounded by the design state of the facilities and equipment.

E3.2.2 Step 2: Describe Base Case Scenarios

In this step, the base case scenarios are defined and characterized for the operations being evaluated. In general, there is one base case scenario for each operation included in the model. The base case scenario:

- Represents the most realistic description of expected facility, equipment, and operator behavior for the selected operation.

- Provides a basis from which to identify and define deviations from such expectations (Step 6).

In the ideal situation (which is seldom achieved), the base case scenario:

- Has a consensus operator model[1]
- Is well-defined operationally
- Has well-defined physics
- Is well-documented in public or proprietary references
- Is realistic.

Since operators and "as built, as operated" information are not currently available for YMP, this information is sought from comparable facilities with comparable operations. Documented reference analyses (e.g., engineering analyses) can assist in defining the scenario from the standpoint of physics and operations. The reference analyses may need to be modified to be more realistic. Expert judgment, engineering documents and applicable industry experience are the keys to defining realistic base case scenarios for YMP operations; Section E4 provides greater detail on how information was collected and the role of subject matter experts in this process.

E3.2.3 Step 3: Identify and Define HFEs of Concern

Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken, or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The classification process is described further in Section E5.1.1. The analyses performed in later steps (i.e., Steps 4 through 7) may identify the need to define an HFE or unsafe action not previously identified in Step 3.

Human errors were identified based upon the three temporal parts generally analyzed by probabilistic risk assessment (PRA) and are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs

---

[1] ATHEANA (Ref. E8.1.23), Section 9.3.1 defines a consensus operator model in the following manner: "Operators develop mental models of plant responses to various PRA initiating events through training and experience. If a scenario is well defined and consistently understood among all operators (i.e., there is a consensus among the operators), then there is a consensus operator model."

- Post-initiator HFEs[2]:
  - Non-recovery
  - Recovery.

Each of these types of HFEs is defined in Section E5.1.1.1; identification of the HFEs for each temporal phase is described in the following sections.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., PSFs). This combination of conditions and human factor concerns then becomes the EFC for a specific HFE. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses.

E3.2.3.1 Identifying Pre-initiator HFEs

Pre-initiators are identified by the system analysts when modeling fault trees, while performing the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human common-cause failure.

E3.2.3.2 Identifying Human-Induced Initiator HFEs

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the site, facility and structures, systems, and components in order to appropriately model the human interface. This iterative process begins with the HAZOP evaluation and MLD development, described and documented in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8), followed by a second iteration during the initial fault tree and event tree modeling, and ending with a third iteration through the preliminary analysis and incorporation of HFEs into the model. Included in this process is an extensive information collection process where industry data was reviewed (Section E4.1) and subject matter experts were interviewed (Section E4.2) to identify potential vulnerabilities and HFE scenarios. HFEs identified include both EOOs and EOCs.

E3.2.3.3 Identifying Non-recovery Post-initiator HFEs

Non-recovery post-initiator HFEs are identified by examining the human contribution to pivotal events in the event tree analysis. The event sequence analysts, with support from the human reliability analysts, identify HFEs that represent the operator's failure to perform the proper action to mitigate the initiating event and/or the unavailability of automatic mitigation functions as called for in the emergency operating procedures or in accordance with their emergency response training. This identification includes all actions required, whether in a control room or locally. Post-initiator EOCs and EOOs are also considered. It should be emphasized that this section presents the methodology that is used to identify non-recovery post-initiator events. However, as shown in Section E6, none of these types of errors have been identified for the

[2] Terminology common to NPPs refer to non-recovery post-initiator events as Type C events and recovery events as Type CR events.

Intra-Site Operations and balance of plant (BOP) Reliability and Event Sequence Categorization Analysis. During the qualitative evaluation, non-recovery post-initiator events were considered and ruled out because it was unnecessary to credit non-recovery actions to demonstrate compliance with the performance objectives stated in 10 CFR 63.111 (Ref. E8.2.1).

E3.2.3.4 Identifying Recovery Post-initiator HFEs

Recovery actions are of limited relevance to YMP operations and, for conservatism, were not credited in this analysis. Recovery post-initiator HFEs are outside the scope of this analysis (Section E2.1).

E3.2.4 Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis

The preliminary analysis is a type of screening analysis used to identify HFEs of concern. A screening analysis is commonly performed in HRA to conserve resources and focus the effort on the subsequent detailed analysis of those HFEs that are involved in the important event sequences. Preliminary values are assigned for the probabilities of HFEs based upon predetermined characteristics of each HFE. This analysis involves the following steps:

- Verification of the validity of HFEs included in the initial PCSA model.
- Assignment of conservative preliminary values to all HFEs included in the initial PCSA model.
- Verification of assigned preliminary probabilities to all HFEs in the PCSA.
- Quantification of the initial PCSA model using preliminary values (i.e., the "initial quantification").
- Identification of HFEs for detailed analysis.

The human reliability analyst performs the first three of these steps with the assistance of the PCSA quantification task leader, who also performs the last two steps. While most of the activities associated with this preliminary analysis are tedious and time-consuming, it is important to perform these tasks conscientiously since the results of the initial quantification are used to identify those HFEs requiring detailed analysis.

Analysts must strike a balance between conservatism and too much conservatism. Using too conservative a value for an HEP can overemphasize the importance of an HFE in the sequence quantification, perhaps masking a significant component failure event. By contrast, using a less conservative preliminary HEP may lead to inappropriately screening out a potentially significant event sequence. Instead of the usual screening process used in PRA, where relatively high screening values of 1.0 or 0.1 for an HEP are often inserted in initial fault tree and event sequence quantification, the PCSA applies an intermediate process where conservative preliminary values are assigned based on the context and failure modes of the HFE. Appendix E.III of this analysis provides specific details on guidelines for preliminary quantification.

Depending on the results obtained with the preliminary quantification, the event sequence and human reliability analysts may conclude that the preliminary results are sufficient for event sequence quantification and that a detailed analysis would not provide a better basis for event sequence categorization or more insights into the human factors issue for a particular waste handling operation. The preliminary quantification process is based on a characterization of each human action with respect to complexity and operational context using a judgment-based approach consisting of the following subtasks:

1. Complete the "lead-in" initial conditions required for quantification.
2. Identify the key or driving factors of the scenario context.
3. Generalize the context by matching it with generic, contextually anchored rankings or ratings.
4. Discuss and justify the judgments made in subtask 3.
5. Refine HFEs, associated contexts, and assigned HEPs.
6. Determine final preliminary HEPs for each HFE and associated context. These HEPs are then entered into the PRA logic structure to see which HFEs call for more detailed evaluation. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a given sequence, and (2) using the preliminary values, that sequence falls in a category (i.e., a Category 1 or Category 2) such that it does not meet 10 CFR 63.111 performance objectives (Ref. E8.2.1).

Appendix E.III of this analysis defines and provides technical bases for the HEP preliminary values recommended to be used in the YMP PRA for different categories of HFEs, depending on the general HFE characteristics. Section E4.2 provides a list of experts used in this process.

E3.2.5 Step 5: Identify Potential Vulnerabilities

This information collection step defines the context for Step 6 in which scenarios that deviate from the base case are identified. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in the HFEs and/or unsafe actions identified in Step 4. Potential traps[3] inherent in the ways operators may respond to the initiating event or base case scenario are identified through the following:

- Investigation of potential vulnerabilities in operator expectations for the scenario
- Understanding of the base case scenario time line and any inherent difficulties associated with the required response

[3] A "trap" is a human failure that is encouraged or enabled by the existence of a specific vulnerability. That is, vulnerabilities influence operators to fall into particular traps.

- Identification of operator action tendencies and informal rules
- Evaluation of formal rules and operating procedures expected to be used in the scenario.

The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). Section E4 provides a description of the information types that comprise this knowledge base.

E3.2.6 Step 6: Search for HFE Scenarios

In this step, the analyst must identify deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These deviations are referred to as HFE scenarios. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions (which form the EFC).

The principal method for identifying HFE scenarios is a HAZOP evaluation-like search scheme, coupled with a means for relating scenario characteristics with error mechanisms for each stage in the information processing model (Ref. E8.1.1). The result of such a search is a description of the HFE scenarios, including system and equipment conditions, along with any resident or triggered human factor concerns (e.g., PSFs). Again, this combination of conditions and human factor concerns then becomes the EFC for a specific HFE. As defined by the ATHEANA document (Ref. E8.1.23), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. (Additions and refinements to this initial EFC are likely in later steps of the process.)

E3.2.7 Step 7: Quantify Probabilities of HFEs

As shown in Section E6, no HFEs requiring detailed analysis have been identified for the Intra-Site Operations event sequence and categorization analysis. Therefore, only a general summary of the methodology associated with detailed quantification is presented here.

Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 (Ref. E8.2.1)after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9, Section E3.2.9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CFR 63.111 (Ref. E8.2.1). The qualitative analysis in steps 3, 5, and 6 sets the stage for the detailed quantification by providing the accident progression(s) for a given HFE and its context. Specifically, the qualitative analysis provides a list of unsafe actions, along with their context, characteristics, and classification (i.e., EOO or EOC). For each unsafe action, the following steps are performed:

1. Qualitative analysis (e.g., identification of PSFs, definitions of important characteristics of the given unsafe action, assessment of dependencies)

2. Selection of a quantification model

3. Quantification

4. Verification that HFE probabilities are appropriately updated in the PCSA database.

There are four HRA methods that have been selected for this quantification:

1. CREAM (Cognitive Reliability and Error Analysis Method) (Basic and Extended)—*Cognitive Reliability and Error Analysis Method, CREAM* (Ref. E8.1.19)[4]

2. HEART (Human Error Assessment and Reduction Technique)/NARA (Nuclear Action Reliability Assessment) - "HEART - A Proposed Method for Assessing and Reducing Human Error" (Ref. E8.1.28) and *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.9)

3. THERP (Technique for Human Error Rate Prediction) (with some modifications)—*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Ref. E8.1.27).

When an applicable failure mode cannot be reasonably found in one of the above methods, then the following HRA method is used:

4. ATHEANA's expert elicitation approach—*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.23).

Appendix E.IV of this analysis provides a discussion why these specific methods were selected for quantification, as well as a discussion of why some methods, deemed appropriate for HRA of NPPs, are not suitable for application in the PCSA. This discussion summarizes the main differences between NPPs and repository operations with respect to contexts and failure modes that affect potential HFEs. It also gives some background about when a given method is applicable based on the focus and characteristic of the method.

E3.2.8 Step 8: Incorporate HFEs into PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. E8.1.23) provides an overview of the state-of-the-art method for performing this step in PRAs. This process is done in conjunction with the PCSA analysts. Appendix E.I of this analysis provides the recommended approach for incorporation of human errors in the YMP PCSA, and Appendix E.V of this analysis provides the recommended naming conventions for HFEs incorporated in the fault tree models.

HFEs are incorporated, in the form of basic events, into the fault trees that support the initiating event and pivotal events of event trees. The HEP that is entered in a basic event is modeled as a

[4]Extended CREAM (Ref. E8.1.19) creates a link between CREAM and HEART (Ref. E8.1.28), and enhances the ability of CREAM to quantify skill-based HFEs.

lognormal distribution, whose mean value is the nominal value of the HEP, to which an error factor is assigned (Section E3.4) to reflect the uncertainty in the probability estimate. In many cases, the equipment failures and the associated HFEs are calculated as part of an integrated HRA. The resulting probability of both equipment and human failures is then placed in the fault tree as a single basic event. Because preliminary values were sufficient to demonstrate compliance, this iteration was unnecessary for Intra-Site Operations.

E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design

This last step in HRA is performed each time the PCSA is quantified. The primary results are the HFEs in dominant cut sets and the associated qualitative inputs to such HFEs. Potential "fixes" to the design or operational environment can be supported by these results.

Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is noncompliant with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1) because the probability of a given HFE dominates the probability of the event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or to completely eliminate the HFE. In such cases, the modification is analyzed for potential new HFEs, and the applicable HFEs are requantified, along with the event sequences.

E3.3 DEPENDENCY

Dependency between human actions is defined to exist when the outcome of a particular human action is related to the outcome of a prior human action or actions. According to THERP (Ref. E8.1.27), the joint probability of human error for a set of dependent human actions is higher than if they were independent.

The possibility of dependencies between human actions and defined HFEs is recognized throughout the HRA task. The concern with respect to dependencies is that the joint probabilities separately assigned to a set of dependent HFEs treated as independent actions can result in a lower event sequence frequency than would result if dependencies among the HFEs were appropriately recognized and treated. This situation is especially important in the HRA activities leading up to and including preliminary analysis where an inappropriately low HEP might lead to an inappropriate screening out of a potentially significant cut set or event sequence. If dependence were properly identified and treated, the resulting HEP might then appear in dominant cut sets and, therefore, be identified for detailed analysis.

E3.3.1 Capturing Dependency

Dependencies between defined HFEs can exist for two reasons:

- Due to the characteristics of the event sequence in which the HFEs are modeled
- Due to the modeling style, especially the degree of decomposition, in HFE definition.

In the first case, dependencies are unavoidable due to the inherent characteristics of the initiator type or event sequence. In the second case, dependencies can be avoided by redefining dependent HFEs into a single HFE. In either case, dependencies can be treated by using a structured method for adjusting probabilities to account for dependencies. However, some HRA quantification methods (e.g., ATHEANA (Ref. E8.1.23)) account for certain types of dependencies within their formulation by combining dependent events as part of the normal process of addressing the accident scenario as a whole. These methods do not require additional treatment.

All event sequences that contain multiple HFEs are examined for possible dependencies. For the preliminary analysis, HFEs are modeled at a high level where several subtasks are combined into a single task so that explicit consideration of dependencies between subtasks is eliminated. For a detailed assessment, where the various actions that constitute an HFE are explicitly quantified, dependencies are explicitly addressed using the formulae in Table E3.3-1 from THERP (Ref. E8.1.27), where N is the independently derived HEP. The THERP dependency model was selected for its formalism and reproducibility. The model itself is not dependent on what the source of the baseline (i.e., independent) HEP is; it can be obtained from any existing model or from expert elicitation. None of the other "objective" quantification approaches used (i.e., HEART (Ref. E8.1.28)/NARA (Ref. E8.1.9) or CREAM (Ref. E8.1.19) has its own dependency model, and NARA (Ref. E8.1.9) specifically endorses the use of the THERP (Ref. E8.1.27) approach.

Table E3.3-1. Formulae for Addressing HFE Dependencies

Level of Dependence	Zero	Low	Medium	High	Complete
Conditional Probability	N	$\frac{1 + 19N}{20}$	$\frac{1 + 6N}{7}$	$\frac{1 + N}{2}$	1.0

Source: Modified from Ref. E8.1.27, Table 20-17, p. 20-33

E3.3.2 Sources of Dependency

The determination of the level of dependence between HFEs is left to the judgment of the HRA analyst. Certain factors typically are recognized as indicators of dependency. Examples of such factors are:

- Common time constraints for task performance
- Common cues or indicators for task performance
- Common diagnosis of situation
- Common facility function or system operation involved in task performance
- Common procedure steps for task performance
- Common personnel and location for task performance
- Common PSFs.

In addition, any human-induced failures of equipment that can directly or indirectly cause other equipment to fail through equipment dependencies are also identified as human dependencies.

E3.4 UNCERTAINTY

As with the values of failure probabilities used for active and passive components used in other parts of the PCSA, it is important that HFE quantification accounts for uncertainty. The HRA quantification, therefore, provides a mean HEP and an expression of the uncertainty. There are a number of ways to approach this task, as each of the HRA methods discussed in Section E3.2.7.2 provides recommendations on uncertainty parameters or bounds for HEPs. These recommendations run from the specific to the general and are often inconsistent. After a review of various recommendations, the HRA team has determined that to use any of them in their specific applications is both impractical and questionable. Rather, it was decided to develop a simple set of generic error factors developed through the use of the judgment by the HRA team, based on a holistic overview of the various recommendations presented in the following sources:

- Section 6 of NARA (Ref. E8.1.9)
- HEART (Ref. E8.1.28)
- Chapter 9 of CREAM (Ref. E8.1.19)
- Chapter 20 of THERP (Ref. E8.1.27).

Although ATHEANA (Ref. E8.1.23) does not provide specific recommendations regarding uncertainty estimation, it stresses that it is important to consider uncertainty in HRAs and that one way to approach it is through the use of expert judgment. To this extent, it can be said that the approach follows the guidance established in ATHEANA.

After review and due consideration of the uncertainty recommendations, the HRA team determined that for the purposes of this study it would be both reasonable and acceptable to establish a generic set of uncertainty parameters based on the calculated (total) HEP for any given HFE. The HRA team reached a consensus on the following error factor values to be applied to a lognormal distribution based on the mean HEP, as shown in Table E3.4-1. For each HEP range, the error factor reflects the HRA team's degree of confidence in the probability estimate.

Table E3.4-1. Lognormal Error Factor Values

Calculated Mean HEP	Lognormal Error Factor
≥ 0.05	3
>0.0005–<0.05	5
≤0.0005	10

NOTE: HEP = human error probability.

Source: Original

The same error factors are applied to both preliminary values and results of detailed HRAs. Therefore, after the HRA team has decided on an appropriate mean value, the corresponding generic error factor is assigned unless there is a basis from the detailed analysis to do otherwise.

E3.5 DOCUMENTATION OF RESULTS

The following information is included in the documentation of the results for the YMP PCSA HRA:

- General discussion of the overall set of PSFs (e.g., error-producing conditions (EPCs), common performance conditions) on human performance that are applicable to or especially important for the YMP PCSA and how they apply to the operations of the facility in question

- A list of all HFEs (by basic event name and category, along with a brief description of the HFE) included in the PCSA model, with their final assigned HFE probabilities

- Identification of preliminary values used for these HFEs

- Identification of all expected pertinent procedures or, if no procedures are expected to exist, alternative evidence that supports the identification and quantification of HFEs and recoveries or substantiates the likelihood of human actions (e.g., normal operating practices, formal training)

- References to sources of input information (e.g., thermal-hydraulic calculations) used in detailed quantification

- Results of qualitative and preliminary analysis.

The following information is generally included in the documentation of the results for the YMP PCSA HRA, but it is not applicable to the Intra-Site Operations HRA:

- Identification of the HFEs analyzed in detail

- A more detailed description of each HFE analyzed in detail

- For each HFE analyzed in detail, identification of the quantification method, associated input parameters (e.g., PSFs), and any approximations or required procedural controls used to determine probabilities for that HFE

- Results of detailed quantitative analysis.

E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT

This section addresses how and what information was collected to support the HRA analysis and how expert judgment was used in the identification and quantification of HFEs.

E4.1 FACILITY FAMILIARIZATION AND INFORMATION COLLECTION

E4.1.1 General Information Sources

As with all of the tasks in the PCSA, facility information is required to support the HRA steps. In addition to the information that is gathered to support the other modeling tasks (e.g., initiating events, systems), the analysts obtain specific additional information that is needed to support the HRA task.

Since the YMP is in the design phase, there are limits on facility-specific information available to support the HRA. Sources utilized in this analysis include the following:

- Design drawings and design studies
- Concept of operations documents
- Engineering calculations
- Discussions of event sequences with knowledgeable individuals
- Event trees and supporting documentation
- Fault trees and supporting documentation.

Information from similar facilities is used, including NPPs (particularly those with ISFSIs), chemical agent disposal facilities, and any other facilities whose primary function includes handling and disposal of very large containers of hazardous material. This was conducted primarily for ISFSI activities at NPPs. The use of this information in place of YMP plant-specific information is pursuant to the third analytical boundary condition specified in Section E2.2. The following are sources of information from ISFSI that are applied to support the YMP PCSA:

- Interviews with plant operators, operations personnel, and/or other ISFSI knowledgeable personnel

- Pertinent ISFSI procedures (e.g., operating procedures, test and maintenance procedures)

- Plant walk-downs (e.g., at locations where operations similar to those at repository may be performed) and operations reviews

- Studies, including PRAs and HRAs, conducted at these facilities that would substitute for the previously mentioned sources.

This information was acquired from two sources. First, information was obtained by the HRA team from outside sources specifically for use on the YMP, such as from NPPs, industry organizations, and governmental sources. Some of this information may have been obtained directly by the HRA team or may have been provided to the HRA team by members of the Licensing and Nuclear Safety, Engineering, or Operations departments who had obtained the information as a part of their regular duties on the YMP (Section E4.2.2). Second, information was obtained by the HRA team directly from internal sources, including members of the aforementioned departments who had past experience and information on ISFSIs from prior employment and projects before joining the YMP (Section E4.2.1).

Initially, information is gathered to support the identification of pre-initiator, human-induced initiator, and non-recovery post-initiator HFEs. This information is needed to:

- Identify test and maintenance activities performed for equipment included in the PCSA model
- Determine the frequency of test and maintenance activities
- Identify the procedures used to perform test and maintenance activities
- 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 PSF.

E4.1.2 Industry Data Reviewed by the HRA Team

The following sources of industry data were reviewed by the HRA team for potential vulnerabilities and HFE scenarios applicable to the YMP:

- "Summary Tables." *Large Truck Crash Causation Study.* (Ref. E8.1.14)
- "Speeding Counts...on All Roads!" (Ref. E8.1.11)
- *Traffic Safety Facts 2002: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System* (Ref. E8.1.13)
- *Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report* (Ref. E8.1.12)
- *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*, NUREG-1774 (Ref. E8.1.20)
- *Control of Heavy Loads at Nuclear Power Plants*, NUREG-0612 (Ref. E8.1.21)

- Navy Crane Center, Naval Facilities Engineering Command Internet Web Site. The database includes the following information:
  - Navy Crane Center Quarterly Reports ("Crane Corner") 2001 through 2007
  - Fiscal Year 06 Crane Safety Report (covers fiscal years 2001 through 2006)
  - Fiscal Year 06 Audit Report.
- U.S. Department of Energy (DOE) Operational Experience Summary (2002 through 2007) (http://www.hss.energy.gov/CSA/analysis/orps/orps.html)
- Institute of Nuclear Power Operations (INPO) database (https://www.inpo.org). The INPO database contains the following information:
  - Licensee Event Reports
  - Equipment Performance and Information Exchange System
  - Nuclear Plant Reliability Data System.
- *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)* (Ref. E8.1.4)
- All Scientech/Licensing Information Service data on ISFSI events (1994 through 2007) Scientech LIS Database and Dry Storage Information Forum (New Orleans, LA, May 2-3, 2001). This database includes the following information:
  - Inspection reports
  - Trip reports
  - Letters, etc.

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 is provided in the *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8).

E4.2.1 Role of HRA Team Judgment

Preliminary and detailed analyses were primarily performed by the HRA team in a consensus-based process. For the preliminary analysis, the judgment process can be summarized in the following fashion:

- 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 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 HRA 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 Intra-Site 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 (SHARP), 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 Novovoronesh Russian nuclear reactor HRAs for the DOE. 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., SHARP 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 (ORE) (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 (ASEP), HEART, NARA, Failure Likelihood Index Methodology (FLIM), Success Likelihood Index Method/Multi-Attribute Utility Decomposition (SLIM/MAUD), Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H), CREAM, Methode d'Evaluation de la Relisation des Missions Operateur pour la Surete (MERMOS), Cause-Based Decision Tree (CBDT), and HCR/ORE.

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.

Below 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)
- Site prime mover (SPM), railcar, truck trailer, cask tractor and cask transfer trailer (HCTT), and site transporter design and operation
- Crane design—No-single failure proof cranes (i.e., jib cranes designed to NUM-1 Type 1B (Ref. E8.1.2)
- Gas sampling process
- Radiation protection (e.g., cask shielding/shield rings; locks, interlocks, and procedural controls for entering high radiation areas)
- General facility (including aging pad and drifts) layout and time line of operations
- Interlocks (general)
- Design and handling of the following: aging overpacks, horizontal shielded transfer casks (HSTC), transportation casks that are never upended (HTCs), transportation casks that are upended using a tilt frame (TTC) and transportation casks that are upended on a railcar (VTC)
- Horizontal aging module (HAM) design and operation
- Ventilation and inspection of cask on the aging pads
- 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.[5]

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

[5] 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 National Aeronautics and Space Administration 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.

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:

- 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[6]—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[7]) 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.

The HRA did not take credit for post-initiator human actions, and no post-initiator HFEs were identified.

[6] The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

[7] 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.

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:

- 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. E8.1.23) 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 Intra-Site Operations

A list of personnel involved in Intra-Site Operations with a brief description of their duties is provided below:

HCTT operator—The person who is designated to operate the cask tractor with cask transfer trailer for HCTT cask transfer activities.

Crane operator—The person who is designated to operate the crane for a given operation (i.e., mobile crane).

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

Forklift operator—The person who is designated to operate the forklift for transferring drums of low-level radioactive waste (LLW).

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 location of casks which come into the geologic repository operations area (GROA)).

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

Signaling crew member—The person who is designated to provide signals to the crane operator. This person is predesignated and is distinguished from the verification crew member (most likely through an orange hard hat, orange gloves, or an orange vest as per the high-level radioactive waste (HLW) *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)* (Ref. E8.1.10)).

SPM operator—The person who is designated to operate the SPM to bring a railcar or truck trailer into the facility.

Site Transporter operator—The person who is designated to operate the site transporter to move an aging overpack into and around the facility.

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

Vendor vehicle operator—The person who operates a vehicle of an authorized vendor transporting materials or personnel into the facility.

Vendor vehicle escort vehicle operator—The person who is designated to operate the vehicle (e.g., golf cart) that escorts a vehicle of an authorized vendor transporting materials or personnel into the facility.

Verification crew member—The person who is designated to assist with crane operations that require a second spotter. This person can only give the stop signal to the crane operator.

E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES

This section discusses the general human performance issues that characterize the human interaction with the YMP facilities.

Limited Automation (Significant Human Interaction)—The types of operations being performed in the Intra-Site Operations are not always conducive to automation. In particular, crane and transport operations are generally performed both manually and locally. Even those that are performed remotely require significant interaction by the operators. The dependence on human performance is quite high, and that dependence provides many opportunities for unsafe actions.

Limited Nature of Procedures—Other than those operations that are performed remotely from a control room, YMP operations are not highly proceduralized, but rather they depend primarily on skills learned and training. That is, while written procedures exist for all activities and training of all personnel is thorough, the actual use of procedures and checklists during operation (i.e., the step-by-step following of written procedures) generally occurs only during operations in a control room. The vast majority of local operations (e.g., skill-of-craft activities performed outside the control room) does not use written procedures at all during the actual performance of the tasks and does not have formal checklists or verbal confirmation requirements spelled out in procedures physically in the possession of the crew performing the operation. This circumstance is consistent with observations of activities at NPPs during ISFSI operations.

Communication Difficulties—There are significant challenges in communication between the team members performing certain Intra-Site Operations. The environment in the entrance and exit vestibules of a facility contains a not insignificant amount of background noise, predominantly machine noise. Although headsets may be used by key participants for communication, they do not eliminate the potential for misunderstanding. 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. For example, local crane operations can create visual challenges. The crane operator can only be at one given distance and orientation with relation to the operation, and therefore cannot be viewed on all three axes. In addition, views may be obstructed, such as by the load being moved or some other structure or equipment. Thus, the operator is often put in the position of being the hands for someone else's eyes, which make the operations vulnerable to the communication vulnerabilities discussed previously.

Unchallenging Activities—The activities involved in Intra-Site Operations are, in general, 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 OVERVIEW OF THE HRA ANALYSIS

Intra-Site Operations cover the following four high-level operational activities:

1. Site transportation of SNF and HLW (rail car and truck trailer)
2. Aging Facility operations (i.e., aging overpack transit, placement, and retrieval from the aging pads)

3. Low Level Waste Facility (LLWF) operations

4. BOP facilities that directly or indirectly establish or support the repository infrastructure and operating services systems.

This section documents the qualitative and quantitative analysis of HFEs associated with the Intra-Site Operations. Since the activities involving site transportation of SNF and HLW, Aging Facility, LLWF, and BOP were treated as separate nodes of the same ESD, the discussion of the relevant HFEs will be discussed sequentially for these facilities rather than as separate groups. Note that no HFEs were identified for BOP activities and the one LLW HFE involving forklift operation was quantified using industry data (Attachment C).

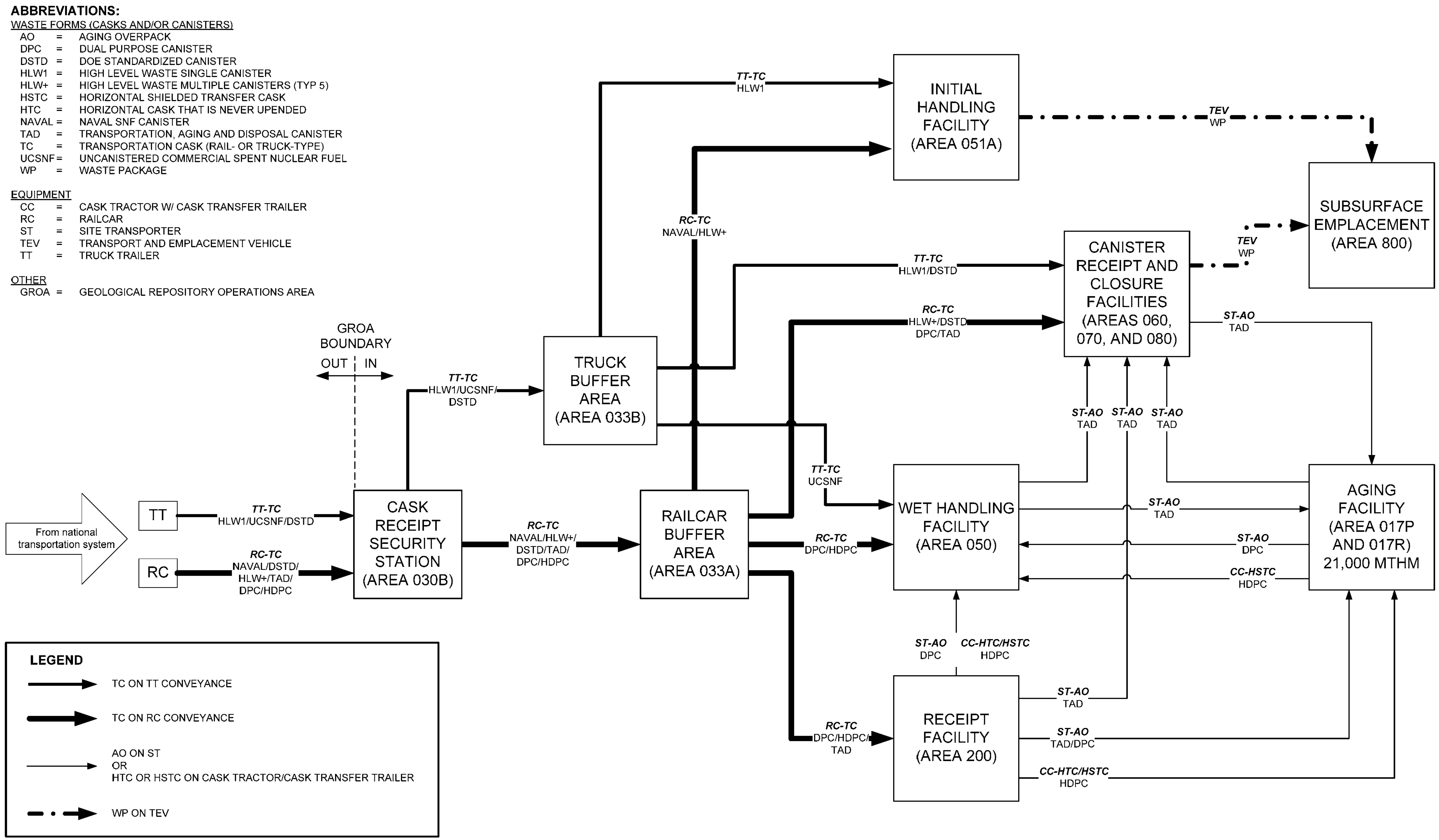
Each high-level operational activity is described in Section E6.1 and Section E6.2 provides a description and quantification for the corresponding HFEs. Table E6.0-1 provides a link between the high-level operational activities described in Section E6.1 and the ESD and the HAZOP nodes. Figure E6.0-1 provides an illustration of the movement of waste forms through the GROA. 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.

Table E6.0-1. Correlation of Intra-Site Operations to ESDs and HAZOP Evaluation Process Flow Diagram Nodes

Activity	HAZOP Evaluation (PFD) Node	ESD
Site Transportation of SNF and HLW (Section E6.1.1)		
Site Transportation – Railcar with Transportation Cask (Section E6.1.1.1)	1, 3-6	1, 9
Site Transportation – Truck with Trailer with Transportation Cask (Section E6.1.1.2)	1, 2, 4-6	
Aging Facility Operations (Section E6.1.2)		
Aging Facility Operations – Aging Overpack (Section E6.1.2.1)	7-8	2, 9
Aging Facility Operations – Transport of HTC or HSTC (Section E6.1.2.2)	10	3, 9
Aging Facility Operations – HAM Activities (Section E6.1.2.3)	11-13	4, 9
Low-Level Waste Facility Operations (Section E6.1.3)		
Low-Level Waste Facility Process (Section E6.1.3)	14-15	5-8
Balance of Plant (Section E6.1.4)		
Balance of Plant Facility Process (Section E6.1.4)	N/A	N/A

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HAZOP = hazard and operability; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; N/A = not applicable; PFD = process flow diagram; SNF = spent nuclear fuel.

Source: Original



Source: Modified from *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8, Figure 15).

Figure E6.0-1. Movement of Waste Forms through the GROA

INTENTIONALLY LEFT BLANK

E6.1 DESCRIPTION OF INTRA-SITE OPERATIONS BASE CASE SCENARIOS

E6.1.1 Site Transportation Activities

The national transportation system delivers transportation casks containing the various waste forms to the site via either rail or truck. Once the conveyance is accepted, the SPM is connected to the conveyance to move it from the security gate to other surface facilities. The SPM, a multi-wheel, tractor-tired and rail-guided vehicle, is used to tow or push railcars, trailers, and other heavy load conveyances.

Movement between repository facilities is accomplished using a site transporter for transportation, aging, and disposal (TAD) canisters and dual-purpose canisters (DPCs), and a HCTT for horizontal DPCs. Figure E6.0-1 provides an illustration of this movement. TAD canisters and DPCs are transferred between facilities in aging overpacks (Section E6.1.2). The boundary of Intra-Site Operations for site transportation activities begins at the entrance to the GROA and ends at the entrance to the preparation area of a facility (i.e., Intra-Site Operations includes the entrance vestibule of a facility).

The primary mode of human failure was considered to be the potential for collisions of other site vehicles with waste forms. These other site vehicles could include site owned-and-operated vehicles (e.g., fork lifts, equipment and supply trucks, etc) as well as externally owned and operated vehicles (e.g., welding gas delivery, LLW pick-up, etc.). The following conditions were anticipated regarding the operation of these vehicles:

- Although speed limits have not yet been established, it is anticipated that they will be established based on imparting less kinetic energy to the potential target than the current PEFA calculations being performed (e.g., less energy than an aging overpack at 2.5 mph, less energy than a 12-ft drop of a transportation cask, etc.). This allows, as a first approximation, the conditional failure probability of the waste form that is calculated for these cases to be used as the conditional failure probability for the collision event.

- All site owned-and operated vehicles are equipped with speed governors or the equivalent set at or below these speeds.

- All externally-owned vehicles are escorted by a member of the security force using a site-owned escort vehicle (e.g., a "golf cart") that is equipped with a speed governor. The externally owned vehicle is required to follow the escort vehicle at all times.

- Whenever a waste form is being moved on site, the security force erects and mans barriers at each road crossing where a site road crosses the path of the waste form.

This sets up a system of multiple, independent actions that would have to be violated in order for a "high-speed" collision to occur.

In similar fashion, vehicles that operate within the facilities, such as forklifts moving supplies, are also be equipped with speed governors.

The general procedure for entering a facility with a SPM attached to a railcar or truck trailer is as follows:

Two crew members are at the facility entrance vestibule. The railcar or truck trailer is pushed by a SPM (a diesel/electric vehicle with on board controls), and is driven by the SPM operator who is located in the cab of the SPM. When the railcar or truck trailer approaches the facility, the conveyance is visually inspected and one crew member opens the outside overhead door and the other crew member uses hand signals to direct the railcar/truck trailer into the facility entrance vestibule, ensuring there are no vehicles or obstructions in the path. The crew members follow all relevant restrictions and procedures regarding railcar/truck trailer speed and direction of travel. Once the railcar/truck trailer has cleared the door, the first crew member closes the outside door then opens the inside overhead door so the railcar/truck trailer can proceed to the facility cask preparation area where it will stop. A crew member then sets the railcar/truck trailer brakes and chocks the wheels. The SPM detaches from the railcar/truck trailer and proceeds back through the facility entrance vestibule to the outside.

E6.1.1.1 Railcar with Transportation Cask

When a cask shipment arrives by commercial rail at the repository site security gate, the conveyance is moved through the outer security gate by the commercial rail locomotive. The locomotive is disconnected and exits the area through the outer security gate. Once the conveyance is released by YMP security, the inner security gate is opened and the SPM is connected to the railcar. Railcars loaded with transportation casks are moved either directly to the various surface facilities or stored in the Railcar Buffer Area. The following is a general description of railcar/personnel interactions:

1. The railcar is pulled by the SPM which runs on a rail, so it cannot be steered.
2. The operator can control the speed of the SPM, but there is a speed limiter (~5 mph) on the SPM.
3. The operator can abruptly stop the railcar.
4. After parking, the operator must set the brakes and chock the wheels of the railcar.
5. In the rail yard, the operators can switch the railcars. Switching the railcars involves engaging or disengaging the connector and air hoses for the braking system of the SPM.
6. There is an interlock that, if the air hoses for the braking system fail, sever, or disconnect, then the mechanical brakes automatically engage. Therefore, if the railcar separates from the SPM, the railcar automatically stops.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

E6.1.1.2 Truck Trailer with Transportation Cask

When a cask shipment arrives by commercial trailer at the repository site security gate, the conveyance is moved through the outer security gate by the commercial truck. The commercial truck is disconnected and exits the area through the outer security gate. Once the conveyance is released by YMP security, the inner security gate is opened and the SPM is connected to the truck trailer. Truck trailers loaded with transportation casks are moved either directly to the various surface facilities or stored in the Truck Buffer Area. The following is a general description of truck trailer/personnel interactions:

1. The truck trailer is pulled by the SPM and runs on a paved road, so the truck trailer can be steered.
2. The operator can control speed of the SPM, but there is a speed limiter (~5 mph) on the SPM.
3. The operator can abruptly stop the truck trailer.
4. After parking, the operator must set the brakes and turn off the SPM's ignition.
5. In the truck yard, the operators can switch the truck trailers. Switching the trailers involves engaging or disengaging the connector and air hoses for the braking system of the SPM.
6. There is an interlock that, if the air hoses for the braking system fail, sever, or disconnect, then the mechanical brakes automatically engage. Therefore, if the trailer separates from the SPM, the trailer automatically stops.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

E6.1.2 Aging Facility Operations

The Aging Facility consists of a series of concrete pads whose purpose is to provide an area for the safe cooling of TAD canisters and DPCs containing commercial spent nuclear fuel (CSNF). The TAD canisters and DPCs requiring cooling are placed into an aging overpack for cooling at one of the two aging pads. DPCs, which arrive in HTCs, do not get placed in aging overpacks, but are placed into a HAM on the southern aging pad. The TAD canisters and DPCs are aged until the thermal heat load of the TAD canister or waste content of the DPCs has decayed to a level low enough to be accepted by a waste package for underground emplacement. The Aging Facility is located north of the North Portal Pad. Figure E6.0-1 provides an illustration of the movement of waste forms between the waste handling facilities and the Aging Facility.

Aging cask and cask transfer equipment support the aging of the CSNF at the Aging Facility. Aging casks consist of aging overpacks and HAMs. The aging casks are either oriented vertically (i.e., aging overpacks, Section E6.1.2.1), or oriented horizontally (i.e., HAMs, Section E6.1.2.3). Cask transfer equipment consists of cask tractors, cask transfer trailers, and crawler-type site transporters. The cask transfer trailers and the site transporters are used to move the aging overpacks and the HAMs containing canisters of CSNF between the various waste handling facilities of the repository to the aging pads.

Generally, transportation casks arriving at the GROA containing CSNF that require aging in TAD canisters or in DPCs are unloaded in the Receipt Facility (RF) and then transferred to aging overpacks. Site transporters are used to move the aging overpacks to one of the concrete aging pads for long-term thermal management. Once the thermal heat output declines to an acceptable level, the aging overpacks are moved to an appropriate waste handling facility for packaging. The Canister Receipt and Closure Facility (CRCF) can provide the receipt and transfer functions of the RF during the first few years of GROA operations before the RF has been constructed and brought on-line. The boundary of Intra-Site Operations includes and ends at the entrance vestibule of a facility.

DPCs that contain CSNF are moved to the Wet Handling Facility (WHF) where the DPCs are opened and the CSNF contents are transferred to TAD canisters. TAD canisters with heat output low enough to be placed into a waste package are moved to the CRCF for processing and subsequent emplacement. TAD canisters and vertically-handled DPCs that require aging are placed into aging overpacks and transported to an aging pad by a site transporter for long-term cool-down.

The Aging Facility provides the capability to:

- Age up to 21,000 metric tons of heavy metal at the repository
- Store nuclear waste in canisters with high thermal power in a location where they can cool to appropriate levels
- Move waste in canisters between the aging pads and waste handling facilities
- Decouple the receipt of waste from the subsurface emplacement of the waste by creating a location to house and cool waste canisters by natural convection until the handling facilities can accommodate it.

The Aging Facility consists of three basic systems:

- Aging pads
- Aging casks (i.e., aging overpacks and HAMs)
- Cask transfer equipment (crawler type site transporters and HCTTs).

There are two basic variations of Aging Facility operations, as follows:

1. Aging waste forms in a vertical orientation (Section E6.1.2.1), including the following activities:

   A. Transit to an aging pad in aging overpacks via a site transporter

B. Placement of aging overpacks on the aging pads

C. Retrieval of aging overpacks and transit to a waste handling facility via a site transporter.

2. Aging horizontal DPCs in HAMs, including the following activities:

A. Transit of a horizontal DPC in an HTC to the Aging Facility; retrieval of the horizontal DPC in an HSTC from the Aging Facility and transport to the WHF (Section E6.1.2.2)

B. Placement or retrieval of horizontal DPC from HAMs (Section E6.1.2.3).

E6.1.2.1 Site Transporter Movement of an Aging Overpack (TAD canisters and DPCs)

The site transporter is used to transfer aging overpacks between the waste handling facilities and the aging pads. Loaded vertical aging overpacks containing canistered CSNF are lifted and moved to and from the aging pads using a site transporter. The following is a general description of site transporter/personnel interactions:

1. The site transporter runs on a (dirt) road, and can be steered.
2. The site transporter operator can control the speed of the site transporter; however, it is equipped with a speed limiter. In addition, the speed is limited by the power of the motor.
3. The operator can abruptly stop the site transporter.
4. When parking, the operator sets the brakes and turns off the site transporter.
5. Crew members strap the aging overpack in the site transporter.
6. The site transporter does not lift the aging overpack more than ~six in.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

The following activities are associated with site transporter movement of aging overpacks containing TAD canisters and DPCs:

- The loaded aging overpack is moved to the Aging Facility. The operator uses the site transporter to transfer a loaded aging overpack with a TAD canister from the WHF, or a loaded aging overpack with either a TAD canister or DPC from the CRCF or RF, to the Aging Facility.

- The loaded aging overpack is placed in the assigned aging pad location. At the Aging Facility, the aging overpack is lowered into place, the lifting mechanism is disengaged and the site transporter is moved away.
- The aging temperature sensors are installed on the aging overpack (if required) to monitor the age of the loaded aging overpack.
- Temperature sensors are disconnected upon conclusion of the aging process.
- The loaded aging overpack is moved with the site transporter to the CRCF or WHF once the aging process is complete.

E6.1.2.2 Transportation and Positioning of the HTC or HSTC

The transportation of horizontal DPCs in HTCs or HSTC is conducted utilizing a HCTT, a specially designed cask transfer trailer that is towed by a separate cask tractor. The boundary of Intra-Site Operations for moving an HCTT unit into or out of a facility includes and ends at the entrance vestibule of that facility. The following actions are associated with this activity:

- The horizontal DPC in an HTC is moved via the HCTT to the designated HAM on Aging Facility.
- Once aged, the horizontal DPC is unloaded from the HAM. The HCTT is aligned with the HAM access port, the horizontal DPC is loaded into an HSTC, and the loaded HSTC is transported to the appropriate waste handling facility.

E6.1.2.3 Canister Operations at the HAM

Using the cask transfer trailer, the cask is transported from the RF to the Aging Facility. A portable commercial mobile crane capable of lifting the HAMs concrete closure ports and the end cover lids of the transportation casks (and HSTCs) is used to support DPC insertion and retrieval operations to and from the HAM. The casks and HAM are capable of protecting the canister from credible accidents or operator errors associated with lid removal and installation on the casks or HAMs such as a drop of a lid onto the cask or HAMs.

The cask transfer trailer is positioned within a few feet of the HAM. The position of the trailer is checked to ensure that the centerline of the HAM and cask approximately coincide. If the trailer is not properly oriented, the trailer is repositioned as necessary.

Outriggers and jacks are used to stabilize the cask and the cask transfer trailer during the transfer of a DPC into the HAM. A hydraulic ram and hydraulic power unit are set up behind the cask and aligned to engage the hydraulic ram to the DPC ram grapple rings. The hydraulic ram cylinder is actuated to insert the DPC into the HAM. The transfer is facilitated using the support guide rails inside the HAM.

Operations begin, with a DPC loaded in an HTC on the cask transfer trailer (from the RF). The following steps are performed as part of HAM loading and unloading operations:

E6.1.2.3.1 Movement of a DPC from an HTC into a HAM

The following steps are performed to move a DPC from an HTC into a HAM:

1. The loaded HTC is aligned with the access port of the designated HAM. The HCTT operator visually aligns the HCTT with the HAM with the help of a crew member who watches and directs the HCTT operator.
2. The closure door on the HAM and the closure lid on loaded HTC are removed.
3. The DPC inside the HTC is aligned with the DPC cradle inside HAM.
4. The loaded HTC is docked and restrained to the HAM access port. The operators install struts to tie the skid to the HAM.
5. The hydraulic ram access cover is removed from the loaded HTC.
6. The hydraulic ram on the cask transfer trailer is raised.
7. The ram grapple with DPC is engaged and the DPC is inserted from the HTC into the HAM.
8. The hydraulic ram and grapple are retracted from the DPC and undocked from the HAM.
9. DPC restraints are installed, as required.
10. The closure door is installed on the HAM.

E6.1.2.3.2 Age and Monitor DPC in HAM

Aging temperature sensors are installed and the condition of air inlet/outlet ports is verified.

E6.1.2.3.3 Retrieve DPC from HAM and Insert into HSTC

The following steps are performed to retrieve a DPC from a HAM and insert the DPC into an HSTC:

1. The closure door on the HAM and the closure lid on unloaded HSTC are removed.
2. DPC restraints are removed as required.
3. The unloaded HSTC is aligned with the DPC inside of the HAM.
4. The HSTC is docked and restrained to the HAM access port.
5. The hydraulic ram access cover on the HSTC is removed and the hydraulic ram on the cask transfer trailer is raised.

6. The ram grapple is engaged with the DPC and the DPC is moved from the HAM into the HSTC.

7. The loaded HSTC is undocked from the HAM and the hydraulic ram is lowered.

8. The HSTC closure lid and ram access cover are installed and the closure door is placed on the HAM.

9. The loaded HSTC is moved to the WHF.

E6.1.3 Low-Level Waste Facility Activities

The LLWF is designed for the collection, processing, and disposal of LLW streams generated during the handling of HLW and SNF.

The LLWF is designed as a commercially-available structure with a steel frame. Four separate shielded storage bays, with partial-height-walls, are located inside the building on the side of the facility opposite the truck bay. These four bays provide for interim storage of boxes, drums, high integrity containers, filters, and empty DPCs. A concrete storage pad is located outside the facility adjacent to the four storage bays.

A pull-through truck bay is located on one end of the building. This area has hatches through which waste containers are moved. An open process area is located adjacent to the Receipt Area, which contains a scale and areas for the storage of supplies and tools. Other areas that are entered from the open process area include the Cold Support Area, Decontamination Room, Glove Box Area, and two sorting rooms.

E6.1.4 Balance of Plant Facility Activities

The BOP facilities provide the space, layout, and embedded facilities that directly or indirectly establish or support the repository infrastructure and operating services systems.

The BOP facilities extend beyond the GROA to provide infrastructure and to interface with offsite services and functions (i.e., the primary site access road, service roads, South Portal, North Construction Portal, and utility structures).

The BOP facilities provide operational infrastructure and services for waste handling operations and waste emplacement facilities but do not directly perform waste handling or waste emplacement operations or processes.

E6.2 ANALYSIS OF INTRA-SITE 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 HFEs 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 chose 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/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 programmable logic controllers were not credited in this analysis since they won't be declared important to safety.

Crane Drops (Drop of Object onto Cask)—There are several lifts of heavy objects in the Intra-Site Operations involving mobile cranes (considered as jib cranes) which can potentially result in a drop. Crane drop related HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for this failure can be found in Attachment C.

E6.2.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenarios, 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 Intra-Site Operations are summarized in Table E6.1-1. Tables E6.1-2 and E6.1-3 provide additional data to support the analysis in Table E6.1-1. 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.

Table E6.2-1. Descriptions and Preliminary Analysis for Intra-Site Operation HFEs

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
ISO-OPRCCOLLIDE1-HFI-NOD	*Operator Causes Prime Mover Railcar (PMRC) Collision*: Operator causes the collision of a railcar with a facility structure, piece of equipment, or another vehicle while moving through the Entrance Vestibule of a facility.	1	3E−03	The SPM moves the railcar into a facility vestibule. There are three observers with clear visibility, the operation is simple, the railcar speed is low, the distance is short, and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a railcar are limited, and include: • Backward motion beyond the limit could result in collision with the end stops, wall, or vestibule doors. • Improperly attached railcar could continue moving when SPM stops, resulting in collision with the end stops, wall, or vestibule doors. • Forklift or other auxiliary vehicle could collide into the conveyance. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted because there are several ways for a collision to occur, and there are potentially multiple other vehicles (forklifts) that can collide into the conveyance (×3).
ISO-OPRCINTCOL01-HFI-NOD	*Operator Initiates PMRC Runaway*: Operator causes a collision of the railcar at a speed higher than design requirements. If the speed governor of the SPM fails, the operator could collide the railcar into an SSC.	1	1	The operator can cause the SPM to over speed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.
ISO-OPSTCOLLIDE2-HFI-NOD	*Operator Error Causes Site Transporter Collision*: Operator causes a collision of the site transporter with a facility structure, piece of equipment, or another vehicle while entering or exiting a facility.	2	3E−03	In this step, the site transporter, loaded with an aging overpack, enters or exits a facility. There are three observers with clear visibility, the operation is simple, the conveyance speed is low, the distance is short and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a site transporter are limited, and include: • Backward motion beyond the limit could result in collision with the end stops, wall, or vestibule doors. • Forklift or other auxiliary vehicle could collide into the conveyance. The preliminary value was chosen based on the determination that this failure is “Highly Unlikely” (0.001) and was adjusted (×3). consistent with other collision events.
ISO-OPTTCOLLIDE1-HFI-NOD	*Operator Causes Truck Trailer Collision*: Operator causes a collision of the truck trailer with a facility structure, piece of equipment, or another vehicle while moving through the Entrance Vestibule of a facility.	1	3E−03	In this step, the SPM with truck trailer moves into a facility vestibule. There are three observers with clear visibility, the operation is simple, the truck trailer speed is low, the distance is short and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a truck trailer are limited, and include: • Improper (i.e., backward or lateral) motion could result in collision with the end stops, wall, or vestibule doors. • Improperly attached trailer could continue moving when truck stops, resulting in collision with the end stops, wall, or vestibule doors. • Forklift or other auxiliary vehicle could collide into the conveyance. The preliminary value was chosen based on the determination that this failure is “Highly Unlikely” (0.001) and was adjusted (×3) consistent with other collision events.
ISO-OPTTINTCOL01-HFI-NOD	*Operator Initiates Truck Trailer Runaway*: Operator causes a collision of the truck trailer at a speed higher than design requirements. If the speed governor of the SPM fails, the operator could collide the truck trailer into an SSC.	1	1	The SPM can over speed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.