Division of High-level Waste Repository Safety - Interim Staff Guidance
HLWRS-ISG-04, PRECLOSURE SAFETY ANALYSIS - HUMAN RELIABILITY ANALYSIS

INTRODUCTION

The purpose of this Interim Staff Guidance (ISG) is to supplement the Yucca Mountain Review Plan (YMRP) [Ref. 1] for the staff review of human reliability analysis (HRA) contained in the preclosure safety analysis (PCSA). Specifically, this ISG identifies additional U.S. Nuclear Regulatory Commission (NRC) guidance available to aid in the review of HRA in the PCSA, and provides additional considerations in areas of the license application (LA) review that are potentially affected by HRA. In this ISG, "the HRA" refers to any consideration of human performance in the PCSA analyses, i.e., the evaluation of the potential for, and mechanisms of, human errors that may affect safety of the geologic repository operations area (GROA) operations, including consideration of human reliability, as it relates to design and programs such as training of personnel. This ISG revises Sections 2.1.1.2, 2.1.1.3, 2.1.1.4, 2.1.1.6, 2.1.1.7, 2.5.5, and 2.5.6 of the YMRP. Note that High-Level Waste Repository Safety (HLWRS) ISG-02 [Ref. 2] is applicable to HRA, as well.

DISCUSSION

Regulations for licensing a proposed geological repository at Yucca Mountain, Nevada, are contained in the *Code of Federal Regulations*, Title 10, Part 63 (10 CFR Part 63). The risk-informed and performance-based preclosure compliance requirements in Part 63 provide the U.S. Department of Energy (DOE) with the flexibility to develop a design and demonstrate that it meets performance objectives for preclosure operations. NRC licensing decisions will be based on the proposed design and operations that DOE submits with the LA.

There have been no accidents[1] in spent-fuel handling in the commercial nuclear power industry in the U.S., but operational events (process disruptions) can be reviewed for insights into potential precursor incidents (e.g., those that had the potential to affect public and/or worker health and safety, had the event evolved less favorably). Operating experience shows that human errors: (1) contributed to the majority of operational events that have occurred; and (2) may dominate the failure modes for some equipment and systems (e.g., cranes[2]). In addition, operating experience shows that administrative controls are important to safe operations and human reliability. Hence consideration of human reliability in the PCSA may be important in: (1) identifying initiating events and event sequences; (2) categorization of events sequences; and (3) assessing the rigor of administrative and/or procedural safety controls.

---

1 "Accident," in this case, would be a safety incident with radiological consequences to members of the public.

2 For example, NUREG-1774 [Ref. 3] states: "The percentage of crane issue reports caused by poor human performance has increased over time, and for the last several years, averaged between 70 and 80 percent…. Human error, whether directly associated with supervisors or equipment operators represented approximately 94 percent of DOE [Hoisting and Rigging] incidents…. As shown in Navy crane data for 1995-1999, human factors or human errors are the leading causes of Navy crane issues, in that the categories of improper operation, improper rigging, and procedure failure accounted for approximately 88 percent of Navy crane issues" [Ref. 3, p. 70].

Assessing human reliability is qualitatively different and may be more complicated than assessing reliability of hardware components that fail randomly, because human failure events (HFEs) are highly dependent on context. Context includes, for example: (1) the evolution of a particular situation; (2) whether it is practical to use job aids such as written procedures; (3) the training and requisite knowledge of the team carrying out actions; and (4) a variety of other performance-shaping and contextual factors such as stress, fatigue, or environment in which actions must be performed. These performance-shaping and contextual factors vary across: (1) industries (e.g., highly regulated and proceduralized nuclear power industry versus chemical industry); (2) facility-types (e.g., at-power nuclear power-generation operations where rule-based control-room tasks may dominate, versus nuclear materials facility activities where skill-based manual tasks may dominate); and (3) individual facilities and facility sites within a facility type and industry group. The HRA supporting the PCSA in an LA should address site-specific and facility-specific features, as appropriate.

After the YMRP was published, NRC published two major guidance documents in the area of HRA. Although these documents were written in the context of HRA for nuclear power plant applications involving internal events and full-power operations, much of the general guidance is appropriate for other HRA applications, too. This ISG updates and supplements the YMRP, to explicitly refer staff to the generic portions of these key HRA guidance documents, to aid in an LA review, and expands on these guidance documents, to address key HRA issues that are specific to a high-level waste repository. This ISG also recommends the deletion of reference to NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* [Ref. 4], in the YMRP, since the newer NRC guidance documents supersede this older NRC report.

When reading the guidance in this ISG, staff should keep in mind that 10 CFR Part 63 is a risk-informed, performance-based regulation that leaves DOE flexibility in its approach to demonstrating compliance with the performance objectives. DOE may choose from a variety of approaches that, with adequate technical bases, can successfully demonstrate regulatory compliance. The staff review approach and focus necessarily will depend on the approach chosen in the LA. In addition, the staff review should be risk-informed. Staff should not construe guidance in this ISG to mean that staff should expect a full HRA (i.e., encompassing all elements of a complete HRA), including quantification of all human-error probabilities in the PCSA. Staff members should expect to focus their efforts on risk-significant aspects of the review, rather than treating all parts of the PCSA equally. Much of the technical review guidance outlined below applies to the most risk-significant aspects of the LA review, as noted. Risk-informed scrutiny[3] may depend on many factors, such as: (1) focus on the GROA activities and/or facilities that pose the highest potential hazard; (2) uncertainty in the analysis, because of complexity of operations or limitations in supporting data that are available; and/or (3) limitations in available state-of-the-art methods and approaches. The goal of the review is to evaluate whether there is reasonable assurance that the performance objectives in Part 63 will be met, which in turn is determined by: (a) whether an identified event sequence is category 1, category 2, or beyond category 2; and (b) whether the projected consequence(s) meets the performance objective for that category. NRC expects the data and information in an LA to be

3 See Regulatory Guide 1.174 [Ref. 5] for a discussion on general risk-informed integrated decision-making principles. Although this Regulatory Guide is for power reactor applications, the general discussion on the application of NRC's risk-informed regulatory principles is useful for other regulatory applications.

commensurate with supporting these determinations, rather than supporting precise quantification for all event sequences. Staff should also recognize that the analysis of how human performance fits into planned operations and meeting performance goals at the GROA may appear in many different parts of the PCSA, and in varying scopes (in other words, human performance is likely to be addressed in different relevant parts of the PCSA, rather than addressed together in one place).

The guidance in this ISG is written with the expectation that staff will seek the assistance of an HRA specialist(s) for review of risk-significant aspects of an LA affected by human performance.

TECHNICAL REVIEW GUIDANCE

Level of Information

It is important to have a conceptual understanding of how human performance fits into the planned GROA operations and safety. Although quantified reliability estimates are typically needed for categorizing event sequences, much of the HRA review should focus on the HRA tasks, that are performed as part of an overall PCSA, that explain the conceptual understanding of human performance in the planned operations. These tasks are part of the qualitative HRA analysis and would include, for example: (1) identification of HFEs and unsafe actions; (2) identification of important factors influencing human performance; and (3) selection of appropriate HRA quantification method(s), if considered necessary. As part of these qualitative HRA tasks, staff should review the identification of both errors of commission (EOC) and errors of omission (EOO) (although the specific terms “EOC” and “EOO” may not be used in the LA).

For risk-significant human actions in the PCSA, reviewers should verify that the LA contains sufficient information to review the qualitative HRA analyses. Examples of human actions that are risk-significant include: (1) direct manual operator actions that are related to reliability of important-to-safety (ITS) structures, systems, or components (SSCs); (2) administrative or procedural safety controls that are related to reliability of ITS SSCs and involve human actions; or (3) human actions that contribute significantly to the reliability of ITS SSCs. Staff should tailor the scope and emphasis of its review to the approach taken in the LA, and the extent to which human actions are (or are not) relied on to meet Part 63 performance objectives.

Acceptable Methods and Approaches

Staff should expect the HRA approaches in different parts of the PCSA (e.g., for different facilities or operations) to be commensurate with the associated risk significance. Reviewers should verify that the HRA for *risk-significant* processes at the GROA was performed following a complete and technically appropriate HRA process. A complete process includes the following HRA tasks: (a) identification of HFEs, and associated unsafe actions, to be considered in the overall PCSA; (b) identification of important factors influencing human performance (both traditional “performance-shaping factors” and contextual factors); (c) selection of HFE classes, categories, or other terms that assist in selecting the appropriate HRA quantification method(s), if needed[4]; (d) selection of appropriate HRA quantification method(s) (if needed); (e) application

4 Some event sequences may be screened out from further analysis based on a consequence analysis, in which case quantification of a human error probability would not be needed, for example.

of appropriate HRA quantification method(s) (if needed); and (f) documentation of the overall HRA. Using an appropriate process to properly identify the potential HFEs is a crucial step (part of the qualitative analyses), and one that should help form the basis for subsequent tasks, such as quantification of reliability (if needed). Note that staff review should be tempered by the level of risk posed by human actions for different facilities and activities. For example, if the LA demonstrates that acceptable risk is achieved through robust hardware design features that cannot be defeated by human actions (EOOs or EOCs), HRA activities (b) through (e) may be omitted or significantly reduced in scope.

The HRA for the GROA should be appropriately integrated with other aspects of the PCSA. Staff should verify that human reliability, when relevant, was considered for risk-significant activities in all PCSA steps, such as the identification of hazards and initiating events, development and evaluation of event sequences, and identification and evaluation of ITS SSCs and administrative and procedural safety controls.

Staff should verify that any HRA in the LA is consistent with NRC's expectations for quality. NUREG-1792, *Good Practices for Implementing Human Reliability Analysis* [Ref. 6], provides good general guidance on reviewing HRA in a risk assessment. However, because NUREG-1792 was written in the context of a risk assessment for full-power and internal-events nuclear power plant applications,[5] the emphasis of specific "good practices" in this NUREG may be different for application to the GROA PCSA. For example, as mentioned above, the qualitative tasks are likely to be important for the GROA, and NUREG-1792 may not provide sufficient guidance in this area. In addition, in HRAs for nuclear waste facilities, the role of human-induced initiators may be more dominant than that of post-initiator HFEs,[6] and NUREG-1792 does not separately address human contributions to initiating events. For waste-facility initiators that may not have safeguards to prevent events-in-progress, once initiated (e.g., drop events), the human-induced initiator and the sequence of events leading up to the initiator (pre-initiators), may be of especial interest for the HRA/PCSA effort. Staff should verify that HRA treatment of risk-significant human-induced initiators is consistent with generic good practices, in NUREG-1792, for post-initiator HFEs.

Similarly, not all aspects of NUREG-1792 may be appropriate for evaluating the adequacy of HRA in the GROA PCSA. For example, the good practices about quantification need not be considered where quantification is not needed, and the suggested screening values for human error probabilities may not be appropriate for the GROA. Guidance from NUREG-1792 should be considered, along with operating experience from facilities and activities similar to those projected at the GROA, to evaluate the adequacy of the HRA approach in the PCSA. Note that NUREG-1792 alludes to a risk-informed approach in applying the good practices, and that the

5 NUREG-1792 [Ref. 6] states: "...although this report was written for full-power applications, many of the good practices will also apply to low-power and shutdown operations; however, these practices will not be sufficient for addressing the unique characteristics of such modes of operation. In addition, elements of this report may prove beneficial in examining human actions related to nuclear materials and safeguard-related applications" [Ref. 6, p. 2-1].

6 This is in part because compared to nuclear power plants, waste-processing facilities typically involve more manual actions and may employ fewer safeguards against human-induced initiators, because of lower levels of risk and complexity.

level of treatment of human actions in the safety analysis is expected to be commensurate with risk significance.[7]

NUREG-1842, *Evaluation of Human Reliability Analysis Methods Against Good Practices* [Ref. 7], provides guidance on the strengths and weaknesses of different available HRA methods. Although the evaluation criteria in NUREG-1842 were specific to full-power and internal-events nuclear-power-reactor applications, it is still a useful general aid to staff when evaluating the appropriateness of HRA methods used in support of the GROA PCSA. DOE has the flexibility to choose any method(s) to support the PCSA, given there is a sufficient technical basis for applying the method(s) and approach(es) to the GROA.

Consideration of Applicability of Data and Approaches

Staff should expect the use of HRA approaches and data that are based on applications for commercial nuclear power plants or other facilities, to be justified, as there could be uncertainty about whether the approaches and data are applicable to the GROA. If qualitative HRA screening criteria are used, staff should review the justification specifically for the GROA, rather than relying on justification simply by their prior development and use for HRAs for commercial nuclear-power plants or other facilities. Staff should expect the use of any quantification method, either data-driven or model-driven, to be justified regarding its applicability to GROA operations. In addition, if an approach that was used were to rely on an empirical failure rate (e.g., for crane-load drops) for implicit inclusion of human reliability considerations, staff would need to verify that it is justified with an adequate technical basis that demonstrates it is an appropriate approach for the GROA. In such cases, data should reflect the characteristics or features of the GROA, especially if the failure rate is dominated by human-induced failures. Any implicit assumptions on the existence and efficacy of administrative controls contained in the empirical data should be identified for subsequent verification. See Appendix A for an illustrative example.

Relationship to Programmatic Review and Licensing Specifications

Assumptions made in the HRA should be supported by an appropriate personnel training program and other administrative controls. Insights from HRA should also be reflected in the development and implementation of training and administrative programs for safety.

As mentioned in the discussion section, human performance is highly dependent on context and may be sensitive to facility-specific factors such as how administrative controls are implemented. Human reliability is dependent on effective human factors engineering (e.g., development and implementation of training, and design of human-system interfaces). NUREG-0711, *Human Factors Engineering Program Review Model* [Ref. 8], and NUREG-0700, *Human-System Interface Design Review Guidelines* [Ref. 9] provide general review guidance and reference industry standards and guides for human factors engineering. For any risk-significant human actions identified in the PCSA, the staff should identify any assumptions that need to be verified in the program reviews (e.g., adequacy of training program, human-factors evaluations),

7 For example, NUREG-1792 [Ref. 6] notes: "In some cases, the need to meet good practices could potentially be determined through the use of importance measures of the human actions being modeled. Documents such as NUREG-1764… provide guidance for ranking human actions by measures of importance. Such a categorization scheme could help reviewers determine the degree to which a good practice needs to be addressed" [Ref. 6, p. 1-3].

and assumptions that need to be verified during construction or operations (e.g., efficacy of certain administrative and procedural controls). As necessary, the staff should check that DOE verifies risk-significant assumptions and identifies relevant programmatic elements supporting the HRA as probable subjects for license specifications in the LA.

REGULATORY BASIS

The following regulations provide the bases for this ISG [note that 1-7 are the same as the bases for HLWRS-ISG-02 (Ref. 2)]:

1. *Event sequence* means a series of actions and/or occurrences within the natural and engineered components of a geologic repository operations area that could potentially lead to exposure of individuals to radiation. An event sequence includes one or more initiating events and associated combinations of repository system component failures, including those produced by the action or inaction of operating personnel. Those event sequences that are expected to occur one or more times before permanent closure of the GROA are referred to as Category 1 event sequences. Other event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences [10 CFR 63.2, "Event Sequences"].

2. During normal operations, and for Category 1 event sequences, the annual Total Effective Dose Equivalent (TEDE) to any real member of the public located beyond the boundary of the site may not exceed the preclosure standard specified in 10 CFR 63.204 [10 CFR 63.111(a)].

3. The GROA must be designed so that, taking into consideration any single Category 2 event sequence and until permanent closure has been completed, no individual located on, or beyond, any point on the boundary of the site, will receive, as a result of the single Category 2 event sequence, the more limiting of a TEDE of 0.05 Sievert (Sv) (5 rem), or the sum of the deep dose equivalent and the committed dose equivalent to any individual organ or tissue (other than the lens of the eye) of 0.5 Sv (50 rem). The lens dose equivalent may not exceed 0.15 Sv (15 rem) and the shallow dose equivalent to skin may not exceed 0.5 Sv (50 rem) [10 CFR 63.111(b)(2)].

4. A PCSA of the GROA that meets the requirements specified in 10 CFR 63.112 must be performed. This analysis must demonstrate that: (1) The requirements of 10 CFR 63.111(a) will be met; and (2) The design meets the requirements of 10 CFR 63.111(b) [10 CFR 63.111(c)].

5. The PCSA of the GROA must include a general description of the SSCs, equipment, and process activities at the GROA [10 CFR 63.112(a)].

6. The PCSA of the GROA must include an analysis of the performance of the SSCs to identify those that are ITS. This analysis identifies and describes the controls that are relied on to limit or prevent potential event sequences or mitigate their consequences. This analysis also identifies measures taken to ensure the availability of safety systems. The analysis must include, but not necessarily be limited to, consideration of...(8) the ability of SSCs to perform their intended safety functions, assuming the occurrence of event sequences [10 CFR 63.112(e)].

7. The PCSA of the GROA must include a description and discussion of the design, both surface and subsurface, of the GROA, including: (1) The relationship between design criteria and the requirements specified in 10 CFR 63.111(a) and (b); and (2) The design bases and their relation to the design criteria [10 CFR 63.112(f)].

8. The safety analysis report must include the following information concerning activities at the GROA: (1) personnel qualifications and training requirements; (2) plans for startup activities and startup testing; and (3) plans for conduct of normal activities, including maintenance, surveillance, and periodic testing of SSCs of the GROA [10 CFR 63.21(c)(22)(iii)-(v)].

9. The safety analysis report must include an identification and justification for the selection of those variables, conditions, or other items that are determined to be probable subjects of license specifications. Special attention must be given to those items that may significantly influence the final design [10 CFR 63.21(c)(18)].

RECOMMENDATIONS

The following changes to the YMRP are recommended:

1. Page 2.1-16: Revise Section 2.1.1.2.2, "Review Method 6," as follows:

Add the following to the end of the first sentence:

, including key human actions.

2. Page 2.1-18: Revise Section 2.1.1.2.3, "Acceptance Criterion 6, Item (1)" as follows:

Add the following after “activities”:

, including key human actions

3. Page 2.1-21: Revise Section 2.1.1.3.2, "Review Method 2," as follows:

Add a sentence to the end of the second to last paragraph:

Confirm that any human-induced pre-initiators (those actions that can lead to initiating events, such as maintenance acts that inconspicuously reconfigure systems in an unsafe way) as well as human-induced initiating events, are identified.

4. Page 2.1-22: Revise Section 2.1.1.3.2, "Review Method 3," as follows:

Change the last sentence of the last paragraph to:

Guidance from documents such as NUREG-1842 (U.S. Nuclear Regulatory Commission, 2006); NUREG-1792 (U.S. Nuclear Regulatory Commission, 2005); and NUREG-1624 (U.S. Nuclear Regulatory Commission, 2000b); can assist the review.

5. Page 2.1-23: Revise Section 2.1.1.3.3, "Acceptance Criterion 1," as follows:

Change (4) to read:

Assumptions used to identify naturally occurring and human-induced hazards and initiating events, as well as human-induced pre-initiators, are well-defined, have adequate technical bases, and are supported by information on the site and its structures, systems, components, equipment, and operational and maintenance processes.

6. Page 2.1-25: Revise Section 2.1.1.3.5, "References," as follows:

Delete the following reference:

———. NUREG–1278, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application.” Washington, DC: U.S. Nuclear Regulatory Commission. 1983b.

Add the following references:

———. NUREG–1792, “Good Practices for Implementing Human Reliability Analysis.” Washington, DC: U.S. Nuclear Regulatory Commission. 2005.
———. NUREG–1842, “Evaluation of Human Reliability Analysis Methods Against Good Practices.” Washington, DC: U.S. Nuclear Regulatory Commission. 2006.

7. Page 2.1-26: Revise Section 2.1.1.4.2, "Review Method 2," as follows:

Add the following to the end of the second paragraph:

, and that the choice and application of method(s) include appropriate consideration of human factors specific to the GROA design and operations. Verify that any human reliability analysis in the license application is consistent with generic good practices in NUREG-1792 (U.S. Nuclear Regulatory Commission, 2005).

8. Page 2.1-48: Revise Section 2.1.1.6.3, "Acceptance Criterion 2 (1)," as follows:

Replace with:

(1) Management systems and procedures are sufficient to ensure that administrative or procedural safety controls will function properly, taking human reliability into account; and

9. Page 2.1-56: Revise Section 2.1.1.7.2.3, “Review Method 1, (5)," as follows:

Add item (g):

Applicable standards or guides for human factors engineering, such as NUREG-0700 (NRC, 2002) or NUREG-0711, Rev. 2 (NRC, 2004).

10. Page 2.1-59: Revise Section 2.1.1.7.2.3, “Review Method 1," as follows:

Replace 2nd paragraph with:

Verify that the assumptions made for the design of the subsurface facility are technically defensible, including with respect to human actions required for controls.

11. Page 2.1-70: Revise Section 2.1.1.7.3.3, “Acceptance Criterion 2," as follows:

Change (3) to read:

(3) The design of the waste emplacement system is compatible with proposed waste emplacement procedures and required human actions. Interfaces with other systems are identified and assessed, and continuity of operations and safety can be achieved;

Change (6) to read:

(6) Standards and codes used for design of subsurface operating systems are properly applied, including standards or guides for human factors engineering.

12. Page 2.1-76: Revise Section 2.1.1.7.5, "References," as follows:

Add the following references:

———. NUREG–0700, “Human-System Interface Design Review Guidelines.” Washington, DC: U.S. Nuclear Regulatory Commission. 2002.

———. NUREG–0711, Rev. 2, “Human Factors Engineering Program Review Model.” Washington, DC: U.S. Nuclear Regulatory Commission. 2004.

13. Page 2.5-68: Revise Section 2.5.5.2, "Review Method 7," as follows:

Replace first sentence with:

Confirm the license application provides an assessment of testing results and operational lessons learned from similar facilities, including insights on human factors considerations.

14. Page 2.5-72: Revise Section 2.5.5.3, "Acceptance Criterion 7 (1)," as follows:

Replace with:

The license application provides an assessment of testing results and operational lessons learned from similar facilities, including human factors considerations, and this assessment is used to develop testing procedures of adequate scope.

15. Page 2.5-76: Revise Section 2.5.6.2, "Review Method 1," as follows:

Insert the following in the list of items (1)-(9), and renumber item (9) as item (10):

(9) Human factors engineering

16. Page 2.5-78: Revise Section 2.5.6.2, "Review Method 2," as follows:

Insert the following in the list of items (1)-(9), and renumber item (9) as item (10):

(9) Human factors engineering

17. Page 2.5-79: Revise Section 2.5.6.2, "Review Method 3," as follows:

Insert the following in the list of items (1)-(9), and renumber item (9) as item (10):

(9) Human factors engineering

18. Page 2.5-81: Revise Section 2.5.6.2, "Review Method 4," as follows:

Insert the following in the list of items (1)-(9), and renumber item (9) as item (10):

(9) Human factors engineering

19. Page 2.5-83: Revise Section 2.5.6.3, "Acceptance Criterion 1 (4)," as follows:

Insert the following in the list of items (a)-(i), and renumber item (i) as item (j):

(i) Human factors engineering

20. Page 2.5-84: Revise Section 2.5.6.3, "Acceptance Criterion 2 (4)," as follows:

Insert the following in the list of items (a)-(i), and renumber item (i) as item (j):

(i) Human factors engineering

21. Page 2.5-86: Revise Section 2.5.6.3, "Acceptance Criterion 3 (5)," as follows:

Insert the following in the list of items (a)-(i), and renumber item (i) as item (j):

(i) Human factors engineering

22. Page 2.5-87: Revise Section 2.5.6.3, "Acceptance Criterion 4 (5)," as follows:

Insert the following in the list of items (a)-(i), and renumber item (i) as item (j):

(i) Human factors engineering

REFERENCES

1. U. S. Nuclear Regulatory Commission, *Yucca Mountain Review Plan*, NUREG-1804, Revision 2, Final Report, 2003.

2. U.S. Nuclear Regulatory Commission, Division of High-Level Waste Repository Safety - Interim Staff Guidance, HLWRS-ISG-02, *Preclosure Safety Analysis - Level of Information and Reliability Estimation,* 2007.

3. U.S. Nuclear Regulatory Commission, NUREG–1774, *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002,* 2003.

4. U.S. Nuclear Regulatory Commission, NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* 1983.

5. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, 2002.

6. U.S. Nuclear Regulatory Commission, NUREG-1792, *Good Practices for Implementing Human Reliability Analysis*, 2005.

7. U.S. Nuclear Regulatory Commission, NUREG-1842, *Evaluation of Human Reliability Analysis Methods Against Good Practices*, 2006.

8. U.S. Nuclear Regulatory Commission, NUREG–0711, *Human Factors Engineering Program Review Model,* Revision 2, 2004.

9. U.S. Nuclear Regulatory Commission, NUREG-0700, *Human-System Interface Design Review Guidelines*, Revision 2, 2002.

Approved: _____**/RA/**_____ Date:___08/14/07_____
Jack R. Davis, Director
Technical Review Directorate
Division of High-Level Waste Repository Safety
Office of Nuclear Material Safety
and Safeguards

GLOSSARY

APPENDIX A: Example – HRA Considerations for Reliability Estimate of a Crane

GLOSSARY

The definitions provided in this glossary are specific to the way the terms are used in this ISG, and may not be universally appropriate or applicable.

Error of Commission (EOC): A *human failure event,* resulting from an overt, unsafe action, that, when taken, leads to a change in facility configuration, with the consequence of a degraded facility state that may lead to an event sequence.

Error of Omission (EOO): A *human failure event,* resulting from a failure to take a required action, that leads to an unchanged or inappropriately changed facility configuration, with the consequence of a degraded facility state that may lead to an event sequence.

Human Error Probability: The probability of a particular human failure event occurring.

Human Factors Engineering: The application of knowledge about human capabilities and limitations to plant, system, and equipment design. Human factors engineering provides reasonable assurance that the design of the facility, systems, equipment, human tasks, and the work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the facility [NUREG-0711, Ref. 1].

Human Failure Event (HFE): An event that would be modeled as a basic event in the logic models of a safety assessment, and that is the result of one or more unsafe actions.

Human-Induced Initiator: An HFE that represents actions that cause or lead to an initiating event. The GROA is expected to employ various manually controlled waste-handling and transport equipment that may be subject to HFEs that could initiate an event sequence.

Human Reliability Analysis (HRA): HRA evaluates the potential for, and mechanisms of, human errors that may affect the safety of the GROA operations, including consideration of human reliability, as it relates to design and programs such as training of personnel. The main objectives of the HRA are:

1. To ensure that human actions that could affect event sequences are systematically identified, screened, analyzed, and incorporated into the safety analysis in a traceable manner;
2. Where necessary, to quantify the probabilities of success and failure of human actions for event-sequence quantification and screening.

Important-to-Safety (ITS): With reference to systems, structures, and components, *ITS* means those engineered features of the geologic repository operations area whose function is: (1) to provide reasonable assurance that high-level waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of 10 CFR 63.111(b)(1) for Category 1 event sequences; or (2) to prevent or mitigate Category 2 event sequences that could result in radiological exposures exceeding the values specified at 10 CFR 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site [10 CFR 63.2, *Important to Safety*].

Pre-initiator Human Failure Event (HFE): Events that lay the foundation for an initiating event to occur (e.g., latent failures introduced during maintenance acts). Examples of pre-initiator HFEs include: actions that leave valves misaligned or instruments miscalibrated, leading to unavailability of equipment when needed; unscheduled maintenance acts that lead to reconfiguration of a system which does not match the expectations of operating personnel, leading to a human failure event.

Post-Initiator Human Failure Event (HFE): Post-initiator HFEs include both operator actions and inactions that have the result of degraded plant/facility conditions. An example of such an HFE is the failure to manually actuate or manipulate systems or equipment that are required for response to an initiating event, to prevent propagation of an event sequence or to mitigate its consequences. Post-initiator HFEs can be further divided into recovery and non-recovery events, as appropriate for a given event sequence.

Qualitative HRA Analysis: HRA tasks that include: (1) identification of HFEs and unsafe actions; (2) identification of important factors influencing human performance; and (3) selection of appropriate HRA quantification method(s), if considered necessary.

Risk-Significant: Making a significant contribution to the probabilities and/or consequences of one or more event sequences that have the potential to exceed the performance objectives of Part 63 during GROA operations.

Unsafe Action: An action inappropriately taken, or not taken, when needed, by plant personnel, that results in a degraded plant/facility safety condition.

GLOSSARY REFERENCE

1. U.S. Nuclear Regulatory Commission, NUREG–0711, *Human Factors Engineering Program Review Model,* Revision 2, 2004.

APPENDIX A
EXAMPLE – HRA CONSIDERATIONS FOR RELIABILITY ESTIMATE OF A CRANE

Appendix A of High-Level Waste Repository Safety (HLWRS) Interim Staff Guidance (ISG)-02 [Ref. A.1] presented an example to illustrate "...the level of information that typically could be needed for review of a crane that handles canisters" (p. 12). In this appendix, we will build on the crane example to illustrate what further information might be needed for review of crane-related event sequences, if human reliability were a significant contributor to crane reliability.[1] Note that this is just one example of one set of considerations that staff reviewers may face, and it is not meant to be a comprehensive list of all possibly relevant considerations in reviewing human reliability analysis (HRA) for the geologic repository operations area (GROA).

As a reminder, the example in HLWRS-ISG-02 [Ref. A.1] presented the following points:

- "This example is hypothetical in nature and may not be applicable to potential crane systems and operations that DOE may propose for the geological repository operations area (GROA)" [Ref. A.1, p. 11].
- "The rigor of U.S. Nuclear Regulatory Commission (NRC) review will depend on the approach DOE chooses to demonstrate compliance with the requirements of 10 CFR Part 63 and the degree to which the cranes are relied on to limit or prevent potential event sequences in its PCSA" [Ref. A.1, p. 11].
- "In this example, NUREG-1774 [Ref. A.2] data are assumed applicable to the crane design and operations at the GROA" [Ref. A.1, p. 12-13].
- "DOE will need to provide a technical basis for data used from NUREG-1774 [Ref. A.2] or any other source, to represent GROA operations" [Ref. A.1, p. 13].
- "Appropriate examination and evaluation of the empirical data will be needed to determine its applicability to the design, operations, and events analyzed in the PCSA." [Ref. A.1, p. 11]. "The relevance of the empirical data should be evaluated for the proposed design and operations" [Ref. A.1, p. 15].
- Information on "...similarities in operations, maintenance programs, quality assurance (QA), operating environment, and operator training for cranes used in facilities where data have been collected" may be needed to support the crane reliability estimate [Ref. A.1, p. 11].

Suppose that: (1) a load drop from a crane is an initiating event for a risk-significant event sequence in the preclosure safety analysis, and the crane is identified as an important-to-safety structure, system, or component (here we expand the example of HLWRS-ISG-02 [Ref. A.1] to include all loads, not just heavy loads); and (2) the NUREG-1774 [Ref. A.2] data were used to estimate the crane-load-drop probability value for the GROA (one of many possible approaches that could be chosen by the U.S. Department of Energy (DOE); in this case, it may not be appropriate to use NUREG-1774 [Ref. A.2] for all load sizes, but this is a purely hypothetical example). In such a case, staff should look in the license application (LA) for justification that the data accurately reflect the characteristics or features of the GROA that would be important to human reliability. The following are some questions the staff could ask to assess whether the use of the empirical data to establish the crane-load-drop probability has an adequate technical basis from the perspective of human reliability.

1. In the empirical data (i.e., NUREG-1774 [Ref. A.2] in this hypothetical case), did human actions contribute significantly to the rate of load drops from cranes?

1 Crane unreliability here refers to the rate (or probability) of load drops from cranes.

- In the case of NUREG-1774 [Ref. A.2] , the answer is yes. NUREG-1774 specifically notes, "...the percentage of crane issue reports caused by poor human performance has increased over time, and for the last several years, averaged between 70 and 80 percent" for all load sizes [Ref. A.2, p. 7].[2] The reason for citing this statistic is not to imply that human performance is deteriorating over time, but as an indicator that human performance *does* contribute significantly to events in the empirical data in this hypothetical example. In Table 2 of NUREG-1774 [Ref. A.2], descriptions of individual load-drop and load-slip events show operator error, hoisting and/or rigging, and weak administrative controls (e.g., testing program) as common causes.

2. If human actions contribute significantly to crane reliability, does the LA provide justification for use of the data source? Is such justification commensurate with risk and based on relevant qualitative considerations, namely HRA activities (a) and (b), discussed under the "Acceptable Methods and Approaches" guidance in this ISG?

3. *HRA activity (a): Identification of human failure events (HFEs) and associated unsafe actions.* Does the LA include a discussion of general risk insights, from crane operating experience, in the empirical data, with insights into HFEs and the reasons for past unsafe human actions? Does the LA discuss similarities in kinds of HFEs and unsafe actions committed at facilities from which the data were obtained, compared to those expected at the GROA?

4. *HRA activity (b): Identification of important factors influencing human performance.* Does the LA explain the similarities and differences, between the facilities from which the empirical data were obtained, and the GROA, based on a discussion of facility-specific, site-specific, and activity-specific factors that influence human performance? How might the facility-specific factors influence the human reliability at the GROA, compared to the empirical data facilities?

5. What are the implications of any differences identified in answering the questions in HRA activities (a) and (b) in items 3 and 4 above?

    - For example, if relevant, the LA should include a discussion of one potential key difference that, at any one particular facility in the NUREG-1774 [Ref. A.2] data, such as a specific commercial nuclear power plant, there is usually only one kind of load to move (e.g., one kind of fuel assembly, or one type of transfer container). At the GROA, the same crews may have to handle different kinds (e.g., dimensions) of fuel assemblies, canisters, and casks. Might this introduce different kinds of error mechanisms, at the GROA, that are not contained in the NUREG-1774 [Ref. A.2] data? Why or why not? And if so, what is the basis for using the NUREG-1774 [Ref. A.2] data? If this GROA-specific factor turns out to be the dominant human-error mechanism, and one that is not captured in the NUREG-1774 [Ref. A.2] empirical data, staff should look for strong justification from compensating factors. Compensating factors might include, for example, low sensitivity of risk to the crane-drop probability, or a qualitative argument

2 Note that figure 10 of NUREG-1774 [Ref. A.2, p. 16] shows that the load-drop incidence (drops/reactor-year) had been fairly constant over 1991-2002. Note also that there is no one-to-one correspondence between crane-issue reports and load-drop events (e.g., crane -issue reports can be generated for reasons other than a load-slip or load-drop event).

based on the implementation of strong administrative controls, that could compensate for the uncertainty (in which case staff should verify that these administrative controls are feasible – see items (6) and (7), below).

6. What are the key administrative controls (e.g., training, procedures, technical specifications) that contribute to the crane reliability in the NUREG-1774 [Ref. A.2] data? How will similar administrative controls be implemented at the GROA? What are the effects of any differences in administrative controls implemented at the GROA versus facilities captured in NUREG-1774 [Ref. A.2]? It is worth noting that crane-load drops at commercial nuclear power plants in the U.S. have not been frequent, because there are a lot of controls and practices to ensure safety of materials-handling with cranes. For example, administrative controls include training, procedures, and supervisory and/or peer checks and verification of different steps in the process. NUREG-1774 [Ref. A.2] discusses the programmatic requirements for heavy loads handled by cranes in nuclear power plants, captured as good practices in NUREG-0612 [Ref. A.3]. For example, according to NUREG-0612: "...crane operators should be trained, qualified, and conduct themselves in accordance with Chapter 2-3 of ANSI B30.2-1976, 'Overhead and Gantry Cranes'….[Ref. A.4] The crane should be inspected, tested, and maintained in accordance with Chapter 2-2 of ANSI B30.2-1976, 'Overhead and Gantry Cranes'…." [See Ref. A.2, pp. 3-4]

   - Training is an example of a key administrative control, and the following are examples of questions the staff could ask. For the commercial nuclear power plant data in NUREG-1774 [Ref. A.2], was there just-in-time training provided at power plants before every sporadic fuel and heavy load move? Is that likely to be the case for GROA operations that could take place around the clock and calendar year? If not, what are the potential implications for human reliability? What might be the compensating features for GROA operations? For example, might crews at the GROA be more familiar with the operations because of the higher frequency of activities? Is that likely to shift the dominant human error mechanisms for the GROA versus NUREG-1774 [Ref. A.2] facilities? Considering these differences, are alternate administrative safety controls more appropriate for the GROA? How might the empirical drop rate be modified, considering these GROA-specific factors? The LA could include a discussion (which could be qualitative) of why the administrative controls were designed with the GROA-specific performance-shaping factors in mind (e.g., (1) training to address the handling of different kinds of fuel and canister loads; (2) robust design features that cannot be defeated by human actions; and (3) rigorous performance-monitoring program to account for uncertainties), that compensate for elements missing from the NUREG-1774 [Ref. A.2] facilities (e.g., just-in-time training) – and the net effect on the drop probability and associated uncertainties.

7. How are the important administrative controls for crane reliability incorporated into the licensing specifications, or otherwise identified in the LA for future verification?

REFERENCES

A.1 U.S. Nuclear Regulatory Commission, Division of High-Level Waste Repository Safety - Interim Staff Guidance, HLWRS-ISG-02, *Preclosure Safety Analysis - Level of Information and Reliability Estimation,* 2007.

A.2 U.S. Nuclear Regulatory Commission, NUREG–1774, *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*, 2003.

A.3 U.S. Nuclear Regulatory Commission, NUREG-0612, *Control of Heavy Loads at Nuclear Power Plants*, 1980.

A.4 American Society of Mechanical Engineers/American National Standards Institute, ANSI B30.2-1976, Chapter 2-3, “Overhead and Gantry Cranes,” 1976.

3. U.S. Nuclear Regulatory Commission, NUREG–1774, *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002,* 2003.

4. U.S. Nuclear Regulatory Commission, NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* 1983.

5. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, 2002.

6. U.S. Nuclear Regulatory Commission, NUREG-1792, *Good Practices for Implementing Human Reliability Analysis*, 2005.

7. U.S. Nuclear Regulatory Commission, NUREG-1842, *Evaluation of Human Reliability Analysis Methods Against Good Practices*, 2006.

8. U.S. Nuclear Regulatory Commission, NUREG–0711, *Human Factors Engineering Program Review Model,* Revision 2, 2004.

9. U.S. Nuclear Regulatory Commission, NUREG-0700, *Human-System Interface Design Review Guidelines*, Revision 2, 2002.

Approved: _____**/RA/**_____ Date:__08/14/07_____
Jack R. Davis, Director
Technical Review Directorate
Division of High-Level Waste Repository Safety
Office of Nuclear Material Safety
and Safeguards

GLOSSARY

APPENDIX A: Example – HRA Considerations for Reliability Estimate of a Crane

DISTRIBUTION:

HLWRS r/f NMSS r/f HLWRS Staff

ML071900399

OFC	HLWRS	HLWRS	TECHED	HLWRS	OGC
NAME	TGhosh	RJohnson	EKraus	EPeters	MZobler-NLO
DATE	8/6/07	8/14/07	8/13/07	8/14/07	8/8/07

OFC	HLWRS	HLWRS	HLWRS
NAME	TMcCartin	MShah	JDavis
DATE	8/6/07	8/6/07	8/14/07

OFFICIAL RECORDS COPY