Division of High-Level Waste Repository Safety - Interim Staff Guidance
HLWRS-ISG-02, PRECLOSURE SAFETY ANALYSIS - LEVEL OF INFORMATION AND RELIABILITY ESTIMATION

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 design and operational information and reliability estimates required for the preclosure safety analysis (PCSA). This ISG supplements Sections 2.1.1.2, 2.1.1.4, and 2.1.1.7 of the YMRP. This guidance also provides examples that illustrate commonly used approaches for estimating reliability and the level and types of supporting design and operational information that would be necessary for structures, systems, and components (SSCs) at the geologic repository operations area (GROA). A sufficient level of information and adequate technical bases for reliability estimates are needed to demonstrate compliance with the performance objectives in Code of Federal Regulations, Title 10, Part 63, Section 63.111 (10 CFR 63.111).

Discussion

Regulations for licensing the proposed geologic repository at Yucca Mountain, Nevada are contained in 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. The U.S. Nuclear Regulatory Commission (NRC) decision to grant a construction authorization will be based on the proposed design and operations DOE submits with the License Application (LA).

Consistent with a risk-informed approach, the regulation does not specify design-basis events or design criteria for SSCs. Furthermore, the regulation does not specify analytical methods for demonstrating performance of the SSCs, or estimating the reliability of important to safety (ITS) SSCs (whether active or passive), or calculating uncertainty. Rather, 10 CFR 63.111 specifies performance-based dose limits for Category 1 and 2 event sequences. Category 1 event sequences are those that are expected to occur one or more times before permanent closure of the GROA, whereas Category 2 event sequences are those other event sequences that have at least one chance in 10,000 of occurring before permanent closure of the GROA. Event sequences with the probability of occurrence of less than 1 in 10,000 may be screened out and do not have performance-based dose limits.

The PCSA is required to demonstrate compliance with the performance objectives and to identify SSCs that are ITS. The PCSA is defined in 10 CFR 63.2 as a systematic examination of the site and the design, potential hazards, initiating events and event sequences, and their consequences (e.g., radiological exposures to workers and the public). SSCs that are credited with limiting or preventing potential event sequences, or mitigating their consequences, are designated as ITS. Per 10 CFR 63.112 (c)(8), DOE must demonstrate the ability of each ITS SSC to perform its intended safety function(s), and specify design bases, design criteria, and design specifications necessary to keep them functional and meet the performance objectives.

Staff Guidance

Level of Design and Operational Information

The NRC review will focus on the most significant activities, hazards, event sequences, and potential consequences related to the proposed design and operations submitted with the LA. The required level of information will depend on many factors, including:

- The approaches that DOE chooses to demonstrate compliance;
- The use and reliability of particular ITS SSCs to limit or prevent potential event sequences, or mitigate their dose consequences;
- The degree of operating experience with similar systems, versus uniqueness of the ITS SSCs; and
- The level of reliability that DOE attributes to each ITS SSC in its PCSA.

In general, the LA and PCSA should contain two levels of information: (1) general information on the design of facilities, SSCs, equipment, and process activities, to support the PCSA; and (2) specific information about ITS SSCs that demonstrate the ability of the ITS SSCs to perform their intended safety function(s).

General information supporting the PCSA should contain sufficient detail to allow the staff to understand the preclosure facilities and operations, including their size, location, arrangements, purpose, and potential hazards. The staff should ensure that adequate information on design and operation of the facilities has been provided to enable determination of compliance with the performance objectives, and identification of ITS SSCs.

Types of general information that should be in the PCSA include, but are not limited to:

- Description of the facilities and their functions;
- Description of SSCs within the facilities;
- Design bases and design criteria for ITS SSCs;
- Basic operations, controls, and monitoring;
- Key dimensions and materials of construction;
- Relationships and interdependencies of SSCs, as needed; and
- Application of codes and standards, including exceptions.

The staff should focus its review on the specific design and operation information that is needed to verify that ITS SSCs will perform their intended safety functions, with the reliability specified within the PCSA. The staff should confirm that DOE has provided sufficient design information for ITS SSCs to support their design bases and design criteria, estimates of reliability, and their roles in meeting the performance objectives. The specific information needed for the review will depend on the specific function of the ITS SSC. SSCs that are designated as ITS will need greater specificity in the design and operations than SSCs that are not ITS. For example, additional types of specific information could include the following:

- Structural design features, material specifications, and engineering analyses;
- Schematics of component configurations;
- Control logics for critical functions related to SSC reliability;
- Major operational features related to the controls and the human interactions associated with the SSC; and
- Unique operating environments that may adversely affect SSC performance.

Reliability Estimates

The staff should also review the SSC reliability estimates that are needed to calculate event sequence probabilities in the preclosure safety analysis. Reliability is the probability that an SSC will perform its intended function under specified conditions for a specified period of time. This includes consideration of hardware and software failures, as well as failures produced by the action or inaction of operations personnel. Quantified reliability estimates are typically needed for each SSC being relied on in an event sequence in order to categorize it as either a Category 1 or 2 event sequence. The use of mean sequence frequencies to categorize event sequences in the PCSA is acceptable with adequate technical bases and consideration of uncertainty.

DOE should identify all SSCs (ITS SSCs and non-ITS SSCs) that are relevant to the preclosure operations when developing event sequences. DOE has flexibility in determining the reliability required for each SSC, at the system or component level, and in selecting approaches in quantifying the reliability. The quantified reliability estimates should be based on defensible and traceable technical bases to reasonably categorize the event sequence, or screen it out from further consideration in the PCSA. DOE may select a reliability value or assign an SSC a reliability value of zero, so that no credit is taken for the SSC (i.e., it is conservatively assumed to fail), for the purpose of carrying forward an event sequence in the PCSA. Staff should review DOE's justification for the selected reliability value.

The staff should confirm if reliability estimates made at the system level are sufficient and acceptable for categorization of event sequences. For example, the reliability estimate of a crane or other canister handling system at the GROA could be justified by comparison with the experience and reliability data of similar handling systems used in industry. However, there may be insufficient system-level data applicable to the ITS SSC, or existing system-level data may not be completely applicable to unique operations at the GROA. In these cases, the staff should confirm if the reliability estimate is justified by analogous data at the next level down, typically for the subsystems or individual components of the SSC.

There are multiple approaches that DOE could use to estimate reliability of ITS SSCs. Three basic approaches are: (1) accepted engineering practices; (2) empirical analyses; and (3) reliability modeling. Regardless of the approach, the staff should confirm that DOE has provided sufficient technical bases for the method and data used to estimate the reliability. The technical basis should include a discussion of the approaches used to develop the reliability estimate, input parameters, assumptions, references, and sufficient details of the design and operation to enable the staff to independently confirm the estimate. Examples of approaches for estimating reliability for hypothetical crane and canister SSCs are illustrated in Appendices A and B.

Accepted Engineering Practice

Accepted engineering practice could include the application of: (1) appropriate codes and standards; (2) realistic parameters, operating conditions, and safety margins in design performance calculations; (3) redundancies and defense-in-depth considerations; and (4) administrative program controls that provide confidence in hardware performance and human reliability. The application of codes and standards to the design and operation of an ITS SSC is an accepted engineering practice recognized by the Commission in ensuring safety in the nuclear industry. The staff should recognize the high confidence in SSC reliability that is afforded by the codes and standards. However, use of an applicable code or standard to design, fabricate, and operate an ITS SSC does not by itself provide a quantitative reliability

estimate, or ensure a level of reliability sufficient to screen out failure-related event sequences from further consideration in the PCSA (e.g., one chance in 10,000 of occurring during the preclosure period).

It is feasible to justify a very high reliability estimate for certain SSCs. This may include the use of a code and standard, in combination with other technical bases such as: (1) empirical data on reliability of similar SSCs; (2) engineering judgement supported by sufficient technical bases; and (3) engineering analyses that demonstrate sufficient design margins.

Empirical Analyses

Empirical reliability analyses of an SSC could include the quantitative analyses of observed failure rates and performance data for similar SSCs used in industry (e.g., the number of trials, failures), as well as published reliability values based on industry experience and judgement. Based on use of published reliability information and a justification regarding its applicability to the SSC in the GROA, a reliability estimate can be developed. The staff should confirm that DOE has used appropriate empirical techniques and considered failure and performance information to the degree appropriate for each SSC. Numerous sources of reliability information are available for empirical analyses, such as:

- Generic Data Base, developed by Savannah River Site [Ref. 2];
- IEEE-Standard 500, A Guide to the Collection and Representation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Generating Stations [Ref. 3];
- NUREG-1774, A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002 [Ref. 4]; and
- Equipment Performance and Information Exchange (EPIX) System [Ref. 5].

Reliability Modeling

If empirical data are limited or unavailable, modeling could be used to estimate reliability. For some systems, the model could be based on a specific configuration of multiple components. The model typically considers facility design, processes, operations, and human actions. There are various techniques for modeling an SSC, such as developing a fault tree analysis of component failures, or probabilistic fragility analysis. The staff should review the description of the reliability model and applicability of methods and input data.

Uncertainty

The staff should verify that uncertainty is addressed for each reliability estimate in the PCSA. Uncertainty may be considered qualitatively or quantitatively to ensure the categorization of event sequences is reasonable [Ref. 6]. In some cases, it may not be necessary to quantify uncertainty for each SSC reliability estimate, or numerically propagate uncertainties in the entire event sequence. When reviewing the treatment of uncertainty with each reliability estimate in the PCSA, the staff should consider: (1) the degree of reliance on the SSC in limiting or preventing event sequences or mitigating their consequences; and (2) event sequences in which the frequency of occurrence (e.g., from SSC failure) is close to the Category 1 or 2 limits. For example, a reliability estimate for an SSC that is critical in limiting or preventing a potential event sequence or in mitigating an event sequence with a significant dose consequence would warrant more scrutiny than others with lower consequences. Further, a reliability estimate for an SSC that results in an event sequence frequency just below the Category 1 or 2 limits, would also merit closer scrutiny as well.

Regulatory Basis

The following regulations provide the bases for this ISG:

1. 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 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 the ability of SSCs to perform their intended safety functions, assuming the occurrence of event sequences [10 CFR 63.112(e)(8)].

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)].

Recommendations:
The following changes to the YMRP are recommended:

1. Revise Section 2.1.1.2.2, "Review Methods, Review Method 2, *Descriptions of, and Design Details for, Structures, Systems, and Components, and Equipment of Surface Facilities,*" as follows:

Page 2.1-13: Add the following after item (24)

Confirm that DOE has provided: (1) general design and operational information for the surface facilities and the SSCs; and (2) adequate design and operational information about ITS SSCs, for the staff to gain an understanding of the preclosure activities and operations.

Verify that general information includes a description of each facility and its functions; description of SSCs within the facility; design bases and design criteria for ITS SSCs, basic operations, controls, and monitoring; key dimensions and materials of construction; relationships and interdependencies of SSCs, as needed; and application of codes and standards, including exceptions.

Verify that specific, detailed information for ITS SSCs includes (as applicable and necessary): structural design features, material specifications, and analyses and fabrication information; schematics of component configurations within SSCs; control logics for critical functions related to SSC reliability; major operational procedures and activities related to the controls and the human interactions associated with each SSC; and unique operating environments that may adversely affect SSC performance.

2. Page 2.1-17, Section 2.1.1.2.3 Acceptance Criteria, Acceptance Criterion 2: Add the following after the existing (1), and renumber the existing items as appropriate:

(2) The LA includes general information that provides adequate understanding of the preclosure activities and operations, and specific information for ITS SSCs that provides sufficient bases to verify their intended safety function.

3. Page 2.1-25: Revise Section 2.1.1.4.1 "Areas of Review," as follows:

Insert the following before the 2nd paragraph:

Quantified reliability estimates for SSCs are needed to determine event sequence frequencies. The reliability estimates should include consideration of hardware and software failures, as well as failures produced by the action or inaction of operations personnel. Several approaches may be used to estimate reliability, such as accepted engineering practice, empirical analyses, or reliability modeling. The SSCs that are relied on to limit or prevent event sequences or mitigate their consequences at the estimated reliability are designated as ITS, and are evaluated in Section 2.1.1.6 of the YMRP.

4. Page 2.1-26: Revise Section 2.1.1.4.2 - Review Method 2 "*Categories 1 and 2 Event Sequences*," as follows:

Add after the 1st paragraph:

Verify that DOE has appropriately used accepted engineering practice to estimate reliability, if applicable, in categorization of event sequences. As applicable, confirm that DOE has properly considered: (1) appropriate codes and standards; (2) reasonable parameters, operating conditions, and safety margins in design performance analyses; (3) any redundancies and defense-in-depth considerations; and (4) administrative programs that maintain confidence in ITS SSC reliability, such as quality assurance (QA), testing, surveillance, maintenance, and training programs.

Confirm that the application of accepted engineering practices is consistent with the design methodologies and analyses evaluated in Section 2.1.1.7 of the YMRP, and with the administrative programs evaluated in Sections 2.1.1.6 and 2.5 of the YMRP. However, use of an applicable code or standard to design, fabricate, and operate an ITS SSC does not by itself provide a quantitative reliability estimate, or ensure a level of reliability sufficient to screen out failure-related event sequences from further consideration in the PCSA (e.g., one chance in 10,000 of occurring during the preclosure period).

Verify that DOE has appropriately used empirical analyses to estimate reliability, if applicable, in categorization of event sequences. Confirm that DOE has used appropriate empirical techniques and considered failure and performance data to the degree appropriate for each SSC.

Verify that DOE has used appropriate modeling techniques to estimate reliability, if applicable, in categorization of event sequences. Confirm that DOE has appropriately modeled the specific configuration of SSCs and used appropriate failure values.

Verify that DOE has addressed uncertainty in reliability estimates. The staff should focus its review of reliability uncertainty in terms of: (1) risk-significance, or reliance of the ITS SSC in limiting or preventing potential event sequences or mitigating their consequences; and (2) event sequence probabilities that are close to the Category 1 and 2 limits.

Confirm that the reliability estimates used to categorize event sequences are consistent with the design bases and design criteria of proposed ITS SSCs reviewed using Section 2.1.1.7 of the YMRP.

5. Page 2.1-27: Add the following to Section 2.1.1.4.3, "Acceptance Criterion 2" after the existing (1), and renumber the existing criteria as appropriate:

(2) Accepted engineering practices were used appropriately to estimate reliability, where applicable, in categorization of event sequences.

(3) The application of accepted engineering practice is consistent with the design methodologies and analyses and with administrative programs.

(4) Empirical analyses were used appropriately to estimate reliability, where applicable, in categorization of event sequences.

(5) Modeling techniques were used appropriately to estimate reliability, where applicable, in categorization of event sequences.

(6) Uncertainty in the reliability estimates has been addressed appropriately.

6. Page 2.1-51: Revise Section 2.1.1.7.1 "Areas of Review," as follows:

Add as last sentence to first paragraph of this section:

Reviewers will also confirm that the design of ITS SSCs is consistent with the reliability estimates used to categorize event sequences in the PCSA, as evaluated in Section 2.1.1.4 of the YMRP.

7. Page 2.1-52: Revise Section 2.1.1.7.2.1 - Review Method 1, "*Definitions of Relationship between Design Criteria and Design Bases*" *as follows:*

Add as the last sentence of 1st Paragraph in this Review Method:

Confirm that the design bases and design criteria of proposed SSCs are appropriate and consistent with the sources of the reliability data that was evaluated using Section 2.1.1.4 of the YMRP.

References

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

2. Blanton C.H. and S.A. Eide, *Savannah River Site Generic Data Base Development,* WSRC-TR-93-262, June 1993.

3. Institute of Electrical and Electronics Engineers,*Guide to the Collection and Representation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Generating Stations*, IEEE-STD 500, 1991.

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

5. Institute of Nuclear Power Operations (INPO), *EPIX System*, Proprietary - maintained by INPO (covering initiating events October 1987-present).

6. U. S. Nuclear Regulatory Commission, *Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain*, *NV*, Final Rule, Federal Register, November 2, 2001, Vol. 66, No. 213, pp 55732 -55816.

Approved: /RA/ Date: 3/16/07

Lawrence E. Kokajko, Director
Division of High-Level Waste Repository Safety
Office of Nuclear Material Safety
and Safeguards

Glossary

Appendices

Appendix A: Example - Level of Information and Reliability Estimate of a Crane

Appendix B: Example - Level of Information and Reliability Estimate of a Canister

GLOSSARY

DESIGN BASIS: *Design Basis* means that information that identifies specific functions to be performed by a SSCs of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design [10 CFR 63.2, *Design Basis*].

EVENT SEQUENCE: *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 geologic repository operations area 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*].

FAILURE: *Failure* is defined as the loss of ability of an SSC to perform its intended safety function or operate as specified.

IMPORTANT TO SAFETY: With reference to SSCs, *important to safety* 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*].

PRECLOSURE SAFETY ANALYSIS: *PCSA* means a systematic examination of the site, the design, and the potential hazards, initiating events and event sequences, and their consequences (e.g., radiological exposures to workers and the public). The analysis identifies ITS SSCs [10 CFR 63.2, *Preclosure Safety Analysis*].

RELIABILITY: *Reliability* of an SSC is the probability that the item will perform its intended function(s), under specified operating conditions, for a specified period of time.

STRUCTURES, SYSTEMS, AND COMPONENTS: A *structure* is an element, or a collection of elements, to provide support or enclosure, such as a building, free-standing tanks, basins, dikes, or stacks. A *system* is a collection of components assembled to perform a function, such as piping, cable trays, conduits, or heating, ventilation, and air-conditioning. A *component* is an item of mechanical, electrical or electronic equipment, such as a pump, valve, or relay, or an element of a larger array, such as a length of pipe, elbow, or reducer.

APPENDIX A
EXAMPLE - LEVEL OF INFORMATION AND RELIABILITY ESTIMATE OF A CRANE

Introduction

This example illustrates the level of information that typically could be needed for review of a crane that handles canisters. This example also illustrates a method to estimate the reliability(or probability of failure) of the crane in a PCSA. Different approaches may be used to estimate reliability in crane-related event sequences. This example illustrates the use of accepted engineering practice and empirical performance data for similar cranes operated at analogous facilities. Empirical data from relevant studies and collections, such as references A.1 and A.2, can provide the necessary information for estimating the reliability of a crane. However, 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. In addition, the uncertainty associated with the reliability estimate should be examined and considered in the PCSA.

This example is hypothetical in nature and may not be applicable to potential crane systems and operations that DOE may propose for the GROA. The applicability of reliability methods and data will be highly dependent on the specific design and operations proposed by DOE. DOE will be responsible for providing a sufficient technical basis for the reliability methods and for demonstrating the applicability of the data and analysis used in its PCSA. Treatment of uncertainty in reliability estimates may depend on the risk-significance (or reliance) of the crane system in preventing or reducing the occurrence of event sequences; the severity of the potential radiological consequences; and the proximity of the associated event frequency to the categorization limits for preclosure events. The rigor of 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.

Level of Information

The specific information provided for the crane should be sufficient to demonstrate its ability to perform its intended safety function(s) and to verify that the crane reliability estimate is based on empirical data that are applicable to the design and scope of operations. The following types of information may be needed to support the reliability estimate:

- Applicable codes and standards (e.g., American Society of Mechanical Engineers (ASME), Type 1 [Ref. A.3])
- Key design features (e.g., type of grapple, hoisting mechanism, load capacity, etc.)
- Similarities in operations, maintenance programs, QA, operating environment, and operator training for cranes used in facilities where data have been collected.

Reliability Estimate

Use of an accepted consensus standard to design a crane is an accepted engineering practice that gives confidence that the crane can perform with a high degree of reliability. However, specifying a standard for the design does not provide a quantified reliability estimate for the

crane, which is needed for categorizing event sequences. In addition to considering the built-in margins in accepted codes and standards, an analysis using empirical data from analogous facilities may be used to estimate the reliability for a crane.

Performance data for similar cranes in use at analogous facilities are primary sources of reliability information. Databases for similar crane systems contain reliability information based on historical experience and typically include built-in factors such as operations, maintenance programs, QA, and operating environment. As necessary, the method(s) of data collection and limitations in the referenced data should be considered when assessing the applicability of empirical data.

The "Handbook of Parameter Estimation for Probabilistic Risk Assessment" [Ref. A.4], provides additional guidance that should be considered when selecting empirical data from existing databases:

1. The database should contain reliability information for systems (or components, as appropriate) that are identical or comparable to the system (or component) under consideration, in terms of size, boundary definition, intended operating characteristics (e.g., normally operating versus a standby system or component), and expected operating environment.

2. Primary sources of information used to develop the reliability database should be information from other nuclear facilities. Supplemental information from nonnuclear facilities may be used only when necessary to provide the failure probabilities and distributions for components not available from nuclear facilities.

3. It is preferable that the database has failure probabilities and associated distributions derived from actual failure events. Failure probabilities and distributions developed from other methods (e.g., expert judgment) may be limited in their applicability.

4. If a significant trend exists in failure probability data over time, then failure data that represent current (modern) crane configurations and recent events should be used.

Reliability Methodology Using Empirical Data

Determination of the event sequence category for crane failure alone (assuming no other mitigative SSCs) is performed in terms of frequency during the preclosure period.[1] NUREG–1774 [Ref. A.2] provides empirical data that may be used to develop a reliability estimate and address uncertainty in this context. In this example, NUREG-1774 data are

[1] The crane failure rate can also be applied in terms of annual failure frequency. This is advantageous when propagating the crane failure rate with the failure probabilities of other SSCs that could be relied on to prevent or mitigate a release within the event sequence. The likelihood of release can be determined on a frequency basis and categorized as a Category 1 or 2 Event Sequence (or screened-out), in accordance with the Event Sequence definitions of 10 CFR 63.2.

assumed applicable to the crane design and operations at the GROA.[2]

In, NUREG-1774, estimates that the total number of lifts greater than approximately 27 tonnes (30 tons), classified as "very heavy loads," for all U.S. nuclear power plants, was estimated to be approximately 54,000 for the period 1980 through 2002. This estimated number of lifts was developed by considering the number of refueling cycles in each power plant, along with the plant type. During this period, there were three events in which very heavy loads dropped, descended in an uncontrolled manner, or tipped in connection with crane operations in nuclear power plants. Supposing that the three events are relevant to the GROA operations, the estimated conditional drop probability of the population of cranes, given a lifting event, may be calculated using Equation 1.

$$\hat{p} = \frac{x}{n} \tag{1}$$

where $\hat{p}$ = estimated conditional drop probability
x = observed number of drops from industry experience, as reported in NUREG-1774
n = number of lifts

In this case, $\hat{p}$ is

$$\hat{p} = \frac{3\ drops}{54000\ lifts} = 5.6 \times 10^{-5} \text{ drops/lift}$$

At the GROA, the number of drops in L lifts, Y, has a binomial distribution which is typically approximated by a Poisson distribution. Thus, Y can take on the values 0, 1, 2, 3 ..., and has a Poisson distribution with an expected value of $\lambda = Lp$, where p is the drop probability of a single lift. An estimate of λ may be written as $\hat{\lambda} = L\hat{p}$.

Assuming there are 500 lifts per year over an operational period of 30 years, the number of lifts (L) in the time period of interest is 15,000 lifts. Thus, the estimated value of λ for this period is:

$$\hat{\lambda} = \hat{p}\,L = 5.6 \times 10^{-5}\ drops/lift \times 15000\ lifts\ = 0.84 \text{ drops}$$

Assuming a canister lift by a crane and a drop is an event sequence leading to radiological release (i.e., no further credit is given to other potential mitigative SSCs), this event sequence would not be expected to occur (i.e., less than one drop) during the 30-year period. However,

[2] It should be noted that the actual crane systems proposed for the GROA may have different characteristics than those represented in NUREG-1774, in terms of design, operator training, operational environment, training, and QA. DOE will need to provide a technical basis for data used from NUREG-1774 or any other source, to represent GROA operations.

the uncertainty in the estimate should be addressed to support further use in a PCSA.[3]

Treatment of Uncertainty

Different types of approaches may be used to address uncertainty in reliability estimates based on empirical data. These include qualitative approaches such as closer examination of specific crane features and operational procedures, or consideration of administrative controls at the GROA that may increase confidence in an even lower chance of drops. Statistical analyses, such as the confidence interval method of Reference A.5 (page 18-10), could also be used to further characterize the statistical uncertainty in the reliability estimate. This analysis is based on the standard assumption that the number of drops has a Poisson distribution. The confidence interval method yields a range of the conditional drop probability that is consistent with the uncertainty of the empirical data. In this example, using the confidence interval method [Ref. A.5], would result in only 48-percent confidence that the frequency of a drop event sequence during the preclosure period is less than 1.0. The 48-percent level of confidence is analogous to reporting the descriptive level of significance, which is often used in reporting the results of a test of a hypothesis.

Other approaches for estimating uncertainty may be appropriate, depending on the data and importance of the estimate to categorizing an event sequence.

Sensitivity Analysis

Sensitivity analysis determines the impact from changes in the input parameters on the estimate and uncertainty [Ref. A.6]. If there are reasonable alternatives to the number of applicable drop events from empirical data, a sensitivity study could be used to confirm whether the crane reliability estimate would be significantly changed. Alternatively, this analysis could also be used to identify specific operations and design features that may require increased scrutiny of specific administrative controls in the testing, surveillance, maintenance, or training programs, to mitigate the potential for certain types of failures.

NUREG–1774 [Ref. A.2] identifies six events that occurred in which very heavy loads “slipped” during crane operations in the same period. As defined in NUREG–1774 [Ref. A.2], a load slip in crane operation is “an uncontrolled vertical movement of a load that appears to be intermittent.” Assuming that these load slip events could be reasonably considered as additional load drop events, the total number of drop events used in the reliability estimation would increase from three to nine. The estimate of the conditional drop probability could be calculated as 1.7×10^{-4} drops per lift (Equation 1). In this case, the estimated expected value of the number of drops would be 2.6 drops for a 30-year period, assuming 500 lifts per year.

This illustrates the importance of assessing the appropriateness of potential events that may be screened in or out of the database for a specific empirical analysis. The screening process should be supported by a sufficient technical basis. In addition, commitments to specific administrative controls in the actual design and operation of the crane could be used to

[3] Uncertainty may be considered either qualitatively or quantitatively to provide a reasonable categorization of crane-related event sequences. Treatment of uncertainty should consider the risk-significance and reliance of the crane in preventing or limiting event sequences, and the proximity of associated event sequences to Category 1 and 2 limits.

eliminate the need to consider potential failure events that have occurred in the past at similar facilities.

Updating of Reliability Estimate with New Information

When estimating the reliability, it is important to evaluate proposed SSC designs against those designs for which the reliability data were collected. It is also important to evaluate the proposed operating environment against that from which the data were collected. For example, a new crane design may incorporate advanced control features that were not present in older designs. In addition, procedures for operating the crane may be different or improved. Such new information could influence the reliability estimated from older empirical data. In such cases, it may be important to update a reliability estimate with this new information.

Generally, failure of crane systems is infrequent, and consequently, data available for estimating the probability of a lifting failure may be sparse. Bayesian methods permit information from different sources, including expert opinion (e.g., from committees developing codes and standards and experience gained at a particular facility) to be included when estimating the reliability parameters [Ref. A.6]. Operational performance data of cranes may come from various analogous facilities; however, in the analysis, they may be treated as coming from a single plant (or source) (e.g., NUREG–1774 [Ref. A.2]). A Bayesian updating procedure, as suggested by Siu and Kelly [Ref. A.7], might be used if significant variability is expected among the facilities. Similarly, information gained from experts or committees developing codes and standards can be used to update the estimated reliability [Ref. A.7]. Advantages and disadvantages of Bayesian updating are given in Appendix C of NUREG-1489 [Ref. A.6].

Conclusions

This example illustrates the use of empirical data for developing a reliability estimate for a crane. The following points should be considered when using empirical data:

1. A quantified reliability estimate should be developed so that event sequences can be categorized. Designing to applicable codes and standards is an accepted engineering practice that provides high confidence in the reliability of the crane; however, it does not provide a quantified reliability estimate for the crane.

2. Historical performance information for similar cranes in use at analogous facilities is a source of reliability data that can be used in an empirical analysis. Reference information for the crane should be clearly understood. The relevance of the empirical data should be evaluated for the proposed design and operations.

3. When selecting empirical data to estimate the reliability, the uncertainty associated with the data is an integral part of the reliability estimate that should be addressed.

4. The methods and data used to estimate reliability and its associated uncertainty must be supported by sufficient technical bases. The technical bases for a reliability estimate should also account for how data were collected and applied. The amount and type of supporting information necessary will depend on the approach DOE chooses to demonstrate compliance, the uniqueness of the crane system, the reliance of the crane system in preventing event sequences, and the level of reliability that is specified in the PCSA.

References

A.1 U.S. Nuclear Regulatory Commission, *Control of Heavy Loads at Nuclear Power Plants*, USNRC NUREG–0612, July 1980.

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

A.3 American Society of Mechanical Engineers, *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*, ASME–NOG-1–2004.

A.4 U.S. Nuclear Regulatory Commission, *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, US NRC NUREG/CR–6823 SAND2003–3348P, September 2003.

A.5 U.S. Nuclear Regulatory Commission, *Applying Statistics*, US NRC NUREG-1475, February 1994.

A.6 U.S. Nuclear Regulatory Commission, *A Review of NRC Staff Uses of Probabilistic Risk Assessment*, NUREG-1489, March 1994.

A.7 Siu, N. and D. Kelly, *Bayesian Parameter Estimation in Probabilistic Risk Assessment*, Reliability Engineering and System Safety, Vol. 62, pp. 89-116, 1998.

APPENDIX B
EXAMPLE - LEVEL OF INFORMATION AND RELIABILITY ESTIMATE OF A CANISTER

Introduction

This example illustrates the level of information that typically could be needed for review of a spent nuclear fuel canister. This example also illustrates a method to estimate the reliability (or probability of failure) of the canister in a PCSA. Different approaches may be used to estimate reliability in canister-related event sequences. This example uses accepted engineering practice in combination with engineering analysis to estimate reliability of a canister for a potential drop during handling operations. The canister consists of a cylindrical shell with welded base plate and top lid and is designed to be a confinement barrier of the spent nuclear fuel that is contained inside. Failure of a canister in this example is defined as the condition when canister stresses estimated using elastic analysis [Ref. B.1] exceed the ultimate strength of the material, resulting in breach of the confinement barrier. This definition of failure for an energy-limited event, such as a drop, would yield conservative results. Therefore, methods for estimating canister reliability using non-linear analysis and the strain failure criterion may be necessary for drop events resulting in significant non-linear behavior of canister material.

This simplified example is hypothetical in nature and may not be applicable to potential canister systems and operations that the DOE propose for the GROA. The applicability of reliability methods and data will depend on the specific design and operations DOE proposes. DOE will be responsible for providing a sufficient technical basis for the reliability methods and for demonstrating the applicability of the data analyses used in its PCSA. Treatment of uncertainty in reliability estimates may depend on the risk-significance (or reliance) of a canister system in preventing or reducing the likelihood of event sequences; the severity of the potential radiological consequences; and the proximity of the associated event frequency to the categorization limits for preclosure events. The rigor of the 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 canisters are relied on to limit or prevent potential event sequences or mitigate consequences in its PCSA.

Level of Information

The specific information provided for the canister should be sufficient to demonstrate its ability to perform its intended safety function(s) and verify the estimated reliability used in the PCSA. For an example of canister reliability determined with a structural elastic analysis, the following types of information may be needed (but not limited) to support the reliability estimate:

- A general description of the canister, including major components of canister structure, and its internals (e.g., basket assembly);
- Key design parameters (e.g., length, diameter, thickness, weight, weld characteristics) and material of construction;
- Information on fabrication including, methods of closure (e.g., welding vs. bolting);
- Design bases (e.g., loadings on SSCs associated with Category 1, and Category 2 event sequences, such as a canister drop event); and
- Design criteria (applicable codes and standards for the canister design, fabrication,

inspection, and exceptions to the codes, if any).

Reliability Estimate

Reliability of the canister for use in the PCSA should be based on an appropriate methodology. The following methodology is one example that illustrates the use of fragility analysis to estimate canister reliability from an assumed drop impact.

Methodology

1. The canister is assumed to have been designed in accordance with the ASME Boiler and Pressure Vessel Code (B&PV), Sections III, Division 1, Subsection NB [Ref. B.1].

2. The canister is assumed to be fabricated from Type 304 Stainless Steel. The allowable material properties for Type 304 Stainless Steel (SA–240 S30400) [Ref. B.2] at room temperature are given in Table B-1.

3. The approach outlined here is based on methods used for assessment of structural reliability [Ref. B.3]. The safety factor is a measure of reliability of the canister in the context of a design. It is a function of the load or demand on the system from the drop impact and the resistance or capacity of the system. The failure of the system is assumed to occur when the demand is greater than or equal to the capacity or, alternatively, when the ratio of capacity to demand is less than or equal to 1. Thus, the probability of failure, P_f, is given by the probability that the capacity is less than the demand, as given by the following equations:

$$P_f = P(C \le D) \quad or \quad P_f = P(S \le 1) \tag{1}$$

where *C* is the capacity, *D* is the demand, and

$$S = \frac{C}{D} \tag{2}$$

C and *D* are random in nature and the associated variability or uncertainty is represented by probability density functions $f_C(x)$ and $f_D(x)$, respectively. It must be noted that *C* and *D* can be functions of different engineering parameters (some of them uncertain). Combining the variabilities in capacity and demand using Equation 2, a probability density function can be developed for *S* as $f_S(s)$, which is traditionally defined as the limit state function. The probability of failure, defined by $S \le 1$, is calculated by integrating $f_S(s)$ for *s* from 0 to 1 as shown in Equation 3.

$$P_f = \int_0^1 f_S(s)\, ds \tag{3}$$

where, $f_S(s)$ is the probability density function of *S*.

4. The capacity, *C*, can be defined as the material ultimate strength or strain failure. In this example, the capacity is assumed to be represented by the ultimate tensile strength, σ_u.

Hence the uncertainty in the capacity in this example is based only on the variability of σ_u, which is assumed to follow lognormal distribution. Effects of the strain rate and temperature on the material ultimate strength are not considered in this example. The material strength selected for the capacity is the minimum of the canister shell or weld material strength.

5. The demand, *D*, is expressed as the maximum stress intensity in the canister from the impact of a vertical drop and other load combinations, calculated by numerical modeling or other methods. Demand is a function of several parameters, (e.g., drop height, temperature, internal pressure, etc.). Each of the parameters may contribute to overall variability in the demand. To simplify the example, it is assumed here that there is no uncertainty in the demand. However, the methodology can be easily applied to include variability in both demand and capacity.

6. Using the cumulative distribution function of the capacity, and the ASME Code Level D [Ref. B.2] allowable stresses as demand, the probability of failure of the example canister is calculated. Additional calculations for stresses lower than the ASME Code allowable stresses are also performed.

Results

Demand

The demand parameter for this analysis corresponds to the performance requirements of Level D Service Limit for accident condition load combinations in ASME B&PV Code, Section NB 3225 [Ref. B.1]. A Level D service limit, defined in NB 2142.4, permits gross general deformations with some consequent loss of dimensional stability, and damage requiring repair. The acceptance criteria for design, for Level D Service Limit, are given in Table B-2.

The demand in the canister from the hypothetical drop event is assumed to be 497 mega pascals (MPa) [72 kips per square inch (ksi)], which is the allowable Level D stress intensity for the combined primary membrane (local or general) and bending, as given in Table B-2. Thus the ratio of the ASME Code Level D allowable stress intensity to predicted maximum stress intensity or demand, is 1.0. Considering the uncertainties in the capacity of the material (*C*), the probability of failure is estimated corresponding to the demand value of 497 MPa (72 ksi). Additional calculations were performed for stresses lower than the ASME Code allowable stresses.

Capacity

The capacity is defined by the ultimate tensile strength, σ_u, of the material. Loss of safety function of the canister is assumed if the stress intensity exceeds the ultimate tensile strength, σ_u. Information on variability of the tensile strength of Type 304 stainless steel in this example is obtained from the test data discussed by McCoy and Waddell [Ref. B.4]. The test data correspond to a series of tensile tests performed in room temperature on several types of specimen (e.g., plates, bars, etc.). The ultimate tensile strength varied from 538 to 662 MPa (78.0 to 96.0 ksi). The goodness of fit test of the ultimate strength data for “As Received” category in Table 2 of Reference B.4 shows lognormal distribution. The median, m_c, and logarithmic standard deviation, β, for the ultimate tensile strength for this example were

estimated to be 589.5 MPa (85.4 ksi) and 0.0413, respectively. The probability density function of the ultimate tensile, σ_u, strength is shown in Figure B-1.

Probability of Failure

Based on the variability in the capacity parameter and a single demand value equal to 497 MPa (72 ksi), the probability of failure was calculated using Equation 3. The cumulative distribution function of *S* is shown in Figure B-2, and failure corresponds to $S \leq 1$. The failure probability is estimated to be 1.8×10^{-5}. When the demand is equal to the code allowable design value, it corresponds to the maximum allowable drop height. If the demand is reduced by lowering the drop height, the ratio of ASME Code Level D allowable stress intensity to predicted maximum stress intensity increases. Failure probabilities for various values of demands are shown in Figure B-2. Failure probabilities for various values of ratios of ASME allowable stress to these corresponding demand values are given in Table B-3.

Conclusions

This example illustrates the level of information that may be required to support the reliability estimate of a canister. It also illustrates an example methodology for estimating reliability based on the statistical variation of the material properties in the estimation of the capacity for the canister. Actual problems may require consideration of uncertainty in both demand and capacity. The reliability methods and supporting data, including consideration of uncertainty, must be supported by a sufficient technical bases.

References

B.1 American Society of Mechanical Engineers, *International Boiler and Pressure Vessel Code*, ASME Section III, Division 1, ASME International, 2004.

B.2 American Society of Mechanical Engineers, *International Boiler and Pressure Vessel Code,* ASME Section II, Part D, Table 2A, ASME International, 2004.

B.3 Haldar, A, and Mahadevan, S., *Probability, Reliability, and Statistical Methods in Engineering Design*. John Wiley and Sons, Inc., New York. 2000.

B.4 McCoy H.E., Jr. and Waddell R.D., *Mechanical Properties of Several Products From a Single Heat of Type 304 Stainless Steel*, Journal of Engineering Materials and Technology, Vol. 97, 1975.

Table B-1: Allowable Minimum Values for Type 304 Stainless Steel (SA–240) at Room Temperature (ASME B&PV Section II, Part D, Table 2A, [Ref. B.2])

Material Property	Value
Ultimate Tensile Strength, σ_u	517 MPa (75 ksi)
Yield Strength, σ_y	207 MPa (30 ksi)
Design Stress Intensity, S_m	138 MPa (20 ksi)

Table B-2: Level D Stress Intensity Limits for Type 304 Stainless Steel (SA–240) at Room Temperature (ASME B&PV Section III, Appendix F, F-1331.1, [Ref. B.1])

Stress Category	Level D Limiting Criteria	Value
Primary Membrane Stress Intensity, P_m	Minimum of 2.4 S_m and 0.7 σ_u	331 MPa (48 ksi)
Primary Membrane (Local or General) (P_L) Plus Primary Bending (P_b) Stress Intensity, i.e., $P_L + P_b$	150 percent of P_m	497 MPa (72 ksi)

Table B-3: Failure Probability with Decreasing Demand

Demand (Stress Intensity)	Ratio of ASME Level D Allowable Stress to Demand	Probability of Failure
497 MPa (72 ksi)	1	1.8×10^{-5}
473 MPa (69 ksi)	1.05	4.8×10^{-8}
452 MPa (66 ksi)	1.1	6.4×10^{-11}

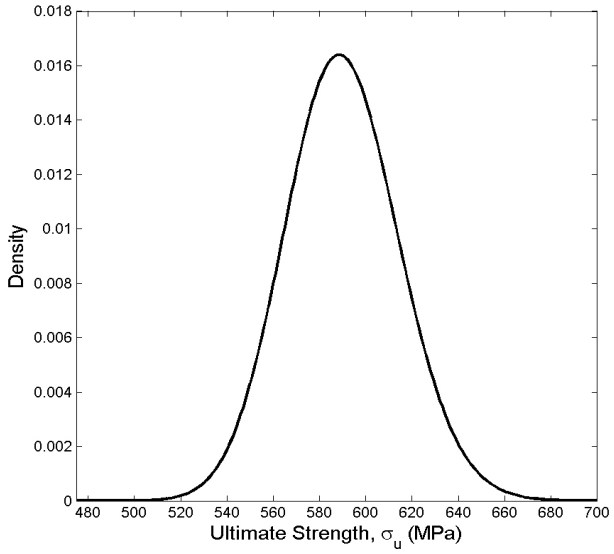

Figure B-1. Capacity of the example canister probability density function of ultimate strength, σ_u.

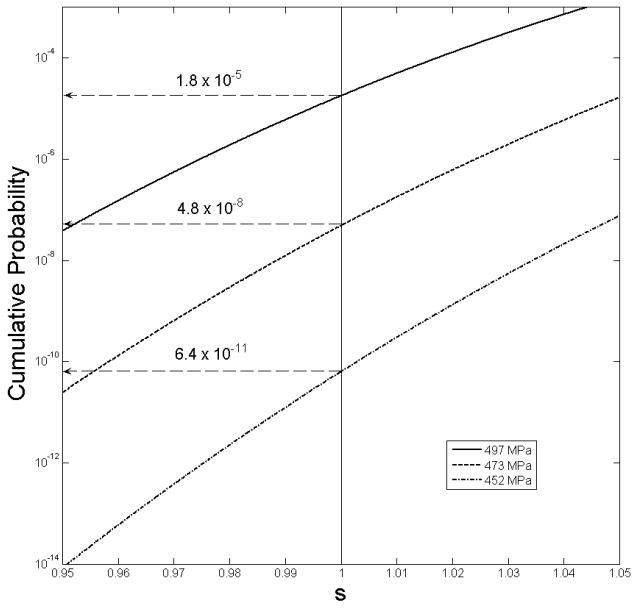

Figure B-2. Cumulative distribution function of S for three demand values.

Approved: /RA/ Date: 3/16/07

Lawrence E. Kokajko, Director
Division of High-Level Waste Repository Safety
Office of Nuclear Material Safety
and Safeguards

Glossary

Appendices

Appendix A: Example - Level of Information and Reliability Estimate of a Crane

Appendix B: Example - Level of Information and Reliability Estimate of a Canister

DISTRIBUTION:
HLWRSr/f NMSSr/f HLWRS Staff

ML070260025

OFC	HLWRS	HLWRS	HLWRS	HLWRS	HLWRS
NAME	CRyder	RJohnson	MShah	TMcCartin	ACampbell
DATE	1/26/07	1/26/07	1/26/07	1/30/07	2/6/07
OFC	HLWRS	TECHED	OGC	HLWRS	HLWRS
NAME	MBailey	EKraus	JMoore	JDavis	LKokajko
DATE	3/1/07	1/28/07	2/26/07	3/7/07	3/16/07

OFFICIAL RECORDS COPY