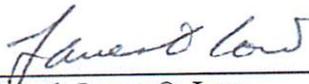


		Number: EA CRAD 31-4 Revision: 0 Effective Date: August 20, 2014
Integrated Safety Basis and Engineering Design Review Criteria Review and Approach Document		
Authorization and Approval	 Director, Office of Nuclear Safety and Environmental Assessments Date: August 20, 2014	 Lead, James O. Low Nuclear Engineer Date: August 20, 2014

1.0 PURPOSE

Within the Office of Enterprise Assessments (EA), the Office of Environment, Safety and Health Assessments (EA-30) mission is to assess the effectiveness of those safety and emergency management systems and practices used by line and contractor organizations in implementing Integrated Safety Management; and to provide clear, concise, and independent evaluations of performance in protecting our workers, the public, and the environment from the hazards associated with Department of Energy (DOE) activities and sites.

In addition to the general independent oversight requirements and responsibilities specified in DOE Order 227.1, *Independent Oversight Program*, this criteria review and approach document (CRAD), in part, fulfills the responsibility assigned to EA in DOE Order 420.1 to conduct independent oversight reviews of implementation of the requirements of the Order.

A key to success is the rigor and comprehensiveness of our process; and, as with any process, we continually strive to improve and provide additional value and insight to field operations. Integral to this is our commitment to enhance our program. We continue to make CRADs available for use by DOE line and contractor assessment personnel in developing effective DOE oversight, contractor self-assessment, and corrective action processes; the current revision is available at: <http://energy.gov/iea/listings/criteria-review-and-approach-documents>.

2.0 APPLICABILITY

The following CRAD is approved for use by the Office of Nuclear Safety and Environmental Assessments (EA-31).

3.0 FEEDBACK

Comments and suggestions for improvements on this CRAD can be directed to the Director, Office of Environment, Safety and Health Assessments, at (301) 903-5392.

4.0 CRITERIA REVIEW AND APPROACH

OBJECTIVE

SBED.1: The contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must establish and maintain the safety basis for the facility. (10 CFR 830 Section 830.202.a)

SBED.2: In maintaining the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: (1) Update the safety basis to keep it current and to reflect changes in the facility, the work, and the hazards as they are analyzed in the documented safety analysis (DSA); (2) Annually submit to DOE either the updated DSA for approval or a letter stating that there have been no changes in the DSA since the prior submission; and (3) Incorporate in the safety basis any changes, conditions, or hazard controls directed by DOE. (10 CFR 830 Section 830.202.c)

SBED.3: In establishing the safety basis for a hazard category 1, 2, or 3 DOE nuclear facility, the contractor responsible for the facility must: (1) Define the scope of the work to be performed; (2) Identify and analyze the hazards associated with the work; (3) Categorize the facility consistent with DOE-STD-1027-92; (4) Prepare a DSA for the facility; and (5) Establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment. (10 CFR 830 Section 830.202.b)

SBED.4: A contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must develop technical safety requirements (TSRs) that are derived from the DSA. (10 CFR 830 Section 205a.1)

CRITERIA

SSC Safety Functions and Engineering Design

1. The DSA for a hazard category 1, 2, or 3 DOE nuclear facility must, as appropriate for the complexities and hazards associated with the facility, derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use. (10 CFR 830 Section 204.b.4)
2. Safety structures, systems, and components require formal definition of minimum acceptable performance in the DSA. This is accomplished by first defining a safety function, then describing the structures, systems, and components, placing functional requirements on those portions of the

structures, systems, and components required for the safety function, and identifying performance criteria that will ensure functional requirements are met. TSRs are developed to ensure the operability of the safety structures, systems, and components and define actions to be taken if a safety structure, system, or component is not operable. (10 CFR 830 Appendix A, Section G.3)

3. Safety analyses must be used to establish (a) the identity and functions of safety class and safety significant structures, systems, and components (SSCs), and (b) the significance to safety of functions performed by safety class and safety significant SSCs. (DOE O 420.1B, Change 1, Chapter I, Section 3.a.1)
4. Nuclear facility design objectives must include multiple layers of protection to prevent or mitigate the unintended release of radioactive materials to the environment, otherwise known as defense-in-depth. (DOE O 420.1B, Change 1, Section 3.b.1)
5. Safety SSCs and safety software must be designed, commensurate with the importance of the safety functions performed, to perform their safety functions when called upon, and to meet the quality assurance program requirements of either 10 CFR 830, Subpart A, or DOE O 414.1C, *Quality Assurance*, as applicable. (DOE O 420.1B, Change 1, Section 3.b.7)
6. The Quality Assurance Program must address the following management, performance, and assessment criteria - Criterion 6—Performance/Design: (1) Design items and processes using sound engineering/scientific principles and appropriate standards; (2) Incorporate applicable requirements and design bases in design work and design changes; (3) Identify and control design interfaces; (4) Verify or validate the adequacy of design products using individuals or groups other than those who performed the work; and (5) Verify or validate work before approval and implementation of the design. (10 CFR 830 Section 122.f)

- Within the scope of the review, do the safety bases (e.g., the DSA) adequately describe the safety requirements and functions of selected safety SSCs and are their technical bases consistent with the logic and assumptions presented in the hazard and accident analyses?
- Are safety SSCs (including credited structures and components of a system) classified and documented according to their significance to safety using a SSC functional classification process consistent with DOE requirements and safe harbor standards?
- Does the DSA identify and describe appropriate system safety functions and performance criteria to provide reasonable assurance that selected system functional requirements will be met?
- Does the definition or description of the SSC's safety functions include:
 - The specific role of the SSC in detecting, preventing, or mitigating analyzed events?
 - The associated conditions and assumptions concerning SSC performance?
 - SSC performance requirements and criteria relied upon in the hazard or accident analysis, including essential supporting SSCs, for normal, abnormal, and accident conditions?
- Are the functional and performance requirements in the DSA appropriately translated into the engineering design through design documents such as drawings, calculations, and specifications?
- Have the design bases and design assumptions identified in the safety analysis and other applicable design inputs been correctly and completely translated into design specifications, drawings, calculations, procedures, and instructions (e.g., for construction, installation, operation, maintenance, and testing of SSCs)?
- Are procedures employed to assure that design activities are carried out in a planned, controlled, orderly and correct manner?
- Are procedures used to control issuance of design documents and changes thereto?
- Are applicable design inputs, such as design bases, regulatory requirements, and codes and standards (such as applicable National Fire Protection Association and American National Standards Institute standards) identified and documented, and their selection reviewed and approved?

- Do the design output documents provide evidence that sound engineering principles and appropriate standards were applied?
- Where the single failure design criteria are applicable, does the design of the SSC ensure that a single failure does not result in the loss of capability to accomplish its required safety functions?
- Are the safety SSCs designed to withstand the effects of (or be compatible with) the environmental conditions associated with operation, maintenance, shutdown, testing, and abnormal conditions?
- Does design and equipment qualification provide assurance that safety SSCs are capable of performing required safety functions under design basis accident conditions, including natural phenomena hazards?
- Do the technical bases of TSRs for the system appropriately reflect assumptions of facility configuration and performance of safety functions, operational parameters, and key programmatic elements?
- Are acceptance criteria for tested parameters supported by calculations or other engineering documents to ensure that design basis assumptions are met?
- Is the adequacy of design verified through the process of reviewing, confirming, or substantiating the design by one or more methods to provide the assurance that the design meets the specified design inputs?
- Was design verification performed by competent individuals or groups other than those who performed the original design (but who may be from the same organization)?
- Based on a walk down of the facility SSCs, document reviews, and personnel interviews, verify the following:
 - Are system boundaries appropriately defined in accordance with the DSA?
 - Are operation and system alignments consistent with design basis assumptions?
 - Will the system configuration, as installed, support system function under postulated abnormal and accident conditions?
 - Will all energy sources (e.g., electric power, diesel fuel, and compressed air) relied on for accident mitigation, including those used for control functions, be available and adequate during abnormal and accident conditions?
 - Is potential degradation of safety SSCs prevented or monitored?
 - Are safety SSCs and associated equipment qualified for the environment expected under all conditions?
 - Are safety SSCs and associated equipment adequately protected from natural external events?
 - Are safety margins being maintained?
- Is guidance established for surveillance, testing, calibration, and maintenance of these SSCs consistent with applicable requirements and standards?

Safety SSC Design Basis and Configuration Control

7. Configuration management must be used to develop and maintain consistency among system requirements and performance criteria, documentation, and physical configuration for the SSCs within the scope of the program. (DOE O 420.1B, Change 1, Chapter V, Section 3.c.1)
8. System design basis documentation and supporting documents must be compiled and kept current using formal change control and work control processes. When design basis information is not available, documentation must include (a) system requirements and performance criteria essential to performance of the system's safety functions, (b) the basis for the system requirements, and (c) a description of how the current system configuration satisfies the requirements and performance criteria. (DOE O 420.1B, Chapter V, Section 3.c.3)
9. Key design documents must be identified and consolidated to support facility safety basis development and documentation. (DOE O 420.1B, Chapter V, Section 3.c.4)

- Is there a formal, controlled list of current safety basis documents, including DOE-approved DSA/TSR (or PDSA)?
- Are valid safety basis documents available at the facility?
- Has the completed design been recorded in design output documents, such as drawings, specifications, test/inspection plans, maintenance requirements, and reports?
- Are design documents (e.g., calculations, drawings, design specifications, procurement specifications, and computer software) associated with safety SSCs prepared, verified, coordinated, approved, tracked, and controlled within a formal process that ensures continued alignment with the design input parameters?
- Is the established technical baseline (e.g., drawings, procedures, 3D models, and master equipment list) comprised of approved documents and databases?
- Are controls to manage changes to the baseline established and implemented?
- Is there a facility-specific list of safety and defense-in-depth SSCs (e.g., a master equipment list) readily available?
- Are the system design basis and supporting documents identified and consolidated in documentation consistent with DOE-STD-3024 on system design descriptions?
- When design basis information is not available, does the documentation include system requirements, basis for the system requirements, essential performance criteria, and a description of how the current system configuration satisfies the specified requirements and performance criteria?
- Have technical and administrative design interfaces been identified and methods established for their control?
- Are design input and functional requirements included in technical task requests, facility/system modifications, and safety component procurements?

APPROACH

Record Review:

- Review applicable DOE site office and contractor requirements documents on nuclear safety documentation, including nuclear safety design criteria to be used in designing, constructing, and modifying the nuclear facility and in preparing its safety basis, functional area manuals, and engineering documents.
- Review the appropriate safety basis documents, including hazard analyses, DSA, TSRs, and supporting documents (e.g., system diagrams, piping and instrumentation diagram, system design descriptions and calculations).
- Review related technical documents that translate the safety basis and design into appropriate controls and procedures for technical activities related to the SSCs, such as construction, installation, operation, maintenance, procurement, and testing.
- Review a sample of technical baseline and design related documents; such as, design criteria, specifications, calculations, drawings, and system design descriptions.
- Review design change and configuration control procedures.
- Review pertinent documents associated with a sample of recent facility modifications.

Interviews:

- Engineering personnel
- Safety basis personnel

- Cognizant system engineers
- Interview appropriate operations, maintenance, and training staff regarding pertinent processes and procedures, as they relate to engineering and design of SSCs.

Observations:

- Walk down the nuclear facility and selected safety SSCs to gain understanding of system dependencies and potential vulnerabilities to adverse conditions.