
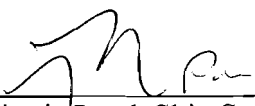


<p>U.S. Department of Energy</p> <p>Office of Independent Oversight</p> <p>Criteria Review and Approach Document</p>	<p>Subject: Engineering Design and Safety Basis Inspection Criteria, Inspection Activities, and Lines of Inquiry</p> <p></p> <hr/> <p>Director, Office of ES&amp;H Evaluations</p> <p>Date: 12/22/09</p> <p></p> <hr/> <p>Criteria Lead, Shiv Seth</p> <p>Date: 12/22/09</p>	<p>HS: HSS CRAD 64-19</p> <p>Rev: 0</p> <p>Eff. Date: December 22, 2009</p> <p>Page 1 of 7</p>
--	--	--

## 1.0 PURPOSE

Within the Office of Independent Oversight, the Office of Environment, Safety and Health (ES&H) Evaluations' mission is to assess the effectiveness of environment, safety, and health 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. 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. Therefore, we have developed the Engineering Design and Safety Basis Inspection Criteria, Inspection Activities, and Lines of Inquiry for internal use, which we are also making available on the Office of ES&H Evaluations webpage for use by DOE line and contractor assessment personnel in developing and implementing effective DOE oversight and contractor self-assessment and corrective action processes.

## 2.0 APPLICABILITY

The following Inspection Criteria document is approved for use by the Office of ES&H Evaluations.

## 3.0 FEEDBACK

Comments and suggestions for improvements on these inspection criteria, activities, and lines of inquiry can be directed to the Director of the Office of ES&H Evaluations on (301) 903-5392.

## **Engineering Design and Safety Basis Inspection Criteria, Inspection Activities, and Lines of Inquiry**

**Scope:** The engineering design and safety basis inspection will evaluate the effectiveness of programs and processes for the design and safety basis of selected safety structures, systems, and components (SSCs) of a nuclear facility. The nuclear facility may be an existing facility, a major modification to an existing facility, or a new facility under construction. Accordingly, the safety basis for the facility, for example, a documented safety analysis (DSA) or a preliminary documented safety analysis (PDSA), may not have been completed and approved by the DOE. The inspection criteria, activities, and lines of inquiry are, therefore, intended to be tailored to the review objectives. Generally, the safety basis aspects to be assessed will focus on the selected SSCs and their safety basis rather than the broader safety basis program and methodologies. The assessment also may address certain other interfacing functional areas, such as configuration management, operations, maintenance, testing, design procedures, personnel training and qualifications, safety SSC procurement, and issues management/corrective action; but only as these functions relate to the engineering design and safety bases of the selected SSCs. The inspection will be performed in the context of integrated safety management.

Presented below are the inspection criteria and suggested inspection activities and lines of inquiry in three related subareas: engineering design and safety bases of safety SSCs; configuration control of the design and safety basis documentation and of the SSCs (as applicable, when procured and/or installed); and feedback and improvement as it relates to safety SSC design and safety bases. (See HSS CRAD 64-32, on Specific Administrative Controls (SACs) Implementation when SACs are used in lieu of safety SSCs.)

### **Inspection Criteria:**

#### **A. Safety SSC Functions and Design**

### **Inspection Criteria:**

- Safety analyses are performed as early as practical in conceptual or preliminary design processes to ensure that the required SSCs and the support systems on which they rely to perform safety functions, are specified in the final design. Safety analyses address hazards inherent to the facility and its activities, natural phenomena hazards, and external man-induced hazards; and are used to establish the identity, functions, and significance of safety SSCs. [DOE O 420.1B, Ch. I, (3)(a)(1) – (3)]
- Nuclear facility design includes multiple layers of protection (defense in depth) to prevent or mitigate the unintended release of radioactive materials to the environment. These multiple layers must include multiple physical barriers unless the basis for not including multiple physical barriers is documented in the safety basis and approved by DOE. [DOE O 420.1B, Ch. I, (3)(b)(1)]
- The safety basis demonstrates the adequacy of controls provided by the system to eliminate, limit, or mitigate identified hazards, and defines the process for maintaining the controls current at all times and controlling their use. [10 CFR 830.204 (4)]

- Functional requirements and performance criteria for SSCs are adequately specified, and technical safety requirements are developed to ensure the operability of the safety SSCs in the normal, abnormal, and postulated accident conditions. [10 CFR 830.205 and App. A, Sec. G (3)]
- Safety SSCs and safety software are designed commensurate with the importance of the safety functions performed, using sound engineering/scientific principles and appropriate standards to perform their safety functions when called upon, and to meet the DOE quality assurance program requirements. Applicable requirements and design bases are incorporated in design work and design changes. Design interfaces are identified and controlled. [DOE O 420.1B, Ch. I, (7) and 10 CFR 830.122(f)(1) - (3)]
- The adequacy of design products is verified or validated by individuals or groups other than those who performed the work. Verification or validation work is completed before approval and implementation of the design. [10 CFR 830.122(f)(4) and (5)]

### **Inspection Activities:**

- Review applicable DOE site office and contractor requirements documents on nuclear safety documentation, including nuclear safety design criteria to be used in designing and constructing the nuclear facility and in preparing its safety basis, functional area manuals, and engineering procedures.
- Review the appropriate safety basis documents, including hazard analyses, facility categorization, PDSA, or DSA, technical safety requirements (TSRs), system design descriptions, and supporting documents (e.g., system diagrams, P&IDs, calculations).
- Walk down the nuclear facility and selected safety SSCs to gain understanding of system dependencies and potential vulnerabilities to adverse conditions.
- Review training and qualifications requirements and records for engineering and safety basis staff.
- Review related technical documents that formulate the translation of the design and safety basis into appropriate controls and procedures for technical activities related to the SSCs, such as construction, installation, operation, maintenance, procurement, and testing.
- Interview appropriate engineering design, safety basis, and configuration management personnel (including design authorities and system engineers), as well as operations, maintenance, and training staff regarding pertinent processes and procedures, as they relate to engineering and design of SSCs.

### **Inspection Lines of Inquiry**

- Is the nuclear facility (or facility segment) appropriately categorized based on hazard inventories (using methodology described in DOE-STD-1027) to provide a basis for the determination of design requirements, level and sophistication of safety analysis, and safety documentation requirements?
- Within the scope of the review, do the safety bases (e.g., the DSA or the PDSA) adequately describe the safety requirements and functions of selected safety SSCs and their technical bases, which are 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 fully identify and describe the appropriate system safety functions performance criteria necessary to provide reasonable assurance that selected system functional requirements will be met?
- Does the definition/description of the safety functions of the system include the following:
  - Specific role of the system in detecting, preventing, or mitigating analyzed events?
  - The associated conditions and assumptions concerning system performance?
  - System requirements and performance criteria for the system and components, including essential supporting systems for normal, abnormal, and accident conditions relied upon in the hazard or accident analysis?
- Are applicable design inputs, such as design bases, regulatory requirements, codes and standards (such as applicable National Fire Protection Association and American National Standards Institute standards) identified, documented, and their selection reviewed and approved? [ANSI N45.2.11; Sec. 3.1]
- Does the safety SSC design ensure that a single failure (where the single failure design criteria are applicable) 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?
- Are procedures employed to assure that design activities are carried out in a planned, controlled, orderly and correct manner? [ANSI N45.2.11; Sec. 2.2 provides what should be covered]
- 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)? [ANSI N45.2.11; Sec. 4.1]
- 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 bases 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? [ANSI N45.2.11; Sec. 6.1]
- 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)? [ANSI N45.2.11; Sec. 6.1]
- Are procedures used to control issuance of design documents and changes thereto? [ANSI N45.2.11; Sec. 7]
- Based on facility/SSC walkdown, document review 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 SSC prevented or monitored?
- Are safety SSC and associated equipment qualified for the environment expected under all conditions?
- Are safety SSC and associated equipment adequately protected from natural external events?
- Are safety margins being maintained?
- Are design and system engineers appropriately qualified and trained for their technical positions and responsibilities? Are they trained in procedures that ensure quality in design and engineering (e.g., documenting design calculations, determination of safety and quality classification, performing inspections and assessments, resolving non-conformance and deficiencies, and supporting procurement specifications and receipt inspections)?

## **B. Safety SSC Design Basis and Configuration Control**

### **Inspection Criteria:**

- The key design documents, including SSC design basis and supporting documents, are identified and consolidated to support facility safety basis development and documentation. They are kept current using formal change control and work control processes. [DOE O 420.1B, Ch. V, 3(c)(3) and (4)]
- An adequate, DOE-approved unreviewed safety question (USQ) process has been implemented at existing nuclear facilities (or appropriate process and criteria established at nuclear facilities under design and construction) to determine the need for DOE approval of changes to facility and procedures. [10 CFR 830.203, for existing nuclear facilities]
- Configuration management is used to develop and maintain consistency among system requirements and performance criteria, documentation, and physical configuration for the SSCs within the scope of the process. [DOE O 420.1B, Ch. V, 3(c)(1)]

### **Inspection Activities:**

- Review a sample of technical baseline and design related documents, such as design criteria, specifications, calculations and drawings; review sample system design descriptions.
- Review design change and configuration control procedures, including the USQ process (or a USQ-like process typically at nuclear facilities under construction) that may be used to screen and evaluate proposed facility design modifications and changes.
- Review pertinent documents associated with a sample of recent facility modifications.

### **Inspection Lines of Inquiry**

- 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? Are the DSA and TSRs for existing nuclear facilities reviewed at least annually to maintain their applicability, and approved by DOE via a safety evaluation report (SER)?

- Has the completed design been recorded in design output documents, such as drawings, specifications, test/inspection plans, maintenance requirements, and reports?
- Are design output 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 maintenance of alignment with the design input parameters?
- Does the established technical baseline (e.g., drawings, procedures, 3D models, and master equipment list) comprise 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? Is guidance established for surveillance, testing, calibration, and maintenance of these SSCs consistent with applicable requirements and standards?
- 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 been established for their control?
- Are design input and functional requirements included in technical task requests, facility/system modifications, and safety component procurements?
- Has an adequate DOE-approved USQ (or a similar process for a facility under design and construction) been established to screen design modifications and changes and to identify those requiring DOE approval?
- Do the screenings and evaluations using the USQ (or a similar process) reflect adequate implementation of the process?
- Is the USQ screening/determination being performed by staff knowledgeable of the safety basis? Are they appropriately trained on the USQ process?

### **C. Safety SSC Design Feedback and Improvement**

#### **Inspection Criteria:**

- Formal processes are effectively implemented to identify engineering design and configuration control problems and deficiencies, to identify their causes; to identify, track, monitor, close, and verify corrective actions; and to derive lessons learned. [Based on 10 CFR 830.122(c); DOE O 226.1(3)(b)]
- DOE line management has established and implemented effective processes for monitoring and assessing contractor programs for ensuring effective design and configuration control of safety SSCs, and for developing and maintaining the nuclear facility safety basis. [Based on DOE O 226.1(4)(e)]

#### **Inspection Activities:**

- Review recent self-assessments and independent assessments pertaining to the engineering design, configuration management, and safety basis of selected safety SSCs.

- Review how design and related configuration control and safety basis issues are tracked, prioritized, and resolved, including any root cause analyses performed.
- Review a sample of corrective actions covering deficiencies identified in assessments.

**Inspection Lines of Inquiry:**

- Has the contractor conducted periodic, rigorous assessments of the engineering design and nuclear safety functional areas?
- Have audits conducted on a routine basis established the adequacy of and conformance to the design quality assurance requirements? [ANSI N45.2.11; Sec. 11.5]
- Were the identified issues adequately tracked and resolved in a timely manner?
- Are there recurring problems or deficiencies in SSC design? If so, why have the corrective actions not been effective?
- Did the responsible DOE line management organization perform an effective review of the safety basis documents, in particular the safety design bases of selected SSCs with appropriately qualified personnel?
- Were DOE review comments on safety SSC engineering and safety basis adequately resolved by the contractor?
- Were any differing professional views/opinions filed? Were those adequately resolved and closed out?