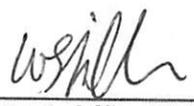
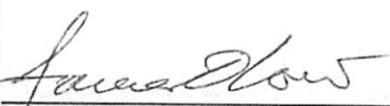


		Number: EA CRAD 31-07 Revision: 0 Effective Date: December 2, 2014
<b>New Nuclear Facility          Documented Safety Analysis and Technical Safety Requirements          Criteria Review and Approach Document</b>		
Authorization and Approval	 Director, Office of Nuclear Safety and Environmental Assessments (EA-31)  Date: December 2, 2014	 Lead, James O. Low Nuclear Engineer  Date: December 2, 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 O 420.1C to conduct independent oversight reviews of implementation 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/node/611001/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***

**SB.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)

**SB.2:** 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 documented safety analysis (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)

**SB.3:** Table 2 sets forth acceptable methodologies for preparing a DSA. (10 CFR 830, Appendix A, Section F.4)

**SB.4:** A contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must: (1) Develop technical safety requirements (TSRs) that are derived from the DSA; and (2) Obtain DOE approval of TSRs and any change to TSRs. (10 CFR 830 Section 205.a.1&2)

### ***CRITERIA***

#### **Hazard and Accident Analysis (Chapter 3)**

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, provide a systematic identification of both natural and man-made hazards associated with the facility. (10 CFR 830 Section 830.204.b.2)
  - Is the application of the graded approach consistent with the facility hazard categorization, mission and complexity?
  - Is the hazard analysis based on the currently approved scope of work at the facility?
  - Does the hazard analysis include hazard identification that specifies or estimates the hazards relevant for DSA consideration (i.e., both natural and man-made hazards associated with the work and the facility) in terms of type, quantity, and form?
  - Does the hazard analysis present a systematic, comprehensive identification of hazardous materials and energy sources present by type, quantity, form, and location; natural phenomena

- hazards, including design basis and beyond-design-basis events; and sources of external hazards, such as nearby airports, railroads, or utilities such as natural gas lines?
- Does the hazards analysis include explicit description or reference to the material at risk (MAR), chemical or radiological, potentially affected in the selected hazard scenarios?
  - Does the hazard analysis include a hazard evaluation that covers the activities for which approval is sought?
  - Is the hazard analysis consistent in approach with safe harbor methodologies?
  - Does the hazard analysis identify preventive and mitigative features for the spectrum of events examined using a proper hierarchy?
  - Does the hazard analysis identify dominant accident scenarios through ranking or an equivalent structure?
  - Do the dominant accident scenarios establish representative, bounding, and unique accidents?
  - Are normal, abnormal, and accident conditions (including consideration of natural and manmade external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials) evaluated?
  - Is the Fire Hazards Analysis current and the results integrated into the hazard analysis?
2. 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, evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility. (10 CFR 830 Section 830.204.b.3)
- Does the accident analysis clearly substantiate the findings and delineations of the hazard analysis for the subset of events examined and confirm their potential consequences?
  - Are results clearly characterized in terms of public safety, defense- in-depth, worker safety, and environmental protection (i.e., the consequence results represent a significant hazard to safety of workers or the public, or represent a significant uncontrolled release of hazardous material to the environment, or challenge or exceed applicable evaluation guidelines)?
  - Does the accident analysis clearly and completely describe accident progression?
  - Is the accident analysis methodology adequate to conservatively assess dose or exposure at receptor locations representing onsite workers and the public?
  - Are all pertinent assumptions (e.g., hazardous material inventory, airborne release fraction, and damage ratio) established?
  - Are the consequences of postulated accidents appropriately compared with the evaluation guidelines and evaluated to functionally classify safety structures, systems or components (SSCs) and specific administrative controls (SACs)?
3. 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 830.204.b.4)
4. Defense- in-depth strategies must include using equipment and administrative controls that restrict deviation from normal operations, monitor facility conditions during and after an event, and provide for response to accidents to achieve a safe condition. (DOE O 420.1B Change 1, Chapter I, Section 3.b.2.(f))

- Are the consequences used appropriately to classify safety SSCs and SACs in accordance with DOE guidance?
- Is the logic behind assessing the results in terms of safety-significant SSCs, SACs, and designation of TSRs understandable and internally consistent?
- Have safety-class and safety-significant SSCs, SACs and associated TSRs been identified for preventing and/or mitigating events potentially exceeding evaluation guidelines?
- Are the results of hazards evaluation summarized to identify significant defense-in-depth strategies and worker safety features, hazard controls, including SSCs, SACs, and key elements of safety management programs?
- Does the selection of hazard controls appropriately follow the principles associated with the hierarchy of controls?
- Are the selected hazard controls, both individually and collectively, adequate to prevent or mitigate the accidents for which they are credited as a control?
- Are mitigated design basis accidents that do not meet the DOE evaluation guideline for the maximally exposed offsite individual evaluated and dispositioned as exigent circumstances (see DOE S-2 Letter: Poneman to Winokur, July 19, 2012)?

### **Beyond Design Basis Accidents (Chapter 3)**

5. 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, evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility. (10 CFR 830 Section 830.204.b.3)
6. Program Offices shall direct contractors responsible for hazard category 1 and 2 nuclear facilities that have the potential to exceed DOE's 25 rem public dose evaluation guideline, based on an unmitigated analysis, to conduct an evaluation using the guidance in Attachment 2 in conjunction with the 2015 annual update of DSAs. [OE-1: 2013-01, Improving Department of Energy Capabilities for Mitigating Beyond Design Basis Events, Action 2]
  - Does the facility have the potential to exceed the DOE evaluation guideline (25 rem) for any unmitigated accidents?
  - Are potential beyond design basis accidents identified and the need for their evaluation considered and evaluated as appropriate?
  - What beyond design basis accidents (DBAs) were identified and considered for evaluation as part of the DSA revision/development? Have these beyond DBAs been identified as bases for additional cost-benefit analysis?
  - If beyond DBAs were evaluated, did the types of events include seismic events, fires, explosions, criticality, floods, lightning, wind and tornados, snow and ice, ash fall, airplane crash, electrical blackout, or cascading effects of DBAs?
  - Was the rationale for excluding any of the types of events above documented?
  - Did the evaluation estimate the consequences associated with failures of SSCs that provide safety functions such as confinement, energy removal, or prevention of energetic reaction?
  - Were any events that could cause an accident with the potential for a release of radioactive material and potentially also impact emergency power supplies identified (i.e., a release of radioactive material from primary confinement barriers with a simultaneous loss of power)?
  - What were the results of any analysis (performed as part of the DSA) of capabilities to address beyond DBAs?

- Were SSCs identified as mitigating beyond DBA consequences subjected to a margins assessment (to provide insight into their margin-to-failure)?
- Has the insight from beyond DBA analysis been used to identify additional facility features (such as non-credited SSCs) that could prevent or reduce severe beyond DBA consequences?
- If so, does the DSA identify these non-credited SSCs as important for providing mitigation of beyond DBAs (for inclusion in the facility configuration management and maintenance programs)?
- Were any additional mitigation strategies identified for beyond DBAs?
- Do the descriptions of the beyond DBA accident scenarios clarify important assumptions needed to support development of abnormal or emergency operating procedures?
- Have actions necessary to support emergency management response plans been identified and included in the DSA?

#### **Safety SSCs (Chapter 4)**

7. 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 830.204.b.4)
8. Safety analyses must be used to establish: (a) the identity and functions of safety class and safety significant SSCs, (b) the significance to safety of functions performed by safety class and safety significant SSCs, and (c) the SACs needed to fulfill safety functions. (DOE O 420.1B, Change 1, Chapter I, Section 3.a.1)
  - Does the DSA satisfactorily document the basis for determining the safety SSCs and their required functions?
  - Are the safety SSCs identified and described in the DSA consistent with the logic presented in the hazard and accident analyses?
  - Are safety functions for safety SSCs defined with clarity and consistent with the bases derived in the hazard and accident analyses?
  - Does the system description of the SSC contain a basic summation of the physical information known about the SSC (e.g., Piping & Instrumentation Diagram (P&ID), safety SSC engineering specifications)?
  - Is the required functional classification of an SSC (e.g., safety-class or safety-significant) based on a proper assessment of the unmitigated accident consequence?
  - Are the boundaries and interface points of safety SSCs (relevant to their safety function), including the support systems, clearly defined?
  - Do the functional requirements and system evaluations derive from the safety functions and provide evidence that the safety functions can be performed when called upon?
  - Are safety functions and the design and functional requirements for safety SSCs defined with clarity, and are they consistent with the bases derived in the hazard and accident analyses? Specifically, for each safety SSC, does the safety basis document:
    - Identify safety functions to be performed or maintained by safety SSCs, consistent with the hazard and accident analyses, in the normal, abnormal, or accident conditions postulated?
    - Identify functional and design requirements (e.g., to address non-ambient environmental stresses, or to withstand seismic and other natural phenomena)?

- Identify the performance criteria necessary to provide reasonable assurance that SSC functional requirements will be met (e.g., surveillance, maintenance, specific operational response, requisite operator training and qualifications)?
- Evaluate the safety SSCs capabilities to ensure that the performance criteria are satisfied?
- Identify and designate as safety SSC the support systems on which safety SSCs rely to perform or maintain safety functions?
- Provide for TSR coverage?
- Was a system evaluation performed to assure that the safety functions can be performed when called upon?
- Does the system evaluation identify the performance criteria necessary to ensure that the identified functional requirements will be met?
- Are the general requirements for safety SSCs (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes) appropriately specified?
- Are codes and standards appropriately specified and tailored, as necessary, based on functional classification and safety function?
- Is the control of safety SSCs relevant to TSR development clearly defined?
- Are the identified safety SSCs adequate to mitigate or prevent the analyzed accidents with potential to exceed evaluation guidelines?
- Does the suite of safety controls provide multiple layers of protection to prevent or mitigate the unintended release of radioactive materials?

### **SSC Safety Function and Engineering Design Integration**

9. Safety SSCs require formal definition of minimum acceptable performance in the DSA. This is accomplished by first defining a safety function, then describing the SSCs, placing functional requirements on those portions of the SSCs 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 SSCs and define actions to be taken if a safety SSC is not operable. (10 CFR 830 Appendix A, Section G.3)
10. 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)
11. 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 414.1D, Change 1, *Quality Assurance*, as applicable. (DOE O 420.1B, Change 1, Section 3.b.7)
12. 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? If deviation to these design inputs are necessary, has the appropriate documentation (i.e., equivalencies, exemptions, etc.) been reviewed and approved by the respective Authority Having Jurisdiction (AHJ)?
- 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?

#### **SACs (Chapter 4)**

13. As appropriate for a particular DOE nuclear facility, the section of the TSRs on administrative controls organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure safe operation of a facility is consistent with the TSR. In general, the administrative controls section addresses (1) the requirements associated with administrative controls, (including those for reporting violations of the TSR); (2) the staffing requirements for facility positions important to safe conduct of the facility; and (3) the commitments to the safety management programs identified in the DSA as necessary components of the safety basis for the facility. (10 CFR 830 Appendix A, Table 4)
14. An SAC exists when an administrative control is identified in the DSA as a control needed to prevent or mitigate an accident scenario, and has a safety function that would be SS or SC if the function were provided by an SSC. (DOE-STD-1186, Section 1.2)
- Does the DSA provide the safety requirements and functions of selected SACs and satisfactorily document the basis for determining the assigned functions are appropriately assigned as administrative controls?
  - Does the safety analysis establish the functions of SACs and their significance to safety?
  - Does the DSA identify the appropriate performance criteria necessary to provide reasonable assurance that selected SAC functional requirements will be met?
  - Are the SACs identified and described consistent with the logic presented in the hazard and accident analyses?
  - Does the suite of safety controls, including SACs where designated, provide multiple layers of protection to prevent or mitigate the unintended release of radioactive materials?
  - Are safety functions for SACs defined with clarity and consistent with the bases derived in the hazard and accident analyses?
  - Is there adequate rationale for controlling the identified hazard through an SAC instead of an SSC?
  - Is the adequacy of SACs to effectively perform their required safety functions documented in the DSA?
  - Are there SSCs whose failure would result in losing the ability to complete the action required by the SAC?
  - Where SACs rely on supporting SSCs to perform their intended safety function, have these SSCs been properly identified, classified with respect to safety, and controlled so that they can meet performance requirements consistent with their safety importance?

- Do the functional requirements and evaluations of SAC provisions provide evidence that the required safety functions can be performed when called upon?
- Do the SAC evaluations contain appropriate analysis (i.e., human reliability analysis) of human performance factors that affect task performance and human factors engineering?
- Do the SAC evaluations identify the time interval for re-verification of the SAC(s) and provide the technical basis for these time intervals?
- Are the SAC controls clearly defined to support future TSR development?
- Do the SACs appropriately reflect assumptions of facility configuration and human performance of safety functions, operational parameters, and key programmatic elements?
- Does the formulation of SACs include conservative “design” safety margins?
- Are the SACs classified using the same criteria as used for classifying safety SSCs?

### **Derivation of TSRs (Chapter 5)**

15. A contractor responsible for a hazard category 1, 2, or 3 DOE nuclear facility must: (1) Develop TSRs that are derived from the DSA; and (2) obtain DOE approval of TSRs and any change to TSRs. (10 CFR 830 Section 830.205.a.1&2)
- Are identified TSRs adequate to preserve the functional and administrative requirements necessary to ensure protection of workers, the public, and the environment (as identified in the hazard and accident analyses)?
  - Have the facility operational modes (e.g., startup, operation, and shutdown) relevant to derivation of TSRs been adequately defined such that the status of safety SSCs/SACs can be distinctively defined; for example, operation during major outages of facility systems for maintenance or operation of multiple segmented areas of the facility?
  - Have the assumptions requiring TSR coverage and the bases for deriving TSRs been identified and described in the safety basis document?
  - Is there sufficient information provided to identify the safety limits, limiting control settings, and limiting conditions for operation that will be needed to support the facility TSR documentation?
  - Are the bases deriving safety limits, limiting control settings, limiting conditions for operation, surveillance requirements, and administrative controls provided and technically accurate?
  - Has each safety-significant or safety-class SSC or SAC identified in Chapter 4 been listed?
  - Have passive SSCs been designated as design features and their performance criteria identified when appropriate?
  - Is there adequate documented explanation for any safety SSCs/SACs or other safety features that will not be provided TSR controls coverage?
  - Have the bases for deriving TSRs been identified and described in the hazard and accident analyses, safety SSC, and SAC chapters?
  - Is the logic for the TSR derivation consistent with the logic and assumptions presented in the analyses?
  - Is the process for maintaining the TSRs current and controlling their use defined?
  - Are the facility design aspects necessary to implement the identified surveillance requirements (e.g., instrumentation, equipment access) adequately identified?
  - Does the design features section identify the important aspects of the passive design features not specifically required to have TSR LCOs?
  - Are TSRs from other adjacent facilities that can affect this facility’s operations identified and summarized?

## **TSRs**

16. TSRs establish limits, controls, and related actions necessary for the safe operation of a nuclear facility. (10 CFR 830 Appendix A, Section G.4)
17. TSRs may have sections on (1) safety limits, (2) operating limits, (3) surveillance requirements, (4) administrative controls, (5) use and application, and (6) design features. It may also have an appendix on the bases for the limits and requirements. (10 CFR 830 Appendix A, Section G.4)
18. Table 4 sets forth DOE's expectations concerning acceptable TSRs. (10 CFR 830 Appendix A, Section G.6)
  - Does Section 1 include the standard use and application explanations for TSR devices such as: logical connectors, completion time, frequency notation, safety limits, limiting control settings, limiting conditions for operation, and surveillance requirements?
  - Do the TSRs accurately reflect the derivation of TSRs in the DSA?
  - Are identified TSRs adequate to preserve the functional and administrative requirements necessary to ensure protection of workers, the public, and the environment (as identified in the hazard and accident analyses)?
  - Have the facility operational modes (e.g., startup, operation, and shutdown) relevant to derivation of TSRs been adequately defined such that the status of safety SSCs/SACs can be distinctively defined; for example, operation during major outages of facility systems for maintenance or operation of multiple segmented areas of the facility?
  - Is there sufficient identification of the safety limits, limiting control settings, and limiting conditions for operation to support safe operation of the facility?
  - Are the requirements relating to test, calibration, or inspection sufficient to assure that the necessary operability and quality of SSCs is maintained, that facility operation is within safety limits, and that limiting control settings and limiting conditions for operation are met?
  - Have passive SSCs been appropriately designated as design features and adequate in-service inspections included?
  - Are the important attributes of the design features that are credited in the hazard and accident analyses identified?
  - Are the bases deriving safety limits, limiting control settings, limiting conditions for operation, surveillance requirements, and administrative controls provided and technically accurate?
  - Are the facility design aspects necessary to implement the identified surveillance requirements (e.g., instrumentation, equipment access) adequately identified?
  - Do the TSR bases identify specific information from the DSA used in the derivation of individual TSRs including operating conditions that limit accident initial conditions, relevant parameters of safety class or safety significant SSCs, instrumentation, operator actions, assumed limits, and design features?
  - Do the TSR bases identify the requirements relevant to the safety basis that have been selected by the facility?

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

19. 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)

20. 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)
21. 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?

#### **Safety Management Programs (Chapters 6-17)**

22. 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, define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection. (10CFR830 Section 830.204.b.5)
- Are the major programs needed to provide programmatic safety management identified?
  - Are the basic provisions of identified programs noted and references to facility or site program documentation provided?
  - Are specific aspects of safety management programs identified in the hazard and accident analysis included in the discussion of the programs in the DSA?

- Do the descriptions of the major program elements include brief abstracts of referenced documentation with enough of the salient facts to provide an understanding of the referenced documentation and its relation to the chapter?
  - Do the program descriptions clearly include key elements identified in the Chapter 3 hazard analysis?
  - Are cross-references to material in other chapters accurate and is the referenced material adequate to address the subject of the chapter under review?
23. 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, with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a criticality safety program that: (1) Ensures that operations with fissionable material remain subcritical under all normal and credible abnormal conditions, (2) Identifies applicable nuclear criticality safety standards, and (3) Describes how the program meets applicable nuclear criticality safety standards. (10CFR830 Section 830.204.b.6)
- Are fissile materials and their locations identified? Is the fissile material form (chemical/physical, isotopic content, concentration, densities, etc.) and maximum quantities involved identified? Is this information summarized in the hazard identification discussion in Chapter 3?
  - Are the criticality safety evaluations covered by the criticality events identified in the hazard analysis?
  - Have controls necessary to prevent or mitigate criticality accidents been considered for inclusion in the DSA and TSR?
  - Are the engineered controls and their design basis and limits identified?
  - Is the application of the Double Contingency Principle clearly described?
  - Do the equipment designs and operations ensure criticality safety under normal, abnormal and accident conditions?
  - Does the criticality safety program have a mechanism to review all changes or potential changes to nuclear criticality safety controls for capture by the revisions and updates to the DSA and TSR?

### **Federal DSA/TSR Review and Approval**

1. As part of the approval process, DOE will review the content and quality of the safety basis documentation. DOE intends to use the approval process to assess the adequacy of a safety basis developed by a contractor to ensure that workers, the public, and the environment are provided reasonable assurance of adequate protection from identified hazards. (10 CFR 830 Appendix A, section E.2)
2. Because DOE has ultimate responsibility for the safety of its facilities, DOE will review each DSA to determine whether the rigor and detail of the DSAs are appropriate for the complexity and hazards expected at the nuclear facility. In particular, DOE will evaluate the DSA by considering the extent to which the DSA (1) satisfies the provisions of the methodology used to prepare the DSA, and (2) adequately addresses the criteria set forth in 10 CFR 830.204(b). DOE will prepare a safety evaluation report (SER) to document the results of its review of the DSA. A DSA must contain any conditions or changes required by DOE. (10 CFR 830 Appendix A, Section F.3)

3. DOE will examine and approve the TSRs as part of preparing the SER and reviewing updates to the safety basis. (10 CFR 830 Appendix A, Section G.5)
4. Approval of DSAs, TSRs, and unreviewed safety question procedures required pursuant to 10 C.F.R. part 830, subpart B, Safety Basis Requirements, must not be further delegated below the most senior-level program officer or deputy at a field element office unless concurrence is obtained from the applicable Central Technical Authority (CTA). (DOE Order 450.2, Appendix A, Section 2.a.(1)(a))
5. Delegations must only be made where the candidate's organization possesses, or has access to, sufficient staff (for example, a Service Center) with the necessary qualifications, experience, and expertise to support the candidate for the authorities being delegated. (DOE Order 450.2, Appendix A, Section 2.a.2)
  - Is the safety basis approval authority delegation document current?
  - Does the delegation of safety basis approval authority to the site office adequately reflect the conditions and assumptions for the delegation?
  - Is authority for approving base DSAs and major revisions to DSA differentiated from authority for DSA changes, DSA annual updates, and TSR change control?
  - Are DOE personnel assigned responsibility for assessing DSA annual updates and DSA and TSR change control?
  - Are procedures and mechanisms in place to address and implement site office responsibilities for review and approval of DSA updates?
  - Are DOE personnel assigned responsibility to review and approve the updated DSAs prepared by the contractors?
  - Are the DOE personnel assigned responsibility to review DSA documents and changes qualified as nuclear safety specialists (i.e. DOE-STD-1183) and qualified for the specific facility represented in the DSA change?
  - Have appropriate criteria been developed and implemented for evaluating the classification of nuclear SSCs?
  - Have DOE personnel developed and implemented a review plan and evaluation criteria to ensure that the analysis provided by the contractor:
    - Properly covers the hazards associated with the work?
    - Is consistent with the Integrated Safety Management System Description?
    - Adequately traces the hazards identified to the control selected to address the hazard?
    - Identifies adequate safety functions, performance characteristics, and functional requirements to ensure an adequate degree of safety?
  - Do SERs meet the guidance in DOE-STD-1104 and establish an adequate basis for the approval of the DSA update?
  - Have issues and comments identified during the review been adequately resolved or included in Conditions of Approval?
  - Has DOE verified that the contractor has adequate methods to track and implement Conditions of Approval?
  - Have SERs been submitted to the appropriate approval authority (in accordance with a current delegation)?
  - Are federal personnel assigned responsibility to verify the adequate development of Preliminary Documented Safety Analyses (PDSAs) for new nuclear facilities or major modifications to nuclear facilities?

## ***APPROACH***

### **Record Review:**

- Revised DSA and associated hazard and accident analysis.
- Revised TSRs.
- DOE direction and guidance documents.
- Technical support documents, including calculations and engineering analyses.
- DOE plans and records of reviews for the DSA submittals.
- DOE review comment record forms, SERs, and associated documentation.
- Procedures and guidance for maintenance and update of the DSA and associated elements.
- 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, P&IDs, 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.

### **Interviews:**

- Safety analysts
- System and design engineers
- Operations personnel
- DSA and TSR review coordinators
- DOE nuclear safety personnel
- DOE delegated approval authority, safety basis review managers, safety basis review team members, and facility representatives (involved in the safety basis reviews)

### **Observations:**

- Facility and building walkdowns and reviews
- Walk down the nuclear facility and selected safety SSCs to gain understanding of system dependencies and potential vulnerabilities to adverse conditions.
- Technical review discussions
- Comment resolution meetings, if applicable