

	Number: EA CRAD 31-35 Revision: 0 Effective Date: November 22, 2019
<p align="center"> Hazard Category 3 Nuclear Facility Documented Safety Analysis and Technical Safety Requirements Criteria and Review Approach Document </p>		
Authorization and Approval	 Kevin G. Kilp Deputy Director, Office of Environment, Safety and Health Assessments (EA-30) Date: November 22, 2019	 Lead, James O. Low Nuclear Engineer Date: November 22, 2019

1.0 PURPOSE

The mission of the U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments (EA-30) is to assess the effectiveness of safety and emergency management systems and practices used by line and contractor organizations and to provide clear, concise, rigorous, and independent evaluation reports of performance in protecting workers, the public, and the environment from the hazards associated with DOE activities.

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

The CRADs are available to DOE line and contractor assessment personnel to aid them in developing effective DOE oversight, contractor self-assessment, and corrective action processes. The current EA CRADs are available at <http://www.energy.gov/ea/criteria-and-review-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.

4.0 CRITERIA AND REVIEW APPROACH

This CRAD focuses on assessing the adequacy of hazard category 3 documented safety analysis (DSA) and technical safety requirements (TSR) to fully comply with the requirements of 10 CFR 830, “*Nuclear Safety Management*,” using DOE-STD-1228-2019 *Preparation of Documented Safety Analysis for Hazard Category 3 DOE Nuclear Facilities*. Concurrently, the CRAD also focuses on assessing the adequacy of the Federal DSA/TSR review and approval in compliance with DOE-STD-1104-2016 *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*. The following criteria and lines of inquiry are independent sections to be used in any combination based on the need of the specific assessment.

DSA Development

OBJECTIVES

SB.1: In establishing the safety basis for a hazard category 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)

CRITERIA

1. Hazard Identification: The DSA for a hazard category 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) [DOE-1228-2019§3.1.1]

- Does the methodology used for hazard identification ensure comprehensive identification of the hazards associated with the full scope of facility processes, associated operations (such as handling of fissionable materials and hazardous waste) and work activities to be covered by the DSA? [1228§3.1.1.1]
- Does the methodology include characterization of hazardous materials (radiological and non-radiological) and energy sources, in terms of quantity, form, and location? [1228§3.1.1.1]

- Are bounding inventory values of radiological or hazardous materials used consistent with the maximum quantities of material that are stored and used in facility processes? [1228§3.1.1.2]
- Is a basis provided for any identified hazards that are excluded (such as hazards covered under 10 CFR 851) from further evaluation? [1228§3.1.1.3]
- Are standard industrial hazards included in the hazard identification if they can be an accident initiator, a contributor to a significant uncontrolled release of radioactive or other hazardous material or considered a unique worker hazard such as explosive energy?
- Has Appendix A.1 of DOE-STD-3009-2014 or Appendix A.2.3 of DOE-STD-1228-2019 been used to guide the screening of standard industrial hazards and chemicals? [1228§3.1.1.3&4]
- Has DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, Change Notice 1, September 1997 been applied to determine the facility hazard category?
- If the final hazard categorization was dependent on key assumptions to preclude criticality, have these analytical assumptions been identified in the DSA and protected? [1228§3.2.1] Has a bounding estimate of the unmitigated radiological consequences to the public (using the guidance in Appendix A.2.1) been performed to confirm the applicability of DOE-STD-1228-2019? [1228§3.1.2.2]
- Is sufficient justification provided in terms of independence if segmentation is relied upon in the hazard categorization? [1228§3.2.1]

2. Hazard Evaluation: a) The DSA for a hazard category 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)

b) The hazard evaluation shall provide (a) an assessment of the facility hazards associated with the full scope of planned operations covered by the DSA, and (b) the identification of controls that can prevent or mitigate these hazards or hazardous conditions. (DOE-STD-1228-2019, Section 3.1.3)

- Are normal operations (e.g., startup, facility activities, shutdown, and testing and maintenance configurations), as well as abnormal and accident conditions, analyzed? [1228§3.1.3.1]
- Does the hazard evaluation address natural phenomena and man-made external events that can affect the facility? [1228§3.1.3.1]
- For complex operations, is the rationale supporting the selected hazard evaluation technique(s) discussed? [1228§3.1.3.2]
- For each initiating event, has an unmitigated hazard scenario, assuming the absence of preventive and mitigative controls, been analyzed? [1228§3.1.3.3]
- Have qualitative or semi-quantitative techniques been used to estimate the likelihood and consequences of unmitigated hazard scenarios? [3009§3.1.3.3]
- Do hazard scenario consequence estimates address potential effects on facility workers, co-located workers, and the public consistent with the consequence levels in Tables 1 and 2 of DOE-STD-3009-2014? [1228§3.1.3.3]
- For each of the unmitigated hazard scenarios, have the controls; structures, systems and components (SSCs), administrative and/or programmatic that can prevent or mitigate the hazard scenario been identified? [1228§3.1.3.5]
- If risk ranking/binning was used to support the selection of hazard controls, was the methodology described in DOE-STD-3009-2014§A.4 and 1228§A.3.1 used? [1228§3.1.3.6]
- Are scoping calculations based on technically justified parameters and underlying assumptions such that the overall consequence evaluation is conservative [1228§3.1.3.7]
- Has a default atmospheric dispersion coefficient value of 3.5×10^{-3} (sec/m³) been used for the 100-meter receptor location? [1228§3.1.3.8]

- If an alternate value for atmospheric dispersion coefficient has been used, has an adequate technical basis been provided? [1228§3.1.3.8]
- Has a mitigated hazard evaluation been performed to determine the effectiveness of safety significant (SS) controls by estimating hazard scenario likelihood with preventative controls and consequences with mitigative controls? [1228§3.1.3.9]

3. Hazard Controls Selection: a) The DSA for a hazard category 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 (10 CFR 830 Section 830.204.b.4)

b) Defense-in-depth 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 420.1C, Chapter I, Section 3.b.2.)

c) SS control designation shall be made on the basis of the control's contribution to: (1) protection of facility workers from fatality, serious injury, or significant radiological or chemical exposure, (2) protection of co-located workers from hazardous chemicals and radioactive materials, (3) protection of the public from release of hazardous chemicals, and (4) defense-in-depth. (DOE-STD-1228-2019, Section 3.2.3)

- Have preventative or mitigative controls been selected using a judgement-based process considering a hierarchy of controls that gives preference to: (1) passive engineered safety features over active features; (2) engineered safety features over administrative controls or SAC's; and (3) preventative over mitigative controls. [1228§3.2]
- Have initial conditions and assumptions of the unmitigated hazard evaluation been reviewed to determine if controls are necessary to maintain the validity of the evaluation? [1228§3.1.3.4, 3.2.1]
- Have assumed passive SSCs which prevent significant consequences been classified as SS? [1228§3.2.1]
- Has the facility's approach to defense-in-depth for the protection of workers, the public, and environment from release of radioactive or other hazardous material been described using the guidance in Appendix A.3.3? [1228§3.2.2]
- Has an unmitigated dose of 100 rem to a worker located at 100 meters from the point of release been used as the threshold for selection of SS controls? [1228§3.2.3.2]
- Is a technical basis provided for the acceptance of mitigated co-located worker (CLW) dose above 100 rem, including why other controls were not selected to reduce consequences below 100 rem? [1228§3.2.3.2]
- Has an unmitigated chemical consequence exceeding PAC-3 to a worker located at 100 meters from the point of release been used as the threshold for selection of SS controls? [1228§3.2.3.2]
- Has an unmitigated chemical consequence exceeding PAC-2 to the public from the point of release been used as the threshold for selection of SS controls? [1228§3.2.3.3]
- Is there a technical basis for not following the preferred DOE hierarchy of controls (e.g., a SAC is selected over an available SSC)? [1228§3.2.4]
- For new facilities or major modifications, are support SSCs designated as SS SSCs if their failure prevents safety SSCs or SACs from performing their safety functions? [1228§3.2.5]
- For new facilities or major modifications, are SSCs whose failure would result in losing the ability to complete an action required by a SAC designated as SS? [1228§3.2.5]
- For existing facilities, are support SSCs designated at the same SS classification as the safety controls they support or are compensatory measures established to assure that the supported SS SSC can perform its safety function when called upon? [1228§3.2.5]
- For existing facilities are SSCs whose failure would result in losing the ability to complete an action required by a SAC designated as SS or are compensatory measures established to assure that the supported SAC can perform its safety function when called upon? [1228§3.2.5]

4. Safety Structures, Systems, and Components: a) The DSA for a hazard category 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. (10 CFR 830 Section 830.204.b.4)

b) Safety analyses must be used to establish: (a) the identity and functions of safety SSCs, (b) the significance to safety of functions performed by safety SSCs, and (c) the SACs needed to fulfill safety functions. (DOE O 420.1C, Chapter I, Section 3.a. (2))

- Does the DSA satisfactorily document the basis for determining the safety SSCs [If any] and their required functions?
- Are 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?
- Do the safety functions state the objective of the SSC in a given accident scenario?
- Are the SSC safety functions associated with specific accident(s) or general rationale (such as to protect the initial conditions)?
- Is the required functional classification of a safety SSCs 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?
- Are support SSCs whose failure could result in the safety SSC losing its ability to perform its safety function, if any, identified?
- 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 functional requirements and system evaluations for any needed support SSCs included?
- Are the design and functional requirements for safety SSCs (and any needed support 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 SSC's 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 an engineering evaluation performed to determine the capability of the SS SSCs and SACs to meet or exceed the performance criteria? [1228§3.2.6]
- Does the system evaluation identify the performance criteria necessary to ensure that the identified functional requirements will be met or identify noted deficiencies and any compensatory measures to ensure the safety functions of the controls? [1228§3.2.6]?
- For existing facilities, does the evaluation include discussion of the relevant SSC design capabilities, including the code of record (to the extent known), and augment as needed with other performance tests, calculations or reliability information that is available? [1228§3.2.6]
- Are the general requirements for safety SSCs (e.g., conservative design features, 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?
- Does the suite of safety controls provide multiple layers of protection to prevent or mitigate the unintended release of radioactive materials?

5. Specific Administrative Controls: a) 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)

- Do the descriptions of the SACs contain sufficient detail to understand their safety functions and the relationship to the safety analysis?
- Does the DSA provide the safety requirements and functions of selected SACs?
- Does the DSA satisfactorily document the basis for determining the assigned functions are appropriately assigned as SACs?
- Does the hazard analysis establish the functions of SACs and their significance to safety?
- Are the specific accidents or general rationale associated with the SAC safety functions identified?
- Does the DSA identify the appropriate performance criteria necessary to provide reasonable assurance that selected SAC functional requirements will be met?
- Are safety functions for SACs defined with clarity and consistent with the bases derived in the hazard and accident analyses?
- 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?
- Where SACs rely on supporting SSCs, the functional requirements and performance evaluation of the supporting SSCs are included in Chapter 4?
- Do the functional requirements and evaluations of SAC provisions provide evidence that the required safety functions can be performed when called upon?
- Is the SAC formulation supported by an adequately prepared job task analysis?
- If needed, have formal engineering calculations been prepared to ensure plant operators have adequate time and resources to carry out required tasks?
- If a SAC relies on operator actions to perform its safety function, has a human factors analysis been performed as part of the SAC formulation?
- Have the consequences of incorrect implementation and measures to prevent failure been factored into the SAC formulation?
- 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 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 material-at-risk SAC follow the guidance of DOE-STD-1228-2019§A.3.2?

6. Safety Management Programs: a) The DSA for a hazard category 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. (10 CFR 830 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?

Technical Safety Requirements

OBJECTIVE

SB.2: A contractor responsible for a hazard category 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 205.a.1&2)

CRITERIA

7. Technical Safety Requirements Content: a) A contractor responsible for a hazard category 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 205.a.1&2)

b) TSRs establish limits, controls, and related actions necessary for the safe operation of a nuclear facility. (10 CFR 830 Appendix A, Section G.4)

c) 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)

d) Table 4 sets forth DOE's expectations concerning acceptable TSRs. (10 CFR 830 Appendix A, Section G.6)

- Does Section 1 include a list of defined terms that contain the terms used in the TSR document that require clarification of the intent of their use? Are the definitions clear and consistent with standard usage and the intended use of the terms?
- Does Section 1 include the standard use and application explanations for TSR devices such as: Logical Connectors, Completion Time, Frequency Notation, 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 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 limiting conditions for operation are met?
- Have passive SSCs been designated as design features, when appropriate, 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 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 SS SSCs, instrumentation, operator actions, assumed limits, and design features?

Federal DSA/TSR Review and Approval

OBJECTIVE

SB.3: With respect to a hazard category 3 new DOE nuclear facility or a major modification to a hazard category 3 DOE nuclear facility, a contractor may not begin operation of the facility or modification prior to the issuance of a safety evaluation report in which DOE approves the safety basis for the facility or modification. (10 CFR 830 Section 207.d)

CRITERIA

8. Federal Safety Evaluation Report: a) 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)

b) 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 DSA 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)

c) DOE will examine and approve the TSRs as part of preparing the safety evaluation report and reviewing updates to the safety basis. (10 CFR 830 Appendix A, Section G.5)

- Under the circumstances above, did the DOE safety basis review team (SBRT) verify that the information in the DSA is consistent with the requirements of DOE-STD-1228-2019?
- Are procedures and processes in place to address and implement site office responsibilities for review and approval of DSA? [1104§3.1]
- Are DOE personnel assigned responsibility to oversee the adequate development of DSA for new nuclear facilities or major modifications respectively?

- Are SBRT personnel assigned responsibility to review the DSAs prepared by the contractors? [1104§3.1]
- Is at least one of the SBRT personnel assigned responsibility to review DSA documents and changes qualified as a nuclear safety specialist (i.e., DOE-STD-1183) and qualified for the specific facility represented in the DSA change? [1104§3.3]
- If SBRT identified conditions of approval (COAs), were defined closure dates or milestones identified? [1104§4.10]
- Have appropriate criteria been developed and implemented for evaluating the classification of SSCs?
- Have SBRT personnel developed and implemented a review plan and evaluation criteria to ensure that the analysis provided by the contractor: [1104§3.3]
 - 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 SSC safety functions, performance characteristics, and functional requirements to ensure an adequate degree of safety?
- Does the SER meet the requirements in DOE-STD-1104 and establish an adequate basis for the approval of the DSA?
- Does the SER document:
 - The conduct of an appropriate review of the safety basis document?
 - The bases for approving these documents (see Sections 4, 5, and 6 of DOE-STD-1104 for approval bases for different safety basis documents)?
 - Any conditions of approval? [1104§7.0]
- Have issues and comments identified during the review been adequately resolved or included in COAs?

REVIEW APPROACH

Record Review:

- DSA and associated hazard and accident analysis
- 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 development of new or upgraded DSA, TSR and associated documents

Interviews:

- DOE Nuclear Safety personnel
- DOE personnel responsible for coordinating DSA and TSR reviews for nuclear operations
- DOE delegated approval authority
- DOE safety basis review managers
- DOE Safety Basis Review Team members
- DOE System Safety Oversight Engineer(s)
- Contractor Nuclear Safety Manager
- Contractor Nuclear Safety Analysts
- Contractor Cognizant System Engineer(s)

Observations:

- Comment resolution meetings, if applicable
- Field walk-down of safety controls