

	Number: EA CRAD 31-07 Revision: 1 Effective Date: November 13, 2019
<b>New or Upgraded Nuclear Facility</b> <b>Documented Safety Analysis and Technical Safety Requirements</b> <b>Criteria and Review Approach Document</b>		
Authorization and Approval	 Kevin G Kilp Deputy Director, Office of Nuclear Safety and Environmental Assessments (EA-31)  Date: November 7, 2019	 Lead, James O. Low Nuclear Engineer  Date: November 7, 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 new or upgraded nuclear facility 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-3009-2014 *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*. 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.

### ***OBJECTIVES***

**SB.1:** 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.2:** When the DOE-STD-3009 methodology is used to satisfy 10 CFR Part 830, Nuclear Safety Management, safety basis requirements, DOE-STD-3009-2014, Preparation of Nonreactor Nuclear Facility Documented Safety Analysis, must be used for new DOE non-reactor nuclear facilities and major modifications to existing DOE non-reactor nuclear facilities. (DOE Order 420.1C change 1, CRD)

### **Criteria:**

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

**1. Hazard Identification:** 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) [DOE-STD-3009-2014§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?
- Does the methodology include characterization of hazardous materials (radiological and non-radiological) and energy sources, in terms of quantity, form, and location?
- 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?
- Is a basis provided for any identified hazards that are excluded (such as hazards covered under 10 CFR 851) from further evaluation?
- 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 of DOE-STD-3009-2014 been used to guide the screening of standard industrial hazards and chemicals?
- 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?
- Is sufficient justification provided in terms of independence if segmentation is relied upon in the hazard categorization?

**2. Hazard Evaluation:** a) 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)

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-3009-2014, 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? [3009§3.1.3.1]
  - In addition to the process-related hazards identified during the hazard identification process, does the hazard evaluation address natural phenomena and man-made external events that can affect the facility? [3009§3.1.3.1]
  - Is the rationale supporting the selected hazard evaluation technique(s) discussed and justified? [3009§3.1.3.1]
  - For each initiating event, has an unmitigated hazard scenario, assuming the absence of preventive and mitigative controls, been analyzed? [3009§3.1.3.1]
  - Have qualitative or semi-quantitative techniques been used to estimate the likelihood and consequences of unmitigated hazard scenarios? [3009§3.1.3.1]
  - Do hazard scenario consequence estimates address potential effects on facility workers, co-located workers, and the public (maximally exposed offsite individuals [MOIs]) consistent with the consequence levels in Table 1 of DOE-STD-3009-2014? [3009§3.1.3.1]
  - Have consequences for determining the need for safety significant (SS) controls based on co-located worker consequences or chemical consequences to the MOI been quantitatively evaluated? [3009§3.1.3.3]
- (Note: If not, see the Evaluation Basis Accidents (EBAs))
- Are hazard scenario likelihood estimates consistent with the classification bins in Table 2 of DOE-STD-3009-2014? [3009§3.1.3.1]

- If risk ranking or risk binning is used, have the consequence and likelihood thresholds in Tables 1 and 2 of DOE-STD-3009-2014 been used? [3009§3.1.3.1]
- Are consequence determinations for co-located workers used in the hazard evaluation supported by an adequate technical basis, such as scoping calculations? [3009§3.1.3.1]
- If probabilistic risk assessment has been used to assign qualitative likelihood estimates, has the process described by DOE-STD-1628-2013 been used and the criteria in Tables 1 and 2 retained?
- 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? [3009§3.1.3.1]
- Has a mitigated hazard evaluation been performed to determine the effectiveness of SS controls (following the preferred hierarchy as described in Section 3.3 of the standard) by estimating hazard scenario likelihood with preventive controls and consequences with mitigative controls? [3009§3.1.3.1]
- Is the mitigated analysis for hazard scenarios included directly in hazard evaluation tables or included as a summary evaluation in DSA? [3009§3.1.3.1]
- Does the analysis include SS controls for hazard scenarios having high estimated chemical consequences to the public, or high radiological or chemical consequences to workers (as defined by Table 1 of the standard)? [3009§3.1.3.1]
- Is the information on the mitigated analyses, along with safety functions for the SS controls, included in the hazard evaluation (or determined as part of the accident analysis (see Section 3.2))? [3009§3.1.3.1]
- Does the DSA hazard evaluation also examine the potential for large-scale environmental contamination and, if necessary, identify preventive and mitigative controls to protect the environment? [3009§3.1.3.1]
- Does the hazard evaluation include events where consequences from criticality itself or subsequent impact to hazardous material exceed the high radiological consequence thresholds for either the co-located workers or the MOI in Table 1, unless it has been determined that an unmitigated criticality accident is not credible? [3009§3.1.3.2]
- Have situations where an active engineered control(s) is required to ensure sub-criticality by the Nuclear Criticality Safety (NCS) analysis been included? [3009§3.1.3.2]
- Does the hazard analysis present a systematic, comprehensive analysis of hazardous materials and energy sources, natural phenomena hazards, and sources of external hazards, such as nearby airports, railroads, or utilities such as natural gas lines? [3009§3.1.1]
- Is the hazard analysis based on the currently approved scope of work at the facility? [3009§3.1.1]
- Are the results of hazards evaluation summarized to identify significant defense-in-depth and worker safety features, hazard controls, including candidate safety structures, systems or components (SSCs), specific administrative controls (SACs), and key elements of safety management programs?
- Does the hazard analysis identify preventive and mitigative features for the spectrum of events examined using a proper hierarchy?
- Is the Fire Hazards Analysis current and are the results integrated into the hazard analysis?
- If the NCS program requires a criticality accident alarm system, is the criticality accident alarm system discussed in the hazard evaluation?

**3. Design/Evaluation Basis Accident Selection:** Two types of EBAs shall be defined for further analysis: representative and unique. (DOE-STD-3009-2014, Section 3.2.1)

- Has at least one bounding accident from each of the major types determined from the hazard evaluation that have the potential to challenge the EG (fire, explosion, spill, etc.) been selected?

- If consequences for determining the need for SS controls based on co-located worker consequences or chemical consequences to the MOI were not quantitatively evaluated in the hazard evaluation, are the appropriate scenarios included in the EBAs?
- Have representative EBAs been selected such that: the control(s) applicable to the EBA are similar and will perform the same function as the controls of the represented hazard scenarios; and the accident environment associated with the EBA envelopes the environment expected from the represented hazard scenarios?
- Does the hazard analysis identify dominant accident scenarios through ranking or an equivalent structure?
- Have all credible hazard scenarios with the potential to challenge the EG been considered as candidates for DBA/EBA accident analysis including: (1) plausible operational events, (2) natural phenomena initiators of magnitude required by DOE O 420.1C (or applicable successor documents), or (3) external man-made accidents with a likelihood less than 10<sup>-6</sup>/year conservatively calculated?
- Do potential natural phenomena hazards (NPH) impacts consider the cumulative effects of releases from NPH-induced structural and equipment failures (e.g., impacts, spills, fires, explosions)?
- When probabilistic risk assessment (PRA) results are used, do the results include an integrated assessment of accident probability and consequences of the accident event to establish the event's risk significance?
- When PRA results are used, are the key assumptions and initial conditions identified and protected (see Section 3.2.2 of the standard)?
- When quantitative estimates are used, are accident likelihood calculations provided to support the analytical and decision-making processes?

**4. Accident Analysis-Unmitigated and Mitigated Consequences Analyses:** a) An unmitigated consequence analysis shall be performed for plausible accident scenarios, NPH events, and external events. (DOE-STD-3009-2014, Section 3.2.2)

b) A mitigated analysis shall be performed to determine the effectiveness of SS and SC controls to protect the workers and the public. (DOE-STD-3009-2014, Section 3.2.3)

- Have the initial conditions and assumptions for the analysis been documented and evaluated to determine if controls are needed to maintain the validity of the evaluation? [3009§3.2.2]
- Are all pertinent assumptions (e.g., hazardous material inventory, airborne release fraction, and damage ratio) established?
- Was an unmitigated analysis performed? [3009§3.2.2]
- 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?
- Does the accident analysis clearly substantiate the findings and delineations of 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?
- Has the presence of any passive SSC, which prevents significant consequences, been assumed? If so, has it been classified as either SS or SC? [3009§3.2.2]
- Have any of the following prohibited conditions been assumed to be available for unmitigated analysis of plausible accident scenarios defined in Section 3.2.1:

- Active safety controls, such as ventilation filtration systems in the case of a spill or fire suppression in the case of a fire?
- Passive safety controls that produce a leak path reduction in source term, such as building filtration?
- Operator intervention actions that may abort the progression of the event (assume the event occurs with no operator intervention)?
- ACs (other than material at risk (MAR) controls) or safety management programs in the unmitigated analysis? [3009§3.2.2]
- Are the consequences of postulated accidents appropriately compared with the evaluation guideline and evaluated to classify safety SSCs and SACs?
  - Where preventive controls are credited as SS or SC, has the DSA evaluated the effectiveness of the controls to either eliminate the hazard or terminate the accident and prevent a release of radioactive or other hazardous materials? [3009§3.2.3]
- Does the analysis demonstrate that SC mitigative SSCs and/or SACs reduce consequences below the EG and SC (if identified) and SS mitigative SSCs and/or SACs reduce co-located worker consequences below 100 rem? [3009§3.2.3]

**5. Accident Analysis – Consequence Calculations:** Calculations shall be made based on technically justified input parameters and underlying assumptions such that the overall consequence calculation is conservative. (DOE-STD-3009-2014, Section 3.2.4)

- Are the MAR values used in hazard and accident analysis consistent with the values noted in hazard identification/evaluation?
- Are the MAR values bounding with respect to each accident being evaluated?
- Does the DSA address the use of Type B containers for material storage and the exclusion of such material from the source term for particular accident scenarios? If so, have the containers been shown to perform their safety functions under accident conditions?
- Has a DR of 1.0 been used, except when there is an applicable standard or technical basis for a different value?
- Does the analysis use airborne release fraction and Respirable fraction bounding estimates from DOE-HDBK-3010, except when a different value is provided in an applicable standard or otherwise technically justified?
- For the unmitigated release calculation, is the leak path factor set to 1?
- For mitigated analysis, are analytical tools used in calculating the LPF appropriate to the physical conditions being modeled, including the use of input parameters, such that the overall LPF would be conservative? [preceding LOIs-3009§3.2.4.1]
- Did the evaluation of the atmospheric dispersion and the resulting  $\chi/Q$  use one of the options from the Standard?
- Were 5 years of representative, recent meteorological data used as input to the dispersion model? If a smaller data set was used, was it properly justified?
- In making comparisons to the Evaluation Guide, is the comparison point the location of the hypothetical MOI?
- Are the  $\chi/Q$  values determined using a method consistent with Reg. Guide 1.145; either directionally independent or directionally dependent (95<sup>th</sup> percentile for directionally independent and 99.5<sup>th</sup> percentile for directionally dependent)? Does alternative  $\chi/Q$  values conform to either Option 2 or 3 of the standard §3.2.4.2?
- Have the following parameters been used (to ensure conservative calculation of offsite doses):
  - Non-buoyant, ground level, point source release?
  - Plume centerline concentrations for calculation of dose consequences?
  - Rural dispersion coefficients?

- A deposition velocity of 0.1 cm/sec for unfiltered release of particles (1-10  $\mu\text{m}$  Aerodynamic Equivalent Diameter), 0.01 cm/sec for filtered particles, or 0 cm/sec for tritium/noble gases?
- A surface roughness of 3 cm?
- A minimum wind speed of 1 m/s?
- Plume meander may be used, consistent with the accident release duration and the appropriate code guidance?
- Building wake factors should not be credited in the plume dispersion, outside of those already incorporated into plume meander?
- If site-specific methods have been used, was appropriateness of the model to the site-specific situation justified, the overall result demonstrated conservative, and the approach submitted to the Safety Basis Approval Authority for approval prior to use? [preceding LOIs-3009§3.2.4.2]
- Did the analysis use a  $\chi/Q$  value of  $3.5 \times 10^{-3} \text{ sec/m}^3$  for the ground level release at 100 meters? [preceding LOIs-3009§3.2.4.2]
- Are dose coefficients consistent with International Commission on Radiological Protection Publication 68, *Dose Coefficients for Intakes of Radionuclides by Workers*, and Publication 72, *Age-dependent Doses to Members of the Public from Intake of Radionuclides*, for adults?
- If neither a radiological dispersion analysis nor a DOE “Toolbox code” is used for the chemical dispersion analysis, does the modeling protocol address the appropriateness of the model to the site-specific situation (including source term characterization), show that the overall result (i.e., chemical consequence) is conservative, and be submitted to the appropriate DOE Safety Basis Approval Authority for approval prior to use?
- When an alternate  $\chi/Q$  value is used, does the DSA provide a technical basis supporting the need for the alternate value and the value selected? [preceding LOIs-3009§3.2.4.3]

**6. Hazard Controls – Development (Chapter 3):** a) 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 (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) If the unmitigated release consequence for a DBA/EBA exceeds the EG, SC controls shall be applied to prevent the accident or mitigate the consequences to below the EG. (DOE-STD-3009-2014, Section 3.3.1)

d) SS control designation shall be made on the basis of the control’s contribution to: (1) defense-in-depth; (2) protection of the public from release of hazardous chemicals; (3) protection of co-located workers from hazardous chemicals and radioactive materials; and (4) protection of in-facility workers from fatality, serious injury, or significant radiological or chemical exposure. (DOE-STD-3009-2014, Section 3.3.2)

- Have assumptions been protected at a level commensurate with their importance? [3009§3.2.2]
- If the presence of any passive SSC was assumed to prevent significant consequences, has it been classified as either SS or SC? [3009§3.2.2]
- When the hierarchy of controls is not used for situations requiring SC/SS controls (e.g., a SAC is selected over an available SSC), does the DSA provide a technical basis that supports the controls selected? [3009§3.3]
- Does the identification of hazard controls incorporate a defense-in-depth approach that builds layers of defense against release of radioactive or other hazardous materials so that no one layer by itself, no matter how effective, is completely relied upon?
- Is the facility’s approach to defense-in-depth for protection of workers and the public from the release of radioactive or other hazardous material described?

- For existing facilities, are support SSCs designated at the same classification (SC or SS) as the safety controls they support (or compensatory measures established to assure that the supported safety SSC can perform its safety function when called upon)?
- Are SSCs whose failure would result in losing the ability to complete an action required by a SAC identified and designated as SC or SS based on the SAC safety function (or justification provided if not so designated)?
- For DBAs/EBAs whose unmitigated release consequence exceed the EG, have SC controls been applied to prevent the accident or mitigate the consequences to below the EG?
- In circumstances where no viable control strategy exists in an existing facility to prevent or mitigate the consequence of one or more of the accident scenarios from exceeding the EG, is the following information provided in the DSA or an attachment:
  - Identification of the accidents that cannot be mitigated or prevented, including the likelihood of the event(s) and the mitigated consequences associated with the event(s)?
  - A discussion of the credited controls, including their reliability and adequacy, and an analysis of the expected likelihood and mitigated offsite consequence estimates of the associated accident(s)?
  - A discussion of the available controls that could reduce the likelihood and/or consequences of the associated accident(s), including their potential failure modes, their potential impact on accident mitigation, any relevant cost/benefit results, and the reasons why they are not selected as credited controls to reduce the consequences to below the EG?
  - A discussion of any planned operational or safety improvements, including potential facility modifications, reductions in MAR, and/or additional compensatory measures, and associated schedules, to further reduce the likelihood and/or mitigate consequences of an accident?
  - A qualitative or semi-quantitative comparison of the facility risk from the identified scenarios and total facility risk? [preceding LOIs-3009§3.3.1]
- Are controls that provide a major contribution to defense-in-depth designated as SS?
- When estimated consequences to the public from chemical releases (based on a peak 15 minute time-weighted average air concentration, measured at the receptor location) exceed AEGL-2, ERPG-2, and/or TEEL-2, have SS controls been designated for their protection?
- For radiation hazards, has a conservatively calculated unmitigated dose of 100 rem TED to a receptor located at 100 meters from the point of release been used as the threshold for designation of SS controls?
- Is the SS designation for protection of co-located workers from chemical releases based on a peak 15-minute time-weighted average air concentration at the receptor location that exceeds PAC-3?
- Have SS controls (SSCs or SACs) been selected for cases where a fatality, serious injury, or significant radiological or chemical exposure to a facility worker may occur? [preceding LOIs-3009§3.3.2]
- Are explicit criticality controls required as a result of hazard evaluation criteria established in Section 3.1.3.2 documented in the DSA and classified in accordance with requirements of Sections 3.3.1 and 3.3.2? [3009§3.3.4]
- Is the logic behind assessing the results in terms of safety-significant SSCs, SACs, and designation of technical safety requirements (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?
- 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?



**7. Hazard Controls – Design (Chapter 3):** A system evaluation supporting the adequacy of safety SSCs and SACs, required to be included in the Preliminary Documented Safety Analyses (PDSA) in accordance with DOE-STD-1189-2008, shall be incorporated into the DSA using guidance provided in Appendix B of this Standard. (DOE-STD-3009-2014, Section 3.4)

- For existing facilities, was an engineering evaluation conducted to assess the performance capabilities of safety SSCs?
- If performance criteria are not met, does the evaluation identify noted deficiencies and any compensatory measures necessary to ensure the safety functions of the SSCs?
- Does the engineering evaluation address the relevant design capabilities of safety SSCs using one of the following methods:
  - Providing a technical basis that includes an evaluation against the code of record, to the extent known, and augmented as needed with calculations, performance tests, or reliability evidence from operating history or industry databases?
  - Comparing the safety SSC design attributes to DOE O 420.1C (or applicable successor document) design requirements, and associated codes and standards that are applicable, to demonstrate compliance?
  - Demonstrating that the existing SSCs satisfy equivalent design requirements of current design codes and standards? [preceding LOIs-3009§3.4]

**8. Beyond Design/Evaluation Basis Accidents (Chapter 3):** a) 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 their DSAs. (OE-1: 2013-01, *Improving Department of Energy Capabilities for Mitigating Beyond Design Basis Events*, Action 2)  
b) Accidents that are excluded from accident analysis based on application of the criteria in Section 3.2.1 shall be scrutinized to determine whether they should be further evaluated as beyond design basis accidents (BDBAs) or beyond evaluation basis accidents (BEBAs). (DOE-STD-3009-2014, Section 3.5)

- Are potential beyond design basis accidents identified and the need for their evaluation considered and evaluated as appropriate?
- What beyond 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)?
- Have descriptions of the performance capabilities of the existing safety SSCs been added or revised to include performance capabilities based on new or relevant information?
- 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?
- Have the descriptions of the beyond DBA accident scenarios been updated to clarify important assumptions needed to support development of abnormal or emergency operating procedures?
- Have improvements necessary to support emergency management response plans been identified and included in the DSA?

**9. Safety Structures, Systems, and Components (Chapter 4):** a) 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. (10 CFR 830 Section 830.204.b.4)

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

c) The DSA *shall* address applicable DSA sections described below, consistent with the format and content described below. (DOE-STD-3009-2014, Section 4)

- Does the DSA satisfactorily document the basis for determining the safety SSCs 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 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?
- Are SSCs whose failure could result in the 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 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 under accident conditions?
- 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?

**10. Specific Administrative Controls (Chapter 4):** 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)  
b) The DSA *shall* address applicable DSA sections described below, consistent with the format and content described below. (DOE-STD-3009-2014, Section 4)

- 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 administrative controls?
- Does the safety analysis establish the functions of SACs and their significance to safety?
- Does the DSA provide identify the preventive or mitigative safety function(s) as determined in the hazard and accident analyses?
- Are the safety functions of the SAC tied back clearly to the hazard evaluation or accident analysis?
- 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 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?
- Where SACs rely on supporting SSCs, the functional requirements and performance evaluation of the supporting SSCs are included in either the SSC or SAC sections of Chapter 4?
- 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? Does the analysis examine:
  - Adequacy of the task description in the facility procedures?
  - Level of difficulty of the task?
  - Design of the equipment and feedback mechanisms?
  - Time available to accomplish the task or recover from error?
  - Stress caused by environmental and protective clothing, for example?
- If needed, have formal engineering calculations been prepared to ensure plant operators have adequate time and resources to carry out required tasks?
- Have the consequences of incorrect implementation and measures to prevent failure been factored into the control 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 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?

**11. Derivation of TSRs (Chapter 5):** a) 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)

b) The DSA *shall* address applicable DSA sections described below, consistent with the format and content described below. (DOE-STD-3009-2014, Section 4)

- 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?
- Have the bases for deriving TSRs been identified and described in the hazard and accident analyses, safety SSC, and SAC chapters?
- Are the bases deriving safety limits, limiting control settings, limiting conditions for operation, surveillance requirements, and administrative controls provided and technically accurate?
- If a limiting control setting is specified for a variable, is the setting chosen such that the protective action, either automatic or manual, will correct the abnormal situation before a safety limit is exceeded?
- Has each safety-significant or safety-class SSC or SAC identified in Chapter 3 and 4, which provides protection for the worker or public or defense-in-depth, been listed?
- Does the discussion of SACs include the specific actions or conditions related to the individual accident scenarios?
- Have passive SSCs been designated as design features and their performance criteria identified when appropriate?

- Does the discussion of design features include safety functions, performance criteria and periodic surveillance?
- Has the information necessary to derive surveillance requirements for testing, calibration, or inspection activities (to assure the necessary quality of systems and components is maintained and the facility operations remain within the safety limits, limiting control settings or limiting conditions for operation) been provided?
- Is there adequate explanation for any safety SSCs/SACs or other safety features that will not be provided TSR controls coverage?
- Is the logic for the TSR derivation consistent with the logic and assumptions presented in the analyses?
- 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 Limiting Condition of Operation?
- Are TSRs from other adjacent facilities that can affect this facility's operations identified and summarized?
- If an adjacent facility provides the necessary controls to protect the facility addressed in the DSA, are those controls identified and summarized?

**12. Prevention of Inadvertent Criticality (Chapter 6):** a) 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. (10 CFR 830 Section 830.204.b.6)

b) The DSA *shall* address applicable DSA sections described below, consistent with the format and content described below. (DOE-STD-3009-2014, Section 4)

- 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 (CSEs) 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?
- Is an overview of the organizational structure of the Criticality Safety Program, its interfaces, and the technical and administrative practices of the criticality protection policy provided?
- Is the facility-wide training program on the configuration of equipment used to store, handle, transport, or process fissile material described? If this information is provided in Section 7.5, "Training," is it cross-referenced in this Chapter?
- Is the program for reporting and follow-up of criticality infractions described?
- Is the criticality alarm and detection system summarized (including the method used to determine placement of monitoring equipment, functions, and sensitivity) if needed? If this system is determined to be unnecessary, is a reference for that determination provided?

**13. Safety Management Programs (Chapter 7):** a) 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. (10 CFR 830 Section 830.204.b. (5))  
b) The DSA *shall* address applicable DSA sections described below, consistent with the format and content described below. (DOE-STD-3009-2014, Section 4)

- 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.3:** 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 205.a.1&2)

### **CRITERIA**

**14. Technical Safety Requirements Content:** a) 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 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, 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 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 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 SS SSCs, instrumentation, operator actions, assumed limits, and design features?

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

### ***OBJECTIVE***

**SB.4:** With respect to a hazard category 1, 2, or 3 new DOE nuclear facility or a major modification to a hazard category 1, 2, or 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***

**15. 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)

d) When delegated, review and approve safety basis and safety design basis documents in accordance with DOE-STD-1104-2016. (DOE Order 420.1C, section 5.d.(13))

- If no viable control strategy exists in an existing facility to prevent or mitigate the offsite dose consequence of one or more of the accident scenarios from exceeding the Evaluation Guideline (EG), has the responsible PSO served as the DOE approval authority? [1104§3.2]
- 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-3009-2014?
- If no viable control strategy exists in an existing facility to prevent or mitigate the offsite dose consequence of one or more of the accident scenarios from exceeding the Evaluation Guideline (EG), have the Central Technical Authority and the Office of Environment, Health, Safety, and Security concurred in the technical adequacy of the submittal? [1104§3.2, 4.9]
- Are procedures and processes in place to address and implement site office responsibilities for review and approval of new or upgraded DSA? [1104§3.1]
- Are federal personnel assigned responsibility to oversee the adequate development of new or upgraded DSA for new nuclear facilities or major modifications respectively?
- Are DOE SBRT personnel assigned responsibility to review and approve the new or upgraded DSAs prepared by the contractors? [1104§3.1]
- Is at least one of the DOE 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 DOE 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 nuclear SSCs?
- Have DOE 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?
- Do SERs meet the guidance in DOE-STD-1104 and establish an adequate basis for the approval of the new or upgraded DSA?
- Does the SER document: [1104§7.0]
  - 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?
- Have issues and comments identified during the review been adequately resolved or included in Conditions of Approval?



## ***REVIEW APPROACH***

### Record Review:

- New or upgraded DSA and associated hazard and accident analysis
- New or 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 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 new or significantly modified safety controls