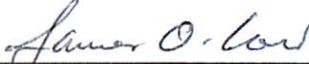


		Number: EA CRAD 31-29 Revision: 0 Effective Date: October 8, 2015
Review of Nuclear Facility Preliminary Safety Basis Development Criteria Review and Approach Document		
Authorization and Approval	 Director, Office of Nuclear Safety and Environmental Assessments Date: October 8, 2015	 Lead, James O. Low Nuclear Engineer Date: October 8, 2015

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 workers, the public, and the environment from the hazards associated with Department of Energy (DOE) activities and sites.

In addition to the general independent oversight requirements and responsibilities specified in DOE Order 227.1, *Independent Oversight Program*, this criteria review and approach document (CRAD), in part, fulfills the responsibility assigned to EA in DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*, to conduct independent assessments of high hazard facilities.

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://www.energy.gov/ea/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

OBJECTIVES

PD.1: The contractor responsible for 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 must prepare a preliminary documented safety analysis (PDSA^{1,2}) for the facility. (10 CFR 830.206.a)

PD.2: The contractor responsible for 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 must obtain DOE approval of the nuclear safety design criteria to be used in preparing the PDSA unless the contractor uses the design criteria in DOE Order 420.1C, *Facility Safety* (or successor). (10 CFR 830.206.b.1)

PD.3: The contractor responsible for 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 must obtain DOE approval of the PDSA before the contractor can procure materials or components or begin construction; provided that DOE may authorize the contractor to perform limited procurement and construction activities without approval of a PDSA if DOE determines that the activities are not detrimental to public health and safety and are in the best interests of DOE. (10 CFR 830.206.b.2)

CRITERIA

Note: It is intended that the content of a Preliminary Safety Design Report (PSDR) or PDSA be commensurate with the design development stage of Safety-in-Design process. For example, hazards analyses that are documented in a PSDR would be expected to include process hazards analyses and process level hazard controls. The PDSA would be expected to include activity level hazard controls.

1. The PSDR/PDSA will demonstrate the adequacy of the hazards analyses and the selection and classification of the hazard controls, including consideration of the application of the principles associated with the hierarchy of controls. (DOE-STD-1189, Section 6.3)

¹ PDSA means documentation prepared in connection with the design and construction of a new DOE nuclear facility or a major modification to a DOE nuclear facility that provides a reasonable basis for the preliminary conclusion that the nuclear facility can be operated safely through the consideration of factors such as a safety analysis that derives aspects of design that are necessary to satisfy the nuclear safety design criteria. (10 CFR 830.3)

² If the commitments made in the PDSA and design documents are met, the result should be a final design and a constructed facility that could be approved for operation without major modifications. (DOE-STD-1189, Section 6.3)

General Information

- Is site information of the type that can affect Safety-in-Design (e.g., location of nearby facilities and external hazards, meteorological data, seismic and other natural phenomena hazard (NPH) information) process included?
- Are facility and process descriptions, including facility structure types, layout, general arrangements, flow sheets, and summary system descriptions for safety structures, systems & components (SSCs), consistent with the level of design?;
- Is the facility design complete enough to provide information required for the hazards analysis? Information may include, but is not limited to:
 - Facility site/location selection;
 - General arrangement drawings;
 - MAR estimates or assumptions and material flow balances;
 - Sizing calculations for major process system equipment including pumps, vessels, piping, and similar items;
 - Process block flow diagrams or equivalent documentation of the required major process flow steps and their sequence;
 - Preliminary one-line diagrams for ventilation, electrical power and distribution, material handling, and instrumentation and control system architecture;
 - Summary process design description and sequence of major operation; and
 - Safety design strategy
- Is criticality safety information regarding aspects of the preliminary design presented?

Hazard and Accident Analysis

- Is a summary of the hazard analysis (HA); including process hazards evaluation, fire hazard analysis (FHA), selected design basis accidents (DBAs); selected SSCs and their safety function; functional classification; and required seismic and other natural phenomena design criteria, including their bases; included?
- Does the unmitigated accident consequence assessment properly indicate the required functional classification (i.e., safety class vs. safety significant)?
- Have the seismic and other NPH design requirements (i.e., the proper seismic design criteria and performance category (PC)) for the SSCs been provided?
- Does the analysis of DBAs identify the functional requirements and accident conditions (e.g., environmental qualifications) that the safety SSCs need to address? (STD-1189, Appendix I, Section I.1.1)?
- Is the hazard and accident analysis sufficiently complete to develop facility-level DBAs that provide the necessary input to the identification and classification of important safety functions? (DOE-STD-1189, preface)?

- Is the methodology and criteria by which SSC's are functionally classified (i.e., safety class, safety significant, or defense-in-depth) during project phases justified and documented? (STD-1189 §2.4.5)?
- Does the Hazard Analysis provide the following information:
 - The spectrum of accidents that may impact design and which may be initiated by facility operations, NPH, and external man-induced events are identified; (STD-1189, §4.3)
 - Postulated accident scenario's that could lead to the release of hazardous materials;
 - A conservative estimate of the initiating event frequency;
 - An unmitigated consequence evaluation that describes the hazardous material release with respect to facility workers, collocated workers, and offsite personnel;
 - The safety functions of controls needed to prevent or mitigate the hazardous material release event;
 - A list of all SSCs and administrative controls (ACs) that have the potential to prevent the initiating event or reduce the frequency of accident scenario progression;
 - All SSCs and ACs that could detect the event;
 - A list of all SSCs and ACs that potentially could mitigate the event by limiting consequences after the event has occurred;
 - The suite of hazard controls, including safety SSCs, that will be relied upon to detect, prevent, or mitigate each event;
 - The estimated consequences for the identified receptor(s) after applying the hazard controls; and
 - A list of remaining analysis or assumption validations and risk/opportunities associated with the selected safety design strategies. (STD-1189, Appendix G)
- Is the basis for the design, safety functional analysis, and performance requirements of selected safety SSCs to prevent or mitigate the postulated accidents adequately defined and described?
- Are the safety SSCs identified and described consistent with the logic presented in the hazard and accident analyses?
- Is the state of maturity of the associated hazard and accident analyses adequate to support the identification of the SSC safety functions?
- Are the selected controls evaluated for effectiveness in adequately preventing or mitigating the accidents?
- Do system evaluations provide evidence that the safety functions can be performed when called upon?
- Are the selected controls evaluated for defense in depth, based on accident frequency and reliability, adequately described?
- Are the general design requirements for safety SSCs (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes) appropriately specified?

- Are design safety functions and performance criteria of the 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 preliminary safety basis document:
 - Identify safety functions to be performed by safety SSCs (consistent with the hazard and accident analyses) in the normal, abnormal, or accident conditions postulated?
 - Identify internal/external hazards functional and design requirements (e.g., to address non-ambient environmental stresses, or to withstand seismic and other NPH)?
 - Identify the performance criteria necessary to provide reasonable assurance that safety SSC functional requirements will be met (e.g., surveillance, maintenance, specific operational response, requisite operator training and qualifications)?
 - Identify, and designate as safety SSCs, the support systems on which safety SSCs rely to perform or maintain safety functions?
 - Provide for requiring TSR coverage?
- Are the boundaries and interface points of safety SSCs (relative to their safety function), including the support systems, clearly defined?
- Is information regarding aspects of the preliminary design that are required to support the prevention of inadvertent criticality included?
- Does the PSDR or PDSA follow the expectations in the Safety Design Strategy?

Preliminary Design

- Does the design address the nuclear facility design requirements of DOE O 420.1C?
 - Is the design integrated with the safety analyses and is a viable design solution (e.g., safety SSCs) identified to provide the safety functions required by the safety analysis?
- Are appropriate supplemental design criteria specified for safety SSCs:
 - Are general requirements for safety SSCs specified (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes);
 - Are technical studies still needed to complete the safety-in- design process identified and described;
 - Are safety design risks and risk mitigation strategies for the final design phase identified? (STD-1189, Appendix I, Section I.1.1)
- Are any exceptions or alternate approaches to DOE O 420.1C (or successor), including analyses performed to meet the safety analysis expectations, identified and included in the SDS?
- Does the facility design address:
 - Multiple layers of protection (i.e. defense in depth) to prevent or mitigate the unintended release of radioactive materials?
 - The means to confine the hazardous materials to minimize their potential release during normal operations and during and following accidents?
 - The ability of safety SSCs and safety software to perform their safety functions when called upon?

- Single point failure for safety class electrical systems?
 - Is the description of how the nuclear safety design criteria of DOE O 420.1C (or successor) have been satisfied by the design adequate?
 - Are the applicable codes and standards appropriately specified, as necessary, based on SSC safety function?
 - Is there documentation of how the safety design criteria of DOE O 420.1C are met, including any exceptions or alternate approaches, which may include analyses performed to meet the safety analysis expectations? (STD-1189, Section 6.3)
 - Are those codes and standards not included in DOE G 420.1-1 and DOE G 420.1-2 guidance identified; including a brief description as to why they are appropriate?
 - Are seismic design criteria correctly identified?
 - Does the fire protection system design include:
 - Complete fire-rated construction and barriers, commensurate with the applicable codes and FHA, to isolate hazardous areas and minimize fire spread and loss potential consistent with limits as defined by DOE-STD-1066?
 - Automatic fire extinguishing systems throughout all significant facilities and in all facilities and areas with potential for loss of safety class systems (other than fire protection systems), significant life safety hazards, unacceptable program interruption, or fire loss potential in excess of limits defined by DOE-STD-1066?
 - Does the integrated fire protection program, including design, provide a level of safety sufficient to fulfill requirements for highly protected risk, prevent loss of safety SSC functions as determined by safety analysis, and provide defense-in-depth?
 - Are technical safety issues requiring resolution identified, tracked and resolved in a timely manner?
 - Is there a project design crosswalk between the top-level safety design criteria of DOE O 420.1C (or successor) and associated implementation guidance, to the specifics of the design description and the specified safety SSCs?
 - If a graded approach of design criteria is used, is an adequate basis for the approach provided?
2. It is not expected that Specific Administrative Controls (SAC) will be developed in detail during preliminary or final design. However, the safety function of SACs needs to be fully defined so that the decision to use an SAC rather than a safety SSC can be understood. In addition, any design requirements needed to implement the SACs are identified. (DOE-STD-1189, section 4.5)
- Are the identified SACs described consistently with the logic presented in the hazard and accident analyses?

- Are the SACs adequate to prevent or mitigate the hazards/accidents for which they were identified, and is there adequate rationale for controlling the identified hazard through an SAC instead of an SSC?
 - Does the PSDR or PDSA provide a satisfactory basis for determining the SACs and their required safety functions?
 - Are safety functions for SACs defined with clarity and are they consistent with the bases derived in the hazard and accident analyses?
 - Do the functional requirements and evaluations of SAC provisions provide evidence that the required safety functions can be performed when called upon?
 - Are any SSCs required to perform the actions in the SACs appropriately identified? Are these SSCs identified as safety SSCs?
 - Are the attributes of the SACs relevant to future TSR development clearly defined?
3. DOE may authorize the contractor to perform limited procurement and construction activities without approval of a PDSA if DOE determines that the activities are not detrimental to public health and safety and are in the best interests of DOE. (10 CFR 830.206.b.2)
- Are the safety functions and performance requirements of the affected (i.e. limited procurement) SSCs completely understood and acceptable?
 - Are safety functions and performance criteria of the affected SSCs based on conservative estimates of frequency and consequences for the accidents that potentially involve these SSCs?
 - If the proposed design of the SSC is based on preliminary information, will the affected SSC fully meet required safety criteria in the final DSA? If not, are appropriate compensatory measures identified and implemented?
 - Is the functional classification, reliability, or rigor of the design code for an affected SSC appropriately conservative?
 - Have any consequences due to early procurement or construction, been identified that could be detrimental to public health and safety? If so, are appropriate compensatory measures identified, approved and implemented?

APPROACH

Record Review:

- Hazard identification records such as chemical and radiological inventories
- Hazard identification tables
- Hazard analysis procedures and guides
- Hazard analysis output documents including hazard event records and hazard tables
- Hazard analysis reports
- System design descriptions
- System design information including piping and instrumentation drawings, logic diagrams, electrical one-line drawings, detail drawings and calculations
- System and safety function requirements documents
- Supporting safety calculations
- Approved safety design strategy
- Process flowsheets and calculations
- Preliminary Safety Design Report
- Preliminary Documented Safety Analyses

Interviews:

- Hazard analysis team members and team leaders
- Safety analysts
- Responsible safety managers
- Supporting engineering personnel
- Operations personnel

Observations:

- Facility and building walkdowns and reviews
- Hazard analysis team meetings
- Control decision meetings

Federal DSA/TSR Review and Approval

CRITERIA

Preliminary Safety Validation Report (PSVR)

1. The reviewer should refer to DOE-STD-1189-2008, Appendix I, for detailed guidelines on the expected contents for a PSDR and the reviewer of the PSVR and PSDR shall confirm that it adequately addresses the following safety design basis aspects for the preliminary design phase. (DOE-STD-1104-2014, Section 8.5)
 - Does the PSVR verify the PSDR conclusions on the design meet the nuclear facility design requirements of DOE O 420.1C?
 - Does the PSVR verify that the PSDR present a viable design solution (e.g., safety SSCs) to provide the safety functions assessed to be necessary by the hazard and accident analysis? As follows:
 - The unmitigated accident consequence assessment properly indicates the required functional classification (i.e., safety class versus safety significant) and seismic and other NPH design requirements (i.e., the proper seismic design criteria for seismic design and performance criteria for other NPH design).
 - The analysis of DBAs identifies the functional requirements that the safety SSCs and SACs perform and the conditions (e.g., normal and accident) under which these functions are required to be performed. As discussed in DOE-STD-1189-2008 Section 4.3, “SACs should only be selected if engineered controls cannot be identified or are not practical.” Where SACs are included in lieu of an SSC, an explanation should be provided in the PSDR for DOE to determine the adequacy of that rationale. Other expectations for the discussion of SACs in the PSDR are included in Appendix I of DOE-STD-1189-2008.
 - The safety systems can meet the functional requirements and any unique technology development that may be needed has been identified.
 - Are appropriate supplemental design criteria (DOE O 420.1C, Attachment 3) specified for safety SSCs? As follows:
 - General requirements for safety class and safety significant SSCs are specified (e.g., conservative design features, design against single failure, environmental qualification, safe failure modes, as appropriate).
 - Based on the functional classification and the safety SSC design function, appropriate codes and standards are specified and tailored, as needed, or alternate codes and standards are identified and justified.
 - Descriptions of the technical studies needed to complete the safety design.
 - Safety design risks and risk mitigation strategies for the final design phase.
 - Resolution of any open Conditions of Approval identified in the CSVR.

PDSA Safety Evaluation Report (SER)

2. The PDSA is, in part, to ensure that DOE and the contractor agree that safety has been adequately integrated into the design before construction begins. (DOE-STD-1104-2014, Section 8.6)

- Does the SER verify that the PDSA addresses activity-level hazards and hazard controls and evaluate facility/process hazards?
- Does the review of the SER verify that the PDSA confirm that:
 - The design safety analysis is complete and demonstrates the adequacy of the design from the safety perspective? (The PDSA does not need to show the progression of the design that led to the final choices, only the final choices and the justification for their adequacy.)
 - The safety design requirements specified at the end of the preliminary design have been met?
 - The hazards and accident analysis is consistent with DOE-STD-1189-2008, Section 4.4?
 - The description of the final design of the facility is adequate with respect to safety SSCs and safety design features?
 - Safety SSCs, SACs, and other hazard controls are identified and their performance requirements are clearly stated? Note: In addition to the review consideration presented in Section 8.4 of DOE-STD-1104 regarding SACs, expectations for the discussion of SACs in the PDSA are included in Appendix I of DOE-STD-1189-2008;
 - The description of how the selected safety controls prevent and/or mitigate identified hazards and accidents is adequate?
 - The description of how selected safety controls provide defense-in-depth is adequate, based on mitigated accident frequency and on control reliability?
 - The initial list of safety management programs is complete?
 - The description of how the nuclear safety design criteria of DOE O 420.1C (or applicable version) have been satisfied by the design is adequate?
 - Any technical issues that required research or other data collection to finalize the design have been resolved?
 - Preliminary approaches to startup and operations management have been documented?
 - Any open Conditions of Approval identified in the PSVR have been resolved?

APPROACH

Record Review:

- PDSA/PSDR and associated hazard and accident analysis documents
- Preliminary Safety Validation Report
- Safety Evaluation Report
- Approved safety design strategy
- DOE direction and guidance documents
- Technical support documents, including calculations and engineering analyses
- DOE plans and records of reviews for the PDSA/PSDR submittals
- DOE review comment record forms and associated documentation
- Procedures and guidance for maintenance and update of the PSDR or PDSA and associated elements

Interviews:

- DOE Nuclear Safety Specialists
- 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

Observations:

- SBRT comment resolution meetings with Contractor personnel, if applicable