

		Number: IEA CRAD 31-02 Revision: 0 Effective Date: July 25, 2014
Preliminary Documented Safety Analysis Criteria Review and Approach Document		
Authorization and Approval	 Director, Office of Nuclear Safety and Environmental Assessments Date: July 21, 2014	 Lead, James O. Low Nuclear Engineer Date: July 21, 2014

1.0 PURPOSE

Within the Office of Independent Enterprise Assessments (IEA), the Office of Environment, Safety and Health Assessments (EA-30) mission is to assess the effectiveness of those safety and emergency management systems and practices used by line and contractor organizations in implementing Integrated Safety Management; and to provide clear, concise, and independent evaluations of performance in protecting our workers, the public, and the environment from the hazards associated with Department of Energy (DOE) activities and sites.

In addition to the general independent oversight requirements and responsibilities specified in DOE Order 227.1, *Independent Oversight Program*, this Criteria Review and Approach Document (CRAD), in part, fulfills the responsibility assigned to IEA in DOE Order 420.1C to plan and conduct independent oversight reviews of implementation of the requirements of this Order.

A key to success is the rigor and comprehensiveness of our process and, as with any process, we continually strive to improve and provide additional value and insight to field operations. Integral to this is our commitment to enhance our program. We continue to make CRADs available for use by DOE line and contractor assessment personnel in developing effective DOE oversight, contractor self-assessment, and corrective action processes; the current revision is available at: <http://energy.gov/iea/listings/criteria-review-and-approach-documents>.

2.0 APPLICABILITY

The following CRAD is approved for use by the Office of Nuclear Safety and Environmental Assessments (EA-31).

3.0 FEEDBACK

Comments and suggestions for improvements on this CRAD can be directed to the Director, Office of Environment, Safety and Health Assessments, at (301) 903-5392.

4.0 CRITERIA REVIEW AND APPROACH

OBJECTIVE

PDSA.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 for the facility. (10 CFR 830.206.a)

PDSA.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 preliminary documented safety analysis unless the contractor uses the design criteria in DOE Order 420.1, Facility Safety. (10 CFR 830.206.b.1)

PDSA.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 preliminary documented safety analysis 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 preliminary documented safety analysis 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

1. Preliminary documented safety analysis 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)
 - Is the basis for the design, functional, and performance requirements of selected safety SSCs to prevent or mitigate the postulated accidents adequately defined and described?
 - Are the safety (safety-class and safety-significant) 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?
 - Are the selected controls evaluated for defense in depth, based on accident frequency and reliability adequately described?
 - 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 general requirements for safety SSCs (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes) appropriately specified?
 - Are the general safety functions and performance requirements for the safety SSCs accurately specified?
 - Are specific safety functions and the design and functional requirements 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 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)?
 - 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?
 - Do system evaluations provide evidence that the safety functions can be performed when called upon?
 - Is information regarding aspects of the preliminary design that are required to support the prevention of inadvertent criticality included?
 - Does the PDSA follow the expectations in the Safety Design Strategy?
2. Preliminary documented safety analysis 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 the nuclear safety design criteria to be satisfied. (10 CFR 830.3)
- Is the description of how the nuclear safety design criteria of DOE O 420.1B (or successor) have been satisfied by the design adequate?

- Are any exceptions or alternate approaches to DOE O 420.1B (or successor), including analyses performed to meet the safety analysis expectations, identified and included?
 - Does the facility design address:
 - Multiple layers of protection to prevent or mitigate the unintended release of radioactive materials (otherwise known as defense in depth)?
 - The means to confine the uncontained radioactive materials to minimize their potential release in facility effluents during normal operations and during and following accidents?
 - The ability of safety SSCs and safety software, commensurate with the importance of the safety functions performed, to perform their safety functions when called upon?
 - Single point failure for safety class electrical systems?
 - Are the applicable codes and standards appropriately specified, as necessary, based on functional classification and safety function?
 - 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 fire hazards analysis, to isolate hazardous areas and minimize fire spread and loss potential consistent with limits as defined by DOE?
 - 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?
 - Does the integrated fire protection program, including activities and design, provide a level of safety sufficient to fulfill requirements for highly protected risk, prevent loss of safety functions and safety systems as determined by safety analysis, and provide defense-in-depth?
 - Are the nuclear safety technical issues requiring resolution identified?
 - Does the PDSA follow the expectations in the Safety Design Strategy?
 - Is there a crosswalk between the top-level safety design criteria of DOE O 420.1B (or successor) and its implementation guide (DOE G 420.1-1A or successor), or any approved substitute criteria and implementation, and 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?
3. Preliminary documented safety analysis 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 an initial listing of the safety management programs that must be developed to address operational safety considerations. (10 CFR 830.3) 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 understood 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 Specific Administrative Controls (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 are there adequate rationale for controlling the identified hazard(s) through an SAC instead of an SSC?
 - Does the safety document provide a satisfactory basis for determining the safety SACs and their required 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 controls of the SACs relevant to future TSR development clearly defined?
4. DOE may authorize the contractor to perform limited procurement and construction activities without approval of a Preliminary Documented Safety Analysis 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)
- As described in justification documents (e.g. Justification for Continued Operations), are the safety functions and performance requirements of the affected SSCs completely understood and acceptable?
 - As described in justification documents, are safety functions and performance criteria of the affected SSCs based on conservative estimates of frequency and consequences for the events that potentially involve these SSCs?
 - As described in justification documents or the draft PDSA, if the proposed design of the SSC is based on preliminary information, will the SSC fully meet required safety criteria in the final DSA? If not, are appropriate compensatory measures available and identified?
 - As described in justification documents, is the functional classification, reliability, or rigor of the design standard for an 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 available and identified?

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
- Process flowsheets and calculations
- 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