

		Number: EA CRAD 31-13 Revision: 0 Effective Date: May 4, 2015
Conduct of Engineering Criteria Review and Approach Document		
Authorization and Approval	 Director, Office of Nuclear Safety and Environmental Assessments Date: May 4, 2015	 Lead, Charles Allen Nuclear Engineer Date: May 4, 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 our workers, the public, and the environment from the hazards associated with Department of Energy (DOE) activities and sites.

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

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 of this CRAD 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) for use on DOE Hazard Category 1, 2, and 3 nuclear facilities.

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

This CRAD focuses on review of the engineering function at nuclear facilities either in operation or under construction. The engineering function may be comprised of various elements as governed by the design/construction or operational stage of the facility. Requirements have been segregated into four areas as denoted by the objectives outlined below, focused on engineering processes and products, the cognizant system engineering program, configuration management, and processes for feedback and improvement.

4.1 OBJECTIVES AND CRITERIA

OBJECTIVE 1

Design engineering work is being performed consistent with technical standards, DOE requirements, and safety basis requirements and commitments, using approved procedures and sound engineering/scientific principles in accordance with the requirements of 10CFR830.

CRITERIA

The engineering function for a Hazard Category 1, 2, or 3 nuclear facility is tasked with developing and maintaining the technical baseline for the facility. The technical baseline is comprised of the fundamental design documents (including criteria, drawings, analyses, calculations, specifications, and characteristics) pertaining to the systems, structures and components (SSCs) of the facility necessary to demonstrate that the facility meets the requirements and commitments established in the safety basis documents for that facility.

Requirements pertinent to the engineering function are found in numerous DOE regulations, orders, and technical standards. A summary of those requirements applicable to design engineering is provided in Attachment 1. In aggregate, those requirements and guidance form the review criteria for this objective.

1. Design criteria establish the fundamental requirements pertinent to the design:
 - Applicable codes and standards (including any exemptions and equivalencies)
 - Codes of Record
 - Functional and operational performance requirements
 - Classification of SSCs
 - Natural phenomena hazard design requirements
 - Safety basis compliance
 - Single failure design criteria

2. Engineering procedures are in place and contain appropriate detail to control development, approval, issuance, and revision of deliverables, as well as key processes essential to the design engineering function:

- Preparation, approval, and issuance of design criteria and system design description documents
- Preparation, approval, and issuance of design drawings
- Preparation, approval, and issuance of design analyses and calculations
- Preparation, approval, and issuance of commodity, component, and/or procurement specifications
- Preparation, approval, and issuance of design change documents
- Field change request process
- Design verification (to a level commensurate with importance to safety and design complexity) by individuals other than those who performed the work

Engineering procedures provide barriers against poor performance, require participation and review by appropriate organizations, and drive communication between distinct groups. Verbatim compliance is required.

3. Documents comprising the project technical baseline are readily identifiable and subject to appropriate control measures. System design documents and supporting documents must be identified and kept current using formal change control and work control processes. DOE-STD-3024-2011, *Content of System Design Descriptions*, describes an acceptable methodology to achieve this function. (See also Objective 2)
4. Analyses and calculations are:
 - Categorized according to safety significance
 - Prepared with design inputs clearly identified, assumptions technically justified, or unverified assumptions clearly identified and tracked to resolution
 - Prepared consistent with the design criteria and safety basis
 - Prepared with sufficient explanation, detail, and clarity of approach (including references) to permit duplication by another similarly qualified individual
 - Conservative in establishing both adequate margin against failure and adequate performance margin
 - Checked by a second party and verified by an independent verifier, as appropriate
5. Specifications for commodities, equipment procurement, and construction adequately reflect:
 - Design criteria and safety basis functional and performance requirements
 - Technical requirements, including reference to applicable drawings and industry codes and standards
 - Safety classification
 - Endurance requirements for natural phenomena hazards
 - Quality requirements
 - Environmental qualification criteria
 - Labeling criteria
 - Test, inspection, and acceptance criteria
6. Design drawings are:
 - Categorized per DOE standards
 - Drafted in accordance with DOE HDBK 1016 standards
 - Subject to interdisciplinary review as appropriate prior to issuance
 - Accessible and retrievable in the most current version
 - In accordance with applicable design criteria and industry standards

7. System and component interfaces are appropriately defined and coordinated to ensure that support functions required from other systems (e.g., cooling water, power supply, control signals) and interfaces with other systems are defined and will support required operability and functionality.

OBJECTIVE 2

A cognizant system engineer (CSE) program has been implemented in accordance with the requirements of DOE O 420.1B or 420.1C, as applicable; to ensure continued operational readiness of identified systems to meet their safety functional requirements and performance criteria.

CRITERIA

Refer to the applicable revision of DOE O 420.1 for specific requirements based on contract provisions for the facility under review.

1. CSEs have been designated, trained, and qualified (for safety class and safety significant systems, as a minimum) in accordance with DOE requirements:
 - CSEs are fully qualified with up-to-date training records.
 - CSE are responsible for compliance of their system with safety basis requirements and facility design criteria. They are an integral part of the design change process, ensuring that all design documents applicable to their system remain consistent.
 - CSEs have working level knowledge of engineering documents pertaining to their system and provide technical support to operations and maintenance.
 - CSEs initiate actions as necessary to correct problems on their system.
2. CSEs are involved in developing and maintaining System Design Descriptions (SDDs). SDDs identify the requirements associated with the facility's safety SSCs, explain the technical bases for the requirements, and describe the features of the system design provided to meet those requirements. The SDD often serves as the central coordination link among the engineering documents, facility safety basis, and procurement and construction documents:
 - Documentation of system specific requirements necessary to implement the safety basis
 - Safety classification of SSCs
 - Redundancy and single failure criteria
 - Applicability of DOE STD 3024-2011, *Content of System Design Descriptions*
 - Compliance with DOE STD 1189-2008 Appendix A, *Safety System Design Criteria*

CSEs keep system design documents and supporting documents current using formal change control and work control processes. (DOE-STD-3024-2011, *Content of System Design Descriptions*, describes an acceptable methodology to achieve this function.)

3. At operating facilities, system assessments are performed on a periodic basis (recommended quarterly) examining:
 - Operating status of the system; ability to perform design and safety functions
 - System and component performance relative to established criteria
 - Status of maintenance, including equipment out-of-service, other equipment issues, overdue activities, and life cycle issues.
 - Analysis of system reliability, operability, and material condition
 - Identification of outstanding work orders and corrective actions

- Summary of system risks to operability
4. (Non-mandatory) On operating facilities, system assessments (item 3 above) are used to generate system health reports for management consideration/review and system notebooks are maintained by the CSEs as a source of information on design, operability, maintenance, and on the bases for inspections, tests, and maintenance, such as applicable codes and standards and vendor manuals/records.

OBJECTIVE 3

A documented configuration management (CM) program has been established and implemented in accordance with DOE O 420.1 that ensures consistency among system requirements and performance criteria, system documentation, and physical configuration of the systems within the scope of the program. DOE STD 1073-2003 provides an acceptable methodology to accomplish this requirement and may be invoked contractually on the specific facility.

CRITERIA

1. Design input and output documents are appropriately established. Requirements from upper tier documents are appropriately incorporated into successor (or lower tier) documents. System design basis documents are kept current using formal change control and work control processes.
2. A design change process is in place which:
 - Ensures that all documents affected by a change, both predecessor and successor, are identified.
 - Ensures that impacts are considered, and all affected documents are revised as part of the change process to ensure that the design remains consistent.
 - Ensures changes are reviewed by all potentially affected disciplines and organizations to ensure that proposed changes are technically acceptable, implementable, and consistent with the design basis.
 - Ensures that extant changes against technical documents are tracked from initial issuance until incorporation in an approved revision.
3. A work control process is in place to ensure that physical changes are installed and tested in accordance with the design output. Change documents are posted against the affected parent documents and incorporated following completion of the change.
4. A field change request process is in place to identify proposed field changes and drive engineering review and approval. Approved field changes result in design changes which adequately identify all affected documents and ensure that revisions occur as appropriate.
5. An unreviewed safety question (USQ) process has been established as required by 10CFR830 and is being appropriately implemented to control changes to systems including documents governing work on the systems.
6. A records management system has been implemented which provides:
 - The official electronic record copy for approved records including procedures and vendor manuals.

- Accessibility to engineering documents using a process that defaults to the most recent revision.
- Enables the ready identification of predecessor and successor documents for issued records.
- Tracks unincorporated changes outstanding against issued documents.
- Limits outstanding changes against engineering documents such as drawings to avoid negative impacts from excessive change paper and difficulties in determining the current design configuration.
- Ready access to the records system current version of each record as well as archival access to prior versions.

OBJECTIVE 4

Programs and processes are in place to identify and correct problems, ensure that personnel are appropriately trained and qualified, and assess internal performance, identifying lessons learned and implementing appropriate corrective actions.

CRITERIA

1. An effective contractor assurance process is in place wherein problems are identified and corrective actions are determined and accomplished in a timely manner. Corrective actions are effective in addressing both the extent of condition of the problem identified and recurrence control.
2. A qualification program is in place for engineering personnel establishing minimum qualification and training standards.
3. A training program is in place which identifies required training on an individual basis, performs notifications, and tracks completion. Requirements are established to identify retraining periodicity for key procedures. Revisions to key project documents and procedures result in training to the revised requirements in a timely manner. Failure to accomplish required training can result in disqualification from performance of assigned tasks.
4. Internal assessments are performed on a periodic basis to examine performance with regard to procedural and programmatic requirements. Assessors are independent of the area being examined. Lessons learned are identified and communicated to engineering personnel. Problems identified are documented using the contractor assurance system and tracked to completion of corrective actions.

4.2 APPROACH

Record Review:

- Portions of the approved facility safety basis applicable to the engineering SSCs within the review scope to establish safety basis requirements and commitments
- Codes of Record
- Contractor requirements documents (manuals, procedures)
- System design descriptions
- System assessments and periodic system health reports; system notebooks
- Piping & Instrumentation Diagrams
- Physical layout drawings
- Engineering analyses pertinent to establishing and/or implementing the design basis for selected systems
- Calculations used to develop set points used in the Technical Safety Requirements
- Configuration Management Plan and implementing procedures
- Engineering procedures for SDDs, drawings, calculations, specifications, design verification, records processing, design changes
- Procurement specifications
- Design change packages, including USQ determinations
- Training and qualification requirements and records
- Problem reports, root cause analyses, and corrective action documents
- Field Office oversight assessments

Interviews:

- Program owners for CM, system engineering, document control
- Responsible individuals for key procedures
- Cognizant system engineers
- Safety basis, engineering, and training personnel (random sampling)
- Quality assurance and corrective action program personnel
- Field Office engineering oversight group

Observations:

- System walkdown with designated CSE
- Design change review board meeting
- System design coordination meeting

ATTACHMENT 1

SOURCE DOCUMENTS

10CFR830 Subpart A, *Quality Assurance Program*, provides specific requirements pertinent to the design engineering function. The contractor Quality Assurance Program must address how the contractor will meet the following criteria:

- *Establish and implement processes to detect and prevent quality problems. (10CFR830.122(c))*
- *Identify, control, and correct items, services, and processes that do not meet established requirements. (10CFR830.122(c))*
- *Prepare, review, approve, issue, use, and revise documents to prescribe processes, specify requirements, or establish design. (10CFR830.122(d))*
- *Specify, prepare, review, approve, and maintain records. (10CFR830.122(d))*
- *Perform work consistent with technical standards, administrative controls, and other hazard controls adopted to meet regulatory or contract requirements, using approved instructions, procedures, or other appropriate means. (10CFR830.122(e))*
- *Identify and control items to ensure their proper use. (10CFR830.122(e))*
- *Maintain items to prevent their damage, loss, or deterioration. (10CFR830.122(e))*
- *Design items and processes using sound engineering/scientific principles and appropriate standards. (10CFR830.122(f))*
- *Incorporate applicable requirements and design bases in design work and design changes. (10CFR830.122(f))*
- *Identify and control design interfaces. (10CFR830.122(f))*
- *Verify or validate the adequacy of design products using individuals or groups other than those who performed the work. (10CFR830.122(f))*
- *Verify or validate work before approval and implementation of the design. (10CFR830.122(f))*
- *Procure items and services that meet established requirements and perform as specified. (10CFR830.122(g))*

DOE further establishes design criteria for safety SSCs for new facilities and major modifications to existing facilities in DOE Order 420.1C, Attachment 3 (paraphrased):

- *Safety-SSCs must be designed, commensurate with the importance of the safety functions performed, to perform their safety functions when called upon, as determined by the safety analysis.*
- *Safety-SSCs must be designed with appropriate margins of safety, as defined in applicable DOE or industry codes and standards.*
- *The single failure criterion, requirements, and design analysis identified in Institute of Electrical and Electronics Engineers standard 379-2000, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, must be applied to safety-class SSCs during the design process as the primary method of achieving reliability.*
- *Safety-class SSCs must be designed to perform all safety functions with no failure mechanism that could lead to common cause failures under postulated service conditions.*

- *Safe Failure Modes. The facility design must provide reliable safe conditions and sufficient confinement of hazardous material during and after all design basis accidents.*
- *Support SSCs must be designed as safety-class or safety-significant SSCs if their failures prevent safety-SSCs or specific administrative controls from performing their safety functions.*
- *Interfaces must be evaluated to identify SSC failures that would prevent safety-SSCs from performing their intended safety function.*

DOE Order 420.1C, Attachment 3, also contains lists of recommended industry consensus standards to be used in facility design. It should be noted that the previous revision of this order, DOE O 420.1B, contains significantly less specificity with regard to these requirements. Some DOE facilities remain committed to the previous revision rather than the current one.

Finally, DOE STD 1189-2008, *Integration of Safety into the Design Process*, contains the following general guidance in Section 5.0:

Demonstrating compliance with the requirements in DOE O 420.1B generally involves a design analysis or series of analyses. For example, some safety SSCs are required to be designed to withstand common cause effects and adverse interactions from natural phenomena hazard (NPH) events. The design analyses must demonstrate that those safety SSCs that are required to function before, during, or after the NPH event will continue to do so. This may entail evaluation of a number of nearby or overhead SSCs that perform no direct safety function. Design documentation to demonstrate this requirement for “source SSCs” may involve design criteria for the facility or system and calculations demonstrating acceptable seismic design. Each applicable analysis for a project should be considered as important technical basis information that is to be maintained in support of the safety basis for the life of the facility.