		Number: EA CRAD 31-15 Revision: 1 Effective Date: April 29, 2019
Safety Systems Management Review Criteria Review and Approach Document		
Authorization and Approval	C. E. (Gene) Carpenter Jr. Director Office of Nuclear Safety and Environmental Assessments Date: 4/29/19	Lead: Charles R. Allen Title: Nuclear Engineer Date: 4/29/2019

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 227.1A, *Independent Oversight Program*, this criteria and review 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 is available at: https://www.energy.gov/ea/criteria-and-review-approach-documents

This CRAD supersedes EA CRAD 31-15, Revision 0.

2.0 APPLICABILITY

The following CRAD is approved for use by the Office of Nuclear Safety and Environmental Assessments.

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 AND REVIEW APPROACH

The review of Safety Systems Management will evaluate the effectiveness of programs and processes for engineering design, quality assurance, configuration management, surveillance testing, maintenance, operations, cognizant system engineer (CSE) and safety system oversight (SSO), and feedback and improvement of selected safety systems. The review will also evaluate the effectiveness in maintaining the functionality and reliability of these safety systems. The review of safety systems will be performed in the context of integrated safety management (ISM), although the inspection criteria and approach are organized by functional areas rather than ISM principles and core functions. The following functional areas are designed as stand-alone sections to be used in any combination based on the need of the specific appraisal.

OBJECTIVES

SS.1: Engineering design documents and analyses are technically adequate and implement the requirements of the documented safety analysis such that adequate protection of the public, the workers, and the environment from facility hazards is demonstrated. (DOE-STD-3009-2014, 10 Code of Federal Regulations (CFR) 830.122)

Criteria:

1. Engineered structures, systems, and components (SSCs) and processes are designed using sound engineering/ scientific principles and appropriate standards. (10 CFR 830.122 Criterion 6)
2. Engineering design incorporates applicable requirements from consensus standards and the safety design bases in design work and design changes (e.g., design calculations). (10 CFR 830.122 Criterion 6)
3. The adequacy of design products is verified or validated by individuals or groups other than those who performed the work. (10 CFR 830.122 Criterion 6)
4. Verification and validation work is completed before approval and implementation of the design. (10 CFR 830.122 Criterion 6)

5. Technical baseline documents, including design basis and supporting documents, are identified, developed, and kept current to support facility safety basis development and implementation. (DOE O 420.1B Chapter 5 (or DOE O 420.1C as applicable to the facility)).

   - Does the documented safety analysis (DSA) identify the appropriate performance criteria necessary to provide reasonable assurance that selected system functional requirements will be met?
   - Do authorization basis documents identify and describe the system safety functions?
   - Does the definition/description of the safety functions of the system include:
     - Specific role of the system in detecting, preventing, or mitigating analyzed events?
     - The associated conditions and assumptions concerning system performance?
     - System requirements and performance criteria for the system and active components, including essential supporting systems for normal, abnormal, and accident conditions relied upon in the hazard or accident analysis?
   - Are applicable regulations, DOE directives, and industry standards (such as applicable National Fire Protection Association and American National Standards Institute standards) incorporated into the program?
   - Are the system design basis and supporting documents identified and consolidated in documentation consistent with DOE-STD-3024-2011, *Content of System Design Descriptions*?
   - Has the completed design been recorded in design output documents, such as drawings, specifications, test/inspection plans, maintenance requirements, and reports?
   - Does the documentation include system requirements, basis for the system requirements, essential performance criteria, and a description of how the current system configuration satisfies the specified requirements and performance criteria?
   - Do the bases for technical safety requirements (TSRs) for the system appropriately reflect assumptions of facility configuration and performance of safety functions, operational parameters, and key programmatic elements?
   - Have technical and administrative design interfaces been identified and methods been established for their control?
   - Is the safety classification of the system (or credited structures and components of the system) commensurate with the level of consequence and consistent with DOE guidance?
   - Have the design bases and design assumptions identified in the safety analysis been appropriately translated into design calculations and procedures?
   - Are acceptance criteria for tested parameters supported by calculations or other engineering documents to ensure that design bases assumptions are met?
   - Verify, by walkdown or other means, that system installed configuration will support system function under accident/event conditions.
   - Are operation and system alignments consistent with design basis assumptions?
   - Verify that all energy sources (e.g., electric power, diesel fuel, compressed air, etc.) relied on for accident mitigation, including those used for control functions, will be available and adequate during accident/event conditions.
   - Verify that potential/actual system degradation is monitored and/or prevented to ensure continued system functionality/operability.
   - Verify that safety related equipment is qualified for the environment expected under all conditions.
   - Verify that safety related equipment is adequately protected from natural external events.
   - Verify that safety margins have been maintained.

SS.2: Quality assurance practices and processes are implemented in a manner that ensures safety systems will conform to required standards and perform as designed.

Criteria:

1. Activities that may affect the safety of DOE nuclear facilities are conducted in accordance with a DOE-approved quality assurance program meeting the quality assurance criteria specified in 10 CFR 830.122. (10 CFR 830.122)
2. Appropriate consensus standards, such as ASME NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications,* and other applicable quality or management system requirements are clearly identified, integrated, and implemented for nuclear-related work activities. (10 CFR 830.121 and DOE Order 414.1D, Chg 1, *Quality Assurance*).
3. Requirements are established for procurement and verification of items and services. (10 CFR 830.122 Criterion 7)
4. Processes are established and implemented that ensure that approved suppliers continue to provide acceptable items and services. (10 CFR 830.122 Criterion 7)
5. Design interfaces are identified and controlled. (10 CFR 830.122 Criterion 6)

- Have safety structures, systems, and components been constructed and installed in accordance with applicable drawings and specifications?
- Has a program been established and implemented for control of suspect/counterfeit materials in accordance with DOE O 414.1D, Chg 1?
- Have qualified quality assurance personnel been involved in the preparation of work packages for construction, modification, or maintenance of safety related SSCs?
- Do work packages include appropriate hold points for inspections and/or tests during installation or maintenance activities?
- Are personnel performing inspections appropriately qualified?
- Do personnel performing inspections understand operational features, safety requirements, and performance criteria for the system?
- Are inspections sufficiently detailed to identify emergent conditions requiring corrective maintenance?
- Are conditions adequately evaluated to ensure the system is capable of performing its safety related functions?
- Are procurement processes defined within the site/facility quality assurance program and are provisions included for supplier qualification, receipt inspection, and document management?
- Did the CSE prepare/approve a formal equivalency determination for commercial procurement and commercial grade dedication of a safety related component?
- Are components and services procured for the system obtained in accordance with the site/facility quality assurance program?
- Are critical or important acceptance parameters and other requirements, such as inspection/test equipment or qualified inspection/test personnel, specified in design documentation?
- Are installation instructions and post-modification testing instructions and acceptance criteria appropriately specified?
- Are inspections and tests performed to verify that physical and functional aspects of items, services, and processes meet requirements and are fit for use and acceptance?
- Have quality assurance assessments been performed? Did the assessments include evaluation of quality of engineering products including calculations?
- Does the nonconformance reporting process include steps to screen dispositions (entry into the unreviewed safety question (USQ) process) that can result in changes in design, such as use-as-is and repair?

SS.3: Configuration management programs and processes are adequate to ensure safety systems continue to meet safety basis requirements and changes are properly controlled.

Criteria:

1. The configuration management process adequately integrates the elements of system requirements and performance criteria, system assessments, change control, work control, and documentation control. [DOE Order 413.3B, Chg 5, Attachment 1, DOE Order 420.1B Chapter V (or DOE O 420.1C as applicable to the facility), DOE O 430.1C, and DOE STD 1073-2016 if applicable].
2. Configuration management is used to develop and maintain consistency among system requirements and performance criteria, documentation, and physical configuration for the SSCs within the scope of the program. (DOE O 420.1B Chapter V (or DOE O 420.1C as applicable to the facility))
3. System design basis documentation and supporting documents are kept current using formal change control and work control processes. (DOE O 420.1B Chapter V (or DOE O 420.1C as applicable to the facility))
4. Systems must be tested following modification to ensure continued capability to fulfill system requirements. (DOE O 420.1B Chapter V (or DOE O 420.1C as applicable to the facility))
5. Applicable requirements and design bases are incorporated in design work and design changes. (10 CFR 830.122 Criterion 6)
6. Changes to system requirements, documents, and installed components are formally designed, reviewed, approved, implemented, tested, and documented.
7. A USQ process has been established and is being appropriately implemented to evaluate changes to safety systems. (10 CFR 830.203)
8. System P&ID's and/or single line diagrams, as appropriate, have been prepared, are maintained, and reflect the installed configuration of the associated safety system. (DOE-STD-1073-2016 Section 5.1)

    - Have as-built drawings and shop drawings been maintained after production to show actual configuration?
    - Are P&IDs available for operators and support personnel as necessary for day-to-day operations?
    - Are materials and installation of system components consistent with the requirements and performance criteria for the system, including quality controls and quality assurance and, as appropriate, software quality assurance?
    - Are system components properly labeled to assure proper configuration and operation?
    - Do identified discrepancies (i.e., system changes) potentially impact (1) the operability or reliability of the system; or (2) the adequacy of the change control or document control processes applied to the system (e.g., presence of unauthorized changes or failure to properly document authorized changes)?
    - Are documents affected by the changes appropriately identified?
    - Are changes accurately described and reviewed and approved, as appropriate?
    - Are SSCs affected by the changes identified by facility management, users, operators or others affected by the changes?
    - Do facility procedures ensure that changes to the system requirements, documents, and installed components are adequately integrated and coordinated with those organizations affected by the change?
    - Are changes to the system reviewed to ensure that system requirements and performance criteria are not affected in a manner that adversely impacts the ability of the system to perform its intended safety function?
    - Are installation instructions and post-modification testing instructions and acceptance criteria appropriately specified?

- Are safety basis and design documents affected by the change revised and kept current using formal change control and work control processes?
- Are new design calculations, tests, or procedures performed as necessary to support the change?
- Is there adequate evidence that the CSE has reviewed and concurred with design changes and the associated system modification work packages?
- Are engineering (including the design authority and technical disciplines), operations, and maintenance organizations made aware of system changes that affect them and appropriately involved in the change process?
- Are other organizations affected by the change such as training, document control, hazard analysis/safety basis, fire protection, etc., integrated into the change process?
- Have design changes been appropriately evaluated using the USQ process?

SS.4: Maintenance activities are properly planned, scheduled, and performed to ensure that safety systems can reliably perform intended safety functions when required.

Criteria:

1. The safety system is included in the nuclear facility maintenance management program and the DOE approved Nuclear Maintenance Management Plan required by DOE Order 433.1B, Chg 1.
2. Maintenance processes for the system are in place to accomplish corrective, preventive, and predictive maintenance and to manage the maintenance backlog; and the processes are consistent with the system's safety classification. (DOE O 433.1B, Chg 1, Attachment 2)
3. The system is periodically inspected in accordance with preventative maintenance requirements.
4. The reliability of the SSC is maintained through performance of vendor recommended preventative maintenance requirements.
5. Maintenance activities associated with the system, including work control, post-maintenance testing, material procurement and handling, and control and calibration of test equipment, are formally controlled to ensure that changes are not inadvertently introduced, the system fulfills its requirements, and that system performance is not compromised. (DOE O 420.1B, Chapter V (or DOE O 420.1C as applicable to the facility) and DOE O 433.1B, Chg 1, Attachment 2)

    - Does maintenance for the system satisfy system requirements and performance criteria in safety basis documents or other site maintenance requirements?
    - Does maintenance address age-related system degradation that could affect system reliability or performance?
    - Are conditions that require component replacement identified?
    - Is component aging incorporated into preventive maintenance?
    - Has the system been evaluated for potential inclusion of suspect/counterfeit parts?
    - Is there a DOE approved nuclear maintenance management program that addresses periodic inspection of components to determine whether degradation threatens performance?
    - Has the responsible DOE line management ensured that sufficient resources are budgeted in a timely manner to accomplish the maintenance program's objective of providing DOE with the highest confidence in the reliable performance of mission-critical, safety systems through proactive maintenance practices?
    - Does the nuclear facility maintenance program include condition assessments, prioritization of maintenance projects, management of deferred maintenance, analyses to determine optimal period for maintenance actions, and reporting results of condition assessments to DOE, as required by DOE O 433.1B, Chg 1?

- Has the responsible DOE line management ensured that the requirements and standards for maintenance of nuclear facilities are incorporated into contracts and subcontracts, including support services contracts, as appropriate?
- Are maintenance source documents such as vendor manuals, industry standards, DOE orders, and other requirements used as technical bases for development of system maintenance work packages?
- Are vendor recommended preventive and predictive maintenance requirements for the SSC included in the maintenance program?
- Are preventive and predictive maintenance activities completed as scheduled?
- Are predictive maintenance results used to identify and schedule maintenance prior to SSC failure?
- Is the system inspected periodically according to maintenance requirements and are deficient conditions evaluated and/or corrected?
- Are acceptance criteria defined and used for system modification, repair, maintenance and test activities?
- Are excessive component failure rates identified?
- Are failure rates used in establishing priorities and schedules for maintenance or system improvement proposals?
- Has preventive maintenance been performed as prescribed?
- Has the corrective maintenance backlog been effectively managed?
- Is there an accurate maintenance history that compiles maintenance, resource, and cost data in a system which is retrievable and capable of entering required-maintenance costs, actual maintenance costs, and availability data and failure rates for mission-critical and safety systems into the DOE Facility Information Management System?
- Have worker qualification requirements been established in accordance with applicable industry standards and have these requirements been met?

SS.5: Surveillance and testing activities are properly performed in accordance with TSR Surveillance Requirements and Specific Administrative Controls.

Criteria:

1. Requirements relating to test, calibration, or inspection assure: that the necessary operability and quality of safety structures, systems, and components is maintained; that facility operation is within safety limits; and that limiting control settings and limiting conditions for operation are met. (10 CFR 830 Subpart B, Appendix A, Paragraph G)
2. System instrumentation and measurement and test equipment are calibrated and maintained. (10 CFR 830.122 Criterion 8)

- Does surveillance and testing of the system demonstrate that all required components within the system are capable of accomplishing their safety functions and continue to meet applicable system requirements and performance criteria?
- Do surveillance and test procedures confirm that key operating parameters for the overall system and its major components remain within safety basis and operating limits?
- Does the procedure contain instructions to perform the test successfully and assure validity of test results?
- Can parameters that demonstrate compliance with the safety basis be measured or physically verified?
- Does the system design include provisions necessary for conducting the tests?
- Are personnel knowledgeable and able to satisfactorily perform the test?

- Does the procedure cite applicable safety requirements?
- Are limits, precautions, system and test prerequisite conditions, data required, and acceptance criteria included?
- Are appropriate data recording provisions included or referenced and used to record results?
- Does the procedure include provisions for listing discrepancies?
- Does the procedure require timely notification to facility management about any failure or discrepancy that could impact operability?
- Did appropriate personnel review the test results and take appropriate action?
- Is there a clear linkage between the test acceptance criteria and the safety documentation, and are the acceptance criteria capable of fully confirming that safety/operability requirements are satisfied?

SS.6: Operations are conducted in a manner that ensures the safety systems are available to perform intended safety functions when required.

Criteria:

1. The operator must establish and implement operations practices to ensure that shift operators are alert, informed of conditions, and operate equipment properly. (DOE O 422.1, Chg 2, *Conduct of Operations*, Attachment 2)
2. The operator must establish and implement operations practices for developing and maintaining accurate, understandable written technical procedures that ensure safe and effective facility and equipment operation. (DOE O 422.1, Chg 2, *Conduct of Operations*, Attachment 2)
3. The operator must establish and implement operations practices for initial equipment lineups and subsequent changes to ensure facilities operate with known, proper configuration as designed. (DOE O 422.1, Chg 2, *Conduct of Operations*, Attachment 2)
4. Operator training must be sufficiently comprehensive to cover areas which are fundamental to the operator's assigned tasks to ensure that personnel are capable of safely performing their job duties. The training program must include a core of subjects; such as instrumentation and control and major facility systems, as applicable to the facility and position. (DOE O 426.2, Chg 1, Attachment 1, Chapter II.6)
5. The training program must include on-the-job and classroom training to ensure personnel are familiar with all aspects of their positions; including but not limited to: normal and emergency procedures, administrative procedures, location and function of pertinent safety systems and equipment, and TSRs. (DOE O 426.2, Chg 1, Attachment 1, Chapter II.6)
6. Formal processes have been established to control safety system equipment and system status to ensure proper operational configuration control is maintained. (DOE O 422.1, Chg 2, *Conduct of Operations*, Attachment 2)

    - Is the system operated in accordance with the system design?
    - Are personnel trained and qualified to ensure they are capable of performing their assigned work?
    - Are personnel provided continuing training to ensure that job proficiency is maintained?
    - Does training reflect system modifications?
    - Can the procedures be performed as written?
    - Does the procedure change process evaluate the need for training on the changes and is there an appropriate administrative program to manage the training (e.g., required reading) process?
    - Are components and equipment accessible for normal and emergency conditions?
    - If special equipment is required to perform procedures or operations, is the equipment available and in good working order?

- Is the knowledge level of the operator(s) adequate concerning equipment location and operation?
- Are system operations associated with the system(s) selected consistent with the control of equipment and systems status requirements of the site's Conduct of Operations program?
- Are shift routines and operation practices associated with the system(s) selected consistent with requirements of the site's Conduct of Operations program?
- Are the Operator Aid and component label programs for the system compliant with the site Conduct of Operations program?
- Is the operational configuration of safety system components including supporting systems and equipment properly maintained?
- Is the indication available to operate the equipment in accordance with applicable operating procedures and instructions?
- For accident conditions, are the environmental condition assumptions adequate for remote operation of the equipment?
- Are support systems and procedures adequate to support the system during event sequences when the system is designed to initiate?
- Are operations personnel trained on procedure use, proper system response, failure modes, and required actions involved in credible accident scenarios in which the system is required to function?
- Are operations personnel knowledgeable of system design and performance requirements in accordance with the facility safety basis?

SS.7: Cognizant System Engineer Program implementation is effective in ensuring safety systems can reliably perform as intended.

Criteria:

1. The DOE contractor has established a system engineer program to ensure continued operational readiness of systems within the program scope. (DOE O 420.1B Chapter V (or DOE O 420.1C as applicable to the facility))
2. The System Engineer Program must be applied to active safety class and safety significant SSCs as defined in the facility's DOE approved safety basis, as well as to other active systems that perform important defense-in-depth functions, as designated by facility line management. (DOE O 420.1B Chapter V.2 (or DOE O 420.1C as applicable to the facility))
3. Hazard category 1, 2, and 3 nuclear facilities must have a System Engineer Program, as well as a qualified CSE assigned to each system within the scope of the Program. (DOE O 420.1B Chapter V.3 (or DOE O 420.1C as applicable to the facility))

- Are CSE qualification and training requirements adequately defined and implemented?
- Does CSE training include knowledge of facility and system safety basis, applicable codes and standards for design and maintenance, failure modes and effects analysis, root-cause analysis, performing periodic system walk-down and reviews, and preparing system health reports?
- Is an appropriately qualified and experienced CSE assigned to each system within the scope of the program?
- Are CSE functions, responsibilities and authorities clearly defined?
- Are CSEs familiar with system's engineering documents (e.g., drawings, calculations, system design descriptions), maintenance and procurements activities, surveillance tests, vendor manuals, and with existing system condition and performance?
- Do CSEs provide technical support for operations and maintenance through the activities described in DOE O 420.1B (or DOE O 420.1C as applicable to the facility), including review of design changes, ensuring effective configuration management, identifying trends in key system

parameters from operations and surveillances, determining operability, performing analysis of problems, and initiating corrective actions?
- Is system configuration formally controlled and managed to develop and maintain consistency among system requirements and performance criteria, documentation, and physical configuration of the system?
- Do system assessments include periodic reviews of system operability, reliability, and material condition?
- Do system assessments include appropriately qualified experts in the necessary engineering and other disciplines?
- Do the detailed and comprehensive assessments include an evaluation of the system design as well as maintenance and operation?
- Are system engineers trending safety system performance?

SS.8: Federal safety oversight programs are established and effective in ensuring safety systems can reliably perform as intended.

Criteria:

1. All applicable DOE organizations must: (1) Establish and implement an effective oversight program consistent with DOE P 226.1B and the requirements of this Order, and (2) Maintain sufficient technical capability and knowledge of site and contractor activities to make informed decisions about hazards, risks, and resource allocation; provide work direction to contractors; and evaluate contractor performance. (DOE O 226.1B Section 4)
2. The DOE site office has established and implemented an effective Safety System Oversight (SSO) program for qualifying staff to apply engineering expertise in its oversight of the assigned safety systems and to monitor performance of the contractor's CSE program. (DOE O 426.1A Appendix C)

    - Has DOE line management established and implemented effective processes for monitoring and assessing contractor programs for ensuring effective design, configuration management, maintenance, and operation of safety systems?
    - Has DOE line management included the review of safety systems in the evaluation and approval of the startup and restart of nuclear facilities and activities?
    - Has the SSO program established appropriate training, qualification, and performance requirements for SSO personnel?
    - Are SSOs appropriately trained and qualified to perform their assigned duties?
    - Is an appropriately qualified and experienced SSO staff member assigned to each safety system?
    - Has the site office developed an adequate plan and schedule for periodic assessments of all the safety systems at different nuclear facilities within its purview?
    - Are the functions, roles, and responsibilities of SSO personnel clearly defined?
    - Do SSO personnel perform periodic assessments of system performance, equipment configuration, and material condition of assigned systems?
    - Are SSO findings adequately tracked and resolved?
    - Do SSO personnel assess contractor's CSE program to ensure operability, reliability, material condition, and performance of the assigned safety systems?
    - Has the site office established formal plans for safety system oversight? Is safety system oversight implemented in accordance with these procedures?
    - Is site office oversight of the safety system activities effective in identifying and correcting deficient conditions?
    - Do site office safety system oversight personnel and/or facility representatives ensure that operations are consistent with the safety basis document?

SS.9: Feedback and improvement processes are effective in addressing and preventing the recurrence of safety system issues.

Criteria:

1. Identify the causes of problems and work to prevent recurrence as a part of correcting the problem. (10 CFR 830.122 Criterion 3)
2. Contractors must monitor and evaluate all work performed under their contracts to ensure work performance meets the applicable requirements for environment, safety, and health; including quality assurance, integrated safety management, safeguards and security, cyber security, and emergency management. (DOE O 226.1B, Attachment 1)

- Does the contractor assurance system include engineering, configuration management, maintenance, surveillance and testing and operations assessment activities and engineering performance indicators/measures for safety systems?
- Has the contractor's assurance system monitored and evaluated engineering, configuration management, maintenance, surveillance and testing, and operations work performed for safety systems?
- Are performance indicators/measures effectively utilized in identifying performance trends and potential problems, allocating resources, and applying lessons learned and good practices?
- Do contractor personnel responsible for managing and performing engineering, configuration management, maintenance, surveillance and testing, and operations assurance activities possess training, experience, knowledge, skills, and abilities commensurate with their responsibilities?
- Are formal processes are in place and effectively implemented to identify and analyze (engineering, configuration management, maintenance, surveillance and testing, and operations) problems and issues; including operational events?
- Are processes in place to identify, track, monitor, and close corrective actions; to verify the effectiveness of corrective actions; to identify lessons learned from external and internal sources; to disseminate lessons learned to appropriate personnel; and to ensure that lessons learned are understood and applied?
- Have formal programs and processes been established and effectively implemented to solicit feedback from workers and work activities on the effectiveness of engineering, configuration management, maintenance, surveillance and testing and operations, and to apply lessons learned?
- Are the results of engineering, configuration management, maintenance, surveillance and testing, and operations assurance processes for safety systems periodically analyzed, compiled and, as appropriate, reported or available to DOE line management as part of contract performance evaluation?
- Have rigorous assessments of engineering, configuration management, maintenance, surveillance and testing and operations processes and their implementation been performed and appropriate corrective actions implemented?
- Have these assessments identified deficiencies and opportunities for improvement? If so, have they been formally tracked and corrected?
- Was an effectiveness review performed of the corrective actions? Have any repeat problems been identified subsequent to completion of the corrective action?
- Has the contractor defined the requirements for experience, knowledge, skills, and abilities for personnel implementing contractor assurance system elements for engineering, configuration management, maintenance, surveillance and testing and operations?
- Has the contractor provided and ensured completion of training for personnel in engineering, configuration management, maintenance, surveillance and testing and operations organizations related to corrective action program(s)? Did the training address the critical aspects of a

corrective action program, including: clearly stated management expectations; initiation process; low initiation threshold; assignment of significance level to a deficiency; requirements to evaluate the impact on operability, reportability, and extent of condition for all deficiencies; requirements to perform a full root cause analysis for a significance deficiency; and feedback to the initiators

- Are events related to engineering, configuration management, maintenance, surveillance and testing and operations of safety systems investigated in accordance with formal programs and processes that identify issues, properly analyze, and report as required by directives?
  - Were the root causes and corrective actions for the system properly identified and characterized?
- Are corrective action plans for various system deficiencies being properly tracked such that responsible individuals can ensure timely resolution of issues and completion of actions?
- Did the corrective actions include training on the changes made and was the training adequately completed prior to placing the system in operation?
- Are there recurring problems or deficiencies in the system? If so why haven't corrective actions been effective?
- Have subcontractors performing engineering work implemented appropriate and effective self-assessment programs and is the contractor's subcontractor oversight program effectively evaluating performance, providing feedback to subcontractors, and ensuring correction of process and performance deficiencies?
- Are assessment activities sufficiently performance based, including an appropriate focus on observation of engineering, maintenance, surveillance and testing and operations work, inspection of field conditions, and review of evidence of compliant and effective performance?
- Are there effective mechanisms for soliciting, reviewing, resolving, and addressing concerns, comments, and suggestions from engineering and other workers?
- Have the appropriate performance indicators and parameters been selected to effectively measure performance and identify adverse trends in a timely manner to ensure prompt mitigation and corrective actions?
- Is the performance indicator program periodically reviewed to ensure the most appropriate sets of data and data analysis parameters are being employed?
- Is performance data being sufficiently analyzed, with conclusions drawn and presented to management, and needed actions identified and taken?
- Are findings related to safety system functionality from previous Independent Oversight appraisal activities effectively corrected?

APPROACH

Record Review:

- Safety basis documents, system design descriptions and supporting documents (e.g., system diagrams, pipe and instrumentation drawings, calculations).
- Documentation related to selected design modifications.
- USQ process procedure(s) and the results of USQ evaluations.
- Engineering and configuration management processes and procedures, particularly those supporting technical product development, design changes, and document control.
- Maintenance records, plans, and schedules for aging system equipment and components.
- Maintenance work backlogs and deferrals.
- Vendor manuals, industry standards, DOE orders, and other requirements used as technical bases for development of system maintenance work packages
- System or component history files for selected system components for the past three years.
- Procedure and process for performing inspections of the system, including interviews with personnel performing the inspections.

- Procurement processes and records for system components and services.
- Surveillance and/or testing procedures and the supporting DSA TSRs and bases for the system and major components and a sample of the test results.
- System alarm response procedures and operating procedures for normal, abnormal, and emergency system operations.
- Operator training for the system, focusing on the technical completeness and accuracy of the training manual and lessons plans.
- Contractor's system engineering program description and procedures.
- CSE training and qualifications requirements.
- CSE system notebook/logs, system health reports, system assessment reports, and observations/findings from oversight activities.
- System modification, maintenance, and procurement work packages.
- Sample database records of system deficiencies, problems, engineering issues, and corrective actions.
- DOE site office's SSO program description and SSO training and qualification requirements.
- Previous and present oversight assessment plans and schedules of planned surveillance and assessment activities.
- Surveillance and assessment reports prepared by SSO personnel.
- Follow-up on sample SSO findings to ascertain how they are tracked and resolved.
- Engineering, configuration management, maintenance, surveillance and testing and operations assessment program descriptions, procedures, instructions, guidance, and contractual requirements.
- Assessment activity schedules for independent, management, and other self-assessments and external reviews/inspections of engineering, configuration management, maintenance, surveillance and testing and operations.
- Self-assessments, independent assessments, causal analyses, corrective action plans, lesson-learned documents, Price-Anderson Amendment Act notifications and corrective action plans, close-out reviews as they relate to the requirements and functions of the system(s) selected for review and/or other safety systems if appropriate.
- Documentation related to engineering, configuration management, maintenance, surveillance and testing and operations deficiencies (e.g., critique minutes, causal analyses and corrective action plans, verification/validation records, and effectiveness determinations).
- Corrective actions which were initiated by engineering, configuration management, maintenance, surveillance and testing and operations organizations as a result of normal daily activities and based on CSE reviews.
- Trend analysis and performance indicator reports.
- Assignment of significance level (priority) to deficiencies by facility management.
- Sample of corrective actions covering deficiencies identified in assessments, daily activities and CSE reviews.
- Sample of corrective actions taken in response to previous Independent Oversight appraisal activities.
- Training and qualification records for personnel performing assessments of engineering, configuration management, maintenance, surveillance and testing and operations.
- Documented Safety Analysis
- Technical Safety Requirements

<u>Interviews:</u>

- CSEs who support the facility
- Surveillance and testing personnel
- Design Engineers
- Engineering Management
- SSO personnel

- Configuration management subject matter expert
- Maintenance Manager
- Maintenance supervisors
- Maintenance Personnel
- Operations personnel
- Facility Manager

Observations:

- Selectively walk down system equipment and components and compare the actual physical installation of the system to documentation of the system design and safety basis; review safety component and services procurement programs (including the quality assurance program) and sample procurement packages.
- Walk-through of the surveillance test procedures with appropriate facility personnel (e.g., test technicians, engineers, operations personnel).
- Walk-through the system operating procedures and the system piping and instrumentation drawings with the operator(s). Conduct walk-throughs to validate the proper configuration of valves, breakers, and other safety system components.
- Local operation of system equipment.
- Walk down assigned systems with SSO.
- Normal maintenance activities.