		Number: EA CRAD 30-11 Revision: 0 Effective Date: February 2, 2023
Safety Systems Management Review Criteria Review and Approach Document		
Authorization and Approval	Kevin G. Kilp Digitally signed by Kevin G. Kilp Date: 2023.02.02 16:48:39 -05'00' Kevin G. Kilp, Director Office of Environment, Safety and Health Assessments	Thomas E. Sowinski Digitally signed by Thomas E. Sowinski Date: 2023.02.02 16:22:05 -05'00' Thomas E. Sowinski, Lead Nuclear Engineer Office of Nuclear Safety and Environmental Assessments

1.0 PURPOSE

The mission of the U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments (EA-30) is to assess the effectiveness of safety and emergency management systems and practices used by line and contractor organizations and to provide clear, concise, rigorous, and independent evaluation reports of performance in protecting workers, the public, and the environment from the hazards associated with DOE activities.

In addition to the general independent oversight requirements and responsibilities specified in DOE Order 227.1A, *Independent Oversight Program*, this criteria and review approach document (CRAD), in part, fulfills the responsibility assigned to the Office of Enterprise Assessments (EA) in DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*, to conduct independent oversight and appraisals of high consequence activities. This CRAD specifically provides objectives, criteria, and review approaches to assess the effectiveness of safety systems management programs and processes.

EA CRADs are available to DOE line and contractor assessment personnel to aid them in developing effective DOE oversight, contractor self-assessment, and corrective action processes.

The current revision of EA's CRADs are available at:
https://www.energy.gov/ea/criteria-and-review-approach-documents

This CRAD supersedes EA CRAD 31-15, Revision 1.

2.0 APPLICABILITY

The following CRAD is approved for use by the Office of Environment, Safety and Health Assessments (EA-30) and sub-tier offices.

3.0 FEEDBACK

Comments and suggestions for improvements on this CRAD can be provided to the Director, Office of Environment, Safety and Health Assessments.

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 (QA), configuration management, surveillance testing, maintenance, operations, cognizant system engineer (CSE) and safety system oversight (SSO), feedback and improvement, and adherence to safety basis requirements 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 area objectives 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 incorporate applicable safety design bases such that adequate protection of the public, the workers, and the environment from facility hazards is demonstrated. (10 Code of Federal Regulations (CFR) 830.122, DOE Order (O) 420.1C)

Criteria:

1. Engineered structures, systems, and components (SSCs) and processes are designed in accordance with the approved quality assurance program (QAP) using sound engineering/ scientific principles and appropriate standards, including those invoked in site-specific contracts. (10 CFR 830.122, criterion 6)
2. Engineering design incorporates applicable requirements from consensus standards and the safety design bases into design work and design changes (e.g., design calculations) as described in the QAP. (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 as described in the QAP. (10 CFR 830.122, criterion 6)
4. Verification and validation work is completed before approval and implementation of the design as described in the QAP. (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 420.1C, chapter V)

Lines of Inquiry:

- 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 Standard (STD) 3024-2011?
- 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 the system's technical safety requirements (TSRs) appropriately reflect the facility configuration and performance of safety functions, operational parameters, and key programmatic elements as incorporated into the facility and SSC designs?
- Have technical and administrative design interfaces been identified and methods been established for their control?
- 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?
- Does the installed system configuration support system function under accident/event conditions?
- Are operation and system alignments consistent with the design?
- Are all energy sources (e.g., electric power, diesel fuel, compressed air, etc.) relied on for accident mitigation, including those used for control functions, available and adequate for accident/event conditions?
- Is potential/actual system degradation monitored and/or prevented to ensure continued system functionality/operability?
- Is safety related equipment qualified for the environment expected under all conditions?
- Is safety related equipment adequately protected from natural external events?
- Are safety margins adequately 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. (10 CFR 830.121, DOE O 414.1D)

Criteria:

1. Activities that may affect the safety of DOE nuclear facilities are conducted in accordance with a DOE-approved quality assurance program (QAP) meeting the quality assurance criteria specified in 10 CFR 830.122. (10 CFR 830.121)
2. Appropriate consensus standards, such as American Society of Mechanical Engineers 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, DOE O 414.1D)
3. Requirements are established for procurement and verification of items and services. (10 CFR 830.122, criterion 7)
4. Processes are established and implemented to select suppliers based on specified criteria and ensure approved suppliers continue to provide acceptable items and services. (10 CFR 830.122, criterion 7)
5. Design interfaces are identified and controlled as described in the QAP. (10 CFR 830.122, criterion 6)

Lines of Inquiry:

- Has the site assigned and maintained the appropriate quality level for credited SSCs considering their safety significance (e.g., whether the SSC is credited as safety class or safety significant in the safety basis)?
- Have safety structures, systems, and components been procured, constructed/installed, and maintained in accordance with applicable drawings, specifications, and the assigned quality level?
- Has a program been established and implemented for control of suspect/counterfeit materials in accordance with DOE O 414.1D?
- 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 and the quality level assigned to the selected SSCs?
- 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. (DOE O 420.1C, attachment 2, chapter V)

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 O 413.3B, attachment 1; DOE O 420.1C, attachment 2, chapter V; 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 420.1C, attachment 2, chapter V)
3. System design basis documentation and supporting documents are kept current using formal change control and work control processes. (DOE O 420.1C, attachment 2, chapter V)
4. Systems are tested following modification to ensure continued capability to fulfill system requirements and functional requirements/criteria identified in the safety basis. (DOE O 420.1C, attachment 2, chapter V)
5. Applicable requirements and design bases are incorporated in design work and design changes as described in the QAP. (10 CFR 830.122, criterion 6)
6. Changes to system requirements, documents, and installed components are formally designed, reviewed, approved, tested, implemented, and documented in a timely manner. (DOE-STD-1073-2016, section 5.0)
7. A USQ process has been established and is being appropriately implemented to evaluate changes to safety systems. (10 CFR 830.203)
8. System piping and instrumentation drawings (P&IDs) 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)

Lines of Inquiry:

- 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 before the change is implemented and kept current in a timely manner 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. (DOE O 433.1B)

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.
2. Maintenance processes for the system are in place to accomplish corrective, preventative, and predictive maintenance and to manage the maintenance backlog; and the processes are consistent with the system's safety classification. (DOE O 433.1B, attachment 2)
3. The system is periodically inspected in accordance with preventative maintenance requirements. (DOE O 433.1B, DOE Guide (G) 433.1-1A)
4. The reliability of the SSC is maintained through consideration and performance of vendor recommended preventative maintenance requirements. (DOE O 433.1B, DOE G 433.1-1A)
5. System maintenance, repair, and modification activities, 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 420.1C, DOE O 433.1B, attachment 2)

Lines of Inquiry:

- 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?
- 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. (10 CFR 830, subpart B, appendix A)

Criteria:

1. Requirements relating to test, calibration, or inspection assure that the necessary operability and quality of safety SSCs 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)

Lines of Inquiry:

- 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. (DOE O 422.1)

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, attachment 2, paragraph 2.b)
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, attachment 2, section 2.p)
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, attachment 2, section 2.h)
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, 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, 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, attachment 2, section 2.h)

Lines of Inquiry:

- 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's 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 (CSE) program implementation is effective in ensuring safety systems can reliably perform as intended. (DOE O 420.1C, chapter V)

Criteria:

1. The DOE contractor has established a CSE program to ensure continued operational readiness of systems within the program scope. (DOE O 420.1C, chapter V)
2. The CSE 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 420.1C, chapter V.2)
3. Hazard category 1, 2, and 3 nuclear facilities must have a cognizant system engineer program, as well as a qualified CSE assigned to each system within the scope of the program. (DOE O 420.1C, chapter V.3)

Lines of Inquiry:

- 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, 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, material condition, aged-related degradation, and obsolescence?
- 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: Feedback and improvement processes are effective in addressing and preventing the recurrence of safety system issues. (10 CFR 830.122, DOE O 226.1B)

Criteria:

1. DOE and its contractors 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)

Lines of Inquiry:

- Does the contractor assurance system include periodic assessments and performance indicators/measures of systems engineering, configuration management, maintenance, surveillance and testing, and operations for credited safety systems?
- Are the results of contractor safety system assessments (including deficiencies and opportunities for improvement) effectively analyzed, tracked, corrected, and, as appropriate, made available to DOE line management?
- Are findings and/or deficiencies related to safety system functionality from previous independent oversight appraisal activities appropriately handled in the issues management process?
- Are performance indicators/measures effectively utilized in identifying and resolving performance trends and potential problems, allocating resources, and applying lessons learned and good practices?

- Does the contractor have defined training programs to ensure personnel responsible for managing and performing safety system quality assurance activities possess the knowledge, skills, and abilities commensurate with their responsibilities?
- Does the contractor provide and ensure completion of corrective action program(s) training for personnel in engineering, configuration management, maintenance, surveillance and testing, and operations organizations?
- Are formal processes in place and effectively implemented to identify, characterize, monitor, close, and verify the effectiveness of corrective actions?
- Are corrective action plans for system deficiencies scheduled and properly tracked to ensure timely resolution?
- Do corrective actions ensure, as appropriate, that training on changes made to safety systems is effectively provided and completed prior to resuming operations?
- Are effectiveness reviews adequately performed for corrective actions to reduce repeat issues?
- Have formal programs and processes been established and effectively implemented to solicit feedback from employees, identify lessons learned from internal and external sources, disseminate lessons learned to appropriate personnel, and ensure that lessons learned are understood and applied?
- Are events related to engineering, configuration management, maintenance, surveillance and testing, and operations of safety systems investigated in accordance with formal programs and processes, properly analyzed to identify issues leading to the event, and reported as required by directives?
- Do subcontractors implement effective self-assessment programs and does the contractor's subcontractor oversight program effectively evaluate performance, provide feedback to subcontractors, and ensure correction of process and performance deficiencies?

SS.9: Active safety systems, as defined in the facility's approved safety basis, have been evaluated/demonstrated to be capable of fulfilling their required safety functions for all required operating and accident conditions. (10 CFR 830, subpart B)

Criteria:

1. The DSA derives the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrates the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and defines the process for maintaining the hazard controls current at all times and controlling their use. (10 CFR 830.204(b)(4))
2. Safety analyses are used to: (1) identify safety class and safety significant SSCs needed to fulfill the safety functions in order to prevent and/or mitigate design basis accidents (DBAs), including natural and man-induced hazards and events and (2) identify the safety functional requirements of the safety class and safety significant SSCs. (DOE O 420.1C, chapter I, sections 3.a.(2)(a) & (b))
3. Safety SSCs require formal definition of minimum acceptable performance in the DSA. TSRs are developed to ensure the operability of the safety SSCs and define actions to be taken if an SSC is not operable. (10 CFR 830, appendix A to subpart B, section G.3)
4. 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. (DOE O 420.1C, attachment 3, section 3)
5. Facilities must be designed, constructed, maintained, and operated to ensure that SSCs will be able to perform their intended safety functions effectively under the combined effects of natural phenomena hazards and normal loads defined in the applicable building codes contained in facilities' codes of record. (DOE O 420.1C, chapter IV, section 3.a)

Lines of Inquiry:

- Are the selected hazard controls, both individually and collectively, adequate to prevent or mitigate the accidents for which they are credited as controls?
- Does the DSA selection of hazard controls follow the principles associated with the hierarchy of controls? When the hierarchy of controls is not used, does the DSA provide a technical basis that supports the control selection?
- Do the selected safety controls provide multiple layers of protection to prevent or mitigate the unintended release of radioactive materials?
- Does the DSA document the basis for determining the safety SSCs and their required functions based on a proper assessment of the unmitigated accident consequences?
- Have the boundaries, interfaces, and support systems, including all components needed for the SSC to perform its required safety function(s), been defined?
- Have components whose failure would result in a safety SSC losing the ability to perform its required safety function been appropriately identified and evaluated?
- Have the performance criteria developed for the SSCs been demonstrated to be adequate to ensure that the required safety functions will be met for all required normal and abnormal/accident conditions?
- Are the required operating ranges and limits for safety SSCs and associated instrumentation identified?
- Where the single failure design criteria are applicable, does the design of the SSC ensure that single failure does not result in the loss of capability to accomplish its required safety functions?
- If all components of SSCs that implement both safety and non-safety functions are not treated as safety SSCs, has it been demonstrated that the safety and non-safety functions are sufficiently independent that the failure of any non-safety component does not result in the failure of the SSC to perform its safety function(s)?
- Have the assumptions requiring TSR coverage and the bases for deriving TSRs been described consistent with the logic presented in the safety analyses?
- Is there sufficient information provided to identify the safety limits (SLs), limiting control settings (LCSs), and limiting conditions for operation (LCO) that will be needed to support the facility TSR documentation and derive surveillance requirements (SRs) to maintain operation of the facility within SLs, LCSs, and LCOs?
- Have the facility operational modes relevant to derivation of TSRs been adequately defined such that the status of safety SSCs can be distinctively defined?
- Are the LCO derivations sufficient to demonstrate that the SSC is capable of performing its credited safety function(s) for all required conditions?
- Are the LCO surveillance requirements sufficient to demonstrate that the required performance criteria are met?
- Are the requirements relating to testing, calibration, or inspection sufficient to assure that the necessary operability and quality of safety SSCs is maintained?

REVIEW APPROACH (<u>tailored to the scope of the specific assessment</u>):

<u>Record Review:</u>

- 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, the supporting DSA TSRs and bases for the system and major components, and a sample of 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.
- 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, lessons-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

Interviews:

- CSEs who support the facility
- Surveillance and testing personnel
- Design engineers
- Engineering management
- Configuration management subject matter expert
- Maintenance Manager
- Maintenance supervisors
- Maintenance personnel
- Operations personnel
- Facility Manager
- Nuclear Safety Manager
- Nuclear safety analysts

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.
- Normal maintenance activities.