Office of Enterprise Assessments
Lessons Learned from Assessment of Engineering Process at U.S. Department of Energy Nuclear Facilities

August 2017

Office of Nuclear Safety and Environmental Assessments
Office of Environment, Safety and Health Assessments
Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Acronyms ii

Executive Summary iii

1.0 Introduction 1

1.1 Background 1
1.2 Scope and Methodology 2
1.3 Requirements and Guidance 4

2.0 Overall Assessment 4

2.1 Engineering Processes 4
2.2 Technical Baseline 6
2.3 Engineering Configuration Management 7
2.4 Cognizant System Engineer Programs 9
2.5 Issues Management 11
2.6 DOE Field Element Oversight of Contractor Engineering Programs 13
2.7 Occurrence Reporting and Processing System (ORPS) Data Analysis 14

3.0 Summary of Results 15

3.1 Best Practices 15
3.2 Recommendations 16

Appendix A: Supplemental Information A-1

Appendix B: Source Documents B-1

Acronyms

CFR	Code of Federal Regulations
CRAD	Criteria and Review Approach Document
CSE	Cognizant System Engineer
DOE	U.S. Department of Energy
EA	DOE Office of Enterprise Assessments
HSS	DOE Office of Health, Safety and Security
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
OAR	Operational Awareness Report
ORPS	Occurrence Reporting and Processing System
SDD	System Design Description
SHR	System Health Report

Office of Enterprise Assessments
Lessons Learned from Assessment of Engineering Process at
U.S. Department of Energy Nuclear Facilities

EXECUTIVE SUMMARY

The U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments, within the Office of Enterprise Assessments (EA), conducted assessments at selected DOE nuclear facilities between 2013 and 2016 that examined, in part, engineering aspects of contractor performance at DOE nuclear facilities. The nuclear facilities were selected based on risk and included facilities under the direction of the Office of Nuclear Energy, the Office of Environmental Management, and the National Nuclear Security Administration. The objective of each assessment was to determine whether the design, as implemented, was adequate to ensure that the safety system or facility could reliably perform its intended role in protecting workers, the public, and the environment from hazards arising from postulated events and natural phenomena.

In developing this report, EA also extracted findings and observations related to the conduct of engineering from other EA assessment reports to create a summary of contractor and DOE field element performance. This lessons learned report focuses on issues that affect multiple sites and/or facilities and identifies both best practices and areas of weakness, with the goal of promoting organizational learning and improving performance.

Best practices were noted, in particular, on large construction projects that typically have strong engineering processes and supplemental measures in place to track design requirements and commitments. Some operating sites exhibited particularly strong cognizant system engineer programs, with effective system health reporting and investments in development of system notebooks that act as repositories of technical and vendor information. Some sites were also found to have strong configuration management programs with effective use of document control software capabilities.

While contractor engineering performance varied substantially from site to site, contractor engineering programs at operating facilities and construction projects are generally adequate. EA observed some weaknesses and areas for improvement as outlined below. Process issues were the dominant challenges for those programs considered to be most problematic. Weaknesses include:

- Inadequate controls for calculations, including guidance for issuance, design verification, and control of open items (e.g., missing vendor information)
- Calculation errors, including math errors, incorrect assumptions, and misapplication of industry standards
- Poor document control practices, including over-reliance on hardcopy documents and drawings and insufficient controls on document submittal
- Inadequate design change control, as evidenced by omissions in issued design change documentation, missing technical justification, and discrepancies between design basis documents and as-built configuration
- Ineffective issues management, as evidenced in several reviews by findings and deficiencies left uncorrected, problems only partially addressed, and inadequate recurrence control. This observation indicates weaknesses in the implementation of site contractor assurance programs.

A review of records from the Occurrence Reporting and Processing System for the timeframe covered in this report identified issues similar to those that EA noted in the areas of design output, calculations, and configuration management.

The weaknesses in contractor engineering programs described above are recommended as areas for consideration in assessment planning by the field elements. Enhanced oversight activities in these areas could be effective in improving contractor performance

Consistent with its responsibilities as defined in DOE Order 227.1, EA also concluded that lack of published DOE requirements for the conduct of engineering at DOE nuclear facilities may contribute to the problems with contractor engineering program effectiveness and consistency noted above, and hinder DOE field element oversight activities. Development of minimum performance standards for engineering processes and products would set clear expectations and may encourage significant improvement in contractor engineering performance at some DOE sites.

Office of Enterprise Assessments
Lessons Learned from Assessment of Engineering Process at
U.S. Department of Energy Nuclear Facilities

1.0 INTRODUCTION

The U.S. Department of Energy (DOE) Office of Environment, Safety and Health Assessments, within the Office of Enterprise Assessments (EA), conducted assessments at selected DOE nuclear facilities between 2013 and 2016 that examined, in part, engineering aspects of contractor performance at DOE nuclear facilities. The nuclear facilities were selected based on risk and included facilities under the direction of the Office of Nuclear Energy, the Office of Environmental Management, and the National Nuclear Security Administration. The objective of each assessment was to determine whether the design, as implemented, was adequate to ensure that the safety system or facility could reliably perform its intended role in protecting workers, the public, and the environment from hazards arising from postulated events and natural phenomena.

In developing this report, EA also extracted findings and observations related to the conduct of engineering from other EA assessment reports to create a summary of contractor and DOE field element performance. This lessons learned report focuses on issues that affect multiple sites and/or facilities and identifies both best practices and areas of weakness, with the goal of driving organizational learning.

1.1 Background

EA manages the Department's independent oversight program. This program is designed to enhance DOE safety and security programs by providing the Secretary and Deputy Secretary of Energy, Under Secretaries of Energy, other DOE managers, senior contractor managers, Congress, and other stakeholders with an independent evaluation of the adequacy of DOE policy and requirements, and the effectiveness of DOE and contractor line management performance and risk management in safety and security and other critical functions as directed by the Secretary. The DOE independent oversight program is described in and governed by DOE Order 227.1, *Independent Oversight Program*. EA implements the program through a comprehensive set of internal protocols and assessment guides.

DOE Order 227.1 states that:

> *Independent Oversight appraisals must be prioritized on areas of greatest potential risks and implemented in a manner that supports DOE line management in accomplishing its line management oversight and achieving DOE mission objectives safely and securely. Higher priority and greater emphasis is placed on conducting Independent Oversight appraisals of high consequence activities, such as nuclear project design, construction and commissioning; high hazard nuclear operations;…*

EA accomplishes this portion of its mission by conducting technical assessments designed to provide assurance that contractor organizations are appropriately implementing the approved facility safety bases in a manner that is compliant with DOE requirements and applicable national consensus standards. The organization must have a technical baseline in place to demonstrate that safety-related structures, systems, and components will perform as required when challenged by postulated accidents, hazards, and natural phenomena events to mitigate the consequences of those events.

Independent oversight assessments have examined technical design aspects for a number of years. In January 2006, EA (then the Office of Independent Oversight) issued a report titled *Essential System*

Functionality, which summarized safety system reviews at ten sites and noted several weaknesses in engineering related technical areas:

> *DOE and contractors have not ensured an appropriate degree of rigor, level of technical justification, and attention to detail in the design and review of safety systems.*
>
> *DOE and contractors have not ensured that seismic evaluations are complete and well documented.*
>
> *Contractors have not rigorously implemented configuration management requirements to ensure that safety systems will continue to be capable of performing their safety functions.*

More recent assessments have also addressed engineering-related elements. Results have been varied; some facilities have well-developed and controlled engineering programs, and other facilities fall short of the necessary rigor. In fiscal year 2016, EA identified conduct of engineering as a focus area in a memorandum to DOE senior line management, "Update on Office of Enterprise Assessments Nuclear Safety Assessment Activities – May 2016" (see Appendix B, Source Documents).

EA prepared this report to summarize the results of engineering assessments completed between 2013 and 2016 by independent assessment teams examining the management of safety systems at various facilities and performing engineering-specific assessments at others. Twenty-one reports were generated during that timeframe that included engineering within the assessment scope (see Appendix B).

1.2 Scope and Methodology

This report reflects collected results of engineering assessments at 12 hazard category 1, 2, and 3 nuclear facilities at seven DOE sites. Key elements examined during this process included:

- Engineering processes and procedures
- Technical baseline development and documentation
- Engineering product quality
- Configuration management within the engineering function
- Cognizant system engineer programs
- Engineering issues management
- Field element technical oversight of DOE contractors.

The sites and facilities assessed, along with associated contractors, local DOE offices, and DOE Headquarters program offices, are listed in Table 1.

The summary statements in Section 2 below reflect aggregated issues from 21 reports published by EA and its predecessor organizations from January 2013 through the present. Those reports remain a snapshot of conditions at the facility at the time of the assessment. The issued reports were provided to the assessed organizations and may have resulted in corrective actions or enhancements that are not reflected in these discussions.

Table 1
Nuclear Facilities, Contractors, DOE Program Offices, and Local DOE Offices in the Assessment

Assessment Site	Facilities Reviewed	Contractor	DOE Headquarters Program Office	DOE Field Element
Hanford Site	Hanford Tank Farms	Washington River Protection Solutions, LLC	Office of Environmental Management	Office of River Protection
Hanford Site	Waste Treatment and Immobilization Plant	Bechtel National Inc.	Office of Environmental Management	Office of River Protection
Lawrence Livermore National Laboratory	Plutonium Facility	Lawrence Livermore National Security, LLC	National Nuclear Security Administration	Livermore Field Office
Los Alamos National Laboratory	Weapons Engineering Tritium Facility	Los Alamos National Security, LLC	National Nuclear Security Administration	Los Alamos Field Office
Los Alamos National Laboratory	Transuranic Waste Facility	Los Alamos National Security, LLC	National Nuclear Security Administration	Los Alamos Field Office
Los Alamos National Laboratory	Technical Area 55 Plutonium Facility	Los Alamos National Security, LLC	National Nuclear Security Administration	Los Alamos Field Office
Savannah River Site	Salt Waste Processing Facility	Parsons Corporation	Office of Environmental Management	Savannah River Operations Office
Savannah River Site	Tritium Facility	Savannah River Nuclear Solutions, LLC	National Nuclear Security Administration	Savannah River Field Office
Idaho National Laboratory	Advanced Test Reactor	Battelle Energy Alliance, LLC	Office of Nuclear Energy	Idaho Operations Office
Y-12 National Security Complex	Highly Enriched Uranium Materials Facility	Consolidated Nuclear Security, LLC	National Nuclear Security Administration	National Nuclear Security Administration Production Office
Y-12 National Security Complex	Uranium Processing Facility	Bechtel National, Inc.	National Nuclear Security Administration	National Nuclear Security Administration Production Office
Waste Isolation Pilot Plant	Waste Isolation Pilot Plant	Nuclear Waste Partnership, LLC	Office of Environmental Management	Carlsbad Field Office

The scope of the assessments included elements from several criteria and review approach documents (CRADs):

- HSS CRAD 45-11, Rev. 3, *Safety Systems Inspection Criteria, Approach, and Lines of Inquiry*
- HSS CRAD 45-21, Rev. 1, *Feedback and Continuous Improvement Inspection Criteria and Approach – DOE Field Element*
- HSS CRAD 45-34, *Fire Protection*

- HSS CRAD 45-52, *Construction – Piping and Pipe Supports*
- HSS CRAD 45-53, *Construction – Mechanical Equipment Installation*
- HSS CRAD 45-58, *Review of Documented Safety Analysis Development for the Hanford Site Waste Treatment and Immobilization Plant (LBL Facilities)*
- HSS CRAD 45-59, *Review of Safety Basis Development for the Los Alamos National Laboratory Transuranic Waste Facility*
- HSS CRAD 64-17, *Nuclear Facility Safety System Functionality*
- EA CRAD 31-4, *Integrated Safety Basis and Engineering Design Review*
- EA CRAD 31-05, *Review of System Operational Test Plans*
- EA CRAD 31-13, *Conduct of Engineering*
- EA CRAD 31-15, *Safety System Management Review.*

EA used these criteria to determine whether the policies, procedures, and operational performance met DOE objectives for technical adequacy in the areas examined. This assessment took into consideration that a few DOE sites were contractually bound to DOE Order 420.1B, while other sites have implemented the revised DOE Order 420.1C.

1.3 Requirements and Guidance

Upper tier requirements for design engineering of nuclear facilities flow down from Title 10, Part 830 of the U.S. Code of Federal Regulations (10 CFR 830), *Nuclear Safety Management*. Other requirements are included in various DOE orders, including DOE Order 226.1B and DOE Order 420.1B (or 1C). Guidance is also taken from DOE standards such as DOE-STD-1189-2008 and DOE-STD-1073-2003.

2.0 OVERALL ASSESSMENT

EA found a mix of strengths and weaknesses in the performance of engineering activities. Stronger programs were generally found at developing projects. Operating facilities with long-established programs generally exhibited the most weaknesses. Developing projects took advantage of contractor design engineering processes, which have typically been honed on multiple nuclear projects. Processes examined at several operating facilities were much less rigorous, reflecting a gradual diminishment of attention to detail and increase in knowledge-based shortcuts. At some facilities the program degradation was to the point that they did not meet the minimum basic requirements established in 10 CFR 830.122.

2.1 Engineering Processes

Criterion: *Design engineering work is 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 10 CFR 830.*

Most of the engineering processes and procedures that EA reviewed were compliant with DOE requirements, defining appropriate activities and processes for the development of engineering deliverables and maintenance of technical configuration control. However, deficiencies in some site engineering procedure requirements and in procedure implementation resulted in technical inadequacies in engineering products and configuration control.

Strengths

Many site contractor engineering programs are sound, reflecting reasonable standards of industry practice. The engineering procedures reviewed at those sites generally define rigorous processes for development of engineering deliverables. Notably:

- Most site calculation procedures had well-defined requirements for calculation origination, review/ checking, and approval. Sites with strong processes typically require that:
  - Unverified assumptions and open items must be listed and tracked.
  - Calculations supporting a design change must contain no open items before the implemented change is placed into service.
  - Inputs must have a verified source reference.
- The design change processes at several sites are effective in driving communication; identifying cross-discipline impacts at an early stage of the design process; and promoting input from the Maintenance, Security, and Operations organizations.
- Some sites use SmartPlant Foundation software to process calculations and other engineering deliverables through issuance, providing a rigorous means of documenting comment resolution and approval.
- One site prepared a failure modes and effects analysis for a system to confirm, through analyses of component-level failures, that the design meets the single failure criterion of Institute of Electrical and Electronics Engineers (IEEE) Standards 379, *IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, and 384, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*.

Weaknesses

EA found programmatic weaknesses at several sites. Contrary to the requirements of 10 CFR 830, Subpart A and DOE-STD-1189-2008, contractor calculation processes at several sites permitted calculations based on unverified assumptions to be used in the implemented design basis for the facility. Further, processes for tracking and closure of the unverified assumptions were either non-existent or inadequate. Some sites also lacked specific requirements or a well-defined method for tracking calculation open items, creating an error-likely condition and representing a deficiency in the calculation process.

- At one site, the calculation procedure did not establish adequate control for identification, accessibility, and retrieval of design calculation records, violating the contractor quality assurance program for that facility.
- A site multi-discipline design review process for safety-related changes is important to ensure that all relevant aspects of a proposed change are adequately identified and considered. However, such a process is not equivalent to the independent review process defined for design verification and is not likely to produce the in-depth validation of design inputs that should result from the design verification process. One site was using multi-discipline review as a replacement for design verification.
- Several site design change procedures did not require justification or a technical basis for why a planned change was technically acceptable from a design standpoint (e.g., code compliance, analytical margin), contrary to 10 CFR 830, Subpart A. This omission is significant, since it procedurally allows changes to safety-related structures, systems, and components without an explanation of any impacts on the technical adequacy of the facility design basis.

- Several site drawing procedures did not limit the number of outstanding design changes before the changes were required to be incorporated, resulting in some drawings being out of date, not reflecting as-built conditions, and having the potential to mislead users. Further, at least one drawing procedure allowed the issuance of a drawing revision without the concurrent incorporation of other known changes, thus posing an egregious challenge to effective configuration management.

2.2 Technical Baseline

Criterion: *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 CFR 830)*

The design basis for a nuclear facility generally consists of those documents necessary to establish and ensure that the facility design is in compliance with the approved safety basis. DOE-STD-1073-2003, *Configuration Management*, notes that these documents may include:

- Design input documents, such as facility or system description documents
- Design constraints, such as industry codes and standards, regulatory commitments, and quality assurance requirements
- Design analysis and calculations necessary to convert the design inputs into design outputs and demonstrate compliance
- Design outputs, such as functional requirements, procurement specifications, and drawings.

Strengths

EA noted that several facilities' technical baseline documentation is generally well-established and in compliance with requirements, including software and hardware quality assurance documentation.

At two facilities currently under construction, technical requirements from the safety analyses are captured in a database (or requirements matrix) to help ensure the dissemination of requirements and aid the design process. EA observed the application of this process during a system design review, which included a validation process to ensure that the system complied with all documented requirements.

While the aforementioned requirements matrices are significant as aids in assessing completed design, one site nuclear safety organization took additional steps to further support design-in-progress by creating two documents that summarized safety basis requirements to be met by safety-related and defense-in-depth plant structures, systems, and components. The documents were created for the engineering group's use, eliminating the need for working-level engineers to search for and identify those requirements. EA considers the consolidation of these requirements into documents useful to the design execution organization a best practice for implementation of safety in the design process.

Other facilities use procedural requirements to drive compliance, typically charging the cognizant system engineers (CSEs) with identifying technical baseline documents for their systems and monitoring compliance. EA generally found the established technical baseline adequate for the systems reviewed, although exceptions were identified as discussed below. Some sites use system design descriptions (SDDs) effectively to provide a formal source of system design information for safety-related systems.

Weaknesses

EA reviewed calculations of various types during the assessment process at numerous facilities. In some cases, these reviews found that the calculations were adequately performed and documented. However, EA often found errors of varying severity:

- Minor errors, most likely reflecting inattention to detail and inadequate checking
- Non-conservative or incorrect inputs and assumptions
- Modeling errors
- Inaccurate references
- Misapplication of industry standards
- Omission of key considerations, such as the unusable volume in a water tank
- Design verification not performed as required
- Design input assumptions that were not verified or technically justified, and that were not tracked for subsequent closure.

Some of these errors affected:

- Fire protection system design
- Seismic qualification of safety class components
- Acceptance criteria for technical safety requirement surveillances
- Severity of potential radiological releases following fire protection system activation.

EA identified at least one facility that had no clear definition of what constituted the technical baseline. Another facility had an inadequately documented technical baseline, with no piping and instrumentation diagrams for some safety class systems. The latter facility's contractor-issued SDD for a safety related system was issued under a single person's signature, with no evidence of checking, design verification, or approval by a second authorized party as required by 10 CFR 830.122.

EA found inconsistencies in requirements while reviewing SDDs at several facilities, an indicator of inattention to detail in engineering deliverables.

One facility had a ventilation analysis performed by an outside contractor who used non-validated software (no software quality assurance) and provided the results to the site contractor via email. Neither the outside contractor nor the facility contractor issued any formal calculation, even though the results were later used.

2.3 Engineering Configuration Management

Criterion: *A documented configuration management program has been established and implemented in accordance with DOE Order 420.1B (or C) and DOE Order 413.3B that ensures consistency among system requirements and performance criteria, system documentation and physical configuration of the systems within the scope of the program. (DOE Order 413.3B, DOE Order 420.1B or C, DOE-STD-1073-2003)*

Requirements in this area derive from DOE Order 413.3B, Attachment 1, DOE Order 430.1C, and DOE Order 420.1C, which is applicable to most DOE nuclear facilities. DOE-STD-1073-2003 provides an acceptable methodology for a configuration management program.

The purpose of a configuration management program is to ensure that a technical baseline is established in compliance with the facility safety basis and that subsequent changes to the facility are accomplished in a manner that ensures continued compliance. Implementing processes must:

- Control design changes to ensure that the technical baseline remains up to date and that design documentation accurately depicts physical conditions in the facility
- Control the field work process to ensure that physical changes are implemented accurately and only in accordance with appropriate design output documentation
- Control the documentation process to ensure that issued design output accurately reflects current design and that changes are incorporated in a timely manner.

Inadequate control of any of these processes can result in loss of configuration management for the facility. DOE-STD-1073-2003 states in its guidance as an acceptable method that "The contractor must formally document and implement the configuration management process to be used for the activity in a configuration management plan." EA found that although most facilities implement this statement, the configuration management plans vary widely in quality and comprehensiveness.

Strengths

EA found several facilities that have established a well-documented technical baseline. During walkdowns of several facilities, EA also noted that the systems examined were consistent with issued engineering drawings.

Some contractors have strong processes for identifying design change-impacted documents, a key aspect in ensuring follow-up actions to update engineering output documents and providing a consistent portrayal of the facility configuration. These contractors use their electronic document management systems to track relationships between documents, creating a valuable tool for identifying impacts.

Weaknesses

Some contractors' configuration management plans either do not address the full scope of the acceptable methodology described in DOE-STD-1073-2003, or are significantly out of date. At one site, control of various aspects of the program is spread through 20 implementing sitewide procedures, reinforcing the importance of having governing upper-tier programmatic documents in essential areas.

At one facility, inadequate controls have led to implementation of field changes that are not documented in the design basis. Interviews with facility personnel indicated that such shortfalls were not uncommon, and EA documented multiple occurrences in its assessment.

At several facilities, the design change process does not require a technical basis or justification for the technical adequacy of the change. Other facilities have specific procedural requirements driving establishment of a technical basis for change, but in some of those facilities, EA determined that the provided analysis or technical justification was incorrect or inadequate.

Multiple occurrences were also noted where design change packages were issued which did not identify and update all affected design documents for a planned change:

- At one facility, several design change packages were issued to correct omissions from previous design change packages. This facility had an electronic document management system but was not using it to track relationships between engineering documents.

- At another facility, one document noted multiple setpoint values for the same instrument.
- At another facility, a fire protection system underwent incremental physical changes that, in aggregate, placed the system outside the configuration analyzed in the hydraulic calculation used to demonstrate compliance with the facility safety basis. At another site, the fire protection system hydraulic calculation had been revised twice without consideration of how the revisions would affect other documents that use information from that calculation.

Some facilities have a substantial backlog of unincorporated drawing updates, making it difficult for engineering staff at those facilities to determine the actual configuration of physical commodities in the field. Timely incorporation of drawing changes allows the technical staff to assess the cumulative impact of multiple design changes more readily. For this reason, some facilities have established time limits for incorporating changes to upper tier drawings – a positive action, from a configuration management standpoint. However, many facilities have established categories of lower tier drawings that do not require incorporation of updates, and changes to those drawings can accumulate without limit.

Documentation of the technical baseline was inadequate in some facilities. One of the earlier assessments covered in this summary report examined the safety class fire protection system at a facility and found that the contractor had issued no piping and instrumentation diagram for the system and no physical drawings showing the as-built piping layout and hanger configurations.

EA documented concerns with document control functions at several facilities:

- One facility was overly reliant on hard copy documents, using the electronic document management system only as an archival repository that working-level individuals could not readily access. The same facility kept quality-related engineering calculations and vendor manuals only in hardcopy. Unofficial versions of technical baseline drawings were available electronically, but the record copies were only on aperture cards.
- Another facility distributed the document control function throughout multiple organizations (Operations, Maintenance, Training), making each responsible for record keeping and submittal. As a result, large stacks of records sat on individuals' desks instead of being entered into the electronic document management system.
- Another facility allowed drawings to be updated by incorporation of some outstanding changes but did not require incorporation of all changes, so overlapping changes could be incorporated in the wrong order, increasing the potential for incorrect results.
- Very few facilities use electronic document management software capabilities to track relationships (predecessor/successor) between documents. Most such programs are capable of tracking these relationships and producing reports that identify successor documents that may be affected by a revision to a predecessor document.

The acceptable method documented in DOE-STD-1073-2003 also suggests periodic assessments of configuration management programs by the implementing organization. EA found some facilities did not fully implement the acceptable method, in that their assessments were not scheduled appropriately or were shallow to the point of being ineffective.

2.4 Cognizant System Engineer Programs

Criterion: *A cognizant system engineer (CSE) program must be established that includes training and qualification requirements and assignment of CSE responsibilities and authorities to ensure continued operational readiness of active safety related systems to meet their safety functional requirements and performance criteria. (DOE Order 420.1B or C)*

Most of the CSE programs and CSE training and qualification requirements that EA reviewed were appropriate and compliant with DOE requirements. These programs appropriately establish CSE roles, responsibilities, authorities, and accountabilities for their assigned systems, including configuration management, safety basis compliance, system health and reliability assessments, technical baseline document control, and support for operations and maintenance. Most of the interviewed CSEs were knowledgeable of facility processes and their assigned systems, and well informed about equipment performance issues. Many sites also assign CSEs the role of Design Authority, further enhancing their role in configuration management.

Several facilities do not have fully qualified CSEs for all safety systems because of attrition and the time needed to qualify on a given safety system. EA also identified instances of inadequate CSE training, including CSE qualification processes that do not include safety system-specific training.

Strengths

Appropriate CSE support for operations and maintenance is apparent at all reviewed sites. In particular, CSEs have proposed or concurred in new or revised operations and maintenance procedures that could affect their assigned systems, supported analysis and development of corrective actions for identified system problems, reviewed and concurred in decisions about system component "use-as-is" and commercial grade dedication, proposed or concurred in post-maintenance/modification test requirements, and reviewed and approved the acceptability of system test results.

Several sites require CSEs to develop and maintain system notebooks to document system walkdown assessments, including observation of the material condition, operations, and configuration control. The notebooks that EA reviewed included a compendium of system design, operations, maintenance, modification, configuration, and performance information, with references to important retrievable items, such as essential system documentation, purchase specifications, and vendor manuals. These system notebooks are effective and efficient roadmaps for navigating the extensive technical baselines and are also effective repositories of the system information needed to perform CSE responsibilities and educate new CSEs. System notebooks represent a best practice that is not currently mandated by DOE.

Many sites require periodic system walkdown assessments to ensure that CSEs remain aware of system configuration, ongoing operations, maintenance and modification activities, system overall health, performance challenges (e.g., accessibility, combustibles, seismic interactions), and operational trends in vibration, noise, temperature, accumulation of combustibles, and cleanliness.

Most CSE programs require periodic system health reports (SHRs) to focus management attention on actions needed to maintain and improve system health. The best SHR processes:

- Require CSEs to develop a system health monitoring basis. Once that basis is approved, the CSE must collect and analyze data and use it to prepare periodic SHRs that assess system function against the metrics and criteria established in the system health basis, providing a meaningful tool for tracking the status of system components, maintenance activities, surveillances, and open issues.
- Establish a "Plant Health Committee" chaired by a senior manager to review and establish prioritized commitments for system health improvements.

Weaknesses

Several sites assign CSEs responsibilities that are outside the CSE functions defined by DOE Order 420.1, distracting those CSEs from effectively discharging the primary responsibilities specified in the

order. These additional unrelated assignments include:

- Assignment of CSEs as the responsible individual for system maintenance activities
- Assignment of responsibilities for development and involvement in system design changes.

Several site CSE training and qualification programs had significant deficiencies:

- Job-specific training and reading requirements were not established using a systematic approach to training as required by DOE Order 426.2.
- CSEs were assigned to active safety systems but did not meet qualification standards.
- Training histories of CSEs were not maintained as required.

Multiple sites do not require documentation of system walkdown assessments. At several sites, CSEs do not rigorously document walkdowns or other activities throughout the year, thereby reducing the effectiveness of monitoring and increasing the chances of losing the highlights, concerns, and important observations from the CSE's system walkdowns.

Improvements are warranted in some SHRs. Common deficiencies include:

- No discussion of the results of CSE periodic system walkdown assessments
- No identification or analysis of trends from operations and maintenance, or proposed corrective actions for declining trends in the performance of specific components
- No discussion or analysis of the backlogs in system maintenance/modifications
- No discussion of the potential risk and recommended path forward for identified degradation or obsolescence of components or shortfalls in the availability of critical spare parts.

2.5 Issues Management

Criterion: *Establish and implement processes to detect and prevent quality problems. Identify, control, and correct items, services, and processes that do not meet established requirements. Identify the causes of problems and work to prevent recurrence as a part of correcting the problem. (10 CFR 830, Subpart A)*

Although specific requirements pertaining to issues management derive from 10 CFR 830 as noted above, facility issues management processes are generally developed as a facet of the broader contractor assurance program mandated by DOE Order 226.1B, *Implementation of Department of Energy Oversight Policy*. Several assessments within the timeframe of this report looked at the role of the facility issues management systems in resolving engineering issues, both technical and performance-related. Some strengths were evident, however issues management processes at most sites were less than effective.

For simplicity, this report will use the term "problem reports" to refer to the documents generated and submitted to the facility/site issues management system to report and track problems.

EA found that some sites have effective issues management systems, but most of the facility programs EA examined within the scope of this report exhibited one or more of the weaknesses outlined below. Strong programs are more prevalent where contractor management is not only deeply involved in the process, but also committed to effective outcomes.

Strengths

A few sites were found to have effective issues management processes, generally accompanied by a high level of management involvement in evaluating identified issues and ensuring that effective corrective actions are implemented. Management involvement included participation in:

- Management observations
- Screening committees
- Issue/corrective action review boards
- Management review committees.

Some of the same functions are specified in the issues management procedures at other sites with programs that were less effective in this area. However, the less-effective programs generally manifest lower management involvement, minimal promotion of the benefits of an effective program, and less commitment and support for identifying and reviewing problems, developing and implementing effective corrective actions, and resolving underlying issues and preventing recurrence.

In addition, sites with effective issues management programs generally have:

- A workplace culture supportive of problem identification
- Assurance personnel involved in the review and classification process
- Rigorous causal analysis processes
- A commitment of resources to post-closure review/validation.

EA observed that independent post-closure corrective action review is an effective way to ensure that corrective actions are implemented as planned and that closure is adequately documented. One facility has established internal management expectations (minimum goals) for the number of issues identified in their issues management system, both to encourage the identification of issues and to increase the likelihood of identifying issues before they become more significant or severe. These expectations came with no consequences if not met, but were effective in removing any potential stigma from the problem identification process.

One facility has also implemented a technical issues management system to help resolve technical issues identified during the design process. This system has been particularly effective in driving both management involvement and communication between the engineering staff and other stakeholder organizations, such as Operations and Maintenance. It has also been used to bring issues to the attention of the supporting DOE office.

Weaknesses

The following issues management program weaknesses were apparent at multiple sites or had a significant negative impact on program success on at least one site:

- Problem reports were sometimes categorized at a lower severity level than warranted and thus did not receive appropriate management attention. For example, at one facility the normal four levels of severity had been supplemented by a fifth level, Level "T," that was not subject to other requirements of the site issues management program, such as causal analysis, extent-of-condition review, or trending. EA noted several problem reports that were inappropriately categorized as Level T.

- Under-reporting of low level issues made it difficult to identify trends that could be leading indicators of more significant issues.
- Corrective actions were sometimes inadequate to correct the identified problems.
- Corrective actions sometimes focused on fixing the immediate problems and did not address the complete extent of the problem conditions.
- Corrective action plans for some problem reports contained inadequate corrective actions to prevent recurrence of the problems. At one facility, some corrective actions intended to prevent recurrence of a problem were canceled by management decision, leading to a repeat problem only a few months later.
- Some problem reports were closed without completion of the planned corrective actions. At one site, a corrective action to add drain lines in a high efficiency particulate air (HEPA) filter plenum was closed based solely on creation and submittal of a "change request" document, which was not implemented and could not be located four years later.
- Some problem reports were closed without appropriate validation of the effectiveness of the corrective actions.
- At one site, average time to complete a causal analysis was 100 days, a significant impediment to problem resolution.
- Training of management review committee members was a weakness at one facility. Training was available but was "recommended," not "required." None of the committee members had completed the training, yet these individuals were performing key roles in the issues management process.
- At one facility, a technical evaluation of the adequacy of part of a safety significant ventilation system subject to weather extremes did not consider the physical condition of the system. The evaluation assumed that the original design values were still applicable and appropriate, when in fact the system was substantially degraded.
- Some sites did not perform extent-of-condition reviews despite multiple, documented occurrences within a limited timeframe, and no actions were taken to prevent recurrence.

The extent of problems found in this area may be indicative of further problems with contractor assurance systems, which typically include internal assessment processes to identify inadequacies such as those found by EA. Contractor inability to detect and address these inadequacies through internal assurance system functions may indicate that assessment programs are not sufficiently critical or introspective.

2.6 DOE Field Element Oversight of Contractor Engineering Programs

Criterion: *An effective Federal oversight program has been established consistent with DOE Order 226.1B and DOE Guide 226.1-2A to monitor and ensure compliance with nuclear facility safety requirements.*

EA generally found conscientious efforts on the part of DOE field element staffs to perform oversight in the manner directed by DOE Order 226.1B. Although EA noted some areas where increased attention is warranted, safety system oversight engineers and Facility Representatives were consistently knowledgeable about their assigned areas and compliant with technical qualification requirements.

Strengths

Many field elements have comprehensive oversight plans, including a mix of independent reviews, reviews performed concurrently with the contractor or external assessors, and self-assessments of their in-house performance. In most cases, the reviews are adequately critical and cover an appropriately broad

spectrum of contractor performance areas. In one assessment that EA observed, the field element team was knowledgeable about the facility and used appropriate, challenging criteria.

After most Federal oversight activities, any identified issues in contractor performance are transmitted formally to the contractor for resolution. These issues may also be tracked internally using other software tools.

At one site, safety system oversight personnel reviewed contractor corrective action documents, providing feedback on inadequate corrective action plans and driving improved contractor performance in that area.

A few field elements prepared internal guides for Federal oversight in key areas.

Field element technical decision-making is generally conservative and includes input from appropriate staff. The technical staff at most field elements is appropriately qualified in accordance with DOE Order 426.1, *Federal Technical Capability Program.* These individuals are generally knowledgeable of their assigned areas.

Weaknesses

Some field element oversight activities lack rigor. At one facility where an EA assessment found multiple findings and opportunities for improvement, oversight by several field element individuals had documented only a single deficiency in the previous two years. Understaffing in oversight positions also poses problems for some offices.

The attention given to recurring issues is often insufficient, and issues may be found in multiple places. One facility reported individual occurrences without assessing whether multiple or repeat occurrences of the same problem might reflect more serious underlying issues. Software (ePegasus) used to report and track issues was not applied effectively to drive improvement.

Similarly, some field element oversight procedures are outdated, contain conflicts, and cite inconsistent or outdated requirements and organizational references.

Other field elements could benefit from increased focus on the CSE program, including SHRs, as a tool for assessing reliability and risk. At one facility, SHRs had degraded to the point where they provided little useful information.

Some field elements are assessing contractor assurance systems ineffectively, particularly in the area of issues management. As noted in Section 2.5 of this report, ineffective contractor performance in issues management may be indicative of inadequate performance in other aspects of contractor assurance. Ineffective contractor issues management systems can also result in inadequate corrective actions and recurring problems. At one facility, field element oversight planning was based on the stated premise of confidence in the contractor assurance system, even though previous assessments of that system had not looked at effectiveness. The weaknesses identified in Section 2.5 indicate that increased oversight is warranted in this area.

2.7 Occurrence Reporting and Processing System (ORPS) Data Analysis

EA examined the DOE ORPS database to determine whether the problems identified in this report were similar to, or validated by, issues reported by the sites. A number of parallels were evident.

EA reviewed ORPS data from January 1, 2013, to April 17, 2017. During that period, a total of 4,575 occurrences were reported into ORPS. EA sorted the database information on the basis of relevance to the topics and recommendations in this EA report, identifying 247 relevant ORPS reports. Of these, 28 referred to configuration management issues, and 6 of the 28 had causal factors attributed, in part, to problems in configuration management processes. These configuration management deficiencies led to inadequate design outputs and failure to update drawings/documentation in line with facility changes. For example, ORPS report EM-PPPO-FBP-PORTSDD-2013-0027, "Recurring Electrical Safety Concerns Identified," documented a breakdown in a site Electrical safety program. A team investigating 11 electrical safety events which occurred over a one-year period July 2012 – July 2013) found that 4 of 11 were attributed to configuration management issues, where either new equipment was introduced without appropriate information being disseminated or drawings were not up to date.

Sixty of the 247 relevant ORPS reports referred to calculation issues, and four of them had causal factors involving use of incorrect/unverified assumptions in calculations. One additional case involved an inadequate calculation process procedure. EM-ID-CWI-IWTU-2013-0003, "Positive USQ - Discovery of New Information Relative to the Functional Testing of the Granular Activated Carbon (GAC) Bed Inlet Valves," is one example of this. It identified a problem and found the root cause to be lack of a formal documented engineering evaluation with supporting approved calculations for a functional test of the valves.

Finally, 160 occurrences were related to design deficiencies, approximately 61 percent (99 occurrences) of which identified design deficiency as a causal factor. Thirty-six of the 99 occurrences were related to less-than-adequate design output. Examples in this area included ORPS NA-PS-BWP-PANTEX-2013-0019 and ORPS NA-PS-BWP-PANTEX-2013-0019, which both identified design output as being less than adequate. One found that a particular design did not consider all possible scenarios and operating conditions for machining and the second involved the design output scope for a machining alignment pad being less than adequate.

Although ORPS is typically used for reporting operational occurrences, EA reviewed enough reports to draw conclusions in several areas. Site-reported events reflected difficulties in configuration management (see Section 2.3 of this report), engineering procedures (see Section 2.1), and design documents (see Section 2.2). These results support the recommended actions outlined below.

3.0 SUMMARY OF RESULTS

3.1 Best Practices

In preparing this lessons-learned report, EA identified the following best practices that may be valuable to other DOE sites:

- **Sites with strong calculation processes, such as the Savannah River Site Tritium Facility, typically require that:**
    - **Unverified assumptions and open items be listed and tracked.**
    - **Calculations supporting a design change contain no open items before the implemented change is placed into service.**
    - **Inputs must have a verified source reference.**

- **At both the Waste Treatment and Immobilization Plant Project and the Uranium Processing Facility Project, technical requirements from the safety analyses are captured in a database (or requirements matrix) to help ensure the dissemination of requirements and to aid the design process.**

- **The Savannah River Site Tritium Facility requires CSEs to develop and maintain system notebooks to document observations of the material condition, operations, and configuration control. These notebooks include a compendium of system design, operations, maintenance, modification, configuration, and performance information and refer to retrievable essential system documentation, purchase specifications, vendor manuals, etc. These system notebooks are effective repositories of system information and an efficient source of information for safety-related systems.**

- **The Uranium Processing Facility Project nuclear safety organization created two documents that provided a consolidated summary of safety basis requirements for safety-related and defense-in-depth plant structures, systems, and components. The documents were created for the engineering group to use during the design process, eliminating the need for working-level engineers to search for and identify those requirements. The consolidation of these requirements into documents useful to the design execution organization supports effective implementation of safety in the design process.**

- **The Uranium Processing Facility Project uses a defined program/process for resolving technical issues, bringing together the engineering staff with management, operations, maintenance, and other stakeholder organizations to ensure resolution in a manner that meets the needs of each group.**

3.2 Recommendations

These recommendations are based on lessons learned identified during EA reviews between 2013 and 2016. While the underlying deficiencies and weaknesses from individual reviews did not apply to every site reviewed, the recommended actions are intended to provide insights for potential improvements at all DOE nuclear sites. Consequently, DOE organizations and site contractors should evaluate the applicability of the following recommended actions to their respective facilities and/or organizations, and consider their use as appropriate in accordance with Headquarters and/or site-specific program objectives.

Facility Contractors

- **Revise engineering procedures as appropriate to adequately define requirements for identifying, tracking, and closing unverified assumptions in calculations. Ensure that calculations with unverified assumptions cannot be used as the basis for implemented design changes in safety-related systems.**

- **Ensure that SHRs adequately capture all information pertinent to system health and reliability and that they adequately convey the system status, including functionality, declining trends, failure rates, operability concerns, future challenges, and recommended corrective/mitigative actions.**

- **Require CSEs to maintain system notebooks to document system walkdown assessments and to provide a compendium of system design, operations, maintenance, modification,**

configuration, and performance information, including references to easily retrievable essential system documentation, purchase specifications, vendor manuals, etc.

- **Establish a senior manager level committee or process to periodically review system health reports; improve senior leadership's understanding of current system challenges to operability, reliability and availability; and identify and prioritize commitments to improving system health.**

- **Enhance document control as a key part of successful configuration management by avoiding over-reliance on hardcopy documents or distributing the document control function throughout multiple organizations. Use electronic document management system capabilities to track relationships (predecessor/successor) between engineering documents to help identify all documents affected by a design change, thereby reducing rework.**

- **Ensure that the issues management process is being used effectively to document and resolve problems, addressing the full extent of the problem conditions and implementing measures to prevent recurrence. Perform periodic internal assessments of process effectiveness.**

- **Ensure that contractor assurance systems are effective in identifying conduct of engineering problems.**

DOE Field Elements

- **Conduct self-assessments of the DOE field element oversight performance and pursue enhancements as needed in the following oversight areas:**

  - **Updating and revising DOE field element procedures;**
  - **Improving oversight of contractor issues management and other assurance system aspects associated with conduct of engineering;**
  - **Improving (within the technical capabilities within the DOE field element) the oversight of engineering elements such as:**
    - **Quality of products associated with the technical baseline, especially to verify accuracy and that there are no open items or unverified assumptions.**
    - **Validation that technical issues documented in contractor issues management systems are fully and completely resolved and do not recur.**
    - **Confirmation that document control is an effective part of facility contractors' configuration management efforts.**

Office of Environment, Health, Safety and Security

- **Establish and publish minimum requirements for the conduct of engineering at DOE nuclear facilities. DOE contractors, as well as DOE field elements and other DOE oversight organizations, need such requirements to ensure effective implementation of facility safety bases.**

- **During the next revision to DOE Order 420.1 consider including a requirement that CSEs maintain system notebooks to document observations of material condition, operations, and configuration control, and to provide a source of system design, operations, maintenance,**

modification, configuration, and performance information, with references to retrievable essential system documentation, purchase specifications, vendor manuals, etc.

Appendix A
Supplemental Information

Office of Enterprise Assessments Management

Glenn S. Podonsky, Director, Office of Enterprise Assessments
William A. Eckroade, Deputy Director, Office of Enterprise Assessments
Thomas R. Staker, Director, Office of Environment, Safety and Health Assessments
William E. Miller, Deputy Director, Office of Environment, Safety and Health Assessments
C.E. (Gene) Carpenter, Jr., Director, Office of Nuclear Safety and Environmental Assessments
Kevin G. Kilp, Acting Director, Office of Worker Safety and Health Assessments
Gerald M. McAteer, Director, Office of Emergency Management Assessments

Quality Review Board

William A. Eckroade
John S. Boulden III
Thomas R. Staker
William E. Miller
C.E. (Gene) Carpenter, Jr.
Michael A. Kilpatrick

Office of Enterprise Assessments Report Contributors

Preparers
Charles Allen (Lead)
Timothy Martin
Glenn Morris

Contributors
David J. Adair
Phillip D. Aiken
Aleem E. Boatright
Ronald G. Bostic
James M. Boyd
Robert Compton
Jimmy S. Dyke
Robert E. Farrell
Robert G. Freeman
Thomas G. Hiltz
Frank A. Inzirillo
Joseph J. Lenahan
James O. Low
Michael A. Marelli
William E. Miller
Glenn W. Morris
David J. Odland
Joseph J. Panchison
Donald C. Prevatte
Joseph E. Probst
Jeffrey L. Robinson
Samina A. Shaikh
Jeff Snook
Edward A. Stafford
Eric R. Swanson
Gregory D. Teese
Peter M. Turcic

Appendix B
Source Documents

- Memorandum for Distribution, Glenn S. Podonsky, May 3, 2016, *Update on Office of Enterprise Assessments Nuclear Safety Assessment Activities – May 2016*

- *Essential System Functionality,* January 2006, U. S. DOE Office of Independent Oversight

- Institute Of Nuclear Power Operations, INPO 90-009, Revision 2, September 2004, *Guidelines for the Conduct of Design Engineering*

- U. S. Nuclear Regulatory Commission, NUREG-1913, August 2009, *DESIGN CONTROL – A Quick Reference Guide for NRC Inspectors*

- HSS Report, *Independent Oversight Review of Management of Safety Systems at the Hanford Tank Farms,* April 2013

- EA Report, *Targeted Assessment of the Double Shell Tank Ventilation Systems at the Hanford Site Tank Farms,* September 2016

- EA Report, *Review of the Hanford Site Waste Treatment and Immobilization Plant Project Engineering Processes*, October 2015

- EA Report, *Targeted Review of the Management of the Safety-Related 480 Volt Diesel Bus Battery-Backed Power System of the Idaho National Laboratory Advanced Test Reactor at the Idaho Site,* September 2015

- EA Report, *Review of the Los Alamos National Laboratory Weapons Engineering Tritium Facility Safety Significant Fire Suppression System,* November 2014

- EA Report, *Review of the Los Alamos National Laboratory Transuranic Waste Facility Safety Basis and Design Development*, July 2014

- HSS Report, *Review of the Los Alamos National Laboratory Weapons Engineering Tritium Facility Tritium Gas Containment Vital Safety System*, January 2013

- EA Report, *Targeted Review of the Safety Significant Ventilation System and Interconnected Portions of the Associated Safety Class Confinement System, and Review of Federal Assurance Capability at the Los Alamos National Laboratory Technical Area 55 Plutonium Facility,* August 2015

- EA Report, *Targeted Review of the Safety-Class Room Ventilation Systems and Associated Final Filtration Stages, and Review of Federal Assurance Capability at the Lawrence Livermore National Laboratory Plutonium Facility,* February 2015

- EA Report, *Assessment of Savannah River Site Tritium Facility Safety System Management,* December 2016

- EA Report, *Review of the Savannah River Site Salt Waste Processing Facility Construction Quality and Startup Test Plans,* June 2015

- HSS Report, *Review of the Uranium Processing Facility Design Requirements and Configuration Management Program*, March 2014

- EA Report, *Assessment of the Uranium Processing Facility Project Engineering Processes*, September 2016

- EA Report, *Targeted Review of the Safety System Management of the Secondary Confinement System and Safety Significant Power Distribution System at the Y-12 National Security Complex Highly Enriched Uranium Materials Facility*, December 2015

- Operational Awareness Report (OAR) EA-WIPP-2014-06-23, *Limited Review of Engineering Configuration Management Processes*

- OAR EA-WIPP-2016-07-12, *Follow-up on Engineering Process Issues from the November 2015 Assessment Report*

- OAR EA-WIPP-2014-12-02, *Follow-up Review of Engineering Configuration Management Processes*

- OAR EA-WIPP-IVS-2016-*05-25, Operational Awareness of the Design and Modification Progress of the WIPP Underground Interim Ventilation System*

- OAR EA-WIPP-IVS/SVS-2015-11-15, *Observations of the Design and Modification Progress of the WIPP Underground Interim Ventilation System and Supplemental Ventilation System*

- EA Report, *Review of Waste Isolation Pilot Plant Engineering and Procurement Processes*, November 2015

- OAR EA-WIPP-2015-03-19, *Follow Up Review of Engineering Processes*