Office of Independent Oversight
Office of Security and Safety Performance Assurance
U. S. Department of Energy

Independent Oversight Status Report on

Safety System Engineer and Oversight Programs

March 2006

SSA

Office of Security and Safety Performance Assurance

OVERSIGHT

Table of Contents

Abbreviations Used in This Report

CSE	Cognizant System Engineer
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
FTCP	Federal Technical Capability Panel
NNSA	National Nuclear Security Administration
NTC	National Training Center
SSO	Safety System Oversight

Executive Summary

The Office of Independent Oversight, within the Office of Security and Safety Performance Assurance, has responsibility for evaluating safeguards and security; cyber security; environment, safety, and health; and emergency management programs and reporting on their status to the Secretary of Energy, senior Department of Energy (DOE) management, and Congress. Independent Oversight periodically summarizes observations from site evaluations to provide the status of implementation of certain important programs. This report provides the status of implementation of the safety system engineer and oversight programs and recommendations to foster improvements across the DOE complex.

In 2000, DOE initiated an effort to improve safety system configuration management and oversight in response to Defense Nuclear Facilities Safety Board Recommendation 2000-2, *Configuration Management, Vital Safety Systems*. Two important elements of DOE's improvement effort were the establishment of requirements for site contractors to establish system engineer programs and for DOE field offices to establish safety system oversight (SSO) programs, which were promulgated in 2002 and 2004, respectively.

DOE and its contractors have made good progress in implementing these requirements, and the resulting programs have had positive impacts on safety system configuration management and the assurance of safety system functionality. Most contractors have established most elements of an effective system engineer program and are providing good day-to-day engineering support for the maintenance and operation of the systems. DOE field offices have defined site-specific SSO programs, assigned responsibilities and resources, and established qualification requirements, and they have begun to perform some effective oversight activities, including system walkdowns and evaluation of system performance.

However, although most contractors have effective system engineer programs, some contractors have not effectively implemented some basic elements, such as developing program documents and establishing responsibilities and performance expectations. Further, many contractors have not established complete and rigorous documentation of the safety system technical basis, do not formally track and trend system performance, and have not established a program for performing detailed system assessments. In addition, some DOE field offices have not clearly defined and implemented some aspects of the SSO program, such as determining the type and frequency of system assessments, documenting assessment results, and tracking corrective actions.

Independent Oversight identified several opportunities for improvement for both the contractor system engineer program and the DOE field office SSO program. Key aspects of these recommendations include:

- Incorporating SSO responsibilities into the new DOE oversight manual, and providing additional guidance on SSO duties
- Establishing a formal, DOE-wide technical qualification standard for SSO personnel
- Establishing and rigorously documenting those aspects of the safety system design basis important for ensuring system functionality
- Expanding the scope of applicability of requirements for SSO programs to include non-defense hazard category 1, 2, and 3 nuclear facilities, including DOE's nuclear reactors
- Improving the formality of tracking and trending of system performance.

DOE program and field offices, site contractors, and the Federal Technical Capability Panel should review the positive attributes, weaknesses, and detailed opportunities for improvement in this report for applicability and needed actions.

The system engineer and SSO programs, though relatively new, have already proven to be beneficial. As discussed in Independent Oversight's status report on essential system functionality (January 2006), the engineering design, analysis, and configuration management of safety systems need further improvement. The system engineer and SSO programs will be a focal point for facilitating some of the needed improvements.

1.0 Introduction

In the period October 2004 to March 2006, the Office of Independent Oversight, within the Office of Security and Safety Performance Assurance, evaluated system engineer and safety system oversight (SSO) programs at eight sites, as identified in Table 1. These programs were evaluated as part of Independent Oversight's review of the effectiveness of programs for managing safety systems' design, configuration management, maintenance, and operation so as to ensure that they can perform their safety functions when needed. This report summarizes the observations and insights about safety system engineer and oversight programs based on these evaluations and review of related U.S. Department of Energy (DOE) requirements, guidance, and other supporting documents.

In March 2000, the Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2000-2, *Configuration Management, Vital Safety System*, which focused on the need for DOE to improve configuration management of vital safety systems. One element of the recommendation called for DOE to evaluate existing practices and industry models for using a cognizant system engineer (CSE) concept to strengthen the engineering resources available for facility configuration management. In response to this specific recommendation, DOE issued a revision to DOE Order 420.1, *Facility Safety*, in May 2002, to include requirements for contractors to establish a system engineer program and to assign CSEs for safety systems. These CSEs are responsible for ensuring configuration management of safety systems and for providing technical assistance to operations and maintenance to ensure continued operational readiness.

Another element of DNFSB Recommendation 2000-2 called for DOE to establish a Federal SSO program to oversee the contractors' system engineer program and the contractors' efforts to ensure safety system functionality. This oversight program, established in 2004, is described in the DOE Federal Technical Capability Panel (FTCP) manual.

Table 1. SSO Evaluation Sites

Safety Management Inspection Site	Headquarters Program Office
Lawrence Livermore National Laboratory	National Nuclear Security Administration (NNSA)
Pantex	NNSA
Argonne National Laboratory	Office of Science
Idaho National Laboratory	Office of Nuclear Energy, Science and Technology
Sandia National Laboratories	NNSA
Y-12 National Security Complex	NNSA
Los Alamos National Laboratory	NNSA
Savannah River	Office of Environmental Management

2.0 Positive Attributes

As described below, several aspects of the system engineer and SSO program are effectively implemented at most of the inspected DOE sites. One site, the Y-12 National Security Complex, has a notably effective approach for performing safety system assessments.

Most contractors have established most elements of an effective system engineer program. The programs are, in general, adequately defined, and personnel assigned system engineer responsibilities are highly motivated and have a very strong sense of ownership of their assigned systems. The training and qualification programs for system engineers are well defined and appropriate. However, as discussed later in this report, the maturity of system engineer programs varies, and some programs are just beginning to be established. Some of the sites with mature programs established their programs prior to issuance of DOE Order 420.1A and required only relatively minor adjustments to become compliant with the order. These contractors recognized the benefits of such a program from previous experience (e.g., work in the commercial nuclear industry), both from the perspective of safety system management and in overall productivity enhancement. Independent Oversight found that sites with more mature programs had better configuration management programs, and Independent Oversight identified fewer and less-significant concerns when performing detailed safety system functionality assessments at these sites.

Contractor system engineer programs have provided good support to operations and maintenance. CSEs have been actively involved in ensuring the technical adequacy of planned corrective and preventive maintenance activities, reviewing maintenance results, supporting troubleshooting, developing minor design change packages, and supporting surveillance activities on a day-to-day basis. This dedicated and competent engineering support to the maintenance and operations activities is a major benefit of the system engineer program.

DOE field offices have made good progress in establishing SSO programs, and SSO personnel have effectively performed some safety system functionality oversight activities. Most field offices have made good progress in establishing the framework for oversight programs to meet the SSO expectations stated in the FTCP manual. For example, most offices have established program documents, assigned SSO personnel, and developed training and qualification requirements. SSO personnel have been involved in technical reviews of corrective actions, walkdowns of systems, and reviews of design changes. These activities are important elements of effective oversight of safety systems, and the technical reviews have typically been detailed, thorough, and adequately documented.

The FTCP has developed and shared appropriate guidance and tools for developing and assessing the adequacy of SSO programs. The FTCP was assigned the lead for developing the SSO program in the DNFSB Recommendation 2000-2 implementation plan. The FTCP has developed some good products supporting development and implementation of the SSO program, including: (1) guidance for SSO programs in the FTCP manual, (2) guidance for performing self-assessments of SSO programs, and (3) an informal generic qualification standard. Furthermore, the FTCP has coordinated performance of SSO program assessments across the DOE complex. The results of the assessments are included on the FTCP web page to facilitate lessons learned. All these efforts have been valuable in establishing effective SSO programs.

The National Training Center (NTC), in conjunction with NNSA's Albuquerque Service Center, has established some good initial training for DOE SSO personnel. The Service Center took aggressive actions to establish SSO training for Los Alamos Site Office personnel that included actual performance of some SSO duties in a Los Alamos facility. The NTC worked with the Service Center in this initial effort and then,

with the Service Center's support, established two SSO training courses that are available DOE-wide. These courses provide good instruction on SSO duties and responsibilities and some intermediate-level instruction on performing assessment activities. Currently, the NTC is working to improve the SSO assessment course to include more advanced training to enhance engineering assessment skills.

The Y-12 site has established a well defined and effective process for performing periodic detailed safety system assessments. Every year, Y-12 performs at least one detailed system assessment and one detailed program assessment (e.g., configuration management or system engineering programs). The system assessments are well defined in an inspection plan, appropriate resources and expertise are allocated to perform them, and the results are well documented. The assessments are based upon and similar to the phase II assessments performed as part of the implementation of DNFSB Recommendation 2000-2. To date, Y-12 has performed detailed assessments of 30 of its 70 vital safety systems. Y-12 is considering improving their assessments by including more detailed engineering design reviews.

3.0 Weaknesses

Although both DOE and its contractors have generally made good progress in implementing the system engineer and SSO program requirements, implementation progress is not far along at some sites, and there are weaknesses in a number of important aspects at many sites, as described below.

Contractors at two DOE sites have not effectively established basic elements of system engineer programs. For example, these contractors have not established clear, documented roles and responsibilities and performance expectations for the system engineer programs. Further, some CSEs lack a detailed understanding of their assigned systems, particularly with regard to their safety bases. At these sites, DOE did not provide adequate oversight of the contractors' implementation of the system engineer requirements stated in DOE Order 420.1A. In addition, as discussed below, most contractors have not established complete and accurate system technical basis documents, effectively tracked and trended system performance, or effectively conducted detailed system reviews.

Most contractors have not established and maintained adequate technical basis documents. DOE Order 420.1A requires CSEs to develop and maintain documents that define the design basis of safety systems (e.g., system design descriptions). The documents should identify system requirements, provide the bases for the requirements, and describe the features of the system design provided to meet those requirements. As part of a configuration management change control process, technical basis documents help ensure consistency among the engineering requirements for systems, the actual installed physical configuration, and the associated documentation. DOE has established good guidance for developing technical basis documents in DOE STD 3024; however, at most sites, the technical basis documents fall well short of these guidelines, are not complete, and/or are inaccurate.

Most contractors do not perform detailed, systematic, and formal periodic reviews of safety systems. DOE Order 420.1A requires system assessments as part of safety system configuration management and refers to DOE STD 1073 for implementation guidance. Although some contractors perform some assessments (e.g., many perform system walkdowns), most assessments are not detailed and formal. For example, most contractors have not established a program for performing system assessments similar to those that were performed as part of the implementation of DNFSB Recommendation 2000-2 (i.e., phase II type assessments). Furthermore, contractors do not perform the design assessments described in DOE STD 1073.

Most contractors have not established formal programs for tracking and trending equipment performance. Although most CSEs informally track system performance, programs and expectations for formal tracking and trending have not been established. Further, maintenance data is not being captured effectively to support such trending. Some contractors have been making efforts to improve in this area.

Some DOE field/site offices have not adequately defined their SSO programs. For example, some field offices have not established SSO program documents that provide details on how the oversight function is to be performed, including expectations for the types of oversight activities (e.g., system walkdowns, design change and maintenance observations, or detailed system reviews) and for documenting and processing the issues identified by such activities. In addition, expectations for documentation of assessment results have not been established and, at some sites, are not formal or rigorous. Further, some field offices have not established effective processes to formally track and trend corrective actions from SSO assessments (utilizing, as appropriate, existing corrective action processes). Finally, one site office's approach for meeting the SSO requirements (by assigning a single SSO person to a facility and all the systems in the facility) has not resulted in effective technical oversight of safety systems as required by the FTCP manual.

Most DOE field offices have not performed detailed safety system assessments. Although SSOs generally maintain oversight of systems and monitor the performance of CSEs, they have not taken actions to conduct periodic detailed system assessments or to participate in or oversee contractors' performance of these types of assessments. A notable exception is the Y-12 Site Office, which participates in the Y-12 contractor's detailed system assessments.

DOE has not identified the responsible office for the SSO program and has not established appropriately formalized requirements. The FTCP manual contains generally appropriate "requirements" for the SSO program; however, this manual is not the appropriate mechanism for establishing and communicating requirements. The purpose of the FTCP is to provide *for the recruitment, deployment, development, and retention of Federal personnel with the demonstrated technical capability to safely accomplish the Department's missions and responsibilities*, not to establish oversight program requirements. Further, although the FTCP manual provides generally appropriate requirements, they are not always complete and clear. In particular, requirements or guidance about the type and frequency of assessment activities is not provided. However, as discussed previously, the FTCP has served a valuable role in developing the SSO program.

DOE has not established requirements for SSO programs for non-defense nuclear facilities, such as hazard category 1 nuclear reactors. Although DOE appropriately included non-defense nuclear facilities within the scope of its DOE Order 420.1A requirements for contractor system engineer programs, it did not include non-defense facilities within the scope of the SSO programs defined in the FTCP manual. Therefore, DOE has not established SSO programs for its nuclear reactors, which are the most complex and potentially the most hazardous nuclear facilities.

4.0 Overall Assessment

Since DNFSB Recommendation 2000-2 was issued, DOE has made important programmatic improvements for ensuring safety system functionality. Most contractors have established most of the basic elements of a system engineer program, as required by DOE Order 420.1A; have allocated appropriate resources for program implementation; and have appropriately trained and qualified their engineers. Most CSEs are very knowledgeable of their assigned systems and perform most of their duties effectively. In particular, CSEs provide effective day-to-day engineering support to plant operations and maintenance.

DOE field offices have made good progress in implementing newly-established SSO program requirements. In general, the field office SSO programs are well defined, have appropriate resources, and are making good progress in training and qualifying personnel. The FTCP has provided good support to SSO program development efforts, including developing program requirements and an informal qualification standard; performing site program assessments; and sharing lessons learned. DOE's NTC, in conjunction with the NNSA Service Center, has developed some appropriate training to support these DOE efforts.

Although most contractors have made good progress in implementing the system engineer program, some have not established some of the fundamental aspects of the program, such as program descriptions. Further, there are weaknesses in several important elements of the system engineering program at many sites, including a lack of processes for periodically performing detailed system assessments, insufficient tracking and trending of equipment performance, and incomplete technical documents defining the system design basis, such as system design descriptions.

Similarly, although most DOE site offices have adequately defined most aspects of the SSO program, some specific aspects of the program need to be better defined, such as the type and frequency of system assessments and expectations for documenting assessment results and tracking corrective actions. Furthermore, SSO program requirements have not been formally promulgated in an appropriate DOE directive and are not currently applicable to non-defense sites that have nuclear hazards equal to or greater than many DOE defense nuclear facilities.

5.0 Opportunities for Improvement

This Independent Oversight evaluation identified the following opportunities for improvement. These potential enhancements are not intended to be prescriptive or mandatory. Rather, they are offered to DOE program and field offices and DOE contractors as ways to improve their programs based upon insights Independent Oversight gained from this evaluation.

Central Technical Authority for Energy, Science, and Environment

1. **Expand the scope of applicability of requirements for SSO programs to include non-defense hazard category 1, 2, and 3 nuclear facilities, including DOE nuclear reactors.** Work with the Office of Environment, Safety and Health to incorporate this requirement in the DOE oversight manual.

Office of Environment, Safety and Health

1. **Incorporate SSO oversight responsibilities into the new DOE oversight manual, and provide additional guidance on SSO duties.** SSO responsibilities are currently defined in the FTCP manual but should be established in the new DOE oversight manual. Some SSO duties (e.g., performing assessments) that are not well defined in the FTCP manual should be better described when incorporated into the oversight manual (e.g., expectations for periodic, detailed assessments and expectations for support of system modifications, including review of documented safety analysis updates). Although flexibility should be allowed in site-specific methods for implementing the SSO program, additional guidance on expectations for performance of some duties would be appropriate. Lessons learned from establishment of the SSO program should be utilized when establishing these requirements, and the responsible organization should provide effective program support, such as that provided by the FTCP.

2. **Consider establishing a Facility Safety point of contact for the DOE Order 420.1A system engineer program requirement.** Evaluate benefits of providing field support similar to that provided by the Facility Safety organization within the Office of Environment, Safety and Health for other DOE Order 420.1A required programs, such as natural phenomenon hazards, construction safety, electrical safety, and fire protection.

Federal Technical Capability Panel

1. **Establish a complex-wide formal functional area qualification standard for SSO personnel.** Base the qualification standard on the informal standard developed by the Office of River Protection that is on the FTCP web page. Enhance this standard based on lessons learned from the site-specific SSO qualification standards developed to date and from refinements in SSO duties that may occur as a result of the development of the DOE oversight manual.

2. **Continue to share SSO program lessons learned via annual meetings or other mechanisms.** DOE meetings to share SSO lessons learned, such as those held in the past two years, have been very beneficial in program development. These meetings are effective for sharing both program lessons learned and detailed system and assessment information that contributes to better safety system oversight. Such efforts should be continued and enhanced based on lessons learned. For the next meeting, consider developing a lessons-learned document from the FTCP's assessments of individual site programs that addresses not only SSO program strengths and weaknesses, but also

lessons learned on performing self-assessments of the SSO program.

National Training Center

1. **Ensure that planned improvements in SSO training are reviewed (and if possible conducted) by experts in performing engineering assessments.** Upcoming SSO courses include planned improvements in instructions for performing engineering assessments. These improvements should be reviewed by experts who perform this type of assessment. Further, it would be beneficial for an expert practitioner to support the presentation of the course. It would also be appropriate to make this training available to contractor system engineers to support their assessment efforts.

DOE/NNSA Field Elements

1. **Establish programs for performing oversight of periodic detailed assessments of safety systems.** Ensure that contractors are performing detailed engineering/operability assessments, and evaluate their effectiveness by participating in them or by performing independent assessments. This opportunity for improvement is consistent with a recommendation provided in the January 2006 Independent Oversight report on essential system functionality.

2. **Establish expectations for formal documentation of assessment results.** For each of the different types of assessments performed by SSO personnel, establish a protocol addressing the format and rigor of documentation. Further, develop databases for assessment results to support tracking and trending of system performance.

3. **Enhance corrective action processes for SSO issues.** Ensure that SSO program documents describe the methods for addressing safety system issues and that these methods use, and are consistent with, the site office's corrective action process.

Site Contractors

1. **Improve the formality of tracking and trending of system performance.** Evaluate and incorporate industry practices. Evaluate the effectiveness of maintenance practices and procedures for documenting information important for trending equipment and system performance, and improve as needed.

2. **Share lessons learned.** As part of configuration management and/or engineering practices groups (e.g., the Energy Facility Contractors Group), share lessons learned on implementation of system engineering programs. Such sharing and communication are particularly important to support sites with immature system engineer programs.

3. **Clearly define the purpose of safety system technical basis documents and complete their development.** Prioritize systems based on their safety significance, history of configuration management, and complexity. During development of technical basis documents (or during detailed system assessments), validate important design assumptions and calculations, implementation of codes and standards, and translation of system requirements into surveillances and tests and operation instructions. This opportunity for improvement is consistent with a recommendation provided in the January 2006 Independent Oversight report on essential system functionality.

4. **Establish programs for performing periodic detailed assessments of safety systems.** Institutionalize the performance of phase II (operability) type reviews. Enhance these assessments by establishing review criteria for the design and operations areas (including review of detailed design information, such as calculations and assumptions) and by including a system engineer from another facility as a part of the review team, to provide expert support and cross-training. This opportunity for improvement is consistent with a recommendation provided in the January 2006 Independent Oversight report on essential system functionality.

5. **Develop self-assessment performance measures for system engineering programs.** Evaluate each activity that CSEs perform to determine whether appropriate performance measures can be established. Some potential performance measures include:

   - Number and type of assessments performed
   - Number and significance of system performance issues identified by the CSE as compared with those found during outside assessments
   - System reliability.

   Track performance to identify areas for improvement.

6. **Evaluate roles and responsibilities of system engineers to ensure that system engineers are adequately qualified and trained to perform their duties.** In particular, evaluate the role and qualification of system engineers in the development and review of engineering design changes.

This page intentionally left blank.