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

Independent Oversight Status Report

Essential System Functionality

January 2006

SSA

Office of Security and Safety Performance Assurance

OVERSIGHT

Table of Contents

EXECUTIVE SUMMARY 1

1.0 INTRODUCTION 3

2.0 POSITIVE ATTRIBUTES 5

3.0 WEAKNESSES 6

4.0 OVERALL ASSESSMENT 8

5.0 RECOMMENDATIONS 9

APPENDIX A: DETAILS OF WEAKNESSES IN SYSTEM DESIGN AND ANALYSIS, CONFIGURATION MANAGEMENT, AND TSR SURVEILLANCES 13

Abbreviations Used in This Report

CFR	Code of Federal Regulations
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
EM	Office of Environmental Management
ESF	Essential System Functionality
HEPA	High Efficiency Particulate Air
HVAC	Heating, Ventilation, and Air Conditioning
NE	Office of Nuclear Energy, Science and Technology
NNSA	National Nuclear Security Administration
SC	Office of Science
SSC	Structures, Systems, and Components
TSR	Technical Safety Requirement

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 (ES&H); and emergency management programs and reporting on their status to the Secretary of Energy, senior Department of Energy (DOE) management, Congress, DOE field elements, and site contractors. To facilitate improvements across the DOE complex, Independent Oversight periodically reports on the status of selected programs based on analysis of its site-specific evaluations. This report provides summary status, positive attributes, weaknesses, and recommendations for improvement from Independent Oversight reviews of essential safety systems at ten sites during 2004 and 2005. Essential safety systems are systems that either prevent or mitigate accidents that could adversely impact the health and safety of the public or site workers.

Although most essential safety systems that were reviewed were well maintained, tested, and operated, there were significant weaknesses in some aspects of engineering design and analysis that, for some safety systems, resulted in design flaws that could have prevented the systems from performing their safety functions. In addition, the seismic analysis and qualification for many safety systems were inadequate to demonstrate that they would adequately prevent or mitigate a release of hazardous material during a seismic event. Many of these weaknesses are attributed to a lack of rigor and attention to detail in performing design analysis. Configuration management continues to be a challenge at DOE sites, largely because of the age of facilities and insufficient control over system design in past years. Some sites have made important efforts to reconstitute their design basis; however, other sites have not made such efforts and have not adequately evaluated the safety ramifications of this condition. Weaknesses were also identified in the translation of design and safety basis documents into technical safety requirements, surveillance procedures, and other procedures and practices, and in the procurement of safety-related components.

DOE and contractor line management need to take actions to ensure essential system functionality across the complex, including:

- Ensure the quality of engineering products, with particular focus on:
  - The rigor and attention to detail of calculations/analysis that demonstrate the functionality of safety systems
  - The implementation of configuration management of safety systems' designs
  - The translation of design products into maintenance, surveillance and test, and operations requirements and procedures.
- Ensure that safety systems will remain functional during seismic events.
- Establish and rigorously apply periodic self-assessments of essential safety systems that include an evaluation of system design.

Specific recommendations for implementing these actions are provided in the body of this report.

Independent Oversight will continue to evaluate essential safety systems and the site programs supporting them, utilizing a bottom-up, "vertical slice" approach that results in detailed evaluation of system design, maintenance, and operation for a limited number of important components. This approach has resulted in the identification of some significant weaknesses that would not have been identified by evaluating systems only at a higher level. This approach may be useful for site contractors and site offices to consider adopting as part of their feedback and improvement processes.

This page intentionally left blank.

1.0 Introduction

In 2004 and 2005, the Office of Independent Oversight, within the Office of Security and Safety Performance Assurance, performed ten evaluations of essential system functionality (ESF). These ESF reviews are highly technical, detailed engineering evaluations of selected essential systems within one or more facilities at each site. This report summarizes the observations and insights from these reviews.

Essential systems include safety-class, safety-significant, and other defense-in-depth systems, such as fire protection, ventilation, and emergency electrical power, intended to prevent or mitigate the release of hazardous materials that could adversely affect the public, site workers, or the environment. The ESF reviews are detailed evaluations of the design, configuration management, maintenance, surveillance and testing, and operation of essential systems utilizing a "vertical slice" approach—that is, reviewing a focused sample in each of these areas from the basic functional requirements to the lowest detailed level implementing the requirements. Independent Oversight's ESF reviews are similar to and complement U.S. Department of Energy (DOE) and contractor line management reviews of vital safety systems performed in response to Defense Nuclear Facilities Safety Board Recommendation 2000-2, *Configuration Management, Vital Safety Systems*, but focus in greater depth on the design of the systems, the implementation of the unreviewed safety question process, and operation of the systems.

During this reporting period, Independent Oversight performed ESF reviews of 20 essential systems at the 10 DOE sites listed in Table 1. Table 1 also identifies the DOE program office that has management responsibility for each site: the National Nuclear Security Administration (NNSA); the Office of Environmental Management (EM); the Office of Nuclear Energy, Science and Technology (NE); or the Office of Science (SC). The systems that were reviewed include fire protection systems, ventilation systems, confinement systems, hoists and cranes, an offgas system, a hot cell, an irradiation cell, high-level waste tanks, a nitrogen system, refueling equipment, and reactor coolant systems.

Table 1. ESF Inspection Sites

Safety Management Inspection Site	Headquarters Program Office	Systems
Savannah River Site	EM/NNSA	Ventilation, offgas, nitrogen, fire protection
Hanford Tank Farms	EM	High-level waste tanks
Oak Ridge National Laboratory	SC	Refueling equipment, reactor coolant system
Lawrence Livermore National Laboratory	NNSA	Ventilation, fire protection
Pantex	NNSA	Hoist and cranes, confinement systems
Argonne National Laboratory	SC	Fire protection, hot cell

Table 1. ESF Inspection Sites (Continued)

Safety Management Inspection Site	Headquarters Program Office	Systems
Idaho National Laboratory	NE	Reactor coolant system (emergency feedwater system and primary pump shutoff system)
Sandia National Laboratories	NNSA	Irradiation cell and pool
Y-12 National Security Complex	NNSA	Fire protection and criticality systems
Los Alamos National Laboratory	NNSA	Ventilation and fire protection

2.0 Positive Attributes

At most sites, the functional requirements for safety systems are generally well defined and safety systems are in good material condition. In addition, a number of specific sites have established and implemented good practices that could be adapted and applied at other sites. However, although there are some program strengths, many systems had significance weaknesses in their design and configuration management, as discussed in Section 3.

Most safety systems' functions are well defined in safety analysis documents, and the systems have a robust design. Documented safety analyses (DSAs) appropriately define the safety functions and describe the accident conditions in which the systems are required to function. Most safety systems have been designed in accordance with industry standards and include appropriate safety margins to ensure that they will be able to perform their safety function. However, as discussed in Section 3, some specific design aspects of safety systems had weaknesses that could result in otherwise well designed systems being unable to perform their safety function under certain accident conditions.

Several sites have recently improved their configuration management programs. Several sites have established the basic elements of an effective configuration management program, including drawing controls, calculation controls, procedure revision protocols and controls, and a design change process to assure that facility modifications are properly evaluated, documented, reviewed, and verified to be within the bounds of the DSA, the technical safety requirements (TSRs), and applicable codes, standards, and DOE orders. However, many sites have not established effective configuration management programs, and implementation concerns were identified at all sites.

TSR surveillances are performed at the required interval and are appropriately tracked. All the sites that were evaluated have effective programs for ensuring that TSR surveillances are performed as required. TSR surveillances have been performed on time, and most results are well documented.

Safety systems are in good material condition, with minimal maintenance backlog. In general, the systems that were reviewed are in good physical condition. Facility management has appropriately prioritized maintenance on the safety systems, and therefore corrective maintenance backlogs are very low.

System operators demonstrated a high degree of competence, training programs are effective, and operations instructions and procedures are generally appropriate to support system operations. In general, management at the evaluated facilities has established effective programs for preparing operators to operate the safety systems under normal, upset, and emergency conditions. Training and qualification programs are formally documented, and the operations and maintenance personnel who were interviewed demonstrated good understanding of system design and operations. With few exceptions, operations procedures are well maintained, and safety system training is effective.

3.0 Weaknesses

Although there are a number of positive attributes, ESF evaluations identified many specific deficiencies. Collectively, these deficiencies indicate a number of broad weaknesses in such areas as system design, configuration management, surveillance procedures, and procurement programs. These weaknesses have resulted in design or other flaws that could render the safety systems unable to adequately perform their safety function to prevent or mitigate an emergency. A summary of weakness is provided below. Appendix A includes detailed examples in three areas: (1) system design and analysis, (2) configuration management, and (3) TSRs and TSR surveillances.

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. Although most of the system components reviewed by Independent Oversight were adequately designed, some important components were not. In many instances, the analysis supporting component or system design was missing or inadequate. These weaknesses can prevent or degrade the ability of safety systems to perform their safety functions under certain accident conditions.

DOE and contractors have not ensured that seismic evaluations are complete and well documented. At most of the sites, concerns were identified in the rigor of seismic analyses, including: (1) seismic qualifications that were based solely on facility walkdowns, which were inadequately performed and inadequately documented; (2) incomplete documentation of the evaluation of the seismically-induced interactions between the non-seismically-supported overhead structures and safety structures, systems, and components (SSCs); and (3) systems that are required to perform an active safety function, as well as passive barriers, not designed or evaluated to survive/function following a design basis accident seismic event. In addition, some isolated concerns were identified; for example, a master equipment list did not identify requirements for non-safety components whose seismic qualifications related only to seismic interactions with other safety-related components, and an evaluation of the impact of a seismic event did not adequately consider a situation in which some ventilation systems remain operating while others fail.

Contractors have not rigorously implemented configuration management requirements to ensure that safety systems will continue to be capable of performing their safety functions. Current configuration management requirements set expectations to ensure that facility designs, operations, testing, maintenance, etc., remain within the bounds established by the DSA, TSRs, applicable design documents (including design analyses), and applicable rules, regulations, codes, standards, orders, etc. Some sites have made significant improvements in configuration management, including development of system design descriptions. However, many of the safety systems that were reviewed did not meet DOE configuration management requirements in several areas, including: (1) establishment of basic configuration management/engineering processes, (2) establishment of configuration management baselines, and (3) implementation of configuration management processes.

Contractors have not ensured that safety systems' surveillance procedures include all surveillances required by the safety analysis and are sufficient to ensure system operability. The evaluated sites have established a set of system surveillance and testing requirements that appropriately test most system functions. However, many specific weaknesses were identified that reduce the assurance that the systems will function as required, including: (1) safety system components not adequately tested, (2) TSR limits/controls not appropriately identified, and (3) inadequate test procedures.

Weaknesses were evident in some specific aspects of safety system maintenance. Although maintenance of safety systems is generally well defined and performed, at many sites maintenance information was not being tracked or trended and/or methods for documenting completed maintenance work were

not sufficient to support performance trending (e.g., maintenance history not captured and maintained in a system that permits timely retrieval). Further, weaknesses were identified in several other areas, including: (1) the preventive maintenance of safety systems for preventing criticality events was not well defined or performed; (2) post-maintenance testing was incomplete—for example, no pump run performed following pump changeout, no vibration test performed after pump changeout, and no post-replacement testing requirements to verify the integrity of the replacement high efficiency particulate air (HEPA) filter; (3) maintenance recommendations from vendor manuals were not performed; and (4) outside organizations' testing and maintenance procedures were not adequately reviewed to ensure that they are appropriate and do not invalidate the safety basis.

Procurement processes have not been appropriately defined and rigorously implemented. Independent Oversight identified concerns in procurement of safety components at several sites. Particular concerns were identified in commercial grade dedication (or "like-in-kind" dedication) of safety components. In some cases, procurement processes had outdated procedures that did not reflect current practices or did not have a formal procedure for control of replacement parts. In addition, commercial grade dedication processes were not adequate in some cases; for example, environmental qualification requirements were not addressed, procurement of quality-significant spare and/or consumable items was not addressed, and an equivalency evaluation procedure for determining the acceptability of non-like-for-like components was not included. Furthermore, procurement processes were not adequately implemented in some cases; for example, spare parts were not certified to the correct quality level, and like-in-kind documentation or other quality-significant dedication procurement documentation was not developed. Also, some critical details (e.g., fluid service conditions, critical dimensions) were not documented on procurement documents, and dedication test requirements were not included on the test data sheet.

There were weaknesses in certain aspects of programs for ensuring appropriate operation of safety systems. Sites generally have established appropriate operating procedures (including normal, alarm response, abnormal, and emergency procedures) and have appropriately trained operators. However, weaknesses were noted in certain areas. For example, a number of alarm response procedures were outdated, and in one case, no procedure had been developed for an important hazardous process (utilizing a bypass key to allow raising a radioactive source into a cell with the cell door open).

4.0 Overall Assessment

Most essential systems that were evaluated are well maintained, tested, and operated, and they are generally well designed in most respects. Most safety systems that were evaluated have been designed in accordance with industry standards and include appropriate safety margins. DSAs appropriately define the safety functions and describe the accident conditions in which the systems are required to function. In most cases, tests for important system controls are adequately specified in TSR surveillances and are appropriately performed and tracked. The material condition of systems is generally appropriate, with timely preventive maintenance and small corrective maintenance backlogs. Some sites also perform predictive maintenance effectively. Most operator procedures, including those for normal, abnormal, alarm, and emergency operations, are clear and provide appropriate instructions. Operator training and qualification programs are good, and as a result, operators are very knowledgeable of the safety systems and demonstrated the ability to operate them safely.

However, some significant design and design analysis weaknesses were identified at many sites that could prevent or degrade the performance of intended safety functions in some of the systems that were reviewed. These weaknesses are primarily attributable to a lack of rigor and attention to detail, and poor configuration management. Further, several safety systems, or other systems that could impact safety systems, have inadequate seismic analysis and qualification. There are also weaknesses in the translation of designs into facility procedures and practices, including TSR surveillance and test requirements. Typical TSR surveillance weaknesses include not addressing all appropriate industry standards and not verifying all of the systems' safety functions. Weaknesses were also identified in some aspects of maintenance and procurement programs. For example, weaknesses were identified in predictive maintenance and tracking and trending and in dedication of commercial-grade components for safety system use.

These conclusions, based on the 2004 and 2005 inspections, are generally consistent with the results of Independent Oversight ESF evaluations performed in 2002 and 2003, which were reported in a safety management lessons-learned report issued by Independent Oversight in 2004. Although improvements since 2004 were noted at some sites, particularly in configuration management, further improvements in the technical quality of engineering design and design reviews are needed to assure that safety systems will perform their required safety functions.

5.0 Recommendations

Because of the significance of the weaknesses and the importance of safety systems in protecting the public, workers, and the environment, DOE line management needs to take comprehensive, rigorous, and timely actions to ensure that improvements are made in a number of important aspects of safety systems and related programs. Further, because the deficiencies are evident in a wide range of facilities and systems, DOE program office leadership is needed to ensure that all DOE field elements and site contractors are adequately evaluating their current systems and identifying and making needed improvements.

DOE/NNSA Line Organizations (Program Offices and Field Elements)

1. **Improve the oversight of the quality of engineering products.** Specific actions to consider include:

    - Perform detailed assessments of contractor-developed design documents, evaluating the degree of rigor, level of technical justification, and attention to detail in safety system design.

    - During design of new safety systems (or modification of existing safety systems), perform independent reviews of design documents, including assessment of supporting calculations.

    - Evaluate the effectiveness of the contractor's quality assurance processes (including independent review) for design calculations.

2. **Improve oversight of configuration management and resolution of configuration management deficiencies.** Specific actions to consider include:

    - Ensure that adequate resources and oversight are provided for new design projects to ensure that as-built drawings and other design products are completed and put into document control prior to project closure.

    - Perform a detailed review of a sample of design modifications, addressing the rigor of translation of design products into maintenance, surveillance and test, and operations procedures; the process for updating drawings and other affected documents; and the training of maintenance and operations personnel.

    - Evaluate contractors' processes for resolving identified configuration management deficiencies. Evaluate whether the impact of configuration management deficiencies on system reliability and operability has been formally considered and whether the contractor has an effective process for reconstituting the design basis of systems.

    - Establish and rigorously apply periodic self-assessments of essential safety systems using an approach and methodology similar to that of Independent Oversight.

Note: The above opportunities for improvement may be implemented as part of the safety system oversight program outlined in the Federal Technical Capabilities Panel manual M426.1 and are consistent with improvement items discussed in Independent Oversight's report on safety system oversight.

Site Contractors

1. **Improve the degree of rigor, level of technical justification, and attention to detail in the design and review of safety systems.** Specific actions to consider include:

- Require that system engineers perform detailed reviews of new design modifications, including detailed review of all supporting calculations.

- Establish design/operations review boards made up of representatives from all technical disciplines. Their function would be to perform detailed technical reviews of all design and technical procedure changes, including supporting analyses, before they are issued for use, in order to assure their technical quality and that the changes will accomplish their intended purpose without compromising any other safety functions or purposes.

- Establish standards/procedures that specify requirements for development, documentation, content, format, rigor, review, and approval of engineering calculations and other similar engineering output documents to assure that such documents meet the quality requirements of 10 CFR 830 and American National Standards Institute (ANSI) standard N45.2.11.

- Enhance quality assurance checks on the adequacy of technical products, and include a performance measure on the number of errors that quality assurance identifies.

- Inventory, catalogue, and properly store for convenient retrieval all existing facility-related calculations and other technical documents, particularly those related to important-to-safety SSCs.

- Review the safety analysis for all statements or implications of performance capabilities of safety SSCs. Verify that all such statements or implications are supported by analyses and, where appropriate, testing. Verify that such analyses and testing are adequate to demonstrate these statements or implications. Where they are missing or inadequate, regenerate them, making appropriate changes to the safety analysis to reflect the results.

2. **Improve procedures for performing and reviewing calculations.** Ensure that procedures include the following requirements: (1) important design inputs are derived from controlled documents, standard reference sources, or documents that have received independent verification; (2) all design inputs are referenced; and (3) the actual computations are included in the calculation, and computations are checked as part of the review.

3. **Improve processes for seismic analyses.** Specific actions to consider include:

    - Ensure that seismically induced interactions between non-seismically-qualified SSCs and important-to-safety SSCs are analyzed to assure that such interactions will not prevent or degrade their safety functions and that documentation of such analyses is complete.

    - Revise the modification process to require a review of the seismic interactions and environmental qualification requirements for any modification of important-to-safety SSCs.

    - Enhance seismic interaction walkdown procedures to require documentation of all seismic hazards and the justification for accepting potential hazards.

4. **Improve configuration management programs.** Specific actions to consider include:

    - Define expectations for configuration control, including timeliness of document updates.

    - Ensure that superseded calculations are identified and controlled in accordance with guidance provided in DOE STD 1073.

    - Establish configuration management performance indicators that measure the effectiveness of keeping system documentation up to date.

- Ensure that new projects include appropriate resources to support configuration management. Also ensure that the priority for bringing new systems or projects online does not override the priority for proper configuration management.

- Establish the status of configuration management of each safety system (for example, the adequacy and completeness of as-built drawings and other technical basis documents). Identify deficiencies, prioritize corrective actions, and track progress.

- Perform a comprehensive review of the safety-related equipment list. This review should identify all safety-related SSCs and all of their safety functions, including seismic integrity required to prevent interaction with other safety-related SSCs.

The last two bulleted items could be performed as part of system engineer duties, including the performance of system assessments required by DOE Order 420.1b. The priority for systems chosen for these efforts should be based upon the importance of the system in preventing or mitigating hazards, the complexity of the system, and the lifetime of the facility.

5. **Review safety system surveillance procedures to ensure that they include all surveillances required by safety analyses and are sufficient to verify all system operability and capability statements.** This review could be performed as part of system engineer duties, including the performance of system assessments required by DOE Order 420.1b. The priority for systems chosen for these efforts should be based upon the importance of the system in preventing or mitigating hazards, the complexity of the system, and the lifetime of the facility.

6. **Improve procurement plans and processes.** Specific actions to consider include:

   - Ensure that procurement procedures adequately prevent installation of materials or components in safety-related systems if the procurement inspections, certifications, and/or tests are not complete and properly documented. As an initial effort, procurement documentation for currently existing spare items that are slated to be used in safety-related applications (e.g., spare motors and belts) should be reviewed and corrected as needed.

   - Establish a thorough review process for new like-in-kind determinations to ensure that the process is correctly implemented and that the final documentation, including the acceptance sheets, is properly completed.

   - Ensure that commercial dedication procedures include steps for ensuring that seismic and environmental qualification evaluations are performed.

This page intentionally left blank.

APPENDIX A

DETAILS OF WEAKNESSES IN SYSTEM DESIGN AND ANALYSIS, CONFIGURATION MANAGEMENT, AND TSR SURVEILLANCES

This appendix provides details of examples of weaknesses in (1) system design and analysis, (2) configuration management, and (3) technical safety requirements (TSRs) and TSR surveillances. The purpose of providing these details is that DOE field offices and contractors may use them as examples of the type of weakness to avoid in initial design or areas to examine when evaluating current system capabilities. These details also provide supporting documentation of the general weaknesses discussed in the main body of the report.

System Design and Analysis Weaknesses

Examples of inadequate system or component design include:

- Several large radioactive waste tanks were not adequately designed to relieve potential vacuum conditions. For example, some actively ventilated tanks did not have relief devices, and for some tanks that had such devices, the vacuum relief function had not been demonstrated as adequate for design considerations. Other installed engineered devices that might have provided some vacuum relief protection had intermediate isolation valves between the devices and the tanks, which is contrary to code requirements and commonly accepted good engineering practice.

- One fire water system had inappropriate design for transferring to the backup water supply, and another had inadequate water supply pressure.

- One safety-related ventilation system had a design flaw in that it could fault to a condition where one supply fan is running with no exhaust fans, thereby inappropriately pressurizing the potentially contaminated area. Another safety-related ventilation system relied on inadequately designed outside static air probes to provide control of heating, ventilation, and air conditioning (HVAC) systems. The probes were located at the roof edges, which were not representative of the building's geometry, and were subject to updrafts, and the probes' hardware geometry was inappropriate for static pressure measurement.

- The descent speed for a radioactive source elevator safety system was not fast enough to ensure protection of workers if cell barriers were violated.

Examples of inadequate design analysis include:

- For ventilation systems at some sites, the potential for failure of the safety-class room exhaust high efficiency particulate air (HEPA) filters due to combustion product loading during a design/evaluation basis fire was not analyzed. In addition, the ability of HVAC ductwork and HEPA filters to withstand the temperatures identified in the fire hazard analysis was not analyzed. Further, at one site the fire hazard analysis did not address the effect of a room fire on oil bubblers for gloveboxes, the resulting effects of this oil on HEPA filter loading, or the potential for fire in the ducts.

- For a site fire protection system, the ability of the safety-class water supply to perform one of its safety functions (supply water to all safety-class deluge nozzles) had not been analyzed. At another site, there was no documented basis for the dry pipe sprinkler air pressure, resulting in insufficient assurance that high pressure would not delay the water supply to activated sprinklers.

- For a site fuel pool system, the structural analysis of some fuel pool components was missing or inadequate. Specifically, a heavy load (fuel pool dam) lifting lug analysis was not rigorously performed (e.g., load path not adequately defined), resulting in uncertainty whether the lug could withstand, with appropriate safety margin, all potential load conditions. Further, there were no

structural analyses for the fuel handling tools. In addition, the analysis of the impacts of fuel pool heatup on loss of normal cooling was incomplete, so the potential thermal stresses on the fuel pool had not been evaluated to assess structural integrity, and there were no supporting calculations for the pool makeup water system's makeup capability.

- Various other issues in the analyses of miscellaneous systems indicated a broad lack of rigor in system design analysis. Examples include:

  - A load drop analysis did not account for dynamic forces of a falling load.

  - The calculation of the ability of crane trolley stops and bridge stops to withstand the impact of a moving trolley/bridge contained errors and oversights.

  - Potential valve leakage from a safety system to a non-safety system was not included in the design calculation for adequacy of safety-system nitrogen supply.

  - An unverified value for uranium concentration was used as input to the calculation of a safety system isolation time. (Isolation time was important to ensure that a critical mass does not accumulate in case of system breach.)

- In a number of instances, safety analysis processes and products did not demonstrate sufficient rigor. Examples include:

  - Safety analyses did not address DOE's design criteria or did not provide a basis for not meeting some design criteria (e.g., single failure criteria). In one case, an exemption from the single failure criteria for a safety-class component was not adequately justified.

  - Safety analysis conclusions and assumptions were not formally documented.

  - Important barriers to release of radioactive material were not appropriately designated as safety-significant or safety-class.

  - The safety designation of components of a safety system did not have a well-documented basis and/or were non-conservative in several instances. For example, several structures, systems, and components intended to prevent acute worker injury or fatality were not appropriately classified as safety-significant in the documented safety analysis (DSA).

  - The airborne release fraction used in the safety analysis was non-conservative for the event that was analyzed. The evaluation did not consider additional combustible material from the design basis event (plane crash), resulting in a release fraction that was too low by a factor of ten.

Configuration Management Weaknesses

Examples of deficiencies in configuration management/engineering processes include:

- Some sites have not established engineering process procedures for functions, such as design calculations and design modifications, to ensure design consistency and compliance with the safety analysis and applicable codes and standards.

- Some quality assurance programs are not well defined to ensure quality in design and configuration management.

- None of the sites that were evaluated have a method for identifying current controlling calculations.

- Some modification processes lack specific requirements to evaluate environmental qualification and seismic interactions.

Examples of deficiencies in the configuration management baseline include:

- Most sites have an incomplete set of facility baseline technical documents (e.g., missing vendor documents).

- Technical basis "summary" documents and indexes (such as system design descriptions) are not fully

developed, not kept up to date, incomplete (e.g., do not reference vendor documentation), and inaccurate.

- System diagrams (e.g., piping and instrument drawings) or other design documents that indicate boundaries and interfaces with other systems are incomplete or out of date.

- Master equipment lists or equipment lists are not sufficiently detailed or are poorly maintained, resulting in an inadequate foundation for the quality assurance program for nuclear grade components.

- Design records cannot be readily retrieved.

Examples of deficiencies in implementation of configuration management processes include:

- Design basis calculations have not been kept up to date and do not reflect the systems' current configurations.

- Lack of rigor and failure to follow procedures are evident in processing and documenting design modifications. Modifications were incompletely documented (e.g., design verifications, supporting calculations, quality control measures, procurement requirements, and required changes to affected procedures), and engineering calculations were not performed according to procedures.

- The fire hazard analysis does not conform to current facility configuration (e.g., does not reflect sprinkler or fire detection system modifications).

- Modifications have been inappropriately performed as maintenance.

- Unreviewed safety question screening procedures and their implementation are deficient, resulting in some facility changes not receiving the appropriate level of review to ensure that the changes were within the safety basis. Independent Oversight issued a lessons-learned memorandum on this topic in October 2005.

- There was inadequate control of safety basis documents (both the currently applicable document and the proposed revision) during the transition to a new DSA.

TSR and TSR Surveillance Weaknesses

- Some safety system components were not tested, including fire protection system check valves that served as boundaries between safety-class and non-safety-class systems, hot cell safety-class backup nitrogen supply solenoid valves, and fuel pool cooling water supply valves.

- TSR limits were not appropriately established in a number of instances. For example, some important parameters for ensuring system functionality did not have a TSR limit; these included liquid nitrogen supply tank levels for a safety system, containment cell pressure, and design minimum temperature for batteries supporting a safety-class system. In addition, some TSR limits were not based upon appropriate engineering or safety analysis criteria, including:

  - Overpressure in fire water tanks was less than that specified in the National Fire Protection Association (NFPA) code, which was utilized for sizing the tanks.

  - The minimum pressure requirement for nitrogen backup tanks was less than the pressure value used in the calculation of record for the original tanks.

  - The identified minimum static fire water header pressure was much less than the pressure needed to achieve the required flow in the sprinkler system, as determined by hydraulic calculations.

  - Limits for combustible material loading were not based on the HEPA filter loading capability.

  - The minimum air compressor starting pressure was less than the value identified in the safety analysis.

- The delta pressure limit between a building interior and exterior had not been established and/or did not account for wind effects.

- The hazardous material limit was greater than specified in the safety analysis criteria.

- A number of tests or test procedures were inadequate. Examples include:

  - Some surveillances inappropriately contained preconditioning steps (such as adjusting wiring, connections, switches, and belts; checking that the starting battery is charged; etc.).

  - A surveillance procedure did not require calibration of TSR instrumentation.

  - Some surveillance procedures did not adequately test safety functions. For example, in one case, the surveillance did not test whether the safety function occurred at the required set point, but rather performed a simple go/no-go test at worst-case conditions. In another case, diesel fire pump test data was not corrected to account for actual engine speed during the test.

  - A surveillance procedure did not perform an internal inspection of check valves to check for wear as required.

  - A surveillance procedure did not verify that leakage through check valves was within acceptable parameters.