A.J. Eggenberger, Chairman
John E. Mansfield, Vice Chairman
Joseph F. Bader
Larry W. Brown
Peter S. Winokur

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700 Washington, D.C. 20004-2901
(202) 694-7000

October 16, 2007

The Honorable Thomas P. D'Agostino
Administrator
National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. D'Agostino:

The Defense Nuclear Facilities Safety Board (Board) continues to be concerned about the safety of nuclear operations at Los Alamos National Laboratory (LANL). Many of the Board's concerns were raised in a public meeting held in Los Alamos, New Mexico, on March 22, 2006, and were reiterated in a letter to the National Nuclear Security Administration (NNSA) dated February 1, 2007. In particular, the Board encouraged NNSA to improve safety bases and ensure the efficacy of safety systems with a "focus on rapidly increasing confidence in these safety systems, particularly safety-class systems."

The Board has become increasingly concerned in the overall lack of progress with respect to safety improvements at LANL. The Board notes that laboratory management has developed a set of multiyear improvement initiatives in an attempt to provide long-term solutions to these significant and persistent safety issues. One initiative is the Safety Basis Improvement Plan which is designed to provide high-quality safety bases that meet current requirements for all nuclear facilities. The Formality of Operations initiative is an effort intended to strengthen and standardize practices relative to conduct of operations, engineering, maintenance, and training. Additionally, limited initial actions are being taken to address significant engineering resource shortfalls highlighted in a recent laboratory staffing analysis. These efforts appear to be positive and mutually reinforcing. However, none of these initiatives are mature, and continued federal and contractor management attention and support are needed to ensure their success. These initiatives will take multiple years to drive tangible improvements at the floor level. The Board remains convinced that NNSA should focus on rapidly improving credited safety systems.

This conviction is supported by the results of a recent review by the Board's staff that assessed the design, function, and maintenance of selected safety systems at three of LANL's principal nuclear facilities: the Plutonium Facility, Weapons Engineering Tritium Facility, and Chemistry and Metallurgy Research Facility. The results of the staff's review, which are included as an enclosure to this letter, indicate that a number of significant and systemic deficiencies exist at LANL related to assuring the design, functionality, and maintenance of

safety systems. These deficiencies appear to be widespread, and of varying levels of severity, at each of the facilities reviewed by the staff. They include the following:

- Incomplete or inadequate descriptions of system safety functions;
- Weak or missing fundamental design information and calculations;
- Failure to verify credited safety functions through periodic surveillance and testing;
- Failure to implement appropriate maintenance activities to ensure that safety systems can continue to perform their credited function;
- Lack of adequate normal and abnormal operating procedures to govern the operation of safety systems;
- Lack of formal setpoint calculations for critical system operating parameters; and
- Outdated and, in some cases, inadequate safety bases.

While it is arguable whether any of the individual system deficiencies identified by the staff constitute an immediate safety concern, their collective importance and widespread nature warrant immediate attention. In particular, these issues cast doubt on the laboratory's ability to demonstrate that credited safety systems can reliably perform their safety functions under all required design basis conditions. Additionally, the Board is concerned that the contractor and Los Alamos Site Office are not providing the level of oversight required to identify the types of issues reflected in the staff's report. Based on the findings in the enclosed staff report, the Board lacks confidence in LANL's efforts to improve the reliability of safety-related systems.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and briefing within 60 days of receipt of this letter describing specific actions NNSA has taken to (1) facilitate timely and effective implementation of ongoing safety improvement initiatives for nuclear operations, (2) rapidly increase confidence in safety systems currently relied upon in operating nuclear facilities, and (3) improve the federal oversight of safety systems at LANL.

Sincerely,

A. J. Eggenberger
Chairman

c: The Honorable J. Clay Sell
Mr. Mark B. Whitaker, Jr.
Mr. Donald L. Winchell, Jr.

Enclosure

**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**

**Staff Issue Report**

August 31, 2007

**MEMORANDUM FOR:** J. K. Fortenberry

**COPIES:** Board Members

**FROM:** J. L. Shackelford

**SUBJECT:** Design, Functionality, and Maintenance of Safety Systems at Los Alamos National Laboratory

This report documents a review of the design, functionality, and maintenance of safety systems at Los Alamos National Laboratory (LANL), performed by the staff of the Defense Nuclear Facilities Safety Board (Board). This review was conducted by B. Broderick, C. Keilers, J. Plaue, C. Roscetti, and J. Shackelford during July 24–26, 2007.

**Background.** The Board's staff conducted a review at LANL to assess the design, functionality, and maintenance of selected safety systems at the Plutonium Facility (PF-4), Weapons Engineering Tritium Facility (WETF), and Chemistry and Metallurgy Research (CMR) Facility. The review focused on the design, safety basis, and other calculations and analyses for the selected systems, and evaluated the functional requirements for the systems during accident or abnormal conditions. The staff reviewed system test, surveillance, and maintenance activities to investigate whether the acceptance criteria specified for these activities were adequately supported by design calculations or other engineering documents. The review included an assessment of the normal and emergency operation of the systems to determine whether such operations were governed by approved operating procedures and were consistent with the design basis.

The staff noted that some earlier assessments, such as the November 2005 inspection by the Office of Independent Oversight, had identified a number of deficiencies at LANL regarding design bases, surveillance, and maintenance. The previous contractor attempted to address these deficiencies through institutional improvement initiatives, including the now terminated "Operational Efficiency" effort. More recently, the present contractor developed and has begun implementing a new approach known as the "Formality of Operations" initiative, which includes elements related to conduct of engineering, operations, maintenance, and training. This effort is not yet mature or fully implemented. As a result, limited benefits have been realized at the floor level from these efforts.

The following sections summarize the staff's findings regarding the safety systems that were reviewed at specific laboratory facilities.

**Plutonium Facility**

*Instrument Air System (IAS)*—The IAS is identified as a safety-significant system whose function is to support the safety function of the ventilation system. The system is intended to supply compressed air for the ventilation system's pneumatic controls and the primary start capability for the non-safety-related standby diesel generator.

While a draft is in progress, no formal system design description existed for the IAS at the time of the staff's review. Further, the system lacked a complete set of approved engineering drawings. As a result, there was inadequate formal design information available to support an effective program of surveillance, testing, and configuration management. For example, it appeared from an operational perspective that both the quality and moisture content of the air were important process variables associated with the system. However, these parameters were not discussed in any of the design documents, and there were no surveillance or test procedures that verified these parameters. Consequently, the inoperability of the system air dryers would likely lead to overall system degradation and operability issues, but no Technical Safety Requirement (TSR) controls or limiting conditions for operation existed to address this situation.

Other IAS deficiencies included (1) a lack of permanent system component identifiers, (2) the absence of normal or abnormal operating procedures, and (3) the lack of a formal calculation for the setpoint associated with the annual system test used to verify the ability of the ventilation system to shut down on a loss of air. Consequently, it was unclear whether the test actually verified the assumptions set forth in the safety basis.

*Vault Water Baths*—The vault water baths are identified as a safety-class system to shield the heat-generating plutonium containers from convective and radiative heat transfer during a fire in the vault room. The system includes a noncredited heat exchanger that is used to remove heat from the containers. The safety function of the water bath cooling system does not appear to have been adequately defined, documented, and assured.

The new and recently approved system design description is inconsistent with Department of Energy (DOE) Standard 3024-98, *Content of System Design Descriptions,* as well as the existing institutional procedure. Specifically, it does not contain an adequate description of the system requirements and bases. For example, the system lacks an adequate design calculation addressing the expected system heat loads. The existing calculation is an informal, poorly documented assessment that contains a number of mathematical errors, nonconservative assumptions, and misconceptions regarding fluid flows and heat transfers. Based on the available system specifications and using conservative assumptions, the staff performed an assessment of the system and determined that at the maximum postulated design loading (a parameter not captured in the system design description, but obtained from the informal calculation), the system heat exchanger is probably significantly undersized to meet normal system cooling needs. DOE and the contractor asserted that the heat exchanger is not credited in the safety basis; however, the staff noted that at the maximum design loading of the plutonium containers, a (much larger) heat exchanger appeared to be required to prevent boiling in the system.

Other deficiencies included the following: (1) not all system valves or components were adequately labeled, and (2) no abnormal operating procedures existed for the system.

**Weapons Engineering Tritium Facility (WETF)**

*Tritium Gas Handling System (TGHS)*—The TGHS is identified as a safety-significant system whose safety function is to provide primary containment during tritium processing activities.

The TGHS has an approved system design description; however, the document is incomplete and does not meet the expectations set forth in the institutional procedure. Additional design information associated with the TGHS is contained in the WETF Final Safety Analysis Report (FSAR) and other documentation. The functional requirements of the system include the following performance criteria:

- TGHS shall be leak tight to $10^{-3}$ std $cm^3/s$ at 1 atm.
- TGHS shall be designed and built to Performance Category (PC)-2 performance criteria.
- TGHS shall be built and designed to have overpressure protection to the maximum allowable working pressure.
- TGHS shall have overtemperature protection on heated sections of the system.

Notwithstanding these explicit performance criteria, the only relevant surveillance associated with the TGHS was an annual in-service inspection of the system that required a visual inspection for signs of wear, degradation, or unauthorized modifications. This inspection consisted primarily of a subjective, qualitative assessment of overall system condition, and did not specifically verify any of the safety functions listed above. Contractor personnel indicated that they relied on various noncredited operational parameters and operators' system awareness during operations to verify the safety function of the system, instead of a formal test or surveillance, in the belief that such testing would be difficult and disruptive. As a result, the staff concluded that surveillance activities did not adequately verify the credited safety functions of the system. With respect to overpressure protection, the staff noted that no formal design calculations were in place to verify that the capacity of the credited system equipment (i.e., the system "dump tank") was sufficient to handle the design basis overpressure volume. In the case of overtemperature protection, it was observed that such protection was afforded by a number of portable monitoring and circuit interruption devices that were attached to the relevant system components. However, the safety pedigree of these devices was uncertain. It also appeared that no formal documented setpoint calculations taking into account loop and instrument uncertainties were available to demonstrate that the devices could carry out their desired safety function. There were also no surveillance requirements associated with verifying and maintaining this credited safety function.

Other deficiencies observed regarding the TGHS included the following: (1) the functional requirement for the TGHS to remain leak tight during an evaluation basis fire had no associated performance criteria; (2) a number of general guidance documents were available to govern system precautions and lineups, but no formal operating procedures existed to prescribe the full range of operational alignments; and (3) the abnormal operating procedures for anticipated system upset conditions were weak and relied heavily on operator knowledge and training in concert with management involvement.

*Inert and Oxygen Monitoring System (I&OMS)*—The I&OMS provides indication and alarm for a high oxygen concentration in the WETF gloveboxes. The inerting function of the system provides and maintains an inert atmosphere to prevent a fire and formation of tritiated water vapor.

A number of deficiencies were identified with respect to the I&OMS. In particular, the system's alarm setpoint of 4 percent oxygen, which is credited in the TSR to prevent combustion, lacked a design calculation. This deficiency was exacerbated by the fact that the methodology for the semiannual surveillance could result in actuating the alarm as high as 4.5 percent. Moreover, some detectors were unfastened, which could lead to improper oxygen measurements due to obstruction of the detectors.

Other deficiencies noted with the I&OMS included the following: (1) the system uses two differently scaled meters (0–5 percent and 0–25 percent) to display the oxygen concentrations, which could lead to inconsistencies in the alarm actuation setpoints; (2) the weekly surveillance procedure only verified that the system had electrical power. The weekly surveillance could not readily detect a failed oxygen sensor; and (3) the limited procedures for response to an elevated oxygen concentration were weak, relied heavily on operator knowledge and training, and would not necessarily result in elimination of the potential combustion hazard.

**Chemistry and Metallurgy Research Facility**

*Wing 9 Hot Cell Door Interlock System*—The hot cell door interlocks are a safety-significant system designed to limit radiation exposure to workers performing operations in the CMR hot cells. The system uses an array of detectors to monitor radiation and prevent the operation of various combinations of doors, if elevated radiation levels are detected.

Based on the geometry of the hot cells and the placement of the detectors, it is not apparent that the calculation used to determine the detector setpoint of 32 mrem/hr is conservative, especially when the sensitivity of the detectors is taken into account. The system design also included a delay of 120 seconds to allow sufficient time for the detectors to detect a high-radiation condition and send a signal to the logic circuits. However, there is no analysis to support a determination of whether this time interval is sufficient to achieve the desired safety function.

Other deficiencies associated with the interlocks included the following: (1) the system lacked a formal system design calculation; (2) the periodic surveillance performed to test the safety function of the interlock only verified the logic circuits and did not physically test whether the interlock would actually work to prevent door operation; (3) no preventive maintenance was specified for the flexible hoses used to convey the high-pressure hydraulic fluid to actuate the 18 ton doors; (4) the backup hydraulic hand pump would not be capable of shutting an open door after a hydraulic rupture, and there were no abnormal operating procedures to guide operator recovery action; and (5) during a walkdown of the system, the staff discovered an unauthorized temporary modification installed on the system, and the cognizant system engineer had not been made aware of the modification or its effects on the system safety function.

*Hot Cell Manipulator Boot Seals*—The hot cell manipulator boot seals are identified as a safety-significant system at the CMR Facility. Their safety function is to prevent or minimize personnel exposure caused by contamination leakage from the hot cell manipulators.

No formal system design description had been developed for the boot seals. Rather, the only relevant design information was contained in the CMR Basis for Interim Operation (BIO) and various system and component drawings. A more recent (though unapproved) BIO specifically defines the boot seal safety function as being able to maintain pressure of at least 0.25 in. wc (water column) with air or nitrogen at a flow rate of less than 30 scfh (standard cubic feet per hour). The staff found that no formal surveillance testing or TSRs existed to confirm or otherwise verify the safety function of the boot seals. Rather, the facility relied on operator knowledge of the system to ensure that it functioned as expected. Indications of system operation were available to the operators via pressure and flow gauges in the vicinity of the controls for the manipulator arms outside the hot cells. In many cases, however, these indications were well above eye level and would be difficult to monitor during normal operation. There were no alarms associated with acceptable leakage thresholds, and the instrumentation provided did not appear to be in a formal calibration program.

Other deficiencies observed with the boot seals included the following: (1) there were no normal or abnormal operating procedures for the system, and as a result, it was unclear whether conservative action would be taken following a loss or malfunction of the boot seal system during operation; (2) maintenance activities associated with the boot seals relied on an "expert-based system," but funding did not exist for such an expert; and (3) system maintenance was documented primarily by means of a system maintenance log, with parts replaced as needed, presumably in a run-to-failure mode rather than a more formal, systematic preventive maintenance protocol.

**Safety Basis Issues.** None of the facilities assessed were operating under safety bases that fully complied with 10 Code of Federal Regulations (CFR) Part 830, *Nuclear Safety Management*. In particular, the CMR Facility is operating under a 1998 BIO and associated TSRs, PF-4 is operating under a 1996 FSAR with more recently developed interim TSRs, and WETF is operating under a 10 CFR 830–compliant documented safety analysis that was approved in 2004, but has undergone none of the required annual updates. It was evident to the

staff that many of the deficiencies identified during the review resulted in part from the lack of modern and compliant safety bases. The laboratory's Safety Basis Improvement Plan includes updates for WETF and PF-4 by the end of fiscal year 2007 and the following year for CMR; however, it is unclear whether these goals will be met.

**DOE Oversight Issues.** The staff observed that the oversight processes of the Los Alamos Site Office and the contractor lacked a mechanism for identifying the types of issues noted by the staff. Many of the issues identified as a result of the staff's review represent fundamental problems related to design bases, operational safety, testing, and maintenance that should be the routine focus of an effective ongoing oversight process. Although some of these types of issues had previously been identified by the contractor and external audits, the staff observed that the site office had not adequately addressed these issues or their root causes.

**Summary.** The staff's review revealed a number of significant deficiencies at LANL with respect to assuring the design, functionality, and maintenance of safety systems. These deficiencies included the following: (1) incomplete or inadequate descriptions of system safety functions, (2) weak or missing fundamental design information and calculations, (3) failure to verify credited safety functions through periodic surveillance and testing, (4) failure to implement appropriate maintenance activities to ensure that safety systems can continue to perform their credited function, (5) lack of adequate normal and abnormal operating procedures to govern the operation of safety systems, (6) lack of formal setpoint calculations for critical system operating parameters, and (7) outdated and, in some cases, inadequate safety bases.

The development and implementation of a formal, systematic approach to ensuring the functionality and operability of safety systems that includes robust design calculations, relevant system testing, fundamental maintenance practices, and adequate system operating procedures is an essential element of sustainable safe operations. However, the staff observed that in many cases, the LANL facilities that were reviewed relied more on expert judgement, operational awareness, and informal guidance to ensure the operability of safety systems. The widespread nature of these deficiencies warrants immediate attention. Consequently, the staff concluded that additional focused actions of an immediate nature are necessary to identify and resolve these issues and to improve confidence in credited safety systems.