

John T. Conway, Chairman  
A.J. Eggenberger, Vice Chairman  
John E. Mansfield  
R. Bruce Matthews

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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



January 27, 2004

The Honorable Linton Brooks  
Administrator  
National Nuclear Security Administration  
U.S. Department of Energy  
1000 Independence Avenue, SW  
Washington, DC 20585-0701

Dear Ambassador Brooks:

The staff of the Defense Nuclear Facilities Safety Board (Board) recently reviewed the conduct of engineering at Los Alamos National Laboratory (LANL). Progress was noted for facility work, which LANL distinguishes from nonfacility work such as research, development, demonstration, testing, and production. However, full implementation of Department of Energy (DOE) Order 420.1A, *Facility Safety*, which provides design requirements for nuclear facilities, continues to experience delays.

Some of the more complex and higher-hazard nonfacility work would benefit from (1) a structured application of engineering standards and practices, (2) a formal conceptual design phase, similar to that for large facility projects, and (3) design reviews following conceptual and final design. For example, if the Technical Area-55 line for aqueous recovery of plutonium-238 scrap had been designed initially to engineering standards appropriate for safety controls and if it had a conceptual design phase and design reviews, the project might not be experiencing delays while safety-related issues are resolved. The benefits of applying engineering concepts to the design of nonfacility work include higher confidence in safe operations, more efficient operations, and lower total cost.

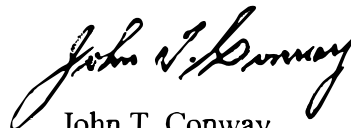
Documented safety analyses written in compliance with the *Nuclear Safety Management* rule, Title 10 Code of Federal Regulations, Part 830, have resulted in a number of existing systems being designated as safety-class or safety-significant. There appears to be little or no internal LANL guidance on how to conduct an engineering evaluation to determine the adequacy of such systems in performing their intended safety function.

As discussed in the enclosed report prepared by the Board's staff, improvement in these areas is desirable. Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report within 90 days of receipt of this letter that:

- Outlines the milestones and completion dates for completing the incorporation of DOE Order 420.1A and its guidance into LANL requirements and guidance documents. This plan should encompass the application of those requirements and the associated guidance to new safety-class and safety-significant structures, systems, and components within existing facilities whether the structures, systems and components are associated with facility or nonfacility work.
- Outlines how to determine when the application of engineering practices such as a conceptual design phase and independent design reviews would improve the safety of nonfacility projects, and what changes are needed in LANL requirements, guidance and training to affect this application.
- Outlines requirements, guidance, and training needed at LANL to ensure that appropriate reviews of design adequacy are conducted for existing structures, systems, and components that are newly designated as safety-class or safety-significant.

The latter two items should also identify actions to be taken to implement the needed changes in a timely manner.

Sincerely,



John T. Conway  
Chairman

c: The Honorable Everet H. Beckner  
The Honorable Jessie Hill Roberson  
Mr. Mark B. Whitaker, Jr.

Enclosure

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

## Staff Issue Report

December 5, 2003

**MEMORANDUM FOR:** J. K. Fortenberry, Technical Director

**COPIES:** Board Members

**FROM:** A. G. Jordan

**SUBJECT:** Application of Engineering Standards and Practices at  
Los Alamos National Laboratory

This report documents observations on the application of engineering standards and practices at Los Alamos National Laboratory (LANL). These observations are based on reviews by members of the staff of the Defense Nuclear Facilities Safety Board (Board) V. Anderson, J. Blackman, B. Broderick, D. Burnfield, A. Gwal, A. Jordan, C. Keilers, R. Quirk, W. Von Holle, and W. White.

**Background.** LANL distinguishes between “facility work” and “nonfacility work.” Facility work is defined as “any combination of engineering, procurement, erection, installation, assembly, disassembly, or fabrication activities involved in creating a new facility or in maintaining, altering, adding to, decontaminating, decommissioning, or rehabilitating an existing facility.” Nonfacility work includes research, development, demonstration, testing, and production. Examples of production at LANL are pit manufacturing and plutonium-238 (Pu-238) scrap recovery. Requirements at LANL generally differ for facility and nonfacility work.

Safety-class and safety-significant structures, systems, and components (SSCs), which are intended for the protection of the public and workers, respectively, are designed, procured, and maintained as being associated with either facility or nonfacility work, depending on the application.

**Facility Work.** Facility work ranges from design and construction of major new facilities, such as the Chemistry and Metallurgy Research Replacement building, with the attendant subcontracting to architect/engineering and construction firms; to major and minor facility modifications; to routine maintenance. It also includes most facility management functions.

LANL has taken some major actions that affect the application of engineering to facility work. The actions are intended to enhance the safe, secure, cost-effective, and efficient management and operation of nuclear facilities; and are being taken to address conclusions of internal and external evaluations, concerns related to the Price-Anderson Amendment Act, and to continue to respond to the Board’s Recommendation 2000-2, *Configuration Management, Vital*

*Safety Systems.* These actions include: (1) reorganizing so that facility managers report to a single manager; (2) initiating the Integrated Facility Management Program to consolidate and develop manuals and procedures for facility engineering, operations, and maintenance; (3) revising the LANL *Engineering Standards Manual*, formerly called the *LANL Engineering Manual*, to address DOE requirements and improve environmental practices; and (4) enhancing training programs for engineering-related functions. LANL has also created the position of chief engineer to help establish policy and programs for facility engineering, including the Integrated Facility Management Program.

*Reorganization*—As a result of the reorganization, the number of facility managers has been reduced from 17 to 9, and the remaining facility managers have been placed in a new Facility Management Unit Organizations group. The realignment includes primarily management and operations that impact facility SSCs, not nonfacility SSCs. This fundamental management change is intended as a means of ensuring the implementation of engineering standards and practices for real property and installed equipment in a consistent manner.

*Integrated Facility Management Program*—The Integrated Facility Management Program is consolidating and developing manuals and procedures for facility engineering, operations, and maintenance. LANL intends to incorporate the best features of programs at other sites, such as the Savannah River Site's Conduct of Engineering and Technical Support procedures.

*Engineering Standards*—Following a review by the Board's staff at LANL, the Board noted in a letter to the Department of Energy (DOE) dated February 22, 2002, that DOE was not aggressively pursuing implementation of DOE Order 420.1, *Facility Safety*, and the related DOE Guide 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE O 420.1, Facility Safety*, which provide design requirements and identifies relevant engineering standards for different types of safety-class and safety-significant SSCs. At the time, many of the engineering standards were not included in the DOE/University of California contract for operation of LANL. LANL had been moving toward implementation of DOE Order 420.1 and its guide, but progress had been slow.

Since that time, LANL, with guidance from DOE, has made additional progress, but is only now completing a gap analysis and an implementation plan to address the remaining gaps. Delays continue to occur. LANL is adding requirements and guidance from DOE Order 420.1 and DOE Guide 420.1 to its *Engineering Standards Manual*. This effort has included adding a chapter on instrumentation and control systems; revising the chapters on mechanical and electrical systems; initiating a revision of the chapter on structures; and developing new chapters on nuclear and hazardous process safety. DOE Order 420.1A, which is a recent revision of DOE Order 420.1, now includes requirements for a system engineer program and has been added to the DOE/University of California contract for operation of LANL. In fiscal year 2003, LANL also launched a major effort to develop a system engineering training and qualification program in response to Recommendation 2000-2; system engineering training is expected to begin shortly.

While progress is being made toward full implementation of DOE Order 420.1A and its guidance, implementation has not been rapid. The Board's staff intends to compare the final results of LANL's efforts with the requirements of DOE Order 420.1A and accepted engineering practices.

*Training*—LANL has developed several courses related to the general use of standards, such as *Introduction to LANL Engineering Standards*, *LANL Electrical Engineering Standards*, and *LANL Drafting Manual*. LANL also makes available vendor-taught courses and a number of discipline-specific courses. The Electrical Safety Committee has been effective in ensuring the availability of electrical safety training; about 25 short courses cover various aspects of electrical safety. Some of the courses are useful to personnel performing nonfacility work. On the other hand, it is not clear that the courses are always required to be taken by the appropriate individuals nor that the content of the courses is fully applied.

The LANL realignment of facility management directly affects facility work. At this time the changes have had little effect on nonfacility work described in the next section.

**Nonfacility Work.** Nonfacility work, which is typically programmatic, includes a broad range of activities—from simple, routine testing to complex, hazardous research and development, demonstration, and production. The focus here is primarily on the design of complex or hazardous activities.

*Fundamentals of Designing for Safety*—Consistent with integrated safety management, proper design of processes and equipment for nonfacility work involves early identification of potential hazards, development of strategies to avoid those hazards where possible and otherwise to minimize them, and the development of reliable hazard controls. The Board has emphasized the desirability of using engineered controls developed by proper design instead of relying on administrative controls.

As with large facility projects for which it is common practice to have a conceptual design phase followed by one or more phases to finalize the design, some nonfacility work would benefit from having a formal conceptual design phase. The conceptual design phase typically would involve development of a hazard avoidance and minimization strategy; completion of a preliminary hazard analysis; identification of design requirements, including functional and operational controls and tentative specification of standards; and determination of whether any controls have the potential to be designated as safety-class or safety-significant. It is important to identify early in the design phase the potential for any controls to be safety-class or safety-significant to help ensure that they are adequately engineered, procured, and installed with appropriate quality assurance.

Some nonfacility work would also benefit from independent design reviews at the end of the conceptual design phase and at the completion of the design to ensure the adequacy of the design. Such reviews would be opportunities to ensure that the design adequately controls the hazards and provides the appropriate operability, maintainability, and flexibility. These reviews

could also ensure the accuracy of calculations important for the mission and/or safety, as well as the adequacy of the documentation of such calculations.

*LANL's Approach to Designing for Safety*—LANL has two Laboratory Implementation Requirements (LIRs)—*Safe Work Practices* and *Documentation of Safe Work Practices*—that outline requirements for work planning for nonfacility work. However, the LIRs provide no guidance on the use of conceptual design phases for complex, hazardous projects. In addition, these LIRs do not require independent review following the design phase and prior to fabrication and assembly of experimental equipment.

As noted in a letter from the Board dated August 7, 2003, the LIRs on safe work practices make no reference to another LIR—*Engineering Standards*—that references requirements and guidance for the use of engineering codes and standards in the design and modification of LANL facilities and in “programmable” work, which is largely nonfacility work. The *Engineering Standards* LIR, however, also states that its requirements do not apply to programmable work unless prior consensus approval is obtained from programmable groups. Thus, in reality LANL provides its scientists and engineers little direction for the use of engineering standards in research, development, demonstration, testing, and production.

An example of a nonfacility project that would have been completed more expeditiously had there been a conceptual design phase is the Technical Area-55 line for aqueous recovery of Pu-238 scrap. This project is experiencing delays while safety-related issues are resolved. Having a conceptual design phase and design review would have resulted in more robust safety features, fewer delays in becoming operational for mission needs, and reduced costs. The review of this project by the LANL readiness assessment (RA) team also noted that no technical review by experienced personnel outside of the group responsible for the project had been conducted prior to the RA and that such reviews would have been advantageous.

**Safety-Class and Safety-Significant Structures, Systems, and Components.** Safety-class and safety-significant SSCs can be associated with either facility or nonfacility work. As a result of the development of documented safety analyses in compliance with the *Nuclear Safety Management* rule, Title 10 Code of Federal Regulations, Part 830, many existing SSCs have now been designated as safety-class or safety-significant because of their importance to protecting the public or collocated workers, respectively. Typically, these SSCs were not originally designed, procured, installed, and maintained as safety-class or safety-significant. In some cases, the need for new safety SSCs has been identified.

There appears to be little or no internal LANL guidance on how to evaluate such newly designated safety SSCs. Such a design adequacy review might involve determining the functional and operational requirements for safety; determining what standards would be used if the SSCs were designed today (e.g., by performing a comparison with DOE Order 420.1A and its guidance); performing a gap analysis, followed by a cost/benefit analysis on potential upgrades; and then making a decision about whether to upgrade. A design adequacy review might also identify minimum operability requirements and actions to be taken should such requirements not be met. An independent design review might also be warranted.

Beyond a design adequacy review, a procedure commonly called commercial-grade dedication is needed to evaluate new or replacement commercial items for their suitability for safety-class or safety-significant applications. Such a procedure would provide the basis for quality assurance requirements.

The design of new SSCs is addressed in DOE Order 420.1A and its guidance. As discussed above, some of those requirements are not included in the LANL *Engineering Standards Manual*. A letter from the Board dated July 9, 2003, points to the need for increased training for personnel responsible for designing new safety SSCs.

Requirements and guidance for performing a design adequacy review on newly designated safety SSCs and procedures for commercial-grade dedication are not by themselves enough to ensure safety. An interesting case is the Weapons Engineering Tritium Facility (WETF), for which the existing lightning protection system was designated as safety-class based on a recent documented safety analysis. WETF management did commission a design adequacy review from a respected outside expert. However, they failed to maintain the lightning protection system to common industrial requirements. Later, when the outside expert concluded that the lightning protection system did not meet safety-class functional requirements, WETF recommended simply reducing the safety functional classification to safety-significant based on the “demonstrated ineffectiveness of the system,” without instituting any additional engineered controls. (See letters from the Board dated August 6, 2002, and August 19, 2003).

**Summary.** LANL is making progress in developing the infrastructure required to apply engineering to facility work, although full implementation of the requirements and guidance of DOE Order 420.1A has been slow. LANL has not made significant progress in the development of requirements and guidance for the application of engineering standards and practices to nonfacility work, including the use of a conceptual design phase to allow early identification of the safety strategy and the use of independent design reviews to ensure the adequacy of the safety strategy. In addition, LANL lacks guidance to ensure that SSCs newly designated as safety related can reliably perform their intended safety function.