DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

July 9, 2003

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 Defense Nuclear Facilities Safety Board (Board) recently reviewed the proposed safety-class instrumentation and control systems for the critical assemblies at Technical Area 18 (TA-18) at Los Alamos National Laboratory (LANL).

As noted in the enclosed report, the existing scram systems do not appear to fully meet the Department of Energy's safety-class requirements. Furthermore, design of the new temperature measurement systems will require additional effort if they are to function as intended in the recently approved safety basis. These designs have not yet had an appropriate independent design review, and it may be difficult to verify that the new systems will fulfill their safety functions when installed.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests that the National Nuclear Security Administration provide a report, prior to removing the interim controls that protect fuel and sample temperature, but no later than September 2004, that demonstrates that the high-temperature scrams will operate reliably and effectively to prevent critical assemblies from overheating.

As a result of its review of the proposed safety-class instrumentation at TA-18, the Board observed deficiencies that appear to be institutional. The Board has raised similar concerns in the past (Board letter dated February 22, 2002), and some corrective actions are being taken. However, additional improvement will be required to address issues such as the consistent use of applicable codes and standards, the use of independent design reviews and the performance of backfit analyses. The Board intends to further evaluate these areas in the future.

Sincerely,

John T. Conway
Chairman

c: Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

May 15, 2003

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: R. Quirk

SUBJECT: Instrumentation and Control Systems at Los Alamos Critical Experiments Facility

This report documents a review by members of the staff of the Defense Nuclear Facilities Safety Board (Board) of instrumentation and control (I&C) systems for the critical assemblies at Technical Area 18 (TA-18) at Los Alamos National Laboratory (LANL). Staff members R. Quirk, C. Keilers, and A. Jordan conducted this review.

The staff identified both strengths and deficiencies during the review. Several deficiencies were similar to findings from previous staff reviews (as documented in letters from the Board dated April 23, 2002, and August 6, 2002) and may indicate systemic issues in the formality of LANL engineering for new and existing safety-related systems. LANL is making improvements in the *LANL Engineering Manual* as part of a multiyear facility revitalization program, and in response to the Board's reporting requirement dated February 22, 2002, related to the implementation of DOE Order 420.1, *Facility Safety*. However, these improvements have not yet been effected.

Chapter 8 of the *LANL Engineering Manual* addresses I&C systems, and among other items, identifies I&C consensus standards that should be followed. However, the communication of best engineering practices, guidance, and directives to engineers has not been completely successful at LANL to date, particularly for research and development efforts such as those at TA-18. Additionally, the manual allows deviating from required standards, but does not require documentation, independent review, and approval of these deviations.

New Safety-Class Controls at TA-18. TA-18 has three remote laboratories housing five operating critical assemblies that are controlled individually from a central control building. Most of the structures are four to five decades old. The critical assemblies include two general-purpose machines (Comet and Planet), one highly reflected spherical benchmark assembly (Flattop), one fast-burst assembly (Godiva IV), and one solution high-energy burst assembly (SHEBA). TA-18 is located approximately 0.5 miles from the nearest site boundary and 3 miles from the town of White Rock. Previous safety analyses of TA-18, dated 1998 and before, did not include unmitigated accident analyses and concluded that the engineered safety features were not required to be functionally classified as safety-class or safety-significant. This approach is inconsistent with 10 CFR 830, which is now in effect.

In July 2002, the National Nuclear Security Administration (NNSA) approved a new TA-18 safety basis that included analyses consistent with current DOE requirements. The analyses concluded that the unmitigated accidents with the highest off-site consequences would be uncontrolled reactivity insertions leading to melting and partial vaporization of fuel and/or irradiated samples. The estimated site boundary dose for these events would exceed DOE's evaluation guideline of 25 rem by more than an order of magnitude.

Accordingly, NNSA approved a peak fuel temperature safety limit. To prevent this safety limit from being reached, NNSA approved a fuel temperature limiting control setting for the initiation of a reactivity scram. New administrative controls to limit excess reactivity and new administrative controls and safety-significant engineered features to limit the reactivity insertion rate were approved to ensure the fuel temperature reactivity scram would be effective in avoiding the safety limit.

NNSA and LANL designated the existing scram mechanisms, the existing scram chains, and the new fuel (incore) temperature measurement systems as safety-class systems. A scram chain is the instrument circuit that will cause the system to scram if certain relays are de-energized. The new fuel temperature measurement system is still being developed and should be completed by September 2004. Two interim controls have been put in place until the new fuel temperature measurement systems are installed: a sample size limit, and a reduction in the trip set point for nuclear instrument scram to one decade above the expected value for any particular experiment.

The staff concurs that these interim controls should provide adequate compensatory protection for the short period until the new fuel measurement system is scheduled to be completed.

Design of Safety-Class Fuel Temperature Limit Controls. The staff reviewed portions of the new temperature measurement design package now under development for all the critical assemblies. The staff also reviewed the existing scram chains for SHEBA and Planet. Subsequent to the on-site review, the staff evaluated the other related controls discussed above. The staff had the following observations on the proposed new fuel temperature measurement systems and existing scram chains:

- The coupled neutronics-thermal analyses used for the new Basis for Interim Operation (BIO) may be appropriate for a safety analysis, but appear to be too coarse to guide engineering development of the new fuel temperature measurement system. For example, the safety basis assumes that the peak fuel temperature and the temperature sensors are collocated at the center. It was not clear to the staff that the peak temperature would be at the center of the critical assembly because the assembly is small and can be significantly affected by potential variations in the sample and reflector materials and locations. During the staff's review, LANL indicated that the temperature sensors would be off-center because of research constraints. There appears to have been no engineering evaluation to identify optimum off-center sensor locations or to assess the impact of other real-world engineering effects that could

increase response time. The latter effects include but are not limited to peak fuel temperature and temperature sensors not being collocated, delays associated with the thermal gradient, air gaps between the fuel and temperature sensors, sensor delays, assembly tolerances, and uncertainties regarding instrument loop components such as response times, drift, calibration errors, and setting tolerances.

- Considering such effects, the engineering justification for the limiting control setting for the fuel temperature is incomplete. It appears NNSA and LANL assumed that the combined uncertainties of real-world engineering effects, such as those discussed above, would be covered in the margin between the limiting control setting and the safety limit. The design of the fuel temperature measurement systems will require careful evaluation to ensure that the approved setpoint will preclude reaching the fuel temperature safety limit.

- The proposed redundant thermocouple temperature sensors would be located together in a single unit. The proposed thermocouple signal cables would also use the same conduit with no additional means to separate the redundant safety-class signals. This approach conflicts with Institute of Electrical and Electronic Engineers (IEEE) STD-379, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Generating Safety System*, and IEEE STD-384, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*. Both DOE guidance and the *LANL Engineering Manual* list IEEE STD-379 and IEEE STD-384 as consensus standards for safety-class I&C equipment. The draft design change package provided no clear justification for failing to be fully compliant with these standards.

- During the review of the existing scram chains, which are newly designated as safety-class, the staff noted this design also is not consistent with IEEE STD-379 or IEEE STD-384. The logic relays are commercial grade and not sealed. Redundant relays are in the same panel without adequate electrical separation from each other or non-safety-class components. Panel wiring is of different types and sizes, with no apparent reason for the variation. It was unclear to the staff that the equipment could fulfill the safety-class functions assigned to it by the safety basis. DOE Standard 3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, Section 4.3.X.4, Evaluation, indicates that engineering judgment may be used to develop performance criteria for existing safety structures, systems, and components. However, LANL does not appear to have used appropriate performance criteria in its evaluation of the existing scram chains. The reliability and availability of the scram chains are of utmost importance in protecting the public and workers from significant radiological consequences.

- In its July 2002 memorandum approving the safety basis, NNSA specified as a condition of that approval that LANL prove the new fuel temperature measurement system will meet the functional requirements in the BIO. It is unclear to the staff how the new system will be validated as meeting these functional requirements (e.g., both

the means and the criteria for declaring the system operational), and additional guidance from NNSA may be warranted.

- The new fuel temperature safety limit could be protected using nuclear-instrument based scrams. However, a senior member of the LANL staff noted it would be difficult to establish a nuclear instrument trip set point to protect fuel temperature because of the variety of reflectors and shielding used at TA-18. The BIO indicates that the nuclear instrument channels have not been calibrated to a power level and that current nuclear instrument limits are based simply on extrapolation of flux levels from past experiments. However, the TA-18 BIO indicates that the nuclear instrument channels have redundancy, have been highly reliable over time, and have never failed to scram when required. The staff believes that a safety-class temperature-based scram system will rely on extrapolations that are perhaps even more significant than those for a nuclear-instrument-based scram system.

Based on the above observations, the staff believes a temperature-based scram meeting standard safety-class requirements will be difficult to implement, and that it will also be difficult to verify that the scram could perform its intended safety function. The staff also believes that the design of new safety systems or the major upgrade of existing systems requires more attention to applicable codes and standards.

LANL Institutional Issues. The staff believes that the LANL personnel designing the new fuel temperature measurement system are aware of many of the above issues. However, they are encumbered by weaknesses in current LANL institutional guidance on what is acceptable. Reviews performed by the Board's staff during the last year have collectively identified several weaknesses in the conduct of engineering, including the following:

- Some LANL personnel responsible for designing new safety systems and components have not been trained in new requirements in the *LANL Engineering Manual*. For example, the manual section on I&C clearly indicates that IEEE STD-379 and IEEE STD-384 are applicable. Yet the TA-18 design engineers were not aware that the manual was applicable to their design, since it is deemed research equipment. The *LANL Engineering Manual* states it is applicable to both facility and research (i.e., programmatic) applications.

- LANL currently has no standard backfit evaluation procedure that would prompt engineers to closely examine the trade-offs involved in designating an existing system as safety-class or safety-significant without improvements. The inadequacies of the existing TA-18 scram chains for a safety-class function might have had more visibility if such a procedure existed and if site personnel had been trained in it. A LANL staff member stated that LANL is considering the use of a backfit procedure developed by Lawrence Livermore National Laboratory.

- LANL currently has no standard commercial-grade dedication procedure to evaluate new or replacement commercial items and determine their suitability for safety-class

or safety-significant applications. The TA-18 design engineers realize this weakness and are in the process of developing such a procedure. That effort is commendable, but this is likely a site-wide need.

- The only design reviews that have been conducted on the new fuel temperature measurement system were conducted by the TA-18 group responsible for operating the assemblies and do not appear to have been of adequate breadth, depth, or independence given the system's safety-class function. The safety significance of the new system is sufficient to warrant proper independent design reviews. During the staff's on-site review, LANL agreed to pursue an independent review, most likely by the LANL Reactor Safety Committee. LANL currently has no standard procedure for independent design reviews of safety-related equipment with rigor comparable to that seen at other DOE sites. Many such reviews are limited to the LANL groups responsible for operating the equipment. If conducted early in the design effort, such reviews could identify problems while they are still relatively easy to correct. Independent reviews would be particularly beneficial for new or existing systems designated as having a higher-level safety function under an updated safety basis, such as the 10 CFR 830 updates.

The staff understands that LANL is preparing new sections of the *LANL Engineering Manual* that will focus on nuclear safety and the interface between safety analysis and design. These sections are expected to be completed in the next fiscal year and may help address the issues raised above.