DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004
(202) 208-6400

November 4, 1997

The Honorable Victor H. Reis
Assistant Secretary for Defense Programs
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0104

Dear Dr. Reis:

Enclosed for your consideration and action, where appropriate, are the observations developed by the members of the staff of the Defense Nuclear Facilities Safety Board (Board) concerning instrumentation and control (I&C) systems that will support the safe restart of Enriched Uranium Operations (EUO) at the Y-12 Plant. The staff observed that although the safety analysis by Lockheed Martin Energy Systems (LMES) identified most I&C systems necessary to prevent or mitigate accidents, the verification process to determine whether those systems can be relied upon to perform their safety functions appears to be significantly lacking or nonexistent. In addition, existing safety-related systems are not being examined to identify improvements in cases where the system is inadequate.

For example, the I&C systems relied upon for emergency shutdown of the E-Wing dry vacuum systems to avoid an inadvertent nuclear criticality all function through the same electrical relay. If this relay failed (because of either a fire or some preexisting fault), the E-Wing dry vacuum system could lose all three of its active design features required for criticality safety. In addition, the staff observed that the configuration management, maintenance, and surveillance requirements implemented for safety-related systems appeared to be inadequate. Most drawings and equipment tags had not been updated to reflect accurately the safety identification of equipment made in the Basis for Interim Operations.

Although it appears that LMES has identified most of the hazards and associated controls necessary for EUO restart, the methodology being used to prepare each process for restart does not verify adequately that the systems involved will perform the necessary preventative and mitigative functions identified in the Basis for Interim Operation recently approved-by the Department of Energy (DOE).

The Board recognizes the importance of restarting EUO without undue delay. In the spirit of assisting DOE in its efforts to safely restart the operations in a timely manner, the Board requests a briefing by DOE and LMES on November 25 to address safety matters raised in this and previous correspondence and the progress being made to resolve safety-related issues.

Sincerely,

John T. Conway
Chairman

c: Mr. Gene Ives
Mr. James Hall
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

September 22, 1997

MEMORANDUM FOR. G. W. Cunningham, Technical Director

COPIES: Board Members

FROM: W. I. White

SUBJECT: Review of the Y-12 Plant, Building 9212 Complex, Instrumentation and Control Systems

This memorandum documents two reviews of the safety-related instrumentation and control (I&C) systems required to support Enriched Uranium Operations (EUO) restart in the 9212 Complex at the Oak Ridge Y-12 Plant. The first review was performed by members of the staff of the Defense Nuclear Facilities Safety Board (Board) W. L. Andrews, A. K. Gwal, and W. I. White during September 9–11, 1997. The second, which addressed maintenance and surveillance requirements of safety-related systems, was performed by W. L. Andrews and outside expert R. West during September 23–25, 1997.

Safety-Related I&C Systems. The staffs review of safety-related I&C systems supporting EUO restart indicated that the designation of a system as safety related has no meaning. As discussed below, there are no defined requirements for new safety-related systems; there has been little evaluation of the adequacy of existing safety-related systems; the procedures for preserving engineered controls are inconsistent, out of date, and poorly implemented; and no clear mechanism exists for feedback and improvement to allow reasonably achievable safety enhancements for existing safety-related systems.

Identification of I&C Systems Necessary to Prevent or Mitigate Accidents—With a few exceptions, Lockheed Martin Energy Systems (LMES) identified I&C systems relied upon to prevent or mitigate potential accidents in the Building 9212 Complex. Among the exceptions, LMES had not identified the Holden furnace flame management system as safety related prior to the staffs review, even though this system is clearly relied upon in the Basis for Interim Operations (BIO) to prevent explosions that might result in worker fatalities. During the staffs review, LMES proposed establishing appropriate controls for the safety functions of this system. This identification of I&C systems important to safety, however, was adequate only from the perspective of systems evaluation in the BIO.

Identification of Standards and Requirements for Safety-Related I&C Systems—LMES safety personnel who briefed the staff stated that, although they had identified the I&C systems important to safety in the BIO, they had made no attempt to verify that those systems were able to perform their intended safety functions. In fact, LMES indicated to the staff that no applicable design or equipment qualification requirements had been identified for safety-related systems.

Given this lack of specific requirements, LMES operations personnel had no design or performance criteria against which they could evaluate the adequacy of existing safety-related I&C systems. Although one would not necessarily expect the older I&C systems to meet current codes and standards, evaluation of the systems according to some defined criteria could lead LMES personnel to identify unacceptable vulnerabilities in existing designs, suggest design changes, or develop additional controls that would significantly improve the reliability Or capability of those systems.

In reviewing the only I&C system for which LMES was able to support a design review, the staff noticed significant deficiencies in the design of safety-related circuits. In particular, the I&C systems relied upon for emergency shutdown of the E-Wing dry vacuum systems all function through the same electrical relay. The failure of this relay, which was not controlled in the LMES drawings viewed by the staff as equipment important to safety, could effectively bypass all of the active emergency shutdown systems.

Configuration ***Management, Surveillance,*** *and Maintenance* ***of Safety-Related*** Systems—Actions to preserve engineered controls are not well defined and, in many cases, not up to date. Several references were provided to the Board's staff in response to questions, but they were found to be inconsistent and sometimes out of date. Specific staff observations on the preservation of engineered controls are summarized below:

. There is no clearly defined and well-implemented program for configuration management for EUO. The requirements foridentifying safety-related items are inconsistent and often out of date. Chapter 18, paragraph C. 16 of the ***Nuclear Operations Conduct of Operations Manual*** requires a special marking of safety-class items, which is to include a red star. No similar marking of safety-significant systems is required. Engineering Standard ES-O. 1-2, ***Safety System Component Identification,*** provides direction for marking of safety system components on engineering documents, but does not distinguish between safety-class and safety-significant systems. Most drawings and equipment tags have not been updated to reflect accurately the safety identification of equipment set forth in the BIO. Those drawings that have been updated are not accurate. For instance, the updates to the E-Wing dry vacuum failed to identify the single key relay used for emergency shutdown as being important to safety.

. Surveillance requirements for safety-related systems appear to have little technical basis. For example, the surveillance periodicity for the level detection circuit (or subsystem) of the E-Wing dry vacuum system (as defined in the ***Building 9212 Operational Safety Requirements*** recently approved by the Department of Energy [DOE]) has decreased by a factor of 4 (annually vs quarterly) from one previous surveillance requirement. Based on discussions with safety analysis personnel, this change appears to have no technical justification.

. The maintenance requirements for safety-related systems are not clearly defined. Procedure Y10-35-016, ***Safety Class Item (SCI) Maintenance Administration, is*** intended to implement a maintenance program to provide assurance that designated facility structures, systems, and components will perform as intended. This procedure, however, does not refer to safety-significant systems and components and is out of date; the term "safety class" as used in this procedure appears to include a broader spectrum of systems than is now encompassed by this term. References are also out of date. A star marking system is used for system component identification maintenance packages, but LMES was unable to provide a procedure or process that indicated the requirements for marking such packages or identified which safety-related systems and components were to be covered.

. Draft procedure Y10-37-036, ***Configuration Management-Change Control Process,*** is being reviewed, but it is not clearly integrated with the above documents and does not adequately address the deficiencies noted.

Feedback and Improvement for I&C Systems—In only one case was the staff able to find evidence that LMES had clearly identified the inadequacy of an existing safety system and proposed improvements for enhanced mitigation or prevention of accident consequences. LMES originally identified the E-wing filter house fire detection, isolation, and Halon extinguisher system as safety class. Since this system clearly was not designed as safety class, LMES has proposed eliminating the need for the safety function by replacing wool bags (which are flammable) with other, nonflammable bags. As mentioned previously, however, the staff found no evidence of any evaluation of safety-related I&C systems that led to improvement of design vulnerabilities.

Electrical Systems. The Board's staff also reviewed issues raised in its April 1997 trip report on electrical and fire protection systems. Among the major issues whose status has changed is the recommended replacement of Motor Control Center (MCC) 230- 1A and its associated conduit systems. LMES now has a capital project to replace this MCC after restart of phase A operations; however, this project has not been approved. The staff believes the issues of reliability, electrical safety, and fire safety raised in April 1997 with respect to this MCC would be corrected by this project.

Future Staff Actions. LMES was not prepared to support a detailed design review of any I&C system except the E-Wing dry vacuum. The Board's staff will request detailed design drawings and equipment specifications for all safety-related I&C systems in the 9212 Complex, and, if required, will conduct additional reviews for those systems when LMES is able to support such reviews. The staff will also continue to follow the resolution of the issues identified in both this and the April 1997 trip reports.