August 26, 2004

Mr. Paul M. Golan
Acting Assistant Secretary for
Environmental Management
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0113

Dear Mr. Golan:

Enclosed is a report containing observations of members of the staff of the Defense Nuclear Facilities Safety Board (Board) concerning a review of the ongoing design and construction of the electrical and instrumentation and control systems of the Waste Treatment Plant (WTP) at the Hanford Site. These observations are based on a review of available documents, as well as discussions with representatives of the Department of Energy and contractor personnel at WTP on June 22–24, 2004.

The Board asks to be kept abreast of the Department of Energy's actions regarding the issues raised in the enclosed report.

Sincerely,

John T. Conway
Chairman

c: Mr. Roy J. Schepens
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

August 3, 2004

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: A. Gwal and R. Quirk

SUBJECT: Review of Electrical and Instrumentation and Control Systems of the Waste Treatment Plant at the Hanford Site

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) of the electrical and instrumentation and control (I&C) systems of the Waste Treatment Plant (WTP) at the Hanford Site. Staff members A. Gwal and R. Quirk met with on-site representatives of the Department of Energy's (DOE) Office of River Protection (ORP) and its contractor, Bechtel National, Incorporated (BNI), on June 22–24, 2004, to discuss the status of issues previously identified by the Board's staff and to review the electrical and I&C systems of WTP.

Background. Based on earlier reviews of the 25 percent design, the Board issued a letter on March 7, 2003, concerning electrical and I&C systems planned for use at WTP. Since then, several actions have been taken by DOE-ORP/BNI to close most of the issues identified in the Board's letter. BNI estimated the design maturity for the electrical systems to be approximately 50 percent at the time of June 2004 review.

Electrical System. Overall the design of the electrical system is progressing well. However, several specific issues related to this system, as well as open issues from previous staff reviews, are detailed below.

Unprotected 13.8 kV Equipment at Substation A-6—During a facility walkdown of substation A-6, the Board's staff observed that the equipment room containing 13.8 kV switchgear does not have an operational fire protection system. Although the building has sprinkler heads installed, the system was intentionally disabled because of concern that the sprinkler system water might enter the equipment that is vented at the top. Water spray from activation of the sprinkler system would penetrate the equipment and could initiate water-induced short-circuiting, a common-cause failure that would leave electrical loads without power. The small portable fire extinguisher in the equipment room does not appear to provide adequate fire protection, especially for a high fault-induced rapid fire.

National Fire Protection Association (NFPA) standard NFPA 13, *Installation of Sprinkler Systems*, requires sprinkler protection in electrical rooms. Institute of Electrical and Electronics

Engineers (IEEE) Standard 979, *IEEE Guide for Substation Fire Protection*, provides guidance related to fixed-pipe fire-extinguishing systems that may be installed in substations. The standard states: "In unattended substations utilizing an automatic system, consideration should be given to a system that automatically shuts off when the fire is extinguished or after a predetermined time interval, and then returns to the automatic operational mode." The standard also cautions about the dangers of water usage. It states that before water is selected for use indoors, it should be determined whether the equipment is watertight. Authorization from the equipment manufacturer is also required. Additionally, the standard states: "If at all possible, company personnel should de-energize the entire substation or, at a minimum, the equipment involved in the fire, before the local fire department is allowed on the site. This is recommended because of the electrocution danger to the fire fighter by either direct contact with energized equipment or indirectly with the water stream and hose acting as a conductor."

This issue could be resolved by providing a raised noncombustible cover at the top, with concurrence from the switchgear vendor, or through some other method that would prevent entry of water into the switchgear instead of disabling the fire protection. The Pantex Plant recently addressed a similar issue.

Medium-Voltage Switchgear—The 4,160 V systems for four of the medium-voltage switchgears have no dedicated ground fault protection for the feeder circuit to the motor starter, making it unsafe to work near this system once it has been energized. The current design uses fuses (an old design concept) that will need to be replaced each time a fault occurs. The use of fuses also makes it difficult to coordinate the protective devices, which could result in the loss of the entire bus during a fault. A design using breakers could provide ground fault protection and permit coordination of protective devices.

Manhole-47—During the facility walkdown, the Board's staff requested that manhole-47 (containing 13.8 kV cables) be opened to assess its condition. The staff observed that concrete had poured through one of the openings in the duct bank and deposited at the bottom of the manhole, partially covering the sump area. BNI staff present during the walkdown stated they would correct this condition by carefully removing the concrete, and would verify that this is not a problem in the other facility manholes.

Safety-Significant Loads on Safety-Class Busses—The staff noted that several safety-significant loads are connected to the safety-class busses. IEEE Standard 384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, requires that non-safety-class loads be appropriately isolated from safety-class busses to ensure that failure of a safety-significant component would not cause failure of the safety-class power system. Because of the large number of connected safety-significant loads (18), it would be prudent to feed these loads from dedicated safety-significant busses instead of using individual isolation devices for each safety-significant load.

Safety Requirements Document (SRD)—The SRD for the electrical systems (Section 4.4-4) does not contain a complete list of required standards as delineated in DOE Order

420.1, *Facility Safety*, and DOE Guide 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE Order 420.1, Facility Safety*. BNI engineers stated that they would revise the standards list for Section 4.4-4 of the SRD.

Electrical Calculations—One-line drawings used for the existing electrical calculations do not match the current one-line drawings. However, BNI has performed an informal estimate of short-circuit and load-flow calculations and expects no major issues in this area. The Board's staff will review the calculations once they have been completed.

Instrumentation and Control Systems. As can be expected with a major new design effort, the I&C design is significantly less mature than the structural, mechanical, process, and electrical designs. Much of the I&C effort to date has focused on requirements definition and development of software engineering processes and procedures. The substantial software engineering requirements, including significant documentation, implemented at WTP appear to be appropriate for high-risk software.

Ventilation Control System—The safety design class (SDC) C5 ventilation system is the key active system used to prevent exceedence of site boundary radioactivity and hazardous chemical limits. One of the two independent C5 ventilation trains will be in service during normal plant operations. The current design calls for starting the standby train when total system exhaust flow falls below a nominal design value. A conservative value of total system flow can be used as a precursor for an imminent loss of system functionality. However, flow imbalances or larger-than-anticipated inleakage into one C5 area could result in meeting the total flow requirement concurrently with inadequate vacuum in other C5 areas. The Board's staff suggested that monitoring the vacuum in each C5 room would be a more appropriate control scheme for this SDC system. Additionally, the American Society of Heating, Refrigerating, and Air-Conditioning Engineers Handbook *Heating, Ventilating, and Air Conditioning Systems and Applications* suggests using static pressure controls for ventilation systems in certain manufacturing processes, clean rooms, and laboratories. These examples are analogous to the C5 ventilation system.

Safety Integrity Level (SIL) Calculations—The principal industry standard adopted for all safety instrumented systems in WTP is Instrumentation, Systems, and Automation Society (ISA) 84.01, *Application of Safety Instrumented Systems for the Process Industries*. For WTP, the probability-based SIL required by ISA 84.01 is developed using BNI's Integrated Safety Management process. BNI reported that the most stringent requirement noted to date has been an SIL-2, which means the safety system, including both hardware and software from sensors through final actuation devices, can fail to operate as often as 1 in 100 attempted operations.

BNI will generate calculations to demonstrate that the delivered systems are reliable enough to support the required SIL. In these calculations, BNI will assume that software developed by its staff will not result in a safety system's failure to operate. The Board's staff will review the reliability analyses for the safety instrumented systems to better understand the technical basis for these positions.

Functional Classification Transition—BNI is in the process of reclassifying structures, systems, and components (SSCs). Instead of using the SDC/safety design significant (SDS)/risk reduction class taxonomy, BNI will use DOE-STD-3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, safety-class (SC)/safety-significant (SS) taxonomy augmented by an additional protection class (APC). It is expected that a number of instruments will be reclassified from SDC to SS, and others from SDS to APC. The Board's staff will review final design documentation to ensure that requirements such as separation and isolation have been met for the reclassified SSCs.

Failure to Invoke Single Failure—The SRD, Section 4.3, addresses the seven criteria for engineered safety systems. Section 2.7.1 of *Preliminary Safety Analysis Report (PSAR) to Support Construction Authorization; General Information, Instrumentation and Control* invokes the appropriate SRD requirements for engineered safety systems except for criterion 4.3-2. Criterion 4.3-2 invokes consensus standards for important-to-safety systems for which single-failure protection is required. BNI engineers stated that not including the single-failure criterion was an oversight; they also said that the SDC/SC I&C systems will be protected from single failures. Although senior DOE staff stated that revising the PSAR was not required because the SRD is an upper-tier document, BNI engineers reported that they would initiate a change to the PSAR to specifically invoke criterion 4.3-2 for SDC/SC I&C systems.