DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

February 5, 2002

The Honorable Jessie Hill Roberson
Assistant Secretary for
Environmental Management
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0113

Dear Ms. Roberson:

Enclosed for your consideration and action, as appropriate, are observations from members of the staff of the Defense Nuclear Facilities Safety Board (Board) concerning electrical and instrumentation and control systems at the Hanford Plutonium Finishing Plant (PFP). These observations are based on reviews of relevant documents and discussions with the staff of the Department of Energy (DOE) and the contractor for PFP during a review at the Hanford Site.

In the enclosed report, the Board's staff notes that several non-safety electrical loads are connected to the safety-significant power distribution busses. The applicable standard of the Institute of Electrical and Electronics Engineers requires that non-safety loads be appropriately isolated from safety-significant busses to ensure that failure of a non-safety component will not cause failure of the safety-significant power system. The report also identifies outdated and deficient electrical calculations and other potential areas for improvement.

The Board asks to be kept informed of DOE's action regarding the issues discussed in the enclosed report.

Sincerely,

John T. Conway
Chairman

Mr. Mark B. Whitaker, Jr.
Mr. Keith Klein

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

December 21, 2001

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: A. K. Gwal

SUBJECT: Electrical and Instrumentation and Control Systems at Hanford's Plutonium Finishing Plant

This report documents a review performed by members of the staff of the Defense Nuclear Facilities Safety Board (Board) of the electrical and instrumentation and control systems of the Plutonium Finishing Plant (PFP) at the Hanford Site. The report, based on a review conducted by staff members A. K. Gwal and C. Graham at PFP, also reflects the results of a follow-up review of documents provided to the staff and telephone conferences held with personnel from PFP and the Department of Energy's Richland Operations Office. The staff reviewed the design and installation of the electrical and instrumentation and control systems at PFP. Related safety-significant systems were reviewed in detail. In addition, the staff walked down PFP to evaluate the design of electrical distribution systems and observe the installed condition of equipment related to electrical and instrumentation and control systems.

Electrical Systems. The electrical distribution system at PFP consists of 230 kV and 13.8 kV transmission lines, transformers, large switchgear units, diesel generators, and a DC battery station. The building distribution system is three-phase 480 V and 208 V/120 V. These components are designated as either safety-significant or general service. Three diesel generators provide backup electrical power to monitoring equipment, alarm and evacuation systems, fire alarm systems, some criticality alarm systems, security systems, emergency lighting, and some building ventilation systems when normal electrical power is not available. PFP also has several uninterruptible power supplies (UPS) that provide continuous power to programmable logic controllers, facility computers, plant monitoring systems, and plant communication systems. Emergency lighting is provided by several self-contained, fully automatic, battery-operated emergency light packs. A circuit breaker controlled by a distributed control system provides power for building emergency loads; exhaust fans; heating, ventilation, and air conditioning control circuits; monitoring circuits; UPS systems; perimeter lighting; and other systems. The Board's staff reviewed the above systems and identified the following issues.

Existing Ground Fault on a Bus System—During a tour of the facility, the Board's staff noticed an existing single line to ground fault of 1.5 amps while observing the ground fault monitoring equipment of the distribution system. At the time of the review, PFP personnel informed the staff that this fault condition had been present for more than a month. Investigation

of the condition would have required bus switching and bus outages to locate and remove the fault. To avoid an outage, PFP chose to delay clearance of the fault. Although Institute of Electrical and Electronics Engineers (IEEE) Standard 142-1991, *Grounding of Industrial and Commercial Power Systems,* does not require immediate clearing of a ground fault for systems using a high-resistance grounding method that limits the fault current to a very low level, it would be prudent to clear such a fault as soon as possible, particularly since this condition could lead to severe damage to the system should a second fault occur. The Board's staff encouraged PFP personnel to locate the fault and clear it as soon as possible. As a result, PFP performed a systematic switching of loads during the weekend of November 10, 2001, and was able to locate and clear the ground fault. The fault was traced to a heat pump unit.

Technical Capabilities of an Electrical System Engineer—During a review of the design and installation of storage batteries, the Board's staff observed that the contractor's system engineer for PFP's electrical systems was not aware of the existence of the *National Electric Safety Code* (American National Standards Institute Standard C2). This standard covers basic provisions for safeguarding of personnel from hazards arising from the installation, operation, or maintenance of electrical systems. The same system engineer was unable to explain PFP's existing electrical calculations. He was neither familiar with the software used for the electrical calculations nor capable of explaining the data or recommendation therein.

Non-Safety Loads on Safety-Significant Busses—The staff noted that several non-safety loads are connected to the safety-significant busses. IEEE Standard 384, *Standard Criteria for Independence of Class IE Equipment and Circuits*, requires that non-safety loads be appropriately isolated from safety-significant busses to ensure that failure of a non-safety component will not cause failure of the safety-significant power system. PFP personnel stated that they will evaluate this condition.

Electrical Calculations—The Board's staff reviewed the electrical calculations, such as comprehensive short-circuit, voltage profile, and coordination studies, that are essential to safeguard personnel and maintain a safe and reliable power system. Such studies are performed in accordance with IEEE Standard 141, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants,* and Standard 242, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*. The existing calculation was performed in 1992 using the commercially available SKM (vendor) system analysis model. Since then, many system design and equipment modifications have occurred, such as the installation of four 1000 kVA transformers 2 years ago in a new configuration to replace the old transformers. The calculations have not been revised using the electrical parameters of the modified system and equipment to determine whether any design modifications are needed.

Adequacy of Diesel Generator Load Test—The diesel generators are tested by running them synchronized with the utility system once a month for approximately an hour to verify the proper operation of the generators. After reviewing one of the test reports, the Board's staff observed that the test method does not indicate the loads on the generator during the test. Measuring and recording the power demand of the load is typically performed to confirm the

adequacy of the generator to support the required full load. The test as performed could not verify that the diesel generator could support all required loads.

Turbine-Driven Exhaust Fans—These exhaust fans are classified as safety-significant components and are required to function during all activities of Building 234-52 (Analytical and Developmental Laboratory). However, the adequacy of these fans to meet the requirements of a safety-significant system could not be verified. Furthermore, the staff observed that the steam supply system that drives the fans is not safety-significant.

Instrumentation and Control Systems. The staff reviewed the instrumentation and control systems at PFP and identified the following issues:

Distributed Control System—The distributed control system (DCS) controls a number of process functions from the PFP control room and is classified as general service. However, the staff learned that a portion of the DCS controls the safety-significant diesel generator control system. Furthermore, the DCS has the capability to override certain interlock functions associated with the normal electrical distribution and diesel generator busses. The staff is concerned that adequate separation may not exist between these systems, and that the DCS could adversely affect the operation of the diesel generators or their bus. It would be prudent for PFP personnel to verify that electrical and software separation exists between these systems and to identify potential DCS failures that could affect the startup, operation, or interlocking features of the safety-significant system.

Design of Safety-Significant Instrumentation and Control Systems—At PFP, the design of safety-significant instrumentation systems is similar to that of general-service systems. The staff encouraged PFP personnel to incorporate lessons learned from the process industry in the design and analysis of safety-related process control systems. Instrumentation, Systems, and Automation Society (ISA) S84.01, *Application of Safety Instrumented Systems for the Process Industries*, presents good fundamental guidelines for the system architecture of safety systems whose primary function is protection of workers or property. This standard consists of a reliability-based approach to the design of safety instrumented systems used in the process industries and also contains a number of useful deterministic guidelines. In the case of existing safety-significant systems used in the recently installed plutonium stabilization and packaging system (W-460 Project), the Board's staff suggested the use of ISA S84.01 to identify areas of weak design in safety-significant systems. The staff also suggested the application of a failure analysis method to safety-significant instrumentation and control systems to correct any potential design deficiencies. In addition, the staff noted that the Hanford guidance on software quality assurance was not used for the design of the software for the W-460 software systems (e.g., the programmable logic controller for process operations).

Design Process Hazard Reviews—Although systems classified as general service are not relied upon in the safety basis to prevent known hazards, some method of design process hazard review would be expected. A system hazard review would confirm that general-service systems as designed do not present unforeseen hazards. The staff mentioned that an opportunity for improvement for the W-460 project would be to evaluate these systems with an analytical

technique such as a system hazard operability study or what-if checklist. On November 21, 2001, a heater failure in the nitrogen generation system resulted in a fire in the system. The cause of this failure has yet to be determined. However, this failure supports the need for analysis of this and other systems in the W-460 project, including the DCS that controls process operations. The staff also believes a root-cause investigation would be prudent to determine the conditions that led to the heater failure. After subsequent discussions with the Board's staff, PFP personnel agreed to further investigate the failure mechanism.

Facility Walkdown—During a walkdown of the DCS, the Board's staff observed an erratic reading for one of the exhaust fan current indications. The staff discussed with PFP personnel that this might be the result of a failed exhaust fan motor. The staff suggested that if this is a transmitter failure, other instruments should be reviewed for similar conditions. The staff also observed that a number of calibration stickers for safety-significant alarms and several breakers in one of the motor control center rooms indicated overdue calibrations. PFP personnel stated that these calibrations had been performed, but that the maintenance procedure was deficient in requiring placement of the stickers. PFP maintenance personnel instituted a change to the calibration procedure to correct this condition.