DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

2/8/96

Mr. Mark Whitaker
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0119

Dear Mr. Whitaker:

Enclosed for your information and distribution are eight Defense Nuclear Facilities Safety Board staff reports. The reports have been placed in our Public Reading room.

Sincerely,

George W. Cunningham
Technical Director

Enclosures (8)

96-0000431

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

January 11, 1996

MEMORANDUM FOR: G. W. Cunningham, Technical Director

COPIES: Board Members

FROM: William White

SUBJECT: Trip Report on Savannah River Site (SRS) Defense Waste Processing Facility (DWPF) Electrical Systems, Distributed Control System (DCS), and Alarm Handling/Management Systems.

1. **Purpose:** This report documents a review of the electrical systems, DCS, and alarm handling/management systems at DWPF by the Defense Nuclear Facilities Safety Board's (Board) staff member William White on November 13-14, 1995.

2. **Summary:** The DCS appears adequately designed and tested for a non-safety computer system, but there are a few questionable interactions between the DCS and various safety-class systems. As noted in the Board's letter to the Department of Energy (DOE) on November 6, 1995, non-safety loads are sequenced to the diesel generators by the DCS. If the DCS malfunctions during loss of power and fails to sequence the loads properly, the diesel generators might not be available to supply power to safety-class loads, such as the Zone 1 exhaust fans and certain radiation monitors. Westinghouse Savannah River Company (WSRC) officials have performed calculations which indicate the diesels would operate within specifications even with DCS and other equipment failures, but the Board's staff has several concerns with these calculations. The DCS also serves as the primary source of instrumentation and control for DWPF operation. Some of the instrumentation, such as temperature monitoring for vessels in the salt process cell, have a safety-related function.

   In September WSRC presented to the staff a plan to install an alarm management system which would diagnose and filter alarms to DWPF operators. WSRC has decided, however, not to install this system before beginning radioactive operations. The system will instead be installed when the DCS is ugraded after July 1996.

3. **Background:** DWPF is currently in startup testing with expected readiness for radioactive operations in early 1996. This review covered issues mentioned in the Board's November 6, 1995, letter to DOE. The review also covered the DCS and the alarm handling and management systems.

4. Discussion/Observations:

a. The review identified the following potentially significant issues with the distributed control system.

1. Sequencing of Non-Safety Loads on the Emergency Diesel Generators: Sequencing of non-safety loads to the emergency diesel generators is currently done by the non-safety DCS. If the DCS malfunctions during loss of power and fails to sequence the loads properly, the diesel generators might not be able to supply power to safety-class loads, such as the Zone 1 exhaust fans and certain radiation monitors. WSRC has conducted simulations to demonstrate that the non-safety loads (which consume roughly 50 percent of diesel capacity) could not cause diesel failure through improper sequencing.

   Board staff had several concerns, however, with these simulations. First, the simulations relied on vendor-supplied operating characteristics for the diesels and electrical loads. Also, the scenarios simulated were not worst case scenarios. Finally, the simulations, as conducted, had the diesels dropping to 82% voltage, which is close to the limit of 80% voltage which would automatically trip the diesel generator off-line.

2. Instrumentation for Safety-Class Systems: All instrumentation (including instrumentation for safety-class systems) is supplied to DWPF operators through the DCS. With one exception, however, instrumentation for safety-class systems is verified locally once per shift (every 12 hours). Temperature monitoring for vessels in the salt process cell is provided exclusively through the DCS. It is possible for operators, relying on false temperature data, to increase temperature in the vessels to a point which would allow buildup of hydrogen to explosive concentrations. This scenario, however, would require operators to simultaneously lower purge rates to the minimum allowed and to ignore other available process data.

b. In an effort to improve human factors in the DWPF control room, WSRC is procuring an alarm management system that will filter and diagnose the alarms received in the control room. This system is in addition to the alarm handling system which is already installed and operational. The alarm handling system had reduced the number of critical alarms to 402, reduced the operator input necessary to respond to alarms, and grouped the alarms by process system.

   The alarm management system will provide additional prioritization and filtering of alarms and will diagnose probable causes of multiple alarm events. WSRC has decided, however, not to install this system since the verification and validation effort required

might delay startup of radioactive operations. The system will be installed when the DCS is upgraded after July 1996.

c. In addition to the above issues, the review covered the following topics from the September trip report.

1. Electrical Isolation of Safety-Class Equipment: To meet the requirements of ANSI/IEEE standard 384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, and ANSI/IEEE standard 379, *Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems*, WSRC completely separated the two redundant safety-class buses. It would now require the failure of the single safety-class breaker on each bus to interrupt all emergency power.

2. Emergency Lighting: The emergency lighting at DWPF is not seismically supported. These lights, which illuminate personnel egress routes during an electrical loss of power, might not be available after a seismic event. WSRC has no plans at this time to provide seismic support for the lighting.

3. Battery Ventilation: ANSI C2, *National Electric Safety Code*, requires adequate ventilation and loss of ventilation alarms for rooms with lead-acid batteries to ensure hydrogen does not build up and result in an explosion. The battery rooms in the vitrification building have recently been redesigned, but WSRC personnel were still unable to confirm that the new design meets all the requirements of ANSI C2.

4. Electrical Calculations: Electrical calculations for voltage profile, short circuit studies, and protective device coordination, as required by ANSI/IEEE Standard 141, *IEEE Recommended Practice for Electrical Power Distribution for Industrial Plants*, and ANSI/IEEE Standard 242, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, are complete with the exception of portions of the protective device coordination study. WSRC plans to complete all calculations before beginning radioactive operations and the Board's staff will review the completed calculations when they are available.