February 7, 2000

The Honorable Carolyn L. Huntoon
Assistant Secretary for
Environmental Management
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0113

Dear Dr. Huntoon:

The Defense Nuclear Facilities Safety Board (Board) has followed with interest several recent occurrences involving the distributed control system used to operate the Defense Waste Processing Facility at the Savannah River Site (SRS). Operator errors have resulted in inadvertent consequences on three occasions: a sludge transfer in February 1997, a glass pour in June 1997, and the shutdown of a safety-class exhaust fan in November 1999. In all cases, the design of the operator interface appears to have contributed to the personnel errors. The enclosed issue report prepared by the Board's staff outlines opportunities for improvement based on lessons learned from these occurrences and is provided for your consideration and use.

The Board is particularly concerned that all of the corrective actions identified following the February 1997 occurrence were not implemented. Indeed, incomplete implementation of appropriate corrective actions contributed to the occurrence in November 1999. The Board encourages SRS to ensure that the corrective actions identified following the most recent occurrence are fully implemented for all SRS facilities. In addition, the Department of Energy (DOE) should carefully examine the applicability of lessons learned from these occurrences to other computer-based process control systems at SRS and elsewhere within the defense nuclear complex. The Board wishes to be informed regarding the progress made by DOE and SRS in addressing these issues.

Despite the above occurrences, the Board was pleased to note the sustained level of effort at SRS in designing, maintaining, and improving process control systems to meet current standards of both the process and commercial nuclear industries. DOE might wish to determine

whether process industry standards for the design of safety-related control systems should be used on a broader scale for safety-significant systems within the defense nuclear complex.

Please contact me if you have any questions on this matter.

Sincerely,

John T. Conway
Chairman

c: The Honorable David Michaels
Brigadier General Thomas F. Gioconda
Ms. Beverly A. Cook
Ms. Gerturde Leah Dever
Mr. Richard E. Glass
Mr. Paul Golan
Mr. Keith A. Klein
Mr. Gregory Rudy
Dr. James M. Turner
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

December 22, 1999

MEMORANDUM FOR: G. W. Cunningham, Technical Director
J. K. Fortenberry, Deputy Technical Director

COPIES: Board Members

FROM: W. White

SUBJECT: Distributed Control Systems at Savannah River Site

This report documents an issue reviewed by the staff of the Defense Nuclear Facilities Safety Board (Board) at the Savannah River Site (SRS). On December 2–3, 1999, staff members W. White and T. Davis met with personnel from Westinghouse Savannah River Company (WSRC) and the Department of Energy (DOE) to discuss the design and operation of computer-based control systems. The primary focus of this meeting was human factors issues associated with the operator interface for various distributed control systems (DCSs) at SRS. As context for the following comments, it is important to note that the DCSs at the Defense Waste Processing Facility (DWPF) and 233-H (tritium facility) are not safety-class or safety-significant systems. Since they serve as the primary interface for operators to control and monitor facility activities, however, they can have a significant impact on the overall safety of the facility.

Background. On November 3, 1999, Process Control and Technology (PC&T) personnel inadvertently commanded a safety-class, Zone 1 exhaust fan at DWPF to stop. The subsequent change in ventilation pressure caused a safety-class interlock to trip, restoring Zone 1 exhaust. Personnel working in contaminated areas were required to evacuate those areas until actions could be taken to verify that no air flow reversal had occurred.

At the time of the occurrence, PC&T personnel were attempting to validate a recent DCS modification. The error occurred when the PC&T personnel, who were not DWPF operators, selected a default device on the graphic screen instead of the correct device. The error was facilitated by a system design that selects default devices as the current active device when operators shift between various screens.

This occurrence was similar to a previous occurrence in February 1997. In that earlier incident, an operator also selected a default device instead of the intended device; the result was an inadvertent transfer of sludge. The operator's action required a supervisor's permission, which was granted through the supervisor's console. As a result of that occurrence, WSRC initiated a corrective action that involved revising all equipment faceplates to ensure that default devices would not be operable equipment. This limited corrective action was applicable only to DWPF and only to certain types of graphics in the DCS interface. The final DWPF occurrence report

(SR--WSRC-WVIT-1997-0002) noted that this corrective action had been completed in November 1997. Yet while investigating the November 1999 occurrence, WSRC personnel found that, although the design had been completed, the software modification had never been installed in the DWPF DCS.

Another incident involving operator error occurred in June 1997 when a DWPF operator selected and operated an incorrect device, causing glass to be poured inadvertently into an empty canister. In this case, faceplates and equipment numbers were too similar. The operator had intended to shut down the primary off-gas exhauster, but shut down the backup off-gas exhauster instead.

Conduct of Operations and Operator Training. In all three of the occurrences discussed above, avoidable personnel errors caused the operation of facility equipment to have inadvertent consequences. In reviewing these occurrences and the general site programs for training DCS operators, the staff noted the following opportunities for improvement in conduct of operations and operator training for DCS-based process control:

- As mentioned above, personnel other than facility operators accidentally operated safety-class facility equipment. In general, only qualified facility operators should operate facility equipment. It is more appropriate for personnel involved in DCS and software modifications to have facility operators test the modifications with operable equipment instead of attempting such operations themselves.

- To command DCS-operated equipment in both DWPF and 233-H, a single command key must be pressed twice: once to initiate the operation and once again to confirm the command. Conversations between the staff and DWPF personnel indicated that operations personnel may be inclined to double-click the command key instead of pressing it once, carefully reviewing the operation about to be commanded, and then pressing the key again. Operator training could stress the importance of proper conduct of operations while operating equipment through a computer interface. An improved interface design (as discussed below) could reinforce this training.

- Given how easily facility equipment can be operated through the DCS interface, WSRC personnel might wish to reevaluate the types of operations that require a supervisor's permission. It might be appropriate to require such permission for operations that have the potential to impact the safety of a facility (such as shutting down Zone 1 ventilation in DWPF). As demonstrated by the February 1997 occurrence, however, this action would be effective only if supervisors carefully evaluated a proposed operation before approving it.

Human Factors. In most cases, WSRC personnel have performed the appropriate human factors analyses for computer-based process control systems, including those used at DWPF. According to WSRC personnel, the analyses were performed in accordance with guidance

contained in the appropriate industry standards[1] on human factors engineering. Nonetheless, the personnel errors discussed above were facilitated by weaknesses in the design of the human interface for the DCSs that were overlooked in the human factors analyses. The staff has the following observations regarding the human interface design and analysis of WSRC process control systems:

- The use of operable equipment as the system default significantly increases the probability that operators (or other personnel) will operate process equipment inadvertently. Although WSRC recognized this fact and initiated limited corrective actions following the February 1997 occurrence, those corrective actions were never implemented for DWPF. It is the staff's understanding that WSRC now intends to fully implement the corrective actions necessary to correct this deficiency at DWPF. It would be prudent for the DOE to apply lessons learned from this occurrence in evaluating all similar process control systems at other defense nuclear facilities and to initiate similar corrective actions where appropriate.

- Although most DCS interfaces have undergone a human factors analysis, a few of the smaller systems, such as those in the canyons, have not. It would be prudent for WSRC management to complete human factors analyses for all process control systems. In addition, any significant upgrades could undergo such an analysis. Moreover, to minimize the possibility of operator error in future systems, WSRC and DOE could incorporate lessons learned from these recent occurrences in all future human factors analyses.

- For new DCSs or significant modifications to existing systems, WSRC might consider changing its approach to the confirmation of operator commands. As discussed above, it is currently too easy simply to double-click the command key and initiate equipment operation. As new systems are installed or existing systems undergo significant upgrades, the confirmation request from the DCS interface could be improved. The request could clearly outline the operation being initiated, and the operator's response to the request for confirmation could require an action different from that required to initiate an operation.

Process Control Systems at SRS. For operational facilities, the PC&T group has the responsibility of providing full engineering support for process control systems, including DCSs. In general, this group employs a well-documented, standards-based approach to the development

[1] WSRC requires use of the following Institute of Electrical and Electronics Engineers (IEEE) and Nuclear Regulatory Commission (NUREG) standards for human factors engineering: IEEE 845, *Guide to Evaluation of Human-System Performance in Nuclear Power Generating Stations*; IEEE 1023, *Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*; IEEE 1289, *Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations*; and NUREG 0700, *The Human-System Interface Design Review Guideline.*

and support of process control systems. The staff was encouraged by the level of effort that has gone into upgrading and maintaining process control systems at SRS as new technology and standards have become available. As the primary providers of support for all SRS process control systems, the PC&T group also serves as the main vehicle for the informal transmission of lessons learned from one facility to another (especially for facilities with significantly different missions, such as DWPF and 233-H). There may be value, however, in adopting a more formal approach to site-wide feedback and improvement based on lessons learned at individual facilities.

The staff was also pleased to note that WSRC is incorporating lessons learned from the process industry in the design and analysis of process control systems. Recently, through the Instrument Society of America (ISA), control and safety engineers in the process industries have begun to implement industry-wide guidelines for safety-instrumented systems in process plants. In particular, 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. In many ways, the available standards for safety systems in the process industries are more applicable to the level of hazard posed to facility workers at SRS than are standards for nuclear power generating stations. For future safety-significant programmable control systems, WSRC will comply with ISA S84.01. The staff would encourage WSRC to consider the application of ISA S84.01 to all safety-significant instrumentation and control systems.