

John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
Joseph J. DiNunno
Herbert John Cecil Kouts
John E. Mansfield

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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



March 11, 1998

The Honorable Ernest J. Moniz
Under Secretary of Energy
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

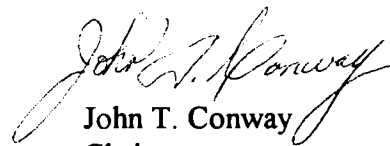
Dear Dr. Moniz:

Defense Nuclear Facilities Safety Board (Board) staff review teams visited the Savannah River Site on January 6–8 and 12–16, 1998, and February 5–7, 1998, to review preparations to resume first-cycle solvent extraction operations at H-Canyon. H-Canyon plays a vital role in nuclear materials stabilization at the Savannah River Site, and it is important that the facility and its personnel be thoroughly prepared before beginning this expanded operation.

The reviews conducted by the Board's staff identified a number of issues that need to be resolved before first-cycle solvent extraction operations begin. Discussions between the staff and Savannah River Site personnel have led to resolution of several issues satisfactorily. Several other matters, particularly those associated with controls preventing hydrogen deflagrations in process vessels, criticality controls, and the programmable logic controller used to implement limits established in the Technical Safety Requirements and Double Contingency Analysis, merit further consideration. The Board believes these issues can be addressed and resolved without affecting the current schedule for commencing first-cycle solvent extraction operations.

The enclosed reports provide a synopsis of the observations resulting from the staff reviews and are forwarded for your consideration. If you need additional information, please do not hesitate to contact me.

Sincerely,


John T. Conway
Chairman

c: Mr. Mark Whitaker

Enclosures

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

DNFSB Staff Issue Report

February 17, 1998

MEMORANDUM FOR: G. W. Cunningham, Technical Director

COPIES: Board Members

FROM: R. T. Davis

SUBJECT: Preparations for H-Canyon First-Cycle Operations

This memorandum documents an issue reviewed by a member of the staff of the Defense Nuclear Facilities Safety Board (Board) R. T. Davis, with the assistance of outside expert R. West. Preparations for H-Canyon first-cycle solvent extraction operations at the Savannah River Site (SRS) were reviewed on January 12–16, 1998, and February 5–7, 1998.

Westinghouse Savannah River Company (WSRC), which manages and operates SRS for the Department of Energy (DOE), will use H-Canyon to stabilize approximately 1900 deteriorating irradiated fuel assemblies during a 3-year campaign. H-Canyon is being restarted in three phases. The first phase, dissolving and head-end operations, began in July 1997. The second phase, first-cycle solvent extraction operations and associated solvent recovery and waste-handling activities, is scheduled to restart on May 4, 1998. The final phase, second product (neptunium) and uranium cycles, is scheduled to restart in late 1998.

WSRC declared readiness to proceed with H-Canyon first-cycle operations and DOE began its Readiness Assessment (RA) on January 26, 1998, and February 2, 1998, respectively. Because of equipment and configuration problems, the RA was suspended on February 5, 1998, at the request of WSRC. WSRC developed a corrective action plan and expects the DOE RA to resume on March 30, 1998, with hot operations to begin on May 4, 1998.

The Board's staff reviewed the implementation of controls identified in the H-Canyon authorization basis documents and facility readiness for first-cycle operations. The principal issues identified by the staff are summarized below.

Implementation of Controls. WSRC installed a new control system that uses a programmable logic controller (PLC) for automatic control of first-cycle operations. This PLC also functions as a safety-significant interlock to shut down first-cycle operations based on indications from a neutron monitor and uranium analyzer. The two Double Contingency Analysis (DCA) controls to prevent a criticality in the mixer-settler are control of stream parameters (using the PLC in some cases) and the PLC interlock. Because both contingencies use the PLC, a single-point or common-mode failure in the PLC could disable both DCA controls. Additionally, the PLC does not appear to meet process industry requirements for design of a safety

instrumented system, as described in American National Standards Institute (ANSI)/Instrument Society of America (ISA) standard ISA-S84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*. For example, the H-Canyon PLC system does not meet requirements for separation of the basic process control functions from the safety instrumented system functions and vendor identification of failure modes and frequencies.

Facility Readiness. Equipment failures and control of process stream parameters appear to be significant problems at H-Canyon. Several equipment failures have occurred during preparations for first-cycle operations (e.g., mixer-settler motor failures, neutron monitor spurious trips, uranium analyzer failure). Additionally, because of material problems, the operators have been unable to maintain some process stream parameters within the required operating range. Several attempts to conduct extended cold-run operations could not be completed because of equipment problems. WSRC corrected most of these problems and completed a 24-hour cold run before declaring readiness. However, some stream parameters were not maintained within the operating range during this 24-hour run. Failure to maintain these parameters during normal operations would have required the process to be shut down because these parameters may affect both DCA controls and process efficiency.

H-Canyon engineers initiated a troubleshooting procedure in October 1997 for modifying the PLC software control algorithms to achieve acceptable automatic control of the mixer-settler stream parameters. Once the troubleshooting procedure has been completed and the proposed PLC software changes have been identified, the software changes will need to be verified and tested in accordance with the software quality assurance plan. Operator training and procedure modifications would then be performed as required. However, this process was not complete prior to the start of the DOE RA, and operators were not aware of some of the PLC software modifications. This situation contributed to the control problems experienced during the DOE RA cold-run demonstration.

These equipment and process problems limited operator cold-run training and required a greater reliance on simulator training. The operators appeared knowledgeable concerning normal operations, and procedures appeared to support verbatim compliance. However, operator knowledge was weak concerning the source of instrument indications and subsystem operation. Additionally, operators appeared to have difficulty in interpreting process indications and responding to unusual conditions. During the DOE RA cold run, operators became distracted by stream temperature control problems and failed to monitor chemical head tanks. As a result, a loss of process stream flow occurred when a chemical head tank was allowed to empty.

The extent of the problems noted during operations caused WSRC to suspend the DOE RA on February 5, 1998. The staff believes WSRC declared readiness even though they had clear indications that the facility was not ready. The DOE RA team did a good job of identifying the facility problems that forced WSRC to suspend the RA; however, DOE-Savannah River (DOE-SR) line management ought to have recognized that the facility was not ready for operations prior to starting the DOE RA.

The Board's staff will continue to monitor DOE-SR and WSRC efforts regarding the DCA controls and use of the PLC interlock. These issues are expected to be resolved prior to facility startup. Additionally, the Board's staff will review WSRC efforts to improve facility readiness to support first-cycle solvent extraction operations beginning May 4, 1998.

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

DNFSB Staff Issue Report

January 27, 1998

MEMORANDUM FOR: G. W. Cunningham, Technical Director

COPIES: Board Members

FROM: R. Tontodonato

SUBJECT: Reviews of Process Safety for H-Canyon Phase II Operations, January 6–7, 1998, and January 22, 1998

This report documents a review by members of the staff of the Defense Nuclear Facilities Safety Board (Board) D. Moyle, R. Robinson, J. Sanders, and R. Tontodonato, conducted at the Savannah River Site (SRS) on January 6–7, 1998. The review focused on process safety for Phase II Operations at H-Canyon. This report also documents a video conference held on January 22, 1998, to follow up on issues discussed during the site visit with personnel from the Department of Energy's Savannah River Operations Office (DOE-SR) and Westinghouse Savannah River Company (WSRC).

H-Canyon is in the first year of a 3-year campaign to stabilize deteriorating spent nuclear fuel currently stored in SRS basins. Phase I operations involving fuel dissolution and head-end processing began in July 1997 following reviews by the Board's staff and a DOE Operational Readiness Review. Phase II operations involve first-cycle solvent extraction operations and associated solvent recovery and waste handling activities. A DOE Readiness Assessment for Phase II is scheduled to begin on February 2, 1998.

Discussions during the site visit centered on the Basis for Interim Operations (BIO) and Technical Safety Requirements (TSRs) that will govern H-Canyon operations. Accident scenarios that were discussed included red oil explosions, criticality accidents, hydrogen deflagrations, solvent fires, transfer errors, uncontrolled reactions in the cold feeds area, steam/cooling coil leaks, ammonium nitrate explosions in the ventilation system, and high radiation exposures in the gang valve corridor. The principal issues identified by the Board's staff are summarized below, along with information obtained during the January 22, 1998, video conference.

Hydrogen Deflagration in Process Vessels. The analysis in the BIO relies on the process vessel ventilation system to perform the safety-related function of providing sufficient air flow through process vessels (excluding the dissolvers and evaporators) to prevent flammable quantities of hydrogen from accumulating in the vapor space. Although there are no engineered features (e.g., dampers) that could obstruct the ventilation flow, the tanks are not instrumented to

measure the air flow rate or the hydrogen concentration. Additionally, the TSRs developed to prevent hydrogen deflagration accidents do not meet the SRS requirement for adding an extra level of control to prevent accident scenarios that could result in explosions.

WSRC personnel stated that a “streamer test” had been done once to verify flow into the air inlet for the last vessel in each leg of the ventilation system. Additionally, during the January 22, 1998, video conference, WSRC stated that the BIO and TSRs would be revised to credit control of ignition sources in the process vessels as a safety-significant control against hydrogen deflagrations. WSRC stated that all electrical connections and motors are external to the vessels, and the only moving parts in the vessels are the agitators.

The Board’s staff agrees that the streamer test showed there were no gross pluggages in the main ducting for the process vessel ventilation system at the time of the test. Also, although static electricity is extremely difficult to eliminate, formal controls on ignition sources should reduce the likelihood of a deflagration to some degree. The Board’s staff believes a better approach would be to use the existing instrument air system and associated flow instrumentation to verify routinely that each tank is receiving adequate air flow. This action would provide better assurance that hydrogen deflagrations will not occur. This system is credited in the BIO to perform this function for the H-Canyon evaporators.

Functional Classification of Criticality Controls. WSRC has prepared a formal double contingency analysis (DCA) to identify controls required to prevent criticality accidents in H-Canyon and the associated outside facilities. The BIO states that equipment and instruments associated with DCA controls were classified as safety significant if automatic actions (interlocks) were involved, or if operator action would be required in less than one shift to prevent a criticality. Other equipment and instruments required to implement DCA controls were not classified as safety significant. This approach is inconsistent with the treatment of other accidents in the BIO, where the functional classification of equipment and instruments is based on accident frequency and consequences, not the required operator response time.

DOE-SR observed that each criticality accident scenario involving the mixer-settlers has at least one level of safety-significant controls. The Board’s staff believes it would also be appropriate to require at least one safety-significant control for other criticality scenarios (e.g., those involving H-Canyon’s outside facilities) with frequencies and consequences that exceed the on-site worker exposure guidelines presented in the BIO. In the January 22, 1998, video conference, DOE-SR and WSRC stated that they now are developing a path forward that is expected to factor in the consequences of the event in assessing the adequacy of the associated controls.

Hydrogen Deflagration in a Mixer-Settler. Organic solvent fires and hydrogen deflagrations are treated separately in the BIO. For the mixer-settlers, the potential for an organic solvent fire is analyzed, but the potential for a hydrogen deflagration is not. In the January 22, 1998, video conference, WSRC stated that the only vapor spaces in the mixer-settlers are in the

chimneys where agitator shafts enter the mixer chambers, and it is unlikely that the shaft seals are tight enough to retain hydrogen generated by the process stream. WSRC also stated that hydrogen generation rates in the process stream are expected to be low, so it is unlikely that a flammable concentration of hydrogen would accumulate. WSRC noted further that the consequences of such an accident would be bounded by the larger deflagrations analyzed in the BIO.

The Board's staff agrees that the consequences of a hydrogen deflagration in a mixer-settler are bounded by other deflagration analyses in the BIO, but it is not clear that the frequency is likewise bounded. There are no TSR controls to prevent a hydrogen deflagration in the mixer-settlers. The TSR controls for solvent fire prevention are intended to maintain the solvent below its flash point. An analysis of the potential for accumulation of flammable quantities of hydrogen in the vapor spaces in the mixer-settlers would determine whether controls for this accident scenario would be appropriate.

Response Time for Evaporator Temperature Interlock Failure. One of the TSR controls to prevent red oil explosions in the evaporators is a temperature limit of 120°C. The TSRs allow the operator 30 minutes to shut the evaporator down manually if the temperature interlock fails, but there is no documented analysis to prove that the evaporator cannot reach an unacceptable temperature within 30 minutes of an interlock failure. However, the TSRs also limit pressure in the evaporator steam coils to 25 psig, corresponding to a saturation temperature of about 130°C. Since the autocatalytic temperature for red oil reactions is somewhat above 130°C, it is unlikely that rapid heating to an unsafe temperature will occur if the temperature interlock fails. The Board's staff believes a calculation needs to be performed to provide a documented basis for the 30-minute response time.

“Immediate” Repairs. Some of the TSRs require that failed equipment be repaired “immediately” while further corrective actions are pursued. It is not clear in all cases that the other compensatory actions specified in the TSRs will maintain the facility in a safe condition while immediate repairs are undertaken. For example, if the canyon ventilation system is not producing a high enough vacuum (a condition that could allow radiological contamination to escape to the environment), the TSRs require restoring canyon vacuum immediately and placing the facility in standby mode within 8 hours. It is not clear that adverse consequences would be avoided if shutdown actually took 8 hours. In the January 22, 1998, video conference, WSRC stated that procedures would require faster shutdown of operations than is specified in the TSRs. The Board's staff believes that if more rapid actions are required for this scenario, or for other scenarios for which “immediate” repairs are specified, the TSRs ought to reflect what is actually required.