DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

July 20, 2001

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

Dear Ms. Roberson:

The Defense Nuclear Facilities Safety Board (Board) has been evaluating preparations at the Savannah River Site (SRS) to start up the HB-Line neptunium/plutonium oxide process, known as HB-Line Phase II. Safe and successful operation of HB-Line Phase II is an important step toward stabilizing actinide solutions at SRS, as committed to by the Secretary of Energy in the Department of Energy's Implementation Plan for the Board's Recommendation 94-1, *Improved Schedule for Remediation in the Defense Nuclear Facilities Complex*. The Board believes thorough and timely analysis of hazards and identification of controls are essential to the success of this project and to the avoidance of further delays in stabilizing these hazardous materials.

The Board's staff has identified several potential safety issues associated with this activity. Some of these issues appear to be the result of insufficient hazard analysis. In general, the hazard identification process used for this project does not appear to be as comprehensive as the Process Hazard Analysis methodology recommended in DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*. The limitations of the methodology used at HB-Line Phase II may have contributed to some accident scenarios not being evaluated effectively in the contractor's hazard analysis.

The Board is aware that additional hazard analysis is being performed, and anticipates receipt of the findings of this analysis, as well as the identification and implementation of additional controls that may be warranted. The Board was pleased to see that a safety system failure mode evaluation has been performed to identify potentially unsafe failure modes for some existing HB-Line systems that provide active safety controls. A similar evaluation may be appropriate for other HB-Line safety systems, including those that perform alarm functions.

During a recent visit to SRS, the Board was briefed on HB-Line Phase II startup preparations. The Board is aware that there are continuing discussions between the Board's staff and SRS personnel, and that work to address staff questions and issues is ongoing.

The enclosed reports prepared by the Board's staff identify several issues that warrant further consideration by project personnel.

Sincerely,

John T. Conway
Chairman

c: Mr. Greg Rudy
Mr. Mark B. Whitaker, Jr.

Enclosures

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 25, 2001

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: C. Graham

SUBJECT: Electrical and Instrumentation and Control Systems, HB-Line Phase II

The staff of the Defense Nuclear Facilities Safety Board (Board) met with personnel from the Department of Energy and the contractor at the Savannah River Site (SRS) on March 20–23, 2001. The Board's staff also reviewed documentation received on April 3, 2001, and held teleconferences with site personnel on April 26, May 1, and June 14, 2001. The focus of these reviews was on evaluating the design of the HB-Line Phase II electrical and instrumentation and control (I&C) systems. The reviews were performed by staff members A. Gwal and C. Graham.

Background. The purpose of the HB-Line Phase II project is to recover plutonium from 34,000 liters of plutonium nitrate solution and convert the plutonium to an oxide powder. The process consists of feed receipt and adjustment, anion exchange, filtration, drying, and other process steps. The project relies on several safety systems currently operating in the facility, including the electrical system (a portion of which is classified as safety-significant), the process air purge system, several ventilation systems, the process vessel vent system, process hold tank interlocks, nuclear incident monitors, and alarm systems. Two additional safety-significant I&C systems have been added for the project: the resin column feed tank interlocks and hydrogen purge low flow alarms. The basic process control system has been upgraded extensively to include a general-service distributed control system (DCS).

Electrical Systems. The Board's staff made the following observations regarding the electrical systems for HB-Line Phase II.

Electrical Distribution System—The Board's staff had reviewed electrical systems for HB-Line prior to the HB-Line restart in 1993. Various equipment modifications have been made since the restart. Therefore, the staff reviewed the revised 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 were performed in accordance with Institute of Electrical and Electronics Engineers (IEEE) STD-141, *IEEE Recommended Practice for Electric Power Distribution for Industrial Plants,* and STD-242, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*. The staff noted that several nonsafety loads are connected to the safety-significant busses. IEEE-384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, requires that nonsafety loads be appropriately isolated from the safety-significant bus to ensure that a failure of a nonsafety component will not cause failure of the safety-significant power system. HB-Line personnel have indicated their intent to evaluate whether isolation of the nonsafety loads is adequate.

Self-Assessment—Industry standards are updated periodically in part because of identified safety concerns and lessons learned. One of the key objectives of an electrical safety program is to develop a self-assessment process that evaluates current practices and design against existing standards. This process would identify any nonconformance with applicable requirements of such standards as National Fire Protection Association 70 (National Electrical Code), the National Electrical Safety Code (American National Standards Institute [ANSI]-C2), and respective parts of the Code of Federal Regulations (29CFR1910 and 29CFR1926). The staff determined that electrical safety program self-assessments are not being performed for HB-Line.

Instrumentation and Control Systems. The Board's staff developed the following observations concerning the I&C systems for HB-Line Phase II.

Hydrogen Purge System—Safety-significant rotameters monitor air flow to each process vessel. The rotameters provide indications on the DCS and alarms on the safety-significant control room alarm panel. Prevention of a hydrogen explosion relies in part on the proper operation of these alarms and correct response by operators. The rotameters require a certain pressure range in their supply header to provide accurate readings. In the current design, rotameter header pressure is indicated by a gauge that operators read locally every 2 months. There is no control room indication or alarm associated with this parameter. If this header pressure were out of the specified range, the rotameters could indicate a higher-than-actual flow. This result could be an actual purge flow rate through the process vessels that is lower than required for sufficient removal of hydrogen generated in these vessels. Adding a safety-significant pressure transmitter to indicate header pressure on the DCS and a pressure alarm on the safety-significant alarm panel would address this issue.

Resin Column Interlocks—Cold-feed preparation tanks for the elution and dilution cycles have interlocks designed to prevent the addition of high-molar nitric acid (greater than 8 molar) to the resin columns. Refractometers measure acid concentration by measuring the refractive index of the process solution and converting this result to a molarity. Molar concentration is displayed on the DCS, and an interlock function prevents opening of the feed valves if the concentration exceeds 8 molar. Project personnel were unable to provide evidence of a failure modes and effects analysis for the refractometer or its embedded software. Also, the refractometer software was not analyzed or failure tested to identify and analyze nonsafe failure modes of the system software, as discussed in the SRS *Conduct of Engineering Manual* (Section 5.3 of Procedure 5.07, "Evaluation of Existing and Acquired Software"). Such evaluations would help determine the frequency and impact of these failure mechanisms. Finally, since this will be the first use of this type of refractometer, no site operating history has been established. Performing periodic sampling (e.g., weekly) of cold-feed tanks for a period of time (e.g., 6–12 months) would be appropriate to establish an operating history that could be used to compare sample results with refractometer output.

Fault Tree Analysis *and Safety Reliability Calculations*—Westinghouse Safety Management Solutions (WSMS) performed calculations as required by Instrument Society of America (ISA) standard S84.01, *Application of Safety Instrumented Systems for the Process Industries*. These calculations support the safety integrity level (SIL) determination and verification of the resin column nitric acid feed interlocks and the process tank hydrogen purge low-flow alarms. The staff identified several issues associated with these calculations and the fault tree analysis, which are identified in the Attachment. It is not clear that the hydrogen purge low-flow alarm is designed to provide the reliability expected of a safety-significant system. A reevaluation of the fault tree analysis and SIL determination would be appropriate to ensure that safety systems will function as required.

Self-Assessment of Existing Instrumentation and Control Systems—Failure mode evaluations and reliability analyses of existing systems are important for identifying safety design weaknesses in I&C systems; they can be particularly important for systems designed using outdated codes and standards. One such evaluation, WSRC-TR-2000-00383, *HB-Line Safety System Failure Mode Evaluation,* was performed in response to occurrence SR-WSRC-HBLINE-2000-008, *Potential Inadequacy in the Safety Analysis (PISA) for the HB-Line Building Pressure Low Building Vacuum Interlock.* This evaluation identified two component failure mechanisms that had not previously been considered. Performing a similar analysis of all instrumented safety systems relied upon for HB-Line Phase II operations, including systems that perform alarm functions (such as the process vessel ventilation system, the air purge dissolver system, and alarm panel circuits), could identify their nonsafe failure modes and help predict their failure frequency.

Software Failure Analysis—The staff reviewed software engineering documents associated with the safety-significant programmable logic controller (PLC) and DCS. It appears that the major portions of the software life cycle have been implemented appropriately for the HB-Line project; the software documents reviewed indicated a reasonable application of IEEE software standards. However, it did not appear that a software hazard operability study or similar evaluation had been performed on the general-service DCS to verify that its potential malfunctions would not impact safety. Performance of such an analysis would be consistent with WSRC-IM-90, *SRS Process Hazards Management Manual,* and would help confirm that the software will perform its intended function and automated control processes reliably.

Attachment

Attachment

Issues Associated with Fault Tree Analysis and Safety Reliability Calculations

The Defense Nuclear Facilities Safety Board's staff identified the following issues with respect to the fault tree analysis and reliability calculations for instrumentation and control (I&C) systems associated with HB-Line Phase II operations.

- *Hydrogen Purge System Safety Integrity Level (SIL) Determination*, S-CLC-H-00826, Section 3.2, provides facility input data. One input item involves checking the flow on process tanks once every 12 hours and references Technical Safety Requirement (TSR) 4.3.4.1. However, this surveillance requirement is not included in WSRC-TS-97-7, *Technical Safety Requirements, Separations Area Operations Building 221-H HB-Line*. SRS personnel agreed to review this issue to determine whether TSR-level controls are required.

- S-CLC-H-00826, Section 4.2, addresses failures in the purge flow path. There is no discussion of flow path failures for piping or other components in the purge flow downstream of the process vessels (i.e., the vessel vent system). Certain vessel vent system failures could cause loss of purge air flow, but these failures were not analyzed in the fault tree for the SIL determination. Section 4.2 addresses flow changes due to a pipe rupture and cites methods used to detect this failure. It was not apparent to the staff whether the hydrogen purge system would provide adequate indication of a pipe failure.

- S-CLC-H-00826, Section 5, provides a recommendation that the I&C system be designed to SIL-1, probability of failure on demand (PFD) of 5.3×10^{-2}. In the SIL verification, S-CLC-H-00792, a PFD value of 3.0×10^{-2} was calculated for the designed safety-significant instrumented system. Given the inaccuracy of failure rate data and potential unidentified failures, it is not clear that the verified design provides adequate reliability and sufficient margin to ensure that the recommended PFD is met.

- *Resin Feed Tank SIL Verification*, S-CLC-H-00827, cites a PFD of 5.5×10^{-7} for the Triplex PLC. This value does not account for software errors that may occur in the software design of the control logic written by site personnel. This PFD may be too optimistic for the PLC when user software is considered. SRS personnel expressed their intent to modify the SIL verification to include discussion of the site's software quality assurance program and its effect on application software.

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 25, 2001

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: R. Robinson, M. Duncan

SUBJECT: Chemical Process Safety, HB-Line Phase II

This report documents issues identified by the staff of the Defense Nuclear Facilities Safety Board (Board) during a review of the chemical processes described in the authorization basis for the HB-Line Phase II startup.

Overview. HB-Line Phase II operations are scheduled to commence in December 2001. The operations involve converting 34,000 liters of H-Canyon plutonium nitrate solutions to oxide powder. The process steps include valence adjustment, separation through ion exchange, concentration, oxalate precipitation, filtration, and calcination to oxide.

Process Chemistry Issues. After performing a review of the authorization basis for HB-Line Phase II, the staff identified weaknesses in the analysis of two hazards: ion exchange resin explosions and chemical reactions in process tanks.

Resin Explosions—Since 1962, there have been no fewer than nine documented incidents of fire, explosion, and/or vessel rupture in anion exchange vessels. These incidents, categorized as "resin explosions," have occurred under various conditions of temperature and nitric acid concentration. All of the systems involved were exchanging either plutonium, neptunium, curium, or uranium.

A document commissioned by the Savannah River Site (SRS) contractor, *Task 15-Phase I Assessment of Additional Pressure Relief Capability 221 HB-Line Anion Exchange Columns,* identified several conditions contributing to a possible resin explosion:

- exposure of resin to greater than 9 molar nitric acid
- exposure of resin to high temperature
- allowing resin to dry
- exposure of resin to strong oxidants other than nitric acid, such as permanganate or chromate ions

- exposure of resin to high radiation doses
- allowing resin to remain in a stagnant, nonflow condition while loaded with exchanged metal and/or in contact with process concentrations of nitric acid
- exposure of resin to strong reducing agents, such as hydrazine
- exposure of resin to catalytic metals such as iron, copper, or chromium

The process design and authorization basis for HB-Line Phase II address some, but not all, of these conditions. Sufficient passive and active controls are designed into the HB-Line Phase II process to prevent possible high nitric acid concentrations or resin dryout. The effect of temperature on the resin exotherms was carefully documented in the March 10, 2000, Savannah River Technology Center (SRTC) report *Qualification of Reillex™ HPQ Anion Exchange Resin for Use in SRS Processes*. The authorization basis specifies controls for temperature effects based on this document. These studies also indicate that the maximum expected radiation dose to the resin during 1 year is much lower than would be required to pose a safety concern. Finally, the design of the process prevents the use of oxidants other than nitric acid, such as permanganate or chromate ions, in the resin columns. However, several conditions that could lead to a resin explosion were not adequately addressed in the hazard analysis, including a stagnant resin bed, exposure to catalytic metal ions, and the possible introduction of strong reducing agents to the resin. It would be appropriate for these three conditions to be identified and analyzed, and for associated controls important to safety to be incorporated, if warranted, in the authorization basis and operating procedures.

Chemical Addition—The combination of certain chemicals during the HB-Line Phase II process will produce heat from exothermic reactions. Some reactions can also generate substantial volumes of gas. A high rate of chemical addition can easily cause an eructation in addition to a large evolution of heat. In a closed process vessel, a sudden generation of heat and gas could result in an explosion caused by overpressure. An informal analysis performed by the SRS contractor determined that the presence of the "ever open" vessel vent system and the relatively low heats of reaction for the potential chemical combinations eliminate this safety issue. Discussions between the staff and the contractor led to agreement that reactions caused by chemical additions to the process tanks are not likely to cause an accident resulting in serious injury to a worker. However, this scenario was not included in the development of the authorization basis and its supporting documents.

The staff believes the hazard analysis for HB-Line Phase II was not consistent with chemical processing industry practice whereby potential runaway reactions in each process vessel are analyzed. However, by installing orifices to limit addition rates and limiting the size of portable chemical addition vessels, efforts are being made to provide controls for hazards originally missed.

A formal analysis of chemical additions to the HB-Line Phase II process has recently been completed, and a determination of the maximum safe addition rates is expected in mid-July

2001. On the basis of preliminary results from the formal analysis, the contractor believes its previous conclusions are valid.

Conclusion. The Board's staff concludes that the contractor has not throughly analyzed and formally documented preventive measures for all the known causes of resin explosion, nor has the analysis of chemical eructations as yet been completed and formalized. A formally documented analysis is needed to support the implementation of adequate controls for HB-Line Phase II.

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

July 6, 2001

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: C. Coones

SUBJECT: Fire Protection Review, HB-Line Phase II

This report documents observations made by the staff of the Defense Nuclear Facilities Safety Board (Board) during meetings held from March through June 2001 concerning fire protection for HB-Line Phase II activities. Staff members C. Coones, F. Bamdad, and J. Troan reviewed the facility, as well as the process and hazard analysis documentation, to evaluate whether the facility was adequately protected from postulated fire events.

Hazard Identification. The staff's review of the HB-Line Basis for Interim Operation (BIO) indicated that not all hazards were analyzed in the BIO, the Hazard Analysis, or the HB-Line Fire Hazards Analysis (FHA). Table 8.1-8 of the BIO indicates that up to 4,500 pounds of acetone, 900 pounds of hydrogen peroxide, and 110 gallons of hydrazine mononitrate may be stored in the facility. A similar table, identified in S-CLC-H-00230, *HB-Line Facility Hazards Analysis*, as the maximum facility chemical inventory, lists the same quantities of acetone and hydrogen peroxide, but 28,000 pounds of hydrazine mononitrate. Westinghouse Savannah River Company (WSRC) personnel have indicated that these chemical quantities are not required for HB-Line operations and that this table indicates permitted quantities of chemicals under environmental regulation. However, aside from these tables, there is no determination of bounding quantities of process chemicals that may be found inside HB-Line. The potential hazard presented by these chemicals in these quantities has not been evaluated; although the FHA addresses a small quantity of hydrazine mononitrate, there is no analysis of any quantity of acetone or hydrogen peroxide in the facility. To properly ascertain the chemical hazard, a consistent bounding quantity of process chemicals needs to be determined and properly analyzed in the BIO.

Functional Classification of Fire Protection Systems. The BIO indicates the need for a safety-class fire suppression system on the third and fourth floors of HB-Line. The safety-class fire suppression system is fed from the H-Area fire protection water supply system and routed through the H-Canyon suppression system, both of which are functionally classified as production support systems. Loss or impairment of the H-Area fire water supply system or part of the system in H-Canyon could result in a loss of the HB-Line sprinkler system without the knowledge of HB-Line operations personnel. The current HB-Line Technical Safety Requirements (TSR) document requires only annual flow testing of the sprinkler system and monthly pressure readings, and contains no controls over the source of fire water. Procedure 2.25, "Functional

Classifications," in the WSRC conduct of engineering manual, states that systems supporting safety-class functions are required to be safety-class as well. DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1, Facility Safety*, states that support systems must be classified as safety-class if their failures can prevent a safety-class system, structure, or component from performing its safety functions. The functions of the H-Area fire water system and the H-Canyon suppression system support the safety-class fire suppression system in HB-Line. To provide safety-class fire suppression in HB-Line, the operation of the fire water supply system must be controlled to the same level. One method would be to functionally classify the H-Area fire water system as safety-class, with attendant TSR controls.

Tornado Dampers. The tornado dampers in the HB-Line supply ducts are credited in the BIO with eliminating the flow of combustion products from HB-Line during intermediate and full facility fires that involve the fifth and sixth levels of HB-Line. Typically, tornado dampers are installed to prevent rapid building depressurization during tornados outside the facility. Depending on its design, the damper may not function properly when triggered by a pressure increase inside the facility, particularly the gradual pressure increase that would accompany a fire in the facility. The TSR operability specifications for the tornado dampers contain only the requirement that the dampers be operable; they include no operating pressure or leak rates. Because of these issues, there is insufficient evidence that these tornado dampers can serve to isolate the facility during a fire. In addition, review of the TSR indicates that if the dampers are determined to be inoperable, a period of 7 days is allowed to restore operability. If operability has not been restored after 7 days, 72 hours is allowed to produce a response plan, and an unlimited time is allowed to repair the equipment. Therefore, although this equipment is required by the accident analysis, it may be out of service for an unlimited period. It may be appropriate for DOE to consider a change to the TSR to require that the facility be placed in a safe condition if this equipment is not restored to service within a limited time.

Combustible Control. The current safety analysis contains requirements for strict control of combustibles in rooms 410N and 410S to protect the JT-71 and JT-72 tanks in the area. The controls limit the total quantity of combustibles to 400 pounds wood equivalent and specify separation distances between combustibles and tank supports. The existing transient combustible control procedure, NOP-221-HB-6903, does not include the third and fourth floors of HB-Line, indicating that this administrative control is not complete. Furthermore, a recent review by WSRC indicated that the quantity of combustibles in the area may actually be as high as 5,670 pounds wood equivalent, providing sufficient fuel to produce a high-temperature (1200°C) flashover fire in the area and boil off the tank contents. Combustible control is no longer a viable administrative control for this area. Instead, WSRC has proposed to limit the concentration of plutonium in these tanks to 5.5 grams per liter to prevent unacceptable consequences due to a fire in this area. This type of control needs to be instituted as a TSR control. WSRC is working to provide the revised safety analysis to the Department of Energy in early July 2001. The Board's staff plans to review the revised analysis once it is complete.