DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

June 18, 2014

Mr. David Huizenga
Acting Assistant Secretary for
Environmental Management
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0113

Dear Mr. Huizenga:

The recently approved Safety Basis for the 242-A Evaporator facility at the Hanford site is not compliant with Title 10, Code of Federal Regulations Part 830, *Nuclear Safety Management*, and other Department of Energy (DOE) requirements. Specifically, a number of identified hazards are not properly addressed and several safety-significant controls do not comply with applicable DOE directives. DOE has begun to address some of the identified inadequacies with the safety control set, but the remaining safety issues require additional action. Given the anticipated need to operate this facility for an extended period of time, it is important to develop a compliant safety basis in a timely manner. Further details on these issues are provided in the enclosed report.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Defense Nuclear Facilities Safety Board requests a report within 90 days of the issuance of this letter, or prior to introduction of radioactive waste into the facility, that:

(1) Identifies the compensatory measures to be applied to the existing safety-significant steam isolation valve until the valve is qualified to perform its safety function, or is replaced with a qualified system;

(2) Describes DOE's plan and schedule to remediate the deficiencies with the safety control set identified in the enclosure to this letter; and

(3) Identifies the actions to be taken for the next annual update to the Documented Safety Analyses for the 242-A Evaporator and the Tank Farms that deal with the inappropriate screening of operational events, exclusion of chemical and toxicological hazards, and reliance on Safety Management Programs in place of credited controls.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

April 16, 2014

MEMORANDUM FOR: S. A. Stokes, Technical Director

COPIES: Board Members

FROM: F. Bamdad
M. Horr

SUBJECT: Safety Basis Review of 242-A Evaporator at Hanford

This report documents the results of a review of the 242-A Evaporator Safety Basis performed by members of the staff of the Defense Nuclear Facilities Safety Board (Board) at the Hanford site. The observations made during this review were discussed with personnel from the Department of Energy's (DOE) Office of River Protection (ORP) and its contractor, Washington River Protection Solutions (WRPS), during the week of March 24–28, 2014.

Facility Description. Originally constructed in 1974, the 242-A Evaporator facility's current mission is to support environmental restoration and remediation of the Hanford Tank Farms by optimizing the efficient use of double-shell tank waste volumes. The Evaporator uses a conventional, forced-circulation vacuum evaporation process to concentrate radioactive liquid tank waste at low pressure and temperature.

Feed (dilute tank waste to be concentrated) for the 242-A Evaporator is staged in 241-AW-102, a one-million gallon double-shell tank. The waste feed is concentrated in the evaporator room in the C-A-1 vessel to a specified concentration, creating product slurry and water vapor. The slurry is returned to another double-shell tank. Offgases and water vapor are passed through a series of condensers, filtered, and released to the environment.

The Evaporator is a Hazard Category-2 nuclear facility. The Documented Safety Analysis (DSA) identified two design basis accidents that require safety-significant controls: (1) flammable gas accidents, and (2) waste leaks and misroutes. Both of these accidents could result from operational events or be initiated by a seismic event. There are three safety-significant systems designed to prevent these accidents. Two are safety instrumented systems (SIS): the C-A-1 vessel flammable gas control system and the C-A-1 vessel waste high level control system. The third is a system that requires operator action, the C-A-1 vessel seismic dump system. These safety systems were recently installed in the facility.

Safety Basis Evaluation. WRPS recently revised the DSA for the 242-A Evaporator facility as part of an upgrade to the Safety Basis in order to meet the requirements of Title 10, Code of Federal Regulations Part 830 (10 CFR 830), *Nuclear Safety Management*, and its safe

harbor methodology found in DOE Standard 3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. The DSA was approved by DOE-ORP in June 2013. The DSA used the methodology described in DOE Standard 3009 supplemented by the recommendations of DOE Standard 1189, *Integration of Safety into the Design Process*, regarding the hierarchy of controls and threshold quantities of the unmitigated consequences for identification and classification of safety-related structures, systems, and components. The DSA relies on the Hazard Evaluation Database to identify the hazards for further evaluation and identification of controls. This Hazard Evaluation Database is part of the approved safety basis for the 242-A Evaporator facility.

Unaddressed Hazards in the Safety Basis—The methodology applied in the Hazard Evaluation Database uses hazard identification and evaluation criteria that in some cases depart from the nuclear safety requirements of 10 CFR 830 and the methodology described in DOE Standard 3009. These inappropriate criteria and some example cases are described below.

The hazard evaluation excludes operational events with estimated likelihoods of beyond extremely unlikely (BEU) (i.e., less than 1E-6 per year) from further analysis, evaluation of consequences, and identification of preventive or mitigative controls. For example, the safety basis credits an analysis for event 242A-FG-03 (release of C-A-1 vessel aerosols due to deflagration) to conclude that in this specific case the probability of hydrogen deflagration is BEU; therefore, no consequences to the facility worker are evaluated and no controls are required even though the unmitigated consequences would be significant and may warrant identification of a safety-significant control. Similarly, in event 242A-FG-05 (release of waste due to deflagration in the slurry sampler cabinet), the safety basis credits the configuration of the slurry sampler cabinet to prevent a hydrogen deflagration by not being airtight. This makes the event's likelihood BEU and therefore prevents evaluation of consequences or consideration of controls instead of identifying the physical configuration of the cabinet as a design feature that needs to be under configuration control. This practice is inconsistent with DOE Standard 3009 which states, "There is no predetermined frequency cutoff value, such as 1E-6 per year, for excluding low frequency operational accidents (i.e. internally initiated)." Consequently, it is not clear how the DSA meets the requirement from 10 CFR 830 that "A contractor must perform work in accordance with the safety basis ... and, in particular, with the hazard controls that ensure adequate protection of workers, the public, and the environment" if all hazards do not have identified controls.

The hazard evaluation screens out chemical and toxicological hazards in the facility that are not byproducts of radiological activities, and assumes that site safety management programs (SMP) would provide for the safety of the workers without a formal mechanism to ensure that site SMPs address the identified hazards. This is inconsistent with the 10 CFR 830 requirements that "A documented safety analysis must address all hazards (that is, both radiological and nonradiological hazards) and the controls necessary to provide adequate protection [emphasis added]..."

The hazard evaluation identifies certain hazards to be "occupational hazards" and categorically relies on the site SMPs to provide adequate protection of the workers without consideration for the safety classification of the needed controls. For example, high direct

radiation hazards to the workers are screened out from consideration and identification of the need for safety-significant controls, and it is assumed that the site radiation protection program will adequately protect the workers. This is inconsistent with the DOE expectations in DOE Standard 3009 of the need for safety-significant controls for "significant radiological or chemical exposures to workers." Additionally, elimination of such hazards from further analysis leads to the lack of identification of the specific attributes of the SMPs that may have been identified for protection of the workers. Section 204 of 10 CFR 830 requires identification of "the characteristics of the safety management programs necessary to ensure the safe operation..." in the safety basis of a nuclear facility.

As a result, the Hazard Evaluation Database and the DSA appear to be limited to the identification of the safety-significant controls for those hazards that meet the threshold values for significant consequences to the workers, supplemented by a few defense-in-depth controls. The DSA relies on the site SMPs to protect the workers from lower consequence hazards with the exception of a few cases. This approach is not consistent with the requirements in Appendix A, paragraph E.4 of 10 CFR 830 that "A documented safety analysis must address all hazards (that is, both radiological and nonradiological hazards) and the controls necessary to provide adequate protection to the public, workers, and the environment from these hazards [emphasis added]."

Deficiencies in the Engineered Safety Control Set—The accident analysis described in the DSA does not identify the need for safety-class controls for protection of the public because the unmitigated consequences at the site boundary are below the DOE Evaluation Guideline of 25 rem total effective dose. The DSA identifies several safety-significant engineered features based on identifying significant on-site accident consequences. However, there are weaknesses associated with some of these safety-significant controls that can result in less than adequate performance, or complete failure, of their safety functions.

The steam isolation valve to the reboiler (steam valve FV-EA1-1) is identified as safety-significant. Its safety function is to isolate steam from the reboiler during an operational upset or after a seismic event, and prevent an increase in the temperature of the waste in the C-A-1 vessel. This valve is part of the safety-significant C-A-1 vessel flammable gas control system, and is part of the C-A-1 vessel seismic dump system whose safety function is to prevent hydrogen deflagration or detonation in the evaporator vessel.

DOE Order 420.1B, *Facility Safety*, requires that safety-related controls be able to reliably perform their required safety function. DOE Standard 3009 (Section 4.4) requires that the DSA contain a system evaluation of the ability of the safety-related control to perform its safety function. WRPS's system evaluation of this steam isolation valve identified that the valve is not seismically qualified despite the requirement to operate after a seismic event. Additionally the evaluation found that the valve's failure would place a demand on the SIS that it is a part of. This is contrary to the requirements of the applicable design standard American National Standards Institute/International Society for Automation 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. Based on this evaluation, WRPS launched an activity to design and install new valves that would allow separation of the safety and non-safety components, as well as seismic qualification of the safety-related valve.

The 242-A Evaporator's original operational schedule prevented completing this upgrade prior to commencing nuclear operations. Therefore, DOE-ORP approved the DSA allowing WRPS to operate the Evaporator with this safety-significant valve not meeting its functional requirements identified in the DSA. This decision was based on a qualitative evaluation by WRPS that this condition presents a low risk based on the low likelihood of a seismic event and the assumed operability of other non-seismically qualified engineered features.

Given that the waste processing campaigns have now been delayed by almost a year, members of the Board's staff believe that the upgraded valves could have been installed prior to nuclear operations or compensatory measures could have been developed. Additionally, this planned upgrade has been identified in the DSA as an "Operational Safety Improvement." This section of the DSA is not intended to be used to address this kind of deficiency of a safety-related system to perform its safety function without identifying interim controls. Section 3.3.2.3.1 of DOE Standard 3009 states, "If the DSA preparer wants to make commitments to planned improvements not yet implemented (as a result of the hazard evaluation), this section will identify those major design and operational improvements." As indicated, these operational improvements should be identified as a result of the hazard analysis and not deficiencies found in the system evaluation required by Section 4 of DOE Standard 3009.

WRPS's failure modes and effect analyses (FMEA) of the new safety-significant systems identified vulnerabilities associated with the safety-significant solenoid valves used in all of the safety-significant SISs. These solenoid valves control the feed valve (valve HY-CA1-1A) and the dump valves (HY-CA1-7A and HY-CA1-9A) as part of the safety-significant SISs and the safety-significant C-A-1 vessel seismic dump system. The FMEAs stated that relatively high temperatures could lead to the failure of the actuation system for these valves, leading to their failure to perform their safety function. As a result, the systems were qualified to 200 °F, which bounds the normal operational environment of the system. This qualification, however, is not adequate to ensure operability of the systems during a fire scenario. As a result, a fire in the Evaporator's condenser room, where these solenoid valves are located, could disable the systems and remove the ability to safely shut down the Evaporator. This would lead to an increased hydrogen accumulation and an increased risk of deflagration in the evaporator vessel. This fire, or a seismic event followed by a fire, could lead to significant unmitigated onsite consequences due to the inability of the safety systems to perform their credited functions. The condenser room is equipped with a fire suppression system; however, this system is not identified as a qualified or credited control in the DSA.

Chapter IV of DOE Order 420.1B requires an evaluation of the safety-related systems for common cause failure, or impact of non-safety related systems, to ensure their operability. This failure of the safety-significant components, though identified in the FMEA, had not been further evaluated or remediated by WRPS personnel, or identified in the DSA. WRPS personnel stated that they had thought a fire in that room was not credible. The DOE-ORP safety basis approval authority was also unaware that a potential fire would induce a common cause failure of all safety-significant SISs. Subsequent to review by members of the Board's staff and identification of this potential safety issue, WRPS declared a Potential Inadequacy in the Safety Analysis for

this unanalyzed condition and determined that it resulted in a positive Unreviewed Safety Question Determination.

Deficiencies in the Administrative Safety Control Set—The DSA identifies many Administrative Controls (AC), some of which are designated as safety-significant and therefore further classified as Specific Administrative Controls (SAC) and key elements of SMPs that are implemented through the Technical Safety Requirements (TSR) document. There are weaknesses in the implementation of some of these controls that are contrary to DOE Standard 3009 and DOE Standard 1186, *Specific Administrative Controls*, and reduce the effectiveness of these credited administrative controls.

The TSR document identifies a SAC to perform a safety-significant function and prevent hydrogen deflagration in the facility during manned activities (e.g., maintenance activities). While the SAC designation is consistent with the expectations of DOE Standard 3009 and DOE Standard 1186, the implementation of the SAC is flawed. The SAC requires implementation of an ignition control program as one of the acceptable means of meeting its safety functional requirement. The ignition control program, however, is implemented through a key element of an SMP. Individual violations of key elements of an SMP would not necessarily constitute a TSR violation, despite the fact that a safety functional requirement was not being met. Therefore, a continued trend of failures is needed before the SMP is declared as ineffective and a TSR violation can subsequently be declared. However, a single failure to comply with a SAC should lead to a TSR violation, consistent with requirements in sections 4 and 5 of DOE Standard 1186. Relegation of the required action of a SAC to an SMP reduces the reliability of the safety-significant control.

The safety-significant function of the Evaporator's C-A-1 vessel seismic dump system is to drain most of the waste in the C-A-1 vessel after an earthquake to prevent hydrogen accumulation and potential deflagration in the vessel. Rather than installing a safety-significant seismic switch to automatically actuate the system (as planned for the Hanford Sludge Treatment Project), DOE-ORP approved WRPS's proposal to make this an operator-actuated system. This approach relies on the control room operator or site emergency response personnel, both of whom are in non-seismically-qualified structures (which may collapse); to recognize initiation of a seismic event, proceed to the seismically qualified shutdown switch mounted on the exterior of the Evaporator building, and manually actuate the system. The DSA also specifies that this is an AC rather than a SAC (which would have a higher reliability for its performance consistent with DOE Standard 1186 requirements)[1]. Consequently, the need for a safety-significant engineered feature to function during an earthquake is being satisfied with an administrative control. This is inconsistent with the requirements of DOE Standard 1186. A SAC would be the appropriate designation for operation of the new seismically-qualified equipment in the 242-A Evaporator, per DOE Standard 1186.

---

[1] WRPS personnel stated that this approach was chosen to be consistent with the actions in a letter from DOE's Office of Environmental Management (EM) to the Board dated July 25, 2011. The referenced letter was related to the Hanford Tank Farm's waste transfer system and the need to stop waste transfers and order the evacuation of the Hanford Tank Farms in the event of an earthquake. In the letter, DOE-EM committed to capture those actions in key elements to ACs. Because the control systems for the waste transfer system pumps in the Hanford Tank Farms are not seismically qualified, an AC key element was appropriate for the emergency response program actions in this case.

Hanford Tank Farms Safety Basis. During the on-site discussions, DOE-ORP and WRPS personnel stated that the approach used for identification and analysis of hazards, identification of controls, their safety classification, and preparation of TSRs for the 242-A Evaporator is the same as the methodology used for the Hanford Tank Farms Safety Basis that has been reviewed and approved by DOE-ORP. This statement has been partially verified by members of the Board's staff subsequent to the onsite review. The safety basis for the Hanford Tank Farms does have the same hazard identification and analysis methodology description as that found in the 242-A Evaporator safety basis, but the results of this process have not yet been reviewed. Therefore, it is possible that weaknesses and deficiencies similar to those discussed above may exist in the Hanford Tank Farm DSA and TSRs.