

Joyce L. Connery, Chair
Thomas A. Summers, Vice Chair
Jessie H. Roberson

**DEFENSE NUCLEAR FACILITIES
SAFETY BOARD**

Washington, DC 20004-2901



July 19, 2022

The Honorable Jennifer M. Granholm
Secretary of Energy
US Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Granholm:

The Defense Nuclear Facility Safety Board's (Board) staff has engaged with personnel from the Office of River Protection (ORP) during development of a revised safety strategy for operating Hanford's 242-A Evaporator facility. This safety strategy modifies commitments that the Department of Energy (DOE) made to the Board following a 2014 Board letter detailing deficiencies in the existing evaporator safety strategy. The original commitment proposed engineered controls to prevent explosions resulting from the accumulation of flammable gas in the evaporator vessel.

The proposed revisions to the safety strategy currently under consideration will not align with requirements in DOE Standard 3009-1994-CN3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*,¹ and other applicable standards unless the safety issues noted in the enclosure to this letter are adequately addressed. DOE has determined that the accident scenarios involving an explosion of flammable gas require safety significant control(s). Whatever systems that DOE will rely upon to satisfy the associated safety significant functional requirements must meet that safety-related classification.

The Board's staff has discussed several concerns with DOE staff regarding the inability of various systems, components, and actions under consideration to satisfy their safety significant functional requirement. The Board remains concerned that, under the revised safety strategy, not all systems, components, and actions that comprise the safety significant layer of control for each scenario will meet safety significant requirements.

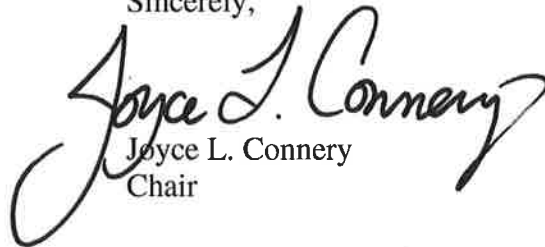
In all cases in which DOE chooses not to follow its preferred hierarchy of controls, DOE Standard 3009-2014 (which clarified DOE's intent behind the 1994 version) requires that the safety documentation "provide a technical basis that supports the controls selected." DOE Standard 1186-2016, *Specific Administrative Controls*, further elaborates: "This discussion should address the various engineered options available and why they were not selected." The Board's and DOE's staffs have discussed the fact that the documentation available to date does

¹ DOE revised DOE Standard 3009 in 2014, but the 1994 version remains the code of record for this facility.

not satisfy the expectations described in these standards, and the need to complete such a technical basis.

Pursuant to 42 United States Code §2286b(d), the Board requests a briefing from DOE within 90 days of receipt of this letter that describes how the final revised safety strategy for operating Hanford's 242-A Evaporator facility will meet DOE's safety requirements and address the Board's concern regarding these safety significant scenarios.

Sincerely,



Joyce L. Connery
Chair

Enclosure

c: Mr. William I. White
Mr. Brian T. Vance
Mr. Joe Olencz

ENCLOSURE

PROPOSED SAFETY APPROACH FOR 242-A EVAPORATOR FACILITY

Summary. Staff members from the Defense Nuclear Facilities Safety Board (Board) have reviewed the Department of Energy's (DOE) proposed changes in the safety strategy for the 242-A Evaporator Facility at the Hanford Site, which affect two types of accident scenarios:

Evaporator Accident Scenarios that Include a Fire—Available accident analyses lead to the conclusion that safety significant controls are required. However, the Board notes that ORP is not planning to credit proposed engineered controls as safety significant and will instead rely on administrative actions as the credited safety significant controls. A proposed fire detection and alarm system that will (a) actuate certain solenoid valves that dump the evaporator vessel and prevent the accumulation of flammable gas, and (b) alert operators to take actions that will protect the functionality of those solenoid valves, will be classified as defense-in-depth. DOE has proposed relying on a safety significant combustible loading specific administrative control (SAC) to protect the functionality of the solenoid valves threatened by a fire. The combustible loading limit is based on the results of fire modeling; however, there is a relatively small margin between the expected operating temperature in the condenser room and the thermal rating of the solenoid valves, and the Board's staff has raised technical questions regarding the adequacy of the fire model for predicting temperatures reached in the condenser room. Therefore, it is not clear that the proposed combustible control is sufficiently reliable to protect the functionality of the solenoid valves.

Further, the Board's staff notes that prompt notification of a fire, should it occur, could allow operators to dump the evaporator contents before the solenoids are damaged. Prompt action would prevent the condition where waste becomes trapped in the evaporator vessel for a duration long enough to allow hazardous flammable gases to accumulate to dangerous levels. The use of a safety significant fire detection and alarm system to support system actuation and/or safety significant operator action (i.e., via a safety significant SAC) to initiate the credited safety system(s) would improve the reliability of the control, preventing an explosion due to the accumulation of flammable gas, comply with DOE's standards that all systems, components, and actions be safety significant, and follow DOE's preferred hierarchy of controls.

Evaporator Accident Scenarios that Include a Seismic Event but no Fire—DOE has proposed relying on operator action via a Key Element, instead of an engineered control such as a safety significant seismic switch. This does not follow DOE's preferred hierarchy of controls. Further, a Key Element does not meet the reliability requirements of a SAC, which represents a further deviation from DOE's expectations for safety significant administrative controls.

Background. The Board communicated its safety concerns regarding the safety basis of the 242-A Evaporator at the Hanford Tank Farms in a letter dated June 18, 2014. In the letter, the Board identified deficiencies in both the engineered and administrative control sets that provide safety significant level protection for workers from the consequences of a flammable gas accident. In its response to the Board's safety concerns, DOE committed to upgrade some

hazard controls to prevent explosions resulting from accumulation of flammable gas in the evaporator vessel. Among the commitments, DOE stated that it would implement design changes for three credited valves in the C-A-1 vessel flammable gas and waste high-level control systems to ensure that they would fail safe in the event of a fire (Design/Operational Improvement 2). Additionally, DOE committed to modify the C-A-1 vessel seismic dump system to automatically initiate upon detection of a seismic event (Design/Operational Improvement 3).

Subsequently, personnel from Washington River Protection Solutions (WRPS) determined that the controls identified in the DOE's commitment would be difficult to implement and proposed two changes to this planned safety strategy that would effectively rescind DOE's commitments and replace the proposed engineered controls with a revised control set that is reliant on administrative controls. Specifically, under the revised strategy:

- During a facility fire, the safety function of protecting the three credited solenoid valves will be carried by: a safety significant combustible loading SAC for the condenser room; a defense-in-depth National Fire Protection Association (NFPA) code compliant fire detection and alarm system that includes a control room alarm indication; and a Key Element in the Emergency Management safety management program directing operators to use a safety significant switch and its supporting transfer system to manually dump the evaporator vessel in the event of a fire. The fire detection and alarm system would also activate the C-A-1 vessel flammable gas control system and the C-A-1 vessel waste high level control system, via the facility Fire Alarm Control Unit, for any facility fire alarm regardless of location. This is a change from the previous planned improvement to upgrade (i.e., replace) equipment to ensure it would perform its safety function in case of a design basis fire.
- After a seismic event, the safety function of dumping the evaporator vessel will be carried by a Key Element in the Emergency Management safety management program directing operators to manually initiate the dump sequence using a seismically qualified, safety significant manual actuation system on the exterior of the evaporator building. This is a change from the previous planned safety improvement to install equipment to detect seismic events and automatically dump the vessel.

Discussion. As presented in the 2014 letter, the Board's safety concern is that a fire near the system-controlling solenoid valves could damage these components and render them incapable of operation before they could perform their safety function (dumping the waste from the C-A-1 vessel to prevent the generation of flammable gases that could lead to an explosion event). DOE's original commitment proposed the design and implementation of engineered controls to protect the valves and prevent the explosion event. The Board's staff has reviewed documents provided by DOE and held several discussions with DOE and WRPS representatives to evaluate the adequacy of the proposed safety strategy that replaces the original DOE safety commitments. Although the documented justification for their safety strategy has changed as a result of the discussions, there has not been any substantial change in the proposed safety strategy.

The Board's staff has identified the following weaknesses and inconsistencies with the DOE safety requirements in the proposed safety strategy:

1. **Lack of Technical Basis for Changes.** DOE and WRPS personnel have stated that it is not practical or economically feasible to accomplish the modifications that DOE originally proposed to the Board for upgrade of control system components to ensure they fail safe in a fire (i.e., upgrading the physical protection for the solenoid valves to withstand design basis fire conditions). However, DOE and WRPS personnel have not clearly demonstrated why other potential engineered solutions are not technically feasible. Additionally, they state that installing an automatic seismic shutdown switch to dump the vessel is no longer warranted because, based on more recent seismic hazard analyses, the seismic hazard level has changed. They now posit that the evaporator control room will survive the reduced-hazard event, thus assuring operator ability to carry out their key element safety function of manually dumping the evaporator vessel. However, they have not shown why the use of an automatic seismic shutdown is not feasible. Further, they intend to use this approach without providing an adequate technical basis within their strategy for using a potentially less reliable key element control instead of an engineered control for a safety significant function that is still required for the seismic event.

DOE Standard 3009-1994-CN3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses [DSA]*,¹ states that “the established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs [systems, structures, and components] be preferable to ACs [administrative controls] or SACs due to the inherent uncertainty of human performance.” The 2014 version of the standard (which clarified DOE's intent behind the 1994 version) further requires that “when the hierarchy of controls is not used for situations requiring SC/SS [safety class/safety significant] controls (e.g., a SAC is selected over an available SSC), the DSA shall provide a technical basis that supports the controls selected” and that “an AC may serve as the most important control or only control, and *may be selected where existing engineered controls are not feasible to designate as SS SSCs* [emphasis added].” Contrary to this approach, WRPS has not provided a defensible technical basis that justifies their use of administrative controls in lieu of the previously proposed or other engineered controls to preclude this event, including showing that engineered controls are not feasible.

2. **Changes to Fire Detection Strategy.** The proposed change in safety strategy relies on a new SAC to limit combustible material, supported by a defense-in-depth (i.e., non-safety-significant) fire detection and alarm system, along with administrative actions, to dump the waste from the evaporator vessel if a fire is detected near the system-controlling solenoid valves. These controls are intended to fulfill the safety significant function of preventing flammable gas accidents. DOE and WRPS personnel stated that they made this decision due to significant challenges arising from applying target probability of failure on demand and hardware fault tolerance requirements of DOE Standard 1195-2011, *Design of Safety Significant Safety*

¹ DOE revised DOE Standard 3009 in 2014, but the 1994 version remains the code of record for this facility.

Instrumented Systems Used at DOE Nonreactor Nuclear Facilities, to a NFPA 72-compliant fire detection and alarm system. In particular, they indicated that the prescriptive design requirements in NFPA 72 do not provide risk reduction criteria comparable to the standard for safety instrumented system design, as specified in DOE Standard 1195.

DOE Standard 1195-2011 explicitly states “ANSI/ISA 84.00.01-2004, Part 1, design methodology should not be used for instrumented systems in [fire protection/detection] applications because they are more appropriately covered by other industry standards such as National Fire Protection Association (NFPA) standards.” Furthermore, DOE Standard 1066, 2016 states “Section A.1 provides general design criteria for **any** type of fire protection system that is used in SC and SS applications. This information is derived from and essentially repeats requirements and guidance contained in DOE [Order] O 420.1C and DOE Guide (G) 420.1-1A, *Nonreactor Nuclear Safety Design Guide for Use with DOE O 420.1C, Facility Safety* [emphasis added].” This affirms that safety significant fire detection and alarm systems may be deployed by following the general design guidance in DOE Order 420.1C.

DOE’s and its contractor’s reasons for deciding to modify the proposed control set are tangential to the Board’s evaluation that DOE should provide an adequate, reliable, and compliant safety approach for protecting the safety significant solenoid valves from fire induced failures. Safety significant fire detection and alarm systems that meet the requirements of NPFA 72, implement the applicable quality control and quality assurance programs in their design, and are maintained under the surveillance and maintenance provisions of technical safety requirements have been adopted and implemented in multiple facilities across the complex and represent viable and reliable safety controls to prevent propagation of incipient fires. Although the use of the proposed SAC to limit combustible materials in the condenser room is appropriate and may help limit the size of a fire, implementation of a safety significant fire detection and alarm system would ensure a timely and reliable notification of the control room operators to take the necessary safety actions in case of an unforeseen fire, improve the likelihood that the evaporator can be successfully dumped before the solenoids are potentially damaged, and would be more consistent with the DOE’s hierarchy of controls.

3. **Lack of Human Response Analysis.** WRPS has not provided a robust analysis that shows the adequacy of the human action to manually activate the evaporator vessel dump system. The proposed safety strategy assumes that the human response will be timely and accurate without providing any analysis to understand potential failure modes. A failure modes and effects analysis of the fire detection and alarm system, seismic manual dump system, and fire manual dump system, combined with a human reliability analysis, would ensure that the design of proposed controls and related implementing procedures adequately prevent evaporator vessel flammable gas explosions.

4. **Lack of Adequate Structural Calculations.** The structural calculations for the control room, which is now being relied upon to remain standing and allow workers to perform safety functions, are rudimentary and not originally intended for use in analyses supporting nuclear safety-related seismic performance. The recent analysis that allows WRPS to credit the control room to survive relies on comparing old design basis ground motions to the latest design basis ground motions for safety-related structures, demonstrating that the original design response spectra was more conservative than the current estimated seismic hazard. Considering that the original design used older commercial codes for basic life safety, a more thorough review of the structure's performance is appropriate given its new credited safety function. Additionally, the original design analysis calculations were performed before the current quality requirements for safety basis analysis were enacted and have not been revised as appropriate per DOE Order 414.1D, *Quality Assurance*, and DOE Standard 1073-2016, *Configuration Management*. To ensure that the operators in the control room can perform the required safety functions and prevent an explosion event, it is desirable to perform new safety analyses, using the more recent seismic hazards curves and methods.

In discussions with the Board's staff, DOE personnel indicated that the reviews of the as-built drawings and detailing were performed to verify that assumptions supporting the original design calculations were sound. Following these discussions, WRPS personnel supported by an outside consultant, performed walkdowns to assess the condition of the structure and verify no configuration changes supersede the as-built drawings. Given that the seismic hazard for the Hanford Site is currently estimated to be less than the design spectra used originally, fully documenting these efforts and preserving them for configuration management purposes would ensure the performance of the facility is understood and can be evaluated in the future as needed.

5. **Inadequate Fire Modeling Code.** WRPS has performed analytical fire modeling of the facility to support the proposed change in strategy. This analysis is used to determine the allowable quantity of combustibles near the safety significant solenoid valves, which will be controlled by a SAC. The selected toolbox code (Consolidated Model of Fire and Smoke Transport—CFAST), however, is not capable of appropriately modeling the effects of the ventilation arrangement and air circulation in the condenser room for fires occurring at heights between the ventilation inlet and outlet. This may result in a non-conservative estimation of exposure temperatures at the solenoid valves. The safety margin between the expected operating temperatures in the process areas and the temperature that could damage the solenoid valves is only 40 degrees Fahrenheit. Consequently, for fire locations between the ventilation inlet and outlet, the fire modeling may not have appropriately defined the combustible material limits imposed by the SAC. The staff review team notes that DOE and WRPS personnel have acknowledged this issue and are exploring the use of an alternate fire model to confirm the initial analysis.

Conclusion. In summary, while it may not be feasible or practical to procure a fail-safe system to protect the safety significant solenoid valves consistent with the DOE's original plan,

the contractor's proposal does not provide a level of safety that is commensurate with the consequences of a flammable gas explosion in the waste tank. A safety significant fire detection and alarm system that meets NFPA 72 requirements, applies appropriated quality control and quality assurance programs to its design, and is maintained under the surveillance and maintenance provisions of technical safety requirements; supplemented by appropriate fire- and seismic-related SACs (i.e., not Key Elements or Safety Management Programs) requiring the control room operator to dump the waste, along with the control of combustible materials in the area, would be more consistent with DOE's hierarchy of controls and would provide a higher level of protection than DOE's and the contractor's current proposal.