



Department of Energy
Washington, DC 20585

February 2, 2026

The Honorable Patricia L. Lee
Board Member
Defense Nuclear Facilities Safety Board
625 Indiana Avenue NW, Suite 700
Washington, DC 20004

Dear Dr. Lee:

On behalf of Secretary Wright, enclosed is the Department of Energy's (DOE) response to the Defense Nuclear Facilities Safety Board's (Board) letter dated June 12, 2025, regarding the Board staff's review of the Safety Integrity Level for the 242-A Evaporator planned design improvement at the Hanford Site.

The Board's letter requested a report and a briefing that address:

- DOE's path forward for improving the reliability of the 242-A Evaporator seismic dump system to ensure protection of the workers
- DOE's approach for providing guidance and requirements for design of safety significant instrumentation and control systems for an existing facility when the design is not a major modification

The enclosed report provides information on the topics requested by the Board. A briefing was given to the Board on September 22, 2025.

DOE appreciates the Board's perspective and looks forward to continued interactions with you and your staff. If you have any questions, please contact me or Ms. Brenda Hawks, Associate Deputy Assistant Secretary for Field Operations Oversight/Chief of Nuclear Safety, at (865) 805-0391.

Sincerely,

Timothy J. Walsh
Assistant Secretary
for Environmental Management

Enclosure

Reliability of the Hanford 242-A Evaporator Safety Significant Support System to Prevent a Post-Seismic Deflagration Event

Introduction

On June 12, 2025, the Secretary of Energy received a letter from the Defense Nuclear Facilities Safety Board (DNFSB, or Board) sharing its concerns regarding the reliability of the safety significant design features to prevent a post-seismic deflagration event at Hanford's 242-A Evaporator. The 242-A Evaporator is a critical component of the tank waste mission at Hanford by optimizing Double-Shell Tank volumes. The Board requested a briefing and report from the Department of Energy (DOE) describing: "(1) DOE's path forward for improving the reliability of the seismic dump system to ensure protection of the workers; and (2) DOE's approach for providing guidance and requirements for design of safety significant instrumentation and control systems for an existing facility when the design is not a major modification."

Board Request

(1) DOE's path forward for improving the reliability of the seismic dump system to ensure protection of the workers

DOE Response

Waste (feed) from double-shell tanks is pumped into the 242-A Evaporator vessel via a double encased transfer line. Waste is processed under vacuum in the Vapor-Liquid Separator (C-A-1) and heated as it passes through a steam reboiler using forced circulation. As the waste enters the vessel, water vapors from the boiling waste are drawn into the condenser system. Process condensate is collected in the process condensate tank (TK-C-100) and pumped to the Liquid Effluent Retention Facility, as shown in Figure 1.

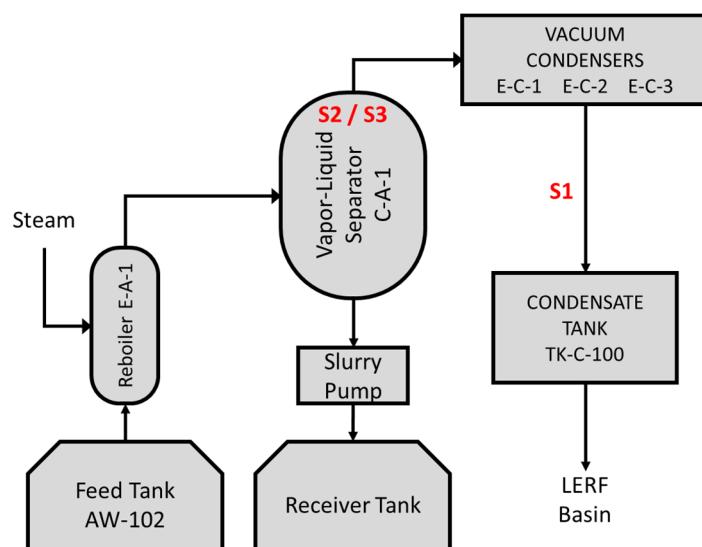


Figure 1: 242-A Evaporator Process

Hazards and Controls

The specific hazards of concern that are addressed with this controls strategy based on DOE Standard (STD) 3009-1994, Change (Chg) Notice 3, *Preparation of Nonreactor Nuclear Facility Documented Safety Analysis*, guidelines are as follows:

1. Flammable gas deflagration in the C-A-1 Vessel – with co-located worker toxicological consequences exceeding Protective Action Criteria level 3 (PAC-3) guidelines and significant facility worker hazard due to toxicological exposure and projectile physical impact from over pressurization.
2. Overflow of waste from the C-A-1 into TK-C-100 inducing a potential flammable gas deflagration in the process condensate tank TK-C-100 – with co-located worker toxicological consequences exceeding PAC-3 guidelines and significant facility worker hazard due to chemical burns, radiation exposure, and projectile physical impact from over pressurization. The overflow from the C-A-1 vessel into the TK-C-100 vessel could contaminate the process condensate system due to vessel liquid level increase due to sudden boiling or foaming. This potential misroute of waste into the process condensate tank introduces the potential flammable gas hazard.
3. Overflow from C-A-1 into TK-C-100 inducing a potential flammable gas deflagration in the process condensate piping and components (except TK-C-100) – with significant facility worker hazard due to chemical burns and projectile physical impact from over pressurization. Similar to the previous hazard, overflow from the C-A-1 vessel into the TK-C-100 vessel could contaminate the process condensate system due to vessel liquid level increase due to sudden boiling or foaming, which could introduce the same hazard in the piping and components between the C-A-1 vessel and the TK-C-100.

The S1 and S2 safety instrumented functions (SIFs) with associated safety instrumented systems as well as safety significant equipment are in place to prevent these hazards. The functions of the S1 and S2 systems are summarized as follows:

(S1) Evaporator Vessel High Level Control System

The evaporator vessel waste high level control system (S1) is identified as a safety significant Structure, System, or Component (SSC) for potential flammable gas accidents. The S1 system detects an evaporator vessel high waste level and places the process in a safe state in response. The evaporator vessel waste high level control system has four safety functions:

- Prevent a deflagration or detonation in the process condensate tank and in other components of the process condensate system by preventing the overflow of waste from the evaporator vessel into the process condensate system and by preventing the carryover of waste due to boiling or foaming;

- Prevent a direct radiation hazard to the facility worker, associated with waste in the process condensate system by preventing the overflow of waste from the evaporator vessel into the process condensate system;
- Prevent chemical burn hazards to the facility worker, associated with waste or contaminated flush water in the process condensate system by preventing the overflow of waste from the evaporator vessel into the process condensate system and by preventing the carryover of waste due to boiling or foaming;
- Support the Specific Administrative Control Evaporator Vessel Flush and Pump Room Sump Rinse by measuring the differential pressure across the lower de-entrainment pad in the evaporator vessel and providing a readout of the measured differential pressure.

(S2) Evaporator Vessel Flammable Gas Control System

The evaporator vessel flammable gas control system (S2) is identified as a safety significant SSC for potential flammable gas accidents. The S2 system monitors several parameters, and when detected to be outside of defined limits, it places the process in a safe state. The evaporator vessel flammable gas control system has two safety functions:

- Prevent a deflagration or detonation in the evaporator vessel by preventing a flammable concentration in the headspace of the vessel by ensuring that vessel vacuum or purge air flow is maintained when the evaporator vessel contains sufficient waste to constitute a flammable gas hazard;
- Protect assumptions used to develop action completion times in Limiting Condition for Operation Evaporator Vessel Flammable Gas Control System by limiting the waste temperature in the evaporator vessel and so limiting the flammable gas generation rate within the vessel and extending the time required to develop a flammable concentration in the vessel headspace.

S3 Seismic Dump System Design and Reliability

The use of safety instrumented systems to prevent hazards is compliant with the requirements in DOE-STD-3009. However, because the S1 and S2 systems cannot be seismically qualified, an automated seismic dump system is being designed to eliminate the hazard. After waste is removed from the C-A-1 vessel, the S1 and S2 systems are no longer required to be operable following a seismic event because they would not contribute to any direct consequence from the event. The frequency and consequence of a seismic event were conservatively assumed to be the same as for the flammable gas deflagration and overflow events.

The automated dump system (S3) design complies with DOE Order (O) 420.1C Chg 3, *Facility Safety*, which states that “safety significant SSCs must be designed to reliably perform all their safety functions.” Reliable design for the seismic dump system to remove the requirement for S1/S2 operability is achieved through application of industry standard International Society of Automation (ISA) 84 and TFC-ENG-DESIGN-P-43, “Control Development Process for Safety-

Significant Safety Instrumented Systems,” which is a contractor design standard. The design includes a safety significant automated interlock with a combination of reliable sensor(s), logic solver, and final elements to place the facility in a safe state.

The Safety Integrity Level (SIL) determination methodology, consistent with ISA-84, considers both consequence and frequency in determining SIL requirements. The Probability of Failure on Demand (PFD) is conservative against ISA-84 requirements for SIL-1, although less conservative than the PFD for a SIL-2 suggested by DOE-STD-1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*, which is only required for major modifications. The design has an increased conservatism in determining target values for probability of failure on demand using the minimum targets shown in Table 1. The probability of failure on demand is 1 in 57, which is higher than SIL-1 requirements but below the SIL-2 requirements. The comparisons are summarized in Table 1 below.

Table 1: Design Approach and Reliability

SIL Target for SIF	Probability of Failure on Demand (ISA - 84)	Probability of Failure on Demand (DESIGN-P-43)	Probability of Failure on Demand of S3
SIL-1 demand mode	Greater than 1 in 10	Greater than 1 in 20	1 in 57
SIL-2 demand mode	Greater than 1 in 100	Greater than 1 in 200	

The event frequency combined with the better than SIL-1 PFD, as well as having the operator manual actuation backup, ensures adequate protection of the worker. The current approach results in an automated response replacing the current Specific Administrative Control dependent on operator response. The design provides a robust safety instrumented function that meets ISA-84 requirements for independence, detection of faults, fail-safe considerations, and component selection. The system is of sufficient reliability given the function of S3, which is to remove the requirement for operability of the S1/S2 systems.

Board Request

(2) DOE's approach for providing guidance and requirements for design of safety significant instrumentation and control systems for an existing facility when the design is not a major modification

DOE Response

DOE is committed to providing guidance and requirements for design of safety significant instrumentation and control systems for an existing facility even when the design is not a major modification. DOE O 420.1C Chg 3 does not impose new design requirements on existing facilities; however, the Order states it may be used to develop comparisons of existing facilities to the requirements for new facilities, as an aid to judge when evaluating the costs and benefits of non-mandatory upgrades to existing facilities. The design of new safety significant instrumentation and control systems for an existing facility necessitates revision to the Documented Safety Analysis (DSA) and the Technical Safety Requirements (TSRs), and Title 10 of the *Code of Federal Regulations* Part 830, *Nuclear Safety Management*, requires DOE approval prior to implementation of these changes.

DOE O 420.1C Chg 3 invokes the use of DOE-STD-1104-2016, *Review and Approval of Nuclear Facility Safety Basis and Safety Design Basis Documents*, for DOE review and approval of all safety basis documents (new facilities and major modifications to existing facilities) to ensure they are adequate and reliable.

Prior to DOE approval of the revised DSA and TSRs and subsequent implementation of the new automated dump system (S3) described above, DOE review includes a verification that functional requirements and performance criteria are defined such that, when met, they ensure that the safety functions can be performed when needed.