DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

June 12, 2025

The Honorable Christopher Wright
Secretary of Energy
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Wright:

The Defense Nuclear Facilities Safety Board (Board) acknowledges that the Department of Energy (DOE) has improved the safety posture of the 242-A Evaporator facility at the Hanford Site in response to the safety issues the Board identified on June 18, 2014. The contractor has identified safety significant design features that are designed to prevent a post-seismic deflagration event in the evaporator vessel to protect facility workers. However, the Board is concerned that the reliability of this system is not commensurate with the significant consequences of the event it is designed to prevent. The enclosure to this letter describes the Board's safety concerns that stem from lack of clear guidance and requirements by DOE for design of safety significant instrumented systems at an existing facility when the design is not a major modification to the facility.

DOE Standard 1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*, provides guidance and requirements for design of instrumentation and control systems to reliably perform their safety functions. DOE issued this standard as an approved method to supplement a voluntary consensus standard to ensure that the design of safety significant systems is consistent with the safety classification methodology established by DOE in the safe harbor standards to 10 CFR 830, *Nuclear Safety Management*. The standard, however, is only required by DOE directives for design of instrumentation and control systems at new facilities or major modifications to existing facilities.

The contractor at the Hanford Site used an internal procedure, not approved by DOE, to supplement the same voluntary consensus standard and to design the 242-A Evaporator seismic dump system instead of using DOE Standard 1195-2011. As a result, the design of the instrumentation and control portion did not produce a system that reliably fulfills its safety function to protect workers from a post-seismic deflagration event.

Pursuant to 42 United States Code §2286b(d), the Board requests a report and a briefing from DOE within 90 days of receipt of this letter that describe:

- DOE's path forward for improving the reliability of the 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.

Sincerely,

Thomas A. Summers

Thomas A. Summers
Acting Chairman

Enclosure

c: Mr. Roger Jarrell, Acting Assistant Secretary, DOE Office of Environmental Management
Mr. Brian Harkins, Acting Manager, DOE Hanford Field Office Manager
Ms. Stephanie Martin, Acting Director, DOE Office of Environment, Health, Safety and Security
Mr. Joe Olencz, Director, Office of the Departmental Representative to the Board

DEFENSE NUCLEAR FACILITES SAFETY BOARD

Staff Report

April 15, 2025

Safety Integrity Level for 242-A Evaporator at the Hanford Site

Summary. The staff of the Defense Nuclear Facilities Safety Board (DNFSB) reviewed the reliability of the seismic dump system for the 242-A Evaporator at the Hanford Site. The staff team concluded that the proposed design would not perform its intended safety function with a reliability commensurate with the consequences of the hazards it is designed to prevent. Additionally, the staff team identified a gap in the DOE directives requirements related to the design of safety significant instrumentation and control systems at defense nuclear facilities when they are not identified as major modifications to the existing facilities.

Background. In a letter to the Department of Energy dated June 18, 2014, the Defense Nuclear Facilities Safety Board identified several weaknesses with the safety posture of the 242-A Evaporator at the Hanford Site. The letter included safety concerns with the capability of the facility to remove flammable gases from the evaporator vessel after a seismic event. Accumulation of flammable gas in the vessel headspace presents a potential deflagration hazard, which could result in significant harm to the workers in the vicinity of the facility. DOE committed, in a letter dated April 17, 2023, to install a safety significant seismic detection system with the capability to automatically actuate an evaporator vessel dump and return the waste back to the Tank Farms, thus preventing the potential deflagration. A DNFSB staff team has evaluated the design adequacy of this seismic dump system to ensure it will function reliably when needed to remove the waste and stop generation of flammable gases in the evaporator vessel.

Discussion.

Design Adequacy—The evaporator seismic dump system is designated as safety significant for protection of the collocated and facility workers and must reliably perform its safety function commensurate with the consequences of a vessel deflagration. The Hanford Site contractor designed the instrumentation and control portion of this system using an internally developed procedure[1] that supplements the guidance provided in the voluntary consensus standard ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. This standard allows the user to define the system's performance level, referred to as the Safety Integrity Level (SIL). Through application of its procedure, the Hanford Site contractor determined that the seismic dump system would be designed to meet the SIL-1 level of performance, which is the least reliable level allowed for use in safety significant applications for DOE. Based on a review of DOE requirements and guidance, the staff team determined that the existing guidance indicates that SIL performance levels below SIL-2 are only allowed when certain defense-in-depth requirements are met. DOE issued Standard 1195-2011,

[1] TFC-ENG-DESIGN-C-47, Rev E-2, Process Hazards Analysis, Engineering Manual, June 26, 2024, Washington River Protection Solutions.

Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities, describing the approved method for applying ANSI/ISA 84.00.01-2004 to the DOE non-reactor nuclear facilities. This standard provides requirements and guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of safety instrumented systems, including the approved method for SIL determination. The Standard states that, "for DOE's application, the accepted methodology is a deterministic method using the number of [independent protection layers] IPLs credited by hazard analysis."

The methodology described in Appendix B to DOE Standard 1195-2011 establishes safety instrumented system SIL determination as a function of the number of IPLs that protect against the same hazard scenario. This effectively roots the SIL determination in defense-in-depth rather than quantitative risk analysis. According to the Standard, a SIL-2 designation would be required in situations where two IPLs can be identified to prevent or mitigate a hazardous event. The Hanford Site contractor has identified only two IPLs in their SIL determination: the Evaporator building structure and the seismic dump system. Therefore, SIL-2 would be the nominal design requirement to align with DOE Standard 1195-2011 for the evaporator seismic dump system unless a third IPL is identified and credited to prevent or mitigate this hazardous event.

Application of the Hanford Site contractor's internal procedure to the seismic dump system has resulted in a SIL-1 designation using a graded approach by accounting for the likelihood of the event. However, DOE Standard 1195-2011 does not allow such gradation because, according to the DOE methodology, safety classifications of structures, systems, and components are based on documented safety analyses, and, therefore, "likelihoods and consequences do not have any further role in SIL determination." DOE Standard 1195-2011 allows a SIL-1 designation when three IPLs can be identified for a safety significant safety instrumented system. Although this would be allowed by the standard and improve the reliability of the system through additional layer of defense-in-depth, it has not been considered in the design of the 242-A Evaporator seismic dump system by the Hanford Site contractor.

The requirements of DOE Standard 1195-2011 are primarily directed at ensuring reliable design of safety significant instrumented systems to assure adequate protection of the workers. The staff team concludes that other approaches used for safety instrumented system design should provide a level of reliability equivalent to or better than the reliability that would result from the use of DOE Standard 1195-2011.

SIL defines the allowable Probability of Failure on Demand-average (PFDavg) range for a specified safety instrumented function along with other characteristics such as fault tolerance. SIL-1 establishes a minimum reliability threshold whereby the allowable PFDavg is 10^{-1} whereas SIL-2 establishes a minimum PFDavg of 10^{-2}. Although the seismic dump system is being designed to exceed the minimum SIL-1 PFDavg, it remains less reliable than the SIL-2 minimum design requirement that would be acceptable by applying the approved methodology specified in DOE Standard 1195-2011.

DOE Guidance—DOE requires use of DOE Standard 1195-2011 for new facilities and major modifications to existing facilities but does not provide clear guidance or requirements for

other cases. Consequently, DOE has created a gap in the requirements for the design of new safety significant instrumentation and control systems at existing facilities, when they are not determined to be major modification.

DOE and its Hanford Site contractor have determined that DOE Standard 1195-2011 does not apply to the design of the new seismic dump system because the system is not a major modification. For designs at existing facilities that are not major modifications, DOE has not provided design requirements or expectations for new safety-related instrumentation and control systems.

DOE Order 252.1A, *Technical Standards Program*, states that, to be used, a VCS (such as ANSI/ISA 84.00.01-2004) must be adaptable and appropriate for DOE purposes. The order further states that DOE technical standards are developed when a suitable VCS does not exist or is not appropriate for the intended application. DOE Standard 1195-2011 identifies that the guidance provided in ANSI/ISA 84.00.01-2004 is not sufficient by itself to be applied to non-reactor nuclear facilities and should be supplemented with the methodology provided in the standard: "Appendices A, C, and D of this standard provide specific information on the use of ANSI/ISA 84.00.01-2004, whereas Appendix B provides an approved method for SIL determination."

Although DOE has determined that the existing voluntary consensus standard for safety instrumented system design must be supplemented to ensure adequate system reliability for non-reactor nuclear facilities, they have not provided guidance for design of new safety instrumented systems at existing facilities when they are not declared as major modification. The lack of guidance has resulted in a system that does not achieve DOE's expected level of reliability equivalent to DOE Standard 1195-2011 criteria as illustrated by the resulting 242-A Evaporator seismic dump system.

Conclusion. The staff team concludes that the reliability of the instrumentation and control portion of the proposed design for the seismic dump system at the 242-A Evaporator is not consistent with the methodology described in the DOE Standard 1195-2011. This discrepancy is a direct result of the lack of clear guidance and requirements in the DOE directives system for design of instrumentation and control systems at defense nuclear facilities when they are not identified as major modification to an existing facility.