

Peter S. Winokur, Chairman
Jessie H. Roberson, Vice Chairman
John E. Mansfield
Joseph F. Bader

**DEFENSE NUCLEAR FACILITIES
SAFETY BOARD**

Washington, DC 20004-2901



May 5, 2011

The Honorable Inés R. Triay
Assistant Secretary for Environmental Management
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0113

Mr. Glenn S. Podonsky
Chief Health, Safety and Security Officer
Office of Health, Safety and Security
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1290

Dear Dr. Triay and Mr. Podonsky:

The Defense Nuclear Facilities Safety Board (Board) is concerned regarding the design of instrumentation and control systems at the Waste Treatment and Immobilization Plant (WTP) at the Hanford Site. Bechtel National, Incorporated (BNI) has implemented a national consensus standard, developed for use in the process industry, in designing safety-significant instrumentation, control, and alarm components. However, the Department of Energy's (DOE) directives do not provide sufficient direction on applying some elements of this standard within DOE's deterministic approach for identifying and classifying safety systems. The element of primary concern to the Board is that independent protection layers, which determine the required design reliability of safety-significant safety instrumented systems, are not protected in the facility safety basis. As a result, during periods when the independent protection layers may be unavailable, facility operations would continue at greater risk; the assumptions used to define the safety-system reliability requirement would no longer be valid.

The Board believes that the operation and maintenance of independent protection layers should be included in facility safety bases. In fact, DOE's implementation of ISA-84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* (the most recent version of the invoked consensus standard) in accordance with DOE's draft standard *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities* (SAFT-0128) would identify requirements that address the Board's concern with the control of independent protection layers.

The enclosed report provides details on the Board's concern with the safety application, effectiveness, and design requirements of independent protection layers. Additionally, the report discusses two instances where BNI specified protection layers that are not independent of the

hazard-initiating event, a practice that is contrary to BNI's project requirements and the implemented national consensus standard. The Board believes that this is an indication of potential inadequacy in the hazard analysis process for WTP, specifically for identifying initiating events and ensuring the adequacy of selected controls.

Therefore, pursuant to 42 U.S.C. § 2286b (d), the Board requests a report and subsequent briefing within 30 days of receipt of this letter. The report and briefing should address:

- the specific instrumentation and control system-related deficiencies noted in the enclosed report;
- the plan to assess gaps between BNI's implementation of American National Standards Institute (ANSI)/International Society of Automation (ISA)-84.01-1996, *Application of Safety Instrumented Systems for the Process Industries* and the approach specified in DOE's draft standard SAFT-0128, specifically regarding control of non-credited independent protection layers that drive design parameters for safety systems; and
- planned improvements to address shortcomings in BNI's hazard analysis process, including the results of any extent-of-condition review and causal analysis performed to address the finding that some protection layers are not independent of hazard-initiating events.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter S. Winokur". The signature is stylized and cursive.

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

February 11, 2011

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: D. Campbell

SUBJECT: Review of the Instrumentation and Control Design for the Waste Treatment and Immobilization Plant, Hanford Site

The staff of the Defense Nuclear Facilities Safety Board (Board) visited the Hanford Site on December 7-10, 2010, to review the instrumentation and control design for the Low Activity Waste (LAW) facility at the Waste Treatment and Immobilization Plant (WTP). Staff members D. Campbell, E. Gibson, R. Oberreuter, R. Quirk, S. Stokes, and R. Verhaagen examined project documentation for WTP to assess the adequacy of several safety-significant safety instrumented systems (SIS). The staff evaluated primarily the process used by Bechtel National, Incorporated (BNI) to select protection layers for safety applications, the independence of protection layers, and the use of operator action and the basic process control system in safety applications.

Overview. BNI has designed multiple safety-significant SISs to a lower reliability level than would be required without the existence of independent protection layers. The independent protection layers are, in effect, important to safety, but they are not identified in the facility safety basis, and no provision currently exists for control of their operation by means of appropriate procedures and/or processes. The Board's staff also identified deficiencies that indicate shortcomings in BNI's hazard analysis process. BNI's design does not meet the project requirement (24590-WTP-GPG-SANA-010, Rev. 5, *Safety Integrity Level Determination for WTP Safety Instrumented Systems*) to ensure hazard initiating events are independent from all protection layers credited in the target safety integrity level (SIL) determination. Specifically, for two systems reviewed by the staff, the failure of components in protection layers intended to mitigate a hazard could act as the initiating event for that hazard.

Background. The code of record for the WTP project implements American National Standards Institute (ANSI)/International Society of Automation (ISA)-84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, for the design and operation of SISs. This consensus standard requires that the system designer derive a target risk reduction factor for each identified hazard. The target risk reduction factor is a measure of the total risk reduction necessary to bring the unmitigated risk level for a particular hazard to an acceptable value. Target risk reduction is achieved by implementation of an SIS and other independent protection layers. Typically, risk reduction factors are specified in order-of-magnitude increments and

represent the inverse of the probability of failure on demand (PFD), i.e., the reliability, of each SIS or protection layer. Thus to meet the required performance criteria for each SIS, BNI combines the as-designed reliability of the SIS with the reliability of each independent protection layer.

ISA-84.01-1996 defines an SIS as a system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated. ISA-84.01-1996 further defines three discrete SILs in terms of PFD. An increase in the SIL indicates an order-of-magnitude improvement in reliability. The three SILs and corresponding PFD values are specified in Table 1.

Table 1. Safety Integrity Levels and Corresponding Probability of Failure on Demand

Safety Integrity Level (SIL)	Probability of Failure on Demand (Average)
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}

Safety Application of Independent Protection Layers. BNI identifies potential process and natural phenomena hazards and the need for safety-significant and safety-class controls as part of its Integrated Safety Management (ISM) process. The ISM process also includes identifying the need for an SIS and the total required risk reduction for each hazard. Once the target risk reduction has been determined, BNI conducts SIL setting meetings to identify independent protection layers that provide protection against each identified hazard. SIL setting meetings utilize the safety layer matrix methodology of ISA-84.01-1996, Annex A, which determines the required SIL for each SIS based on the frequency and consequences of hazardous events and the number of independent protection layers. Thus, in application of ISA-84.01-1996, the final SIS design reliability requirement can depend in part on the successful performance of independent protection layers. Each independent protection layer implemented to prevent or mitigate a hazard allows for an order-of-magnitude reduction in the required reliability of the safety-significant SIS. Current DOE directives, unlike the safety layer matrix methodology of ISA-84.01-1996, do not use the frequency of hazardous events or rely on non-safety related controls as a criterion for determining safety system reliability.

For each of the systems reviewed by the Board’s staff, the LAW facility design incorporates both a safety-significant SIS and one or more independent protection layers to achieve the total required risk reduction for the identified hazard. Independent protection layers identified by BNI include administrative controls, interlocked systems controlled through the Basic Process Control System (BPCS), and operator actions in response to alarms. In each case, the target risk reduction is identified for a hazard, and the required SIL of the SIS is determined as a function of the number of independent protection layers also identified to protect against the same hazard. In the absence of any independent protection layers, the safety-significant SIS would be required to achieve the total target risk reduction for the identified hazardous event. For the LAW systems examined by the Board’s staff, the required reliability of an SIS would

have to increase by a factor of 10 to 100 if the independent protection layers identified by BNI were removed. (The attachment to this report provides more detail on the operation of two systems reviewed by the Board's staff)

The Board's staff believes that the process used by BNI to determine the SIL of each SIS, including the identification of independent protection layers, is consistent with ISA-84.01-1996 and BNI's own SIL determination process as outlined in *Guide for Safety Integrity Level Determination for WTP Safety Instrumented Systems* (24590-WTP-GPG-SANA-010, Rev. 5). However, BNI's process does not address the gaps between ISA-84.01-1996, written largely for application in the process industry, and the deterministic approach used by DOE to establish the safety classification of controls. Ultimately, ISA-84.01-1996 and BNI's requirements do not address the necessary accountability for the proper design, operation, and maintenance of independent protection layers identified in SIL determinations. Nor do they address the fact that those independent protection layers are design basis assumptions that determine the required reliability of safety-significant systems. As a result, BNI does not consider those hazard controls in the preliminary documented safety analysis for the LAW facility. This is inconsistent with the requirements of Title 10, Code of Federal Regulations, Part 830, *Nuclear Safety Management*, Section 830.204 (b) (4), which requires the documented safety analysis to "derive the hazard controls necessary to ensure adequate protection of workers [and] demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards."

Independence of Protection Layer from Initiating Event. BNI's *Guide for Safety Integrity Level Determination for WTP Safety Instrumented Systems* establishes a requirement that "the credited protection layer is independent of the initiating event and all other protection layers credited in the target SIL determination." The staff identified two cases, discussed below, in which BNI had credited protection layers in the SIL determination that were not independent of the initiating event. As a result, the staff concluded that either the ISM and SIL setting processes fail to meet WTP requirements, or the processes are not adequately implemented. During the on-site portion of the staff's review, BNI representatives agreed with this assessment and committed to complete a project issue evaluation report (PIER) to address the issue. Based on the discussion with BNI representatives, the staff anticipates that BNI will evaluate the impact of this issue on other SIS designs (extent of condition) and perform a causal analysis as part of the PIER process.

Wet Electrostatic Precipitator High-Level Interlocks—The SIL setting team identified the following initiating event that would require actuation of the safety-significant SIS to prevent flooding of the Wet Electrostatic Precipitator; the "demineralized water system malfunctions releasing an unscheduled flush volume to the Wet Electrostatic Precipitator." The resultant flooding ultimately causes a blockage of the melter offgas flow path, resulting in a loss of melter vacuum and subsequent release of melter offgas. The SIL setting team failed to identify the potential of the non-safety demineralized flush water isolation valve for the top (flush) nozzles of the Wet Electrostatic Precipitator, which controls flow to the flush nozzles, initiating the unscheduled flush volume. This valve is part of one of the independent protection layers. It has the potential to stick open as a result, for example, of a mechanical failure of the valve or a failure of the BPCS, thus incapacitating the protective function. BNI did not consider

this possibility when identifying the protection layers, or subsequently when determining the required reliability of the safety-significant SIS.

Steam Isolation Interlocks—Credible mechanical failures of either the safety-significant or non-safety steam isolation valves could cause a steam leak and subsequent high temperature inside Room L-0305, potentially damaging safety-related electrical equipment. Such failures could subsequently prevent either the safety-significant steam isolation interlock or the independent protection layer from performing their functions (preventing damage to equipment). Thus the protection layers are not independent from the hazard initiating event. Furthermore, failure of the safety-significant piping upstream of the safety-significant isolation valve (located inside the equipment room) would result in an unisolable steam leak. The hazard analysis did not consider the potential for an unisolable condition or the fact that the identified controls would not necessarily interrupt the accident sequence as designed.

The Board's staff also identified a deficiency in the SIL determination for the High Pressure Steam Isolation Interlock, which isolates the high-pressure steam system upon detection of high pressure downstream of the pressure reducing and isolation valve (i.e., the non-safety isolation valve). BNI's hazard analysis process identified a steam line failure due to "corrosion, fatigue, seismic event or other initiator," but did not appropriately identify the specific initiating events. Potential failure of the pressure reducing and isolation valve (part of the independent protection layer) to regulate the system steam pressure properly could act as an initiating event (overpressurizing the low-pressure steam piping and equipment).

Effectiveness and Design Requirements for Independent Protection Layers. The independent protection layers implemented through the BPCS are credited for providing an order-of-magnitude reduction in risk for the associated hazard. BNI personnel stated that this magnitude of risk reduction is justified based on a note in ISA-TR84.00.04-2005, Part 1, *Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*. The Board's staff agrees that the cited note addresses the risk reduction applied to protection layers controlled through the BPCS, stating that "it is typical to assume a risk reduction factor of 10 for the BPCS layer, if it meets the criteria discussed in this technical report." However, BNI does not implement the guidance contained in the technical report or the requirements of ANSI/ISA-84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. Elements of the technical report and updated standard specifically address the BPCS and its relationship to the SIS. The technical report and standard establish a limit on the amount of risk reduction that can be assumed for the BPCS and provide further information on the validation of BPCS operation, the contribution of the BPCS as an initiating event and as a protection layer, and assessments that should be performed to justify the credit assigned to functions performed by the BPCS. BNI has referenced only one of many elements that are necessary to ensure safety through the design and operation of independent protection layers implemented by the BPCS.

BNI also credits the independent protection layers that require operator action to attain a safe state for providing an order-of-magnitude reduction in risk. The BNI procedure *Hazard Analysis, Development of Hazard Control Strategies, and Identification of Standards*

(24590-WTP-GPP-SANA-002) defines credited operator actions as “a manual action, identified in the hazard or accident analysis that is necessary to cause a safety [structure, system, or component] to perform its safety class or safety significant function.” For the LAW facility, no operator actions meet this definition (all of the operator actions fall into the category of independent protection layers). BNI’s SIL setting meetings entail only basic qualitative analysis, and BNI does not adequately justify that operator action is sufficient to provide the credited risk reduction. Furthermore, this operator response requirement is not administratively controlled in the safety basis to ensure that the design basis assumption for the SIS is protected.

The project team identified the Safety System Requirements Specification (SSRS) documents as providing some level of detail for the maintenance and operation of independent protection layers. Currently, however, no link exists between these documents and the safety basis, and BNI has not established a mechanism to ensure that these systems will be controlled such that they are able to perform properly in the required safety application. In addition, any delay in formalizing the control of SSRS documents as part of the safety basis will adversely affect the quality of these documents during the design process.

Conclusion. Based on its review of several instrumentation and control system designs at LAW, the Board’s staff believes that independent protection layers are not appropriately controlled in the facility safety basis. The independent protection layers, while not explicitly credited for performing safety-significant functions, establish design requirements (i.e., reliability) for the safety-significant SISs, according to BNI’s implementation of ISA-84.01-1996. A comparison of the approach specified in ISA-84.01-1996 with the proposed DOE standard (SAFT-0128) will identify gaps that require closure. Inclusion of accountability for the proper design, operation, and maintenance of the independent protection layers in the facility safety basis and control set, for example, is appropriate and consistent with SAFT-0128. Furthermore, proper identification of controls for LAW and other WTP facilities will be compromised unless the potential deficiencies in BNI’s hazard analysis process identified by the Board’s staff and BNI representatives are addressed.

Attachment

System Background Information

Wet Electrostatic Precipitator High-Level Interlock. The LAW Wet Electrostatic Precipitator High Level Interlock is a safety-significant SIS that closes the demineralized flush water isolation valve to the top (flush) and bottom (mist) nozzles in response to a high level in the Wet Electrostatic Precipitator. The hazardous event identified during the hazard analysis is a melter offgas release from blockage of the offgas flowpath in the Wet Electrostatic Precipitator due to a flooding condition.

Based on the expected frequency and consequences of this hazard, as identified by the hazard analysis, the total risk reduction required to mitigate this hazard is 1,000 to 10,000 (SIL-3). Based on results of its SIL setting meetings, BNI determined that this hazard would be mitigated by the Wet Electrostatic Precipitator High Level Interlock SIS and two independent protection layers. The first protection layer is a non-safety ventilation system for the melter enclosure designed to prevent melter offgas from entering the melter gallery; this is a mitigative feature. The second protection layer is non-safety level detection and an interlocked isolation valve, which isolates the demineralized water supply to the top (flush) nozzles. This protection layer also includes an alarm and a requirement for an operator to manually secure demineralized water flow to the bottom (mist) nozzles. BNI credits these two independent protection layers for reducing the risk of this hazard by two orders of magnitude. As a result, the reliability of the safety system is required to meet SIL-1 criteria (i.e., the SIS must achieve a risk reduction of 10 to 100). Stated another way, the safety system can have a PFD of 1×10^{-1} to 1×10^{-2} .

Steam Isolation Interlocks. The LAW High Temperature and High Pressure Steam Isolation Interlocks are safety-significant SISs that close a steam isolation valve in the high-pressure steam system. The steam isolation valve (YV-2013) is interlocked with high-temperature and high-pressure instrumentation located in a room that contains safety-related electronic equipment (Room L-0305). A high-temperature condition indicates a steam leak in the equipment room. A high-pressure condition indicates high-pressure steam in the low-pressure lines and equipment, both of which could cause damage to the safety-related equipment.

Given the expected frequency and consequences of this hazard, as identified by the hazard analysis, the total risk reduction required to mitigate this hazard is 1,000 to 10,000 (SIL-3). Based on the results of its SIL setting meetings, BNI determined that this hazard would be mitigated by the steam isolation interlock SISs and a non-safety temperature and pressure interlock system that operates similarly to the safety-significant system. This non-safety system utilizes non-safety temperature and pressure instrumentation and a non-safety isolation valve controlled through the BPCS. BNI credits the independent protection layer for reducing the risk of this hazard by an order of magnitude. As a result, the reliability of the safety system is required to meet SIL-2 criteria (i.e., the SIS must achieve a risk reduction of 100 to 1,000). Stated another way, the safety system can have a PFD of 1×10^{-2} to 1×10^{-3} .