**Department of Energy**
Washington, DC 20585

July 1, 2011

The Honorable Peter S. Winokur
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004-2901

Dear Mr. Chairman:

In the Defense Nuclear Facilities Safety Board's (Board) May 5, 2011, letter to the Department of Energy (DOE), the Board expressed its concerns regarding the design of instrumentation and control systems associated with the DOE's Waste Treatment and Immobilization Plant at the Hanford Site and requested that DOE provide subsequent information addressing those concerns.

DOE provided an interim response to the Board on May 27, 2011, informing the Board of its response status and that an additional 30 days would be needed to finalize the information, which is now completed. We believe the actions described in the Enclosure address the specific concerns identified in your May 5, 2011, letter relative to implementation of the International Standards Association (ISA) document for safety instrumented systems. We are also in the process of working with your staff to schedule the requested briefing to provide additional information, e.g., gaps between DOE and ISA standards, and on the status of our corrective actions.

If you have any further questions, please contact Mr. Kenneth G. Picha, Jr., Acting Deputy Assistant Secretary for Safety and Security Program, Office of Environmental Management, at (202) 586-5151 or Dr. James O'Brien, Acting Director for Nuclear Safety, Office of Health, Safety and Security, at (301) 903-1408.

Enclosure

Inés R. Triay
Assistant Secretary for
Environmental Management

Glenn S. Podonsky
Chief Health, Safety and Security Officer
Office of Health, Safety and Security

Printed with soy ink on recycled paper

**Response to the Defense Nuclear Facilities Safety Board (Board): Design of Instrumentation and Control Systems at the Waste Treatment and Immobilization Plant (WTP)**

This Enclosure addresses the specific issues identified in the Board's letter associated with the following:

1. The plan to assess gaps between Bechtel National, Inc.'s (BNI) implementation of American National Standards Institute/International Society of Automation (ISA) *84.01-1996, Application of (Safety Instrumented Systems for the Process Industries* and the approach specified in Department of Energy's (DOE) draft standard SAFT-0128[1], specifically regarding control of non-credited independent protection layers that drive design parameters for safety systems;

2. The specific instrumentation and control systems-related deficiencies noted in the enclosed report to the Board's May 5, 2011, letter; and

3. 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.

**Plan to Assess Gaps Between Implementation of ISA 84.01-1996 and DOE Draft Standard SAFT-0128:**

During meetings with the Board's staff in December 2010, and April 2011, project personnel noted that the Code of Record for the WTP project includes the 1996 version of the ISA-S84.01 standard.

BNI completed a qualitative comparison of the 1996 and 2004 versions of the ISA S84.01 standard, as documented in the project record (Correspondence Control Number (CCN): 226502). DOE agrees with BNI's conclusions that the current Code of Record provides the necessary requirements for controls and instrumentation, considerate of the corrective actions outlined below.

The following description of closure actions comprehensively address items 2 and 3, and will serve to ensure that the plant design is consistent with the WTP Code of Record/work processes, as well as to ensure appropriate control of the independent protection layers in the facility safety basis and plant design.

**Specific Instrumentation and Control Systems-Related Deficiencies:**

With respect to the *"specific instrumentation and control system-related deficiencies"* noted in the Board's report, the Board's staff concluded that the process used by BNI to determine the Safety Integrity Level (SIL) of each Safety Instrumented System (SIS),

[1] The draft standard was approved in April 2011 and is now DOE-STD-1195-2011

including the identification of Independent Protection Layers (IPLs), was 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, the Board's staff also identified two cases associated with the Wet Electrostatic Precipitator High-Level Interlocks and the Steam Isolation Interlocks that had credited protection layers in the SIL determination that were not independent of the initiating event. BNI identified the issues in their Project Issues Evaluation Reporting (PIER) process, 24590-WTP-PIER-MGT-10-1225-B, *Concerns on Independent Layers of Protection for Safety Functions,* and completed an extent of condition and causal analysis. BNI will complete corrective actions before resuming production work involving the SIL determination for facility Safety System Requirement Specifications (SSRS).

BNI further committed to update the design reviewed by the Board's staff, as documented in the draft SSRS for these systems, to ensure any credited protection layers in the SIL determination are independent of the initiating event prior to final issuance of the SSRS. Based on the extent of condition review, this issue will also be addressed and corrected in other draft SSRS documents.

**Planned Improvements:**

As a result of the Board's concern regarding *"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",* BNI initiated an extent of condition review relative to this process. The extent of condition applied to all previously completed meeting minutes to SIL determination. A preliminary evaluation was performed on the Low-Activity Waste SIL determination where the evaluation identified a potential set of layers of protection that will need to be formalized into appropriate design documentation (e.g. CCN or calculation) and further detailed analysis once guidance documents have been updated.

BNI has also performed an apparent cause evaluation, which was performed in accordance with BNI procedures, 24590-WTP-GPP-MGT-043, *Corrective Action Management,* and 24590-WTP-GPG-MGT-004, *Cause Analysis.* BNI concluded that an apparent cause was the result of inadequate detailed guidance and training of personnel in evaluating the initiating events, and documenting the appropriate level of detail in the meeting minutes. Issues identified included:

- SIL meeting minutes are used as the design input into the Control and Instrumentation SSRS documents for defining the SIL levels and the layers of protection. The meeting minutes are informally reviewed by all parties and released under a CCN. BNI's safety analysis (SANA) guidance documents provide the method and requirements for the meetings; however, the issued CCNs

are not formally checked or approved to indicate compliance with the SANA guidance documents.

- The team indicated that at the time of the meetings additional training may have helped in ensuring that all the initiators were discussed and evaluated for their independence. Further guidance is likely to be required to support these SIL meetings regarding crediting independent control functions as layers of protection and the level of design basis documentation (e.g. CCN or calculation) stemming from these meetings.

**Additional Actions Taken:**

In addition to the above, DOE agrees that:

- Selected IPLs are effectively design-basis assumptions that need to be appropriately protected to ensure the required reliability of credited safety-significant instrumented systems;

- The current procedure (24590-WTP-GPG-SANA-010, *Safety Integrity Level Determination/or WTP Safety Instrument Systems)* does not establish the mechanism to ensure that the IPLs will be controlled such that they are able to perform properly in the required safety application; and

- No specific link exists between the SSRS documents and the safety basis.

BNI also initiated and committed to performing a comprehensive review, including appropriate representatives from Environmental and Nuclear Safety and Engineering, of the requirements, processes (e.g., hazards analysis and SIL determination), and documentation associated with the establishment and safety basis control of IPLs associated with safety instrumented functions. To ensure the adequacy of existing and future documentation, the scope of the review and changes to processes will include:

- Updates to safety analysis and engineering procedures (e.g. SANA procedures, engineering procedures, and the Safety and Requirements Document) to provide an integrated set of requirements and guidance to consistently select controls and determine the SIL and IPLs (as needed);

- Training of safety analysis and engineering personnel on the revised procedures and guidance;

- Reviews of existing SIL determinations against updated procedures; and

- Incorporation of SIL and IPL determinations as design basis assumptions of credited safety-significant instrumented systems into the Documented Safety Analysis and Technical Safety Requirements as appropriate.

Specific actions, as necessary, will be added to PIER 10-1225-B for project tracking and resolution based on the above and further work on instrumentation and control systems, and the hazards analysis process.