DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700 Washington, D.C. 20004-2901
(202) 694-7000

March 16, 2009

Gerald L. Talbot Jr.
Assistant Deputy Administrator for
Nuclear Safety and Operations
National Nuclear Security Administration
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. Talbot:

Pursuant to the certification mandate provided in Section 3112 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, the Defense Nuclear Facilities Safety Board's (Board) staff responsible for certification activities has reviewed Chemistry and Metallurgy Research Replacement (CMRR) design data provided to date by the National Nuclear Security Administration (NNSA). The Board's staff is focusing its review on topics previously raised regarding the CMRR nuclear safety design strategy, the Preliminary Documented Safety Analysis, and design of safety-class and safety-significant systems. Those topics were provided electronically to NNSA on November 20, 2008. The Board's staff has documented specific technical issues on a Findings Form. For purposes of the certification review, the Board's staff considers a Finding a design topic related to a concern raised by the Board's staff regarding the CMRR design that has not been adequately resolved and that could preclude Board certification.

Enclosed is a Findings Form with respect to the issue of Inadequate Identification of Safety-related Controls, Functional Requirement, and Performance Criteria. We ask that you reply within seven calendar days from the date of Board's staff signature on the attached Findings Form, informing the Board's staff how long it will take to provide a complete NNSA response. The NNSA response should contain sufficient quantity and quality of technical information necessary for the Board's staff to determine whether the Finding can be resolved. The Findings Form contains a signature block for the NNSA individual with the authority and responsibility for addressing the Finding. Please ensure that this individual signs and dates the returned Findings Form.

Sincerely,

Roy E. Kasdorf

Roy E. Kasdorf
Nuclear Facility Design and
Infrastructure Group Lead

Enclosure

c: Mr. Mike Thompson
Mr. James McConnell
Mr. Patrick Rhoads
Mr. Herman LeDoux
Mr. Mark B. Whitaker Jr.

Board Findings

Chemistry and Metallurgy Research Replacement Facility: Congressional Certification Review

Topic: PDSA and Safety Strategy

Finding Title: Inadequate Identification of Safety-related Controls, Functional Requirements, and Performance Criteria

Finding:

The Hazard Analysis (HA) section of the Preliminary Documented Safety Analysis (PDSA) is to identify the spectrum of hazards potentially posed by the operations, and identify an adequate set of controls to protect the public and the workers. This HA has been documented in Appendix 3B of the PDSA. It appears to be relatively comprehensive for this stage of the PDSA (the project has made a commitment to perform a process HA for the next revision of the PDSA). Appendix 3B highlights (in blue) the "safety-related" controls that are needed to protect the public or the workers from significant consequences.

Section 3.4 of the PDSA quantitatively evaluates the unmitigated consequences of major accidents from the HA, and identifies the "safety-class" (SC) controls for events potentially exceeding 5 rem Total Effective Dose Equivalent (TEDE) at the site boundary. The quantitative analysis should also evaluate the unmitigated consequences to the Collocated Workers (CLW) at 100 meters for comparison with the DOE criterion. This evaluation is not presented in this PDSA (the project has committed to provide that information in the next revision to the PDSA). Chapter 4 of the PDSA collectively lists all the safety-related controls (i.e., safety-significant (SS) structure, systems, and components (SSC) from Appendix 3B and safety-class SSCs from Section 3.4), and identifies functional requirements (FR) and performance criteria to ensure that the controls meet their intended functions.

The following deficiencies have been identified (the Attachment to this Finding provides examples for demonstration purposes only, and by no means is expected to be an all inclusive list):

(1) The set of safety-class and safety-significant controls identified in the PDSA have not been demonstrated that they will ensure adequate protection of the public and the workers.
(2) The functional requirements and performance criteria identified for safety-related controls in Chapter 4 of the PDSA do not support the credit given to them in the Chapter 3 analysis.

Basis for Finding:

10 CFR 830, 202(b): "(4) Prepare a documented safety analysis for the facility; and (5) Establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment."

10 CFR 830, 204(b)(4): "Derive the hazard controls necessary to ensure adequate protection..., demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards."

10 CFR 830, G.3: "Safety structures, systems, and component require formal definition of minimum acceptable performance in the documented safety analysis...by first defining a safety function...then placing functional requirements."

DOE O 420.1B, 3.a.(1): "(a) Safety analyses must be used to establish the identity and function of safety class and safety significant SSCs, and (b) the significance to safety of functions performed by safety class and safety significant SSCs."

Suggested Resolution or Path Forward:

- **Pre-certification:** The project must (1) submit a process plan for addressing the PDSA deficiencies, and (2) prepare a document that briefly, but thoroughly and comprehensively, describes all safety-class and safety-significant controls and their support systems that envelope the identified events in the PDSA, including its Appendix 3B. This document should also identify the functional requirements for all those SSCs, along with their performance categorization, to ensure appropriate credit can be given to them in the hazard or accident analysis. This document should be place in a configuration control system as this document will be part of the Board's certification.

  The process plan should include commitment to:

  - Revise Chapter 2 to describe safety-related SSCs and their support systems as portrayed in the SDDs and credited in the PDSA.
  - Revise Chapter 3 to include the process HA and CLW dose calculations, identify any new controls from these analyses, and implement/incorporate Board specific comments.
  - Revise Chapter 4 to capture all SS and SC controls from Chapter 3 and Appendix 3B including their support SSCs, and clearly identify the FR for all those SSCs along with their performance categorization to demonstrate the credit given to them in the hazard and accident analyses.
- **Post-certification:** Within 6 months of the certification, the PDSA must be revised to (1) address the identified deficiencies, (2) implement the results of the Process hazards analysis, (3) evaluate unmitigated dose consequences to the collocated workers, (4) incorporate the above list, as well as any new safety-related SSCs from the process HA and the CLW dose calculations, and their corresponding performance criteria and system evaluations, and (5) notification of any deviation from the above document of safety SSCs.

NNSA Response:

DNFSB Final Resolution:

DNFSB: Roy E. Kasdorf 3/16/07 Roy Kasdorf Date	NNSA: _____ _____ Date

Attachment

1. **The set of safety-class and safety-significant controls identified in the PDSA have not been demonstrated that they will ensure adequate protection of the public and the workers:**

(a) *Examples of necessary controls that are missing or inadequately identified*:

- There is insufficient information to determine if adequate safety-class (SC) controls have been identified to protect against loss of Long-term Vault (LTV) cooling for an extended period of time. The PDSA concludes that the LTV can reach temperatures that result in adverse consequences to the LTV containers and a release of materials that lead to unmitigated consequences exceeding the evaluation guideline of 25 rem, thus requiring identification of a SC control. However, no SC controls have been identified for this event. Passive cooling of the LTV containers is not adequately demonstrated in the PDSA to negate the need for a SC control (DOE directives requirements do not have provisions for wavering the need for SC controls if the time to develop the event exceeds certain number of days). Additionally, section 4.3.5.5 of the PDSA introduces a Specific Administrative Control to restore cooling; however, no design modifications have been proposed to accommodate this action.

Other examples:

- Page 3-144, Glove Box (GB) fire doors are credited to withstand a fire and prevent it from propagation, it assumes that these doors are "normally closed". GB fire doors are not identified as safety-related design features in Chapter 4.
- Page 3-84, assumes that the fire barrier doors close after 1 minute and all other doors close in 10 minutes for the "controlled" event consequence analysis. It is not clear how these assumptions are captured in Chapter 4.
- Page 3-94, provides examples of controls with "potential for being elevated to SC" that don't appear to have been captured in Chapter 4: e.g., use of non-explosive resin, and heat removal capability for equipment with exothermic reaction.
- Appendix 3B, SRW-013, resin explosion, risk 1 to workers. Credited controls are facility design, filtered ventilation Zone 2 and 3, and Waste Isolation Pilot Plant containers. None of these controls protect the facility workers from an explosion.
- Potential Admin Controls that are missing from the list in Table 3-18 and Chapter 4.5: (i) Limits on hazardous chemicals including Be (page 3-30), (ii) Container transfer between Rad Lab and Nuclear Facility (page 3-24), (iii) Fuel size of vehicles, assumed for outside fire events (page 3-31), (iv) Prohibition of radioactive liquid material storage in LTV (page 3-132).

(b) *Examples of safety-related controls that would not protect against the identified hazard*:

- Spill from an Elevator Accident needs a SC control. This scenario assumes that the containers are intact until they hit the ground and then the material is released. SC containers are credited to "confine" the material "during the drop." This functional requirement protects the assumption. However, it does not protect the material from being released "after the impact" that led to the need for SC control. No evidence has been provided for the SC containers to "withstand the impact" of the accident as the containers are thrown around and hit other objects during and after the fall. It should be noted that the airborne and respirable release fraction values used to calculate the public dose consequences (that led to the need for SC control) are for a crushed container/materials released on the ground.

- Hydrogen deflagration and Detonation in the basement: No analysis has been provided to show that the walls can withstand the consequences of an over-pressurization due to explosion in accounting for the material at risk (also, the ventilation filter plenums are behind an unqualified wall). Additionally, the identified SC controls may be acceptable for a fire scenario, but are NOT effective for an "explosion".
- Seismic event: Case 2c credits the crane, as a safety-class function, not to fall and damage the assumed material at risk. Chapter 4 only requires the "structural" support of the crane to prevent failure, not the entire crane system. The crane is NOT identified as safety-class control with a functional requirement "not to fall" during a seismic event.

2. The functional requirements and performance criteria identified for safety-related controls are inadequate to support the credit given to them in Chapter 3 analysis:

(a) Examples of credited controls without adequate functional requirement (FR):

- The performance criteria for the LTV containers do not address many of the capabilities needed to satisfy the functional requirements:

  i) The performance criteria related to pressure protection is not measureable in-situ and the PDSA relies on the "Vault Heat Transfer" analysis (Ref. 43) to show that the LTV containers meet the functional requirements. The analysis; however, does not address the primary functional requirement of pressure protection. Additionally, no thermal analysis has been performed for the other containers (i.e., "yet to be developed"), other than those that comply with DOE-STD-3013.
  ii) The performance criteria related to thermal protection is missing. There is no performance criteria to protect the containers from damage due to temperatures near, or above, the plutonium-iron eutectic temperature.

Other examples:

- Table 3-12 credits ventilation Zones 1, 2, and 3 as SS for explosion events. It is not clear if these systems are designed to withstand the over-pressure pulse from an explosion since there is no discussion of this over-pressure, nor is there any FR for these systems in Chapter 4 of the PDSA.
- Table 3-12 also credits "enclosure confinements (GB and material transport system)" as SS for explosions. There is no corresponding FR for GBs in Chapter 4 of the PDSA.
- Appendix 3B: NFL-012, explosion in GB, risk 1 to workers: The credited SS control is the GB confinement. There is no FR for the GBs to withstand an explosion.
- Appendix 3B: NFL-014, breach of a GB due to missiles from rotating equipment…etc, risk 1 to workers: the main protection is provided by the "GB confinement" to mitigate the consequences. There is no FR for missile protection of GBs in Chapter 4.

- Hydrogen deflagration (and Detonation) in the basement: No performance criterion is provided for the SC barriers to resist the pressure pulse from an explosion.

(b) Examples of credited Functions not identified as FR for safety-related controls:

- The Facility Management System has a safety-significant functional requirement to prevent filter blow out (Table 4-25). The operators have to manually take action to meet the safety-significant functional requirement. The ventilation system also has a performance criterion (Table 4-22) to operate in a reduced flow mode on the loss of offsite power that requires operator action. Consequently, the operators need to take manual actions to configure ventilation equipment to perform its safety functions. However, the ventilation system functional requirements do not consider protection of control room personnel. The PDSA system descriptions for the support ventilation system do not identify the systems having the ability to maintain the habitability of the control room to ensure operators can perform monitoring of facility conditions or respond to events to place the facility into the configuration required by the PDSA following design basis accidents.

Other examples:

- Fire on the Loading dock includes fires of a refueling tanker truck. Page 3-156 credits waste drums as SS to withstand the consequences of a fire (potentially refueling tanker) without any justification or technical support. Chapter 4 does not identify specific fire resistance, commensurate with the postulated fire, as a functional requirement for waste drums.
- Zone 2 active confinement ventilation system is SS and PC-3, including the filters. Table 4-9 does not require PC-3 qualification of the plenum deluge system.
- Appendix 3B: MM-054, fires with insufficient energy to actuate the sprinklers—credits Fire Detection/Alarm system. Table E-3 does not show fire detection and alarm system as safety-significant. Chapter 4, page 4-33, refers to "other place in the PDSA" for discussion of the Fire Detection and Alarm system, but not clear where that discussion is provided.
- Appendix 3B: NFL-024 Credits GB confinement and Oxygen monitors for fires in gloveboxes. Table 4-19, GB Oxygen Monitors, limits such systems to "GB used for machining plutonium" only [emphasis added]. No GB fire suppression or inerting system has been identified for GBs with remaining pyrophoric materials in Chapter 4.