DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

July 6, 2010

The Honorable Thomas P. D'Agostino
Administrator
National Nuclear Security Administration
U. S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. D'Agostino:

The Defense Nuclear Facilities Safety Board (Board) recently reviewed the Hazard Analysis Reports (HARs) for several nuclear explosive operations at the Pantex Plant. Based on the results of this review, the Board believes the implementation of Department of Energy (DOE) Standard DOE-NA-STD-3016-2006, *Hazard Analysis Reports for Nuclear Explosive Operations*, at Pantex is deficient in certain areas. A synopsis of the issues noted by the Board's staff is given below; additional detail is provided in the enclosed report:

- B&W Pantex has established the practice of using initiating event probabilities to justify its decision that controls are not needed for certain hazard scenarios for which the design agency determined that a weapon response was credible. The Board's staff considers this practice to be inconsistent with the safe harbor defined in DOE-NA-STD-3016-2006.

- In contrast with the mandate of the standard, the HARs reviewed by the staff do not serve as the final safety basis integration documents. The HARs fail to provide documented *verification* that hazards presented by weapon-specific operations are adequately analyzed and controlled in the facility-level Safety Analysis Reports.

- B&W Pantex does not control human impact energies to be consistent with assumptions used by the design agencies in determining weapon response.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a briefing within 60 days of receipt of this letter responding to the issues identified in this letter and the enclosed report.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. Steven C. Erhart
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

March 10, 2010

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: T. Spatz

SUBJECT: Review of Hazard Analysis Reports, Pantex Plant

This report documents issues noted by the staff of the Defense Nuclear Facilities Safety Board (Board) during a review of the Documented Safety Analysis (DSA) for the Pantex Plant, which included an on-site review on November 3–5, 2009. Staff members F. Bamdad, D. Campbell, M. Duncan, B. Laake, C. Martin, R. Rauch, and T. Spatz participated in this review. The staff reviewed the Unreviewed Safety Question process, the new information process, the development of Hazard Analysis Reports (HARs), and the integration of nuclear explosive safety into the DSA process. The staff identified deficiencies in these areas and discussed them with representatives of Babcock and Wilcox (B&W) Pantex and the Pantex Site Office. This report focuses on the deficiencies identified in the four HARs reviewed by the staff.

The HAR development process must ensure compliance with Department of Energy (DOE) Standard DOE-NA-STD-3016-2006, *Hazard Analysis Reports for Nuclear Explosive Operations*, and DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. The staff noted four areas in which either the implementation of the safe harbor methodology for HAR preparation or the implementation of DOE-STD-3009-94 was inadequate, as detailed below.

Application of Initiating Event Probabilities. The *Pantex Plant Integrated Safety Management Authorization Basis Manual* (Pantex AB Manual) presents guidelines for B&W Pantex personnel developing HARs. It defines a "credible" event in the form of a maximum probability for each event consequence. For example, B&W Pantex defines a credible event for a high explosive violent reaction (HEVR) as a probability of greater than 10^{-10} per unit processed. The overall probability of an event is determined by multiplying the probability of the initiating event by the probability of a weapon response for each configuration. The staff noted hazard scenarios for which the design agency had determined that a weapon response is credible, but B&W Pantex has not applied controls. The staff believes this methodology is inconsistent with guidance in DOE-NA-STD-3016-2006 and DOE-STD-3009-94.

DOE-NA-STD-3016-2006 states: "Hazard scenarios that are not screened for HEVR or IND [inadvertent nuclear detonation] consequences are designated as Design Basis Accidents (DBAs), and are retained for consideration in the accident analysis section per DOE-STD-3009, or superseding directives." Further, DOE-STD-3009-94, Appendix A, "Evaluation Guideline," states that the determination of the need for controls is driven solely by the "bounding consequence potential." HEVR and IND events by definition challenge evaluation guidelines, i.e., result in an unmitigated offsite dose greater than 25 rem. Therefore, B&W Pantex should apply safety-class controls to hazards with HEVR or IND consequences unless it could provide a rigorous justification to the contrary.

To illustrate this deficiency, the staff found examples in which the hazard analysis summary table in a particular HAR states, "no control selected to prevent event." In most of these cases, the design agency assigned a probability of 10^{-6} for an HEVR consequence. B&W Pantex applied an initiating event probability of less than 10^{-4}, combined with the weapon response, to determine that an HEVR was not credible and therefore identified no controls. When used in this manner, initiating event probabilities take on a level of importance similar to that of the weapon response screen performed by the design agency. If the National Nuclear Security Administration (NNSA) deems the use of initiating event probabilities to be an acceptable basis for eliminating non-screened hazards from further consideration for controls, the staff believes explicit guidance to that effect should be provided by NNSA. Further, the same rigor and formality used in determining weapon responses ought to be applied to initiating event probabilities.

Integration of Hazard Environments. DOE-NA-STD-3016-2006 states: "The HAR must evaluate all hazards that could impact the NEO [nuclear explosive operation] and must serve as the final safety basis integration document. Another DSA (e.g., a SAR [Safety Analysis Report]) may provide analysis and resulting controls for hazards that are relevant to the NEO. However, the HAR must *verify* [emphasis added] the analysis and controls are adequate for the hazard." At Pantex there are 12 SARs containing hazard scenarios and controls that need to be integrated into the HARs. The HARs reviewed by the staff do not serve as the final integration documents. They do identify the hazards and the SARs in which those hazards are analyzed; however, they do not include verification of the hazard analysis and controls for such operations as hoisting and on-site transportation. To comply with DOE-NA-STD-3016-2006, the HARs must include such verification. The staff found no cases of missing controls.

Single-Failure Faults in the Final Control Set. DOE-NA-STD-3016-2006 states: "Control effectiveness determinations should include a discussion of single failure faults in the final control set." Further, DOE-STD-3009-94 states: "In determining performance criteria for safety-class SSCs [structures, systems, and components], existing criteria traditionally associated with safety-class designation, such as single failure criteria, should be considered in the judgment process." The staff found no such discussion in the HARs reviewed.

To illustrate this deficiency, the W76 HAR contains the event scenario for an electrostatic discharge (ESD) to the weapon from a tool. B&W Pantex has developed an ESD environment control consisting of a dissipative floor covering, conductive footwear, drag straps, and conductive tool coatings. The staff found no discussion of single-failure faults for the ESD environment in the W76 HAR.

Similarly, the W87 HAR contains the event scenario of an ESD to a component that could result in a mechanical insult. This scenario has the potential for an HEVR; however, the identified controls are limited to administrative controls of wrist straps and bonding to a common ground. There is no second control for defense in depth, nor is there any discussion of single-failure faults for the ESD environment.

Analysis of Human Impacts on Weapons. B&W Pantex designs tools and requests weapon responses based on a value for the impact energy of a Production Technician (PT) derived from data compiled in 2001. Based on the 2001 data, the human impact energy is defined as a 280 lb person traveling 2.5 miles per hour.

B&W Pantex does not treat this value as a controlled assumption and could have PTs that exceed the 2001 value performing nuclear explosive operations. If PTs weighing more than 280 lb perform nuclear explosive operations, two issues arise with respect to the HARs: the tooling design safety margins may be exceeded, and the weapon responses are no longer bounding. B&W Pantex has no control in place, either administrative or engineered, to limit impact energies to the value for which the tooling was designed. Tooling designs incorporate a safety factor, but again no control is in place to limit energies to less than the tooling design plus safety factor.

Of greater concern is that the design agency supplies weapon responses for tripping-man impact scenarios based on the energy imparted by a 280 lb PT traveling 2.5 miles per hour. B&W Pantex has no controls in place to limit human impact energies to those having a known weapon response.

To illustrate this deficiency, the staff reviewed an event scenario in the W87 HAR involving the failure of an anti-rotation pin caused by a tripping PT. The tool did not meet the requirement in the B&W Pantex AB Manual to withstand the impact of a 280 lb PT. B&W Pantex accepted this tool because it existed prior to publication of the HAR. B&W Pantex established a functional requirement for the anti-rotation pin to meet a reduced criterion. B&W Pantex did not establish a control to limit the weight of the PT to meet this reduced functional requirement.

The staff believes the maximum PT impact energy does not represent an uncontrolled environment, such as lightning, earthquake, or meteorological conditions. Further, DOE-STD-3009-94 states: "An accident analysis is performed for the bounding accidents." There is no control in place to ensure the assumed impact energy is in fact bounding. B&W Pantex imposes other physical qualifications for PTs (such as age, sight, speech), as well as other limitations specified by the Human Reliability Program. The staff believes that weapon responses should be reevaluated for higher impact energies, if necessary, or B&W Pantex should provide adequate controls to limit impact energy to the conditions analyzed.