DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

August 5, 2010

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

Dear Dr. Triay:

The staff of the Defense Nuclear Facilities Safety Board (Board) conducted a review of the newly revised and implemented Documented Safety Analysis (DSA) at the Hanford Tank Farms during April and May 2010. This review revealed a number of analytical and implementation deficiencies in the DSA that limit the effectiveness of the prescribed safety controls in preventing and mitigating certain postulated accident scenarios. The enclosed report provides the results of the review.

The staff identified that the accident analysis used non-bounding values for (1) the radiological inventory of the tanks and (2) the amount of waste that could be released in a major accident. The staff also found that the tank ventilation systems, which serve to prevent flammable gas detonations and deflagrations, had been inappropriately downgraded to less than safety-significant in favor of a specific administrative control that has significant weaknesses. The enclosed report describes similar concerns regarding the identification and implementation of controls for other hazards.

Collectively, the deficiencies identified by the staff point to an overall reduction in defense in depth and a reduction in safety at a time when the operating tempo of the Tank Farms is expected to increase in preparation for sending tank waste to the Waste Treatment Plant. Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a briefing and report within 60 days of receipt of this letter outlining the activities DOE plans to take to address the deficiencies identified in the enclosed report.

Sincerely,

Jessie Roberson

for Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. David A. Brockman
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 8, 2010

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: J. L. Shackelford

SUBJECT: Hanford Tank Farms Documented Safety Analysis

This report documents the results of a review of the Documented Safety Analysis (DSA) of the Hanford Tank Farms performed by the staff of the Defense Nuclear Facilities Safety Board (Board). This review, conducted by staff members S. Lewis, J. MacSleyne, R. Quirk, and J. Shackelford, included in-office evaluation of the DSA during the months of April and May 2010 and a visit to the Hanford Site during May 10–13, 2010.

The staff identified a number of analytical and implementation deficiencies in the newly revised DSA for the Hanford Tank Farms. These deficiencies included the use of potentially nonbounding input parameters, which call into question the bounding nature of the overall analysis; the use of noncredited equipment to perform safety functions; weak or inadequate specific administrative controls (SAC); and the downgrading of safety-significant engineered features, contrary to the Department of Energy's (DOE) approved hierarchy of controls.

Background. The Office of River Protection (ORP) approved the revised DSA in January 2010. The revision was intended to bring the analysis into compliance with DOE Standard 3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, Change Notice 3, and DOE Standard 1186, *Specific Administrative Controls*. Additionally, the analysis incorporates new evaluation guidelines transmitted by ORP in a letter to the contractor, and the implementation of commitments made as corrective actions for the July 2007 waste spill from Tank S-102.

Hazard Analysis Methodology. The staff identified a number of cases in which the contractor's analysis does not consistently use or consider bounding values for the input parameters. In particular, the staff questioned whether the input values derived from the best-basis inventory (BBI) represent bounding estimates of the material at risk (MAR) values used in the accident analysis. Other, potentially non-bounding values used include volume, density, and temperature estimates. In some cases, the values used by the contractor's analysts are characterized in the DSA as "best estimates." The guidance in DOE Standard 3009-94 explicitly states: "The MAR values used in hazard and accident analysis must be consistent with the

values noted in hazard identification as described in Section 3.3.2.1 of this standard, and should represent documented maxima for a given process or activity." The BBI values, along with the other potentially non-bounding parameters, are propagated throughout the accident analysis. As a result, the staff could not conclude that the calculated consequences consistently represent bounding estimates of the postulated accident scenarios.

Classification and Selection of Controls. The staff found that the contractor's analysis does not always follow DOE's preferred hierarchy in the selection of controls. A number of structures, systems, and components (SSCs) previously categorized as safety-significant were reduced to defense-in-depth features. At a minimum, these SSCs are a "major contributor to defense in depth," and as such would warrant safety-significant classification. Examples of engineered features that were previously credited as safety-significant and are now designated as defense in depth or less include the double-shell tank (DST) ventilation system, the waste transfer leak detection system, and the master pump shutdown system.

DST Ventilation System—Analyses show that 5 of the 28 DSTs currently have gas retained in the waste in quantities greater than 200 percent of the lower flammability limit (LFL), which could be released either spontaneously or due to an induced gas release event. Six others have retained gas quantities of greater than 100 percent of the LFL. Further, irrespective of the gases currently retained in the tank waste, all the DSTs currently generate flammable gases and will eventually develop 100 percent of the LFL in the headspace in the absence of adequate ventilation.

The contractor calculated the time to reach 100 percent of the LFL in the headspace without ventilation and found the time to be as short as weeks for some DSTs. However, the staff notes that these values are based on steady-state gas generation under quiescent conditions and that the calculated time to LFL in the headspace can be reduced significantly by transfers to or from a given tank. Consequently, preventing the accumulation of flammable gas in the headspace is a critical safety strategy at the Tank Farms.

As a consequence of the buildup of flammable gas in the headspace of tanks, the DST ventilation system was previously categorized as a safety-significant, preventive engineered control and was credited in certain flammable gas scenarios. In the revised DSA, the ventilation system is reduced to defense in depth and replaced by a SAC for flammable gas monitoring. ORP and the contractor indicated that a factor leading to the decision to downgrade the ventilation system was the difficulty of pursuing commercial-grade dedication to support the safety-significant classification of controls. The use of an administrative control (AC) in lieu of an engineered feature is contrary to DOE's approved hierarchy of controls as outlined in DOE Standard 3009-94, which states: "The established hierarchy of hazard controls requires that engineering controls with an emphasis on safety-related SSCs be preferable to ACs or SACs due to the inherent uncertainty of human performance." The staff notes that the DST ventilation system is a key element in a Limiting Condition for Operation (LCO 3.4, DST Induced Gas Release Event Flammable Gas Control) that supports a safety-significant SAC, and therefore warrants safety-significant classification itself. The staff concluded that the DST ventilation

system is an important contributor to defense in depth, and that the system should therefore remain as a safety-significant control.

Several significant uncertainties in the revised DSA reinforce the staff's concern about the lack of engineered controls. For the DST detonation scenario, for example, the contractor estimates an offsite consequence of approximately 5 rem. However, this analysis specifically excludes the worst-case source term (from Tank AZ-101). The contractor asserted that the 5 rem consequence does not sufficiently challenge the evaluation guideline (of 25 rem) to warrant a more careful analysis of the source term that might lead to the need for safety-class controls. As noted above, however, the potentially non-bounding nature of the analysis (which in this case applies to estimates of both the source term and time to LFL) with respect to the BBI data is of concern.

In the case of the detonation scenario, the fraction of tank waste released is a critical parameter in determining the source term and resultant dose to the public. The contractor used an expert elicitation process to generate a set of estimates of the amount of respirable radioactive material that would be expelled. The values ranged over several orders of magnitude, and the contractor used a value of 100 kg as an input to the offsite accident analysis. This value corresponds to approximately the 80^{th} percentile of the aggregate distribution. However, the 95^{th} percentile of this same distribution (a threshold more commonly associated with conservative estimates) corresponds to a value of about 500 kg, and the maximum values are much higher. As a result, given the uncertainties in the analysis (with respect to both the BBI information and the expert elicitation process), it is not difficult to postulate offsite doses meeting or exceeding the evaluation guidelines that define the needs for safety controls. However, ORP approved a DSA with no safety-class or safety-significant engineered controls for this accident scenario.

Although the consequences of the deflagration scenarios are somewhat less severe, the same concerns related to the lack of bounding input data and the uncertainty associated with the expert elicitation process apply. The mass of respirable material estimated to be expelled during a deflagration scenario causing tank failure is 1 kg. This value corresponds to the median of the aggregate expert elicitation distribution. The 95^{th} percentile of this same distribution equates to about 50 kg. As a result, severe deflagration scenarios can easily be postulated to result in offsite consequences in the rem-range, with onsite consequences to workers being considerably higher.

In lieu of crediting the DST ventilation system, the contractor implemented a SAC for flammable gas monitoring. The intent of the SAC is to monitor the flammable gas concentration within the DST and if levels exceed 25 percent of the LFL, to initiate actions to reduce the concentration or eliminate potential ignition sources. The SAC involves an operator recording flammable gas readings using a portable measuring device attached to a tank riser using a flexible hose fitting. The staff determined that the SAC has a number of weaknesses that collectively render it inadequate as a safety control. These weaknesses include the following:

- The flexible hose is exposed to the elements and could easily develop a pinhole leak or other defect that would be undetectable given the current SAC. Such a leak would cause a flow bypass condition whereby the portable monitor would actually be

drawing a sample from the outside atmosphere rather than the headspace of the tank. The result would be a false low flammable gas reading.

- The action threshold for the surveillance is inadequate. The threshold is specified as 25 percent of the LFL; however, the measurement is typically taken with ventilation running and the procedure does not specify otherwise. With forced ventilation, the flammable gas reading should be 0 percent, and any appreciable concentration would be evidence of an anomalous condition.

- The portable monitor requires a minimum oxygen concentration to ensure an accurate flammable gas reading. This minimum concentration is not specified in the surveillance procedure. Similarly, the temperature limits of the instrument are not specified in the procedure.

- The instrument calibration procedure does not conform to the manufacturer's recommendations.

- The surveillance is performed by a single operator, with no provision for independent verification.

- The labels on the valves used to establish the flowpath for combustible gas monitoring contain an outdated administrative warning prohibiting operation of the valves. In practice the operators routinely violate the instructions on the labels to perform the task.

Waste Transfer Leak Detection and Master Pump Shutdown Systems—ORP approved downgrading of the leak detection and master pump shutdown systems from safety-significant to defense in depth or less. In lieu of these systems and for associated accident scenarios, the DSA credits the primary waste transfer piping and hose-in-hose transfer line systems as safety-significant controls. Almost all of the newly credited piping systems were not designed, installed, or tested to the ANSI/ASME B31.3 code requirements applicable to safety-significant systems and therefore lack the formal pedigree of a code-compliant SSC. The primary piping system was "grandfathered" by engineering analysis. However, the contractor did not perform an explicit gap analysis or crosswalk to current code requirements. Furthermore, the performance criteria for the safety-significant primary piping allows (dripwise) leakage. The staff determined that, given the issues related to the potentially non-bounding nature of the analysis, as well as the uncertainty associated with the grandfathering process, the leak detection and master pump shutdown systems continue to make significant contributions to defense in depth and should be maintained as safety-significant systems.

Use of Non-Safety-Significant Equipment for Safety-Significant Control Applications—The staff observed a number of instances in which non-safety-significant equipment was being used to fulfill safety functions. Section 4.5 of the DSA describes the technical safety requirement SACs at the Tank Farms, including the flammable gas monitoring programs for the waste tanks, tank annuli, and the double-contained receiver tank (DCRT). These SACs require

inputs from level measuring and temperature monitoring equipment (e.g., DST annulus level, DCRT level, tank temperature) to fulfill their credited safety functions. None of the equipment relied upon to fulfill the requirements of these SACs has been designated as safety-significant.

DOE Standard 1186, Section 3.3 states: "...instrumentation and controls and equipment that support an SAC should meet performance requirements consistent with the importance of the safety function of the Specific AC." Further, DOE Standard 3009-94 guidance states: "Identify SSCs whose failure would result in losing the ability to complete the action required by the SAC. These SSCs would also be considered safety-class or safety-significant based on the significance of the SAC safety function." The staff concluded that the non-safety-related monitoring equipment should be elevated to a safety-significant classification.

Weaknesses Associated with the Waste Compatibility SAC—The staff noted that the SAC associated with waste compatibility has weaknesses that limit its effectiveness as a safety control. Waste compatibility assessments are prepared via the use of a computer program using a number of input parameters. The software used to develop the assessment was not assigned a level of software quality assurance commensurate with the safety classification of the SAC. The uncertainties associated with the nonbounding nature of input parameters discussed earlier in this report also apply to the waste compatibility assessment. The contractor used the reliability and accuracy of the waste compatibility SAC as a basis for screening a number of hazards from further consideration. Most notably, the SAC is relied upon to ensure that waste transfers will not inadvertently create a tank with less favorable flammable gas generation and accumulation characteristics.