Independent Oversight Review of the Hanford Site Waste Treatment and Immobilization Plant Low Activity Waste Melter Process System Hazards Analysis Activity

December 2012

Office of Safety and Emergency Management Evaluations
Office of Enforcement and Oversight
Office of Health, Safety and Security
U.S. Department of Energy

Table of Contents

Acronyms

CFR	Code of Federal Regulations
BNI	Bechtel National, Inc.
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
gpm	Gallons per Minute
HA	Hazards Analysis
LAW	Low Activity Waste
LBL	Low Activity Waste, Balance-of-Plant, and Analytical Laboratory Facilities (of the WTP)
NOx	Nitrogen Oxides (mixture of NO, NO_2 and NO gaseous radicals)
ORP	DOE Office of River Protection
TSRs	Technical Safety Requirements
w.g.	Water Gauge (unit for specification of pressure)
WTP	Waste Treatment and Immobilization Plant

Independent Oversight Review of the Hanford Site
Waste Treatment and Immobilization Plant
Low Activity Waste Melter Process System
Hazards Analysis Activity

1.0 PURPOSE

The Office of Enforcement and Oversight (Independent Oversight), within the U.S. Department of Energy (DOE) Office of Health, Safety and Security (HSS), observed a key activity for developing a hazards analysis (HA) for the melter process system of the Low Activity Waste (LAW) nuclear facility at DOE's Hanford Site.

Independent Oversight is reviewing efforts leading to development of the Documented Safety Analysis (DSA) and Technical Safety Requirements (TSRs) for the LAW, Balance of Facilities (BOF), and Analytical Laboratory (LAB) facility, collectively known as LBL facilities of the Waste Treatment and Immobilization Plant (WTP). The subject HA for the LAW melter process system is one of a series of system-by-system HAs that have been planned and scheduled in support of developing the DSA for LBL facilities. These HAs, which will be consolidated into an HA report, are subject to further review by Bechtel National, Inc. (BNI) and constitute an intermediate step toward preparing LAW DSA Chapter 3, *Hazard and Accident Analyses.*

2.0 BACKGROUND

The LAW facility is part of the WTP being designed and constructed by BNI, a contractor for DOE's Office of River Protection (ORP). The mission of the WTP is to process and immobilize the Hanford tank waste into a stable glass form, suitable for permanent disposal. The purpose of the LAW melter process system is to convert a blended slurry of pretreated liquid low-activity waste and glass former additives into molten glass. This glass is discharged from the melter into cylindrical stainless steel containers where it cools to form the immobilized low-activity waste.

The preparation of a systematic, comprehensive HA is an essential part of developing a DSA according to DOE-STD-3009-94, Change Notice 3, *Preparation Guide for U.S. Department of Energy Non-Reactor Nuclear Facility Documented Safety Analyses*, a safe harbor standard for meeting the nuclear facility safety basis requirements of 10 CFR 830, *Nuclear Safety Management*, Subpart B, *Safety Basis Requirements*. BNI has developed a Hazards Analysis Procedure and a Hazards Analysis Handbook to implement these requirements.

3.0 SCOPE AND METHODOLOGY

BNI conducted the key part of its LAW melter process system HA activity over a period of about 6 weeks, from September 17 through October 25, 2012. The Independent Oversight staff observed the HA Team activity over a 3-week period, October 1 through 18, 2012.

The HA activity consisted of a series of HA Team meetings to systematically discuss potential events and associated scenarios previously identified on a spreadsheet using the "What-If" HA methodology. Independent Oversight staff were not present during the HA Team's process of initially identifying the set of What-If event scenarios. For each What-If event, the HA Team discussed and documented the event description, causes, release mechanisms, assumptions, likelihood, consequence, and candidate preventive and mitigative controls. During these scheduled meetings, Independent Oversight focused on the nature, scope, and depth of the HA Team's technical discussions to explore and analyze each event and to characterize the associated hazards. Independent Oversight staff did not participate in the HA meetings or interview the HA Team members. Independent Oversight staff did not observe either the HA Team's evaluation of natural phenomena hazards and external events, or the hazards evaluation of the melter system in test, maintenance, or shutdown configurations, except when such facility modes were discussed along with melter operations.

While the Independent Oversight staff did not observe the initial kickoff and walkdown for the melter HA, they did review the records and HA documentation from those activities. Independent Oversight staff had the benefit of observing a kickoff meeting and walkdown for another related HA, the melter offgas system, that illustrated the scope and depth of that part of the HA process.

At the invitation of the HA Team Lead, Independent Oversight staff discussed their observations with the HA Team Lead and his designated subject matter experts in debriefs held at the end of the HA Team's daily meetings (during the first two weeks of the observation period). At these debriefs, Independent Oversight staff also discussed the potential issues they identified regarding the HA Team's characterization and evaluation of specific event scenarios and the HA process improvements that the HA Team might consider. The cognizant ORP oversight staff member was present during HA Team meetings and the post-meeting debriefs. At the conclusion of its observation period, Independent Oversight was asked to provide an outbrief summarizing the strengths and weaknesses of BNI's HA activity for the LAW melter process system.

The principal Independent Oversight observations, including identified strengths and potential issues, are summarized in Section 4, and Section 5 summarizes Independent Oversight's conclusions. Also, based on the observations, Independent Oversight identified several opportunities for improvement for BNI to consider in developing HAs. These are presented in Section 6.

4.0 RESULTS

Strengths

BNI appropriately developed its Hazards Analysis Procedure and the supporting Hazards Analysis Handbook to implement the DOE requirements mentioned above. These documents appear generally consistent with DOE-STD-3009 and other DOE guidance on the subject.

The HA Team members collectively had expertise in the relevant disciplines. In particular, the team meetings always involved subject matter experts and knowledgeable representatives from plant engineering, melter design, operations, controls and engineering, and nuclear safety. The HA team members had been specifically trained on conducting HA before initiating this effort. The HA Team had access to reference documents, such as melter arrangement diagrams, piping and instrumentation diagrams, and selected system descriptions, analyses, and calculations. The HA Team discussions followed the agenda and daily schedule; they were always open and unhindered, and did not appear to be limited by schedule or time constraints. Any questions raised by team members were sufficiently discussed in the team meetings. Actions to follow up were identified and assigned, and their status was discussed at the beginning and end of each team meeting.

The HA Team qualitatively evaluated a broad spectrum of event scenarios that could result from failure of the LAW melter system equipment, personnel error, or equipment failures in systems evaluated earlier that could affect the melter. These failures had been identified on a spreadsheet through the What-If HA process. The grouping of the melter subsystems and components into four “nodes” (melter feed transfer, melter, melter riser and discharge, and melter plenum) provided the basis for a structured hazard evaluation. The systems interfacing with the melter were also considered.

The HA Team evaluated the postulated events in sequence, focusing the event discussions on each attribute of the evaluation process as specified on the HA spreadsheet, such as event description, causes, detection, likelihood, consequences, and candidate preventive and mitigative controls. The spreadsheet also included the Team’s record of important additional information, such as scenario and evaluation assumptions, and any notes applicable to HAs for other systems. The HA Team discussions often focused on considerations to better define a postulated scenario in order to evaluate its consequences. Screening logic for binning event frequencies and consequences appeared to be appropriately applied according to the BNI Hazards Analysis Handbook.

Independent Oversight judged that the HA Team’s approach to evaluating molten glass-water interactions was effective. It involved a methodical control volume approach and design diagram evaluation of vulnerabilities to the glass-water reaction hazard. Independent Oversight staff observed methodical identification of hazard sources and failure mechanisms, as well as barrier evaluation and identification of encroachments on design limits. The HA Team discussions included appropriate questioning and discussions of assumptions and conclusions. (The glass-water interaction analysis was incomplete when the Independent Oversight’s observation period concluded. Independent oversight recommends completion of this analysis prior to performing HAs for systems downstream of the melter.)

Weaknesses

Independent Oversight’s observations included potential issues concerning hazards that were identified by the HA Team but did not appear to be adequately evaluated, as well as hazards that were not identified. These observations often involve consideration of failure modes that could lead to different types of consequences or candidate controls. Of concern in these observations is not necessarily the degree of the hazards, but rather the possibility that the HA Team did not adequately explore or identify the hazards. Independent Oversight staff also developed observations on the HA implementation process, as used for this melter process system.

A. Hazards that were not adequately evaluated include:

1. **Water leakage into the space between the melter's refractory outer surfaces and the Inconel shell enclosure not fully considered**. Several potential failure mechanisms could cause cooling water piping or cooler leakage and resultant pressurization by steam or other mechanisms, such as hydrostatic pressure. Since the metal shells and the refractory are not designed as pressure vessels and would have very limited capabilities to withstand pressure – 10 in. water gauge (w.g.) design pressure – they could fail due to overpressure, thereby allowing gross glass out-leakage as well as air in-leakage during a design basis accident beyond the design capabilities of the melter structure and offgas exhaust rates. (The HA Team was reviewing these and other glass-water reactions at the end of Independent Oversight’s observation period.)

2. **Inadequate consideration of failure of the melter refractory in the plenum area and the resultant failure of the Inconel barrier.** The HA Team concluded that there would be no release from such an event until the offgas system could no longer maintain adequate vacuum due to the increasing size of the hole. However, if the melter gas barrier failure is too small to be detectable, a loss-of-power event, with the resultant reduction of capacity of the offgas system, could prevent maintaining the required vacuum on the melter and offgas systems and present an unacceptable

challenge to the offgas system's available capacity.

3. **Inadequate rationale for disposition of hazards associated with a melter Joule heating short circuit caused by molten glass leakage through the refractory.** The HA Team's conclusion that two separate refractory leak paths were required to cause an electrode short circuit, with no resulting concerns, did not clearly disposition the following possibilities: (1) that only one leak path could cause a short circuit to ground, particularly if molten glass contacted a component connected directly to ground, such as the cooler, and the possible resultant deleterious effects on the melter boundaries; (2) that the first short circuit might not be self-revealing; and (3) that an unidentified high resistance fault could operate under the set-point of the heater protection circuitry, allowing ongoing damage to the melter due to current flow and heating of a glass leakage stream in a short circuit path outside the refractory walls to the cooler system or melter structure.

4. **Lack of technical basis for a conservative assumption for the loss of electrode cooling event.** The evaluation of this event did not specifically identify whether electrical power would continue while an electrode melted. Selecting which potential path the event sequence may take could play a key role in identifying the needed controls. Further, the design margins associated with this event were not discussed. (This event was discussed in connection with the glass-water reaction at the close of Independent Oversight's observation period.)

5. **Insufficient basis for accepting "self-healing" to resolve concerns about refractory failures.** Refractory faults may tend to become progressively larger with age and normal wear, so the "self healing" of leaking glass (as the glass cools and its viscosity increases at the non-conductive isotherm) may become less and less effective or reliable as a leak-stopping mechanism. The HA Team did not discuss the expected age-related end-of-life failure when leaking glass might result in a substantial, unacceptable failure of the refractory and damage to the Inconel offgas barrier due to contact with the molten glass.

6. **Incomplete evaluation of the high melter temperature event.** In the evaluation of this event, the possible deleterious structural effects of this event on the outer melter structure itself were not systematically addressed by examining which components might be structurally most challenged or most degraded. Such an evaluation likely would identify the weak link(s) for this event and determine whether the limiting capabilities might be exceeded, which could lead to a loss of confinement. Although the evaluation addressed the potential for burn-through of the melter shell due to leakage of molten glass and concluded that such an event was not likely to cause burn-through, the evaluation did not consider the effects of very high localized temperatures in the shell and the resulting differential thermal stresses, which might be the "weak link" in the melter shell structure.

7. **Insufficient characterization of the vulnerability of cooling system components to glass leakage.** The HA Team based its evaluation of and conclusions about the significance of this vulnerability on an unverified assumption that glass would solidify on contact with the cooler surface. The Team did not explore or obtain a technical basis (e.g., heat balance) to determine whether the cooler would melt or go through functional or structural changes on contact with glass due to the high heat capacity of glass, electrical current flow due to short circuit, and/or other electrical or thermal effects of molten glass contact with the cooler.

8. **Inadequate identification of possible failure modes for the release of molten glass to threaten the integrity of the Inconel confinement shell.** The only mode of shell failure addressed was burn-through, which was qualitatively considered to be unlikely, though the mechanism was not discussed (implicit assumption was that conductive glass that was carrying current would not burn through the relatively thin shell, which provided a current path). However, another possible failure mode was not

considered: thermal stress and warping that could result in exceeding shell material allowable limits, leading to potential confinement failure.

9. **Inadequate analysis of the foaming event.** For the melter glass foaming event, the potential to challenge the melter's first design limit, pressure, was not identified. The HA Team identified that the glass foaming event might plug off or constrict offgas and other pressure relief pathways, thus allowing the melter pressure to rise, possibly causing the level of molten glass to increase in the pour riser to the point of spillover and inadvertent glass pour. However, the Team did not identify that the pressure necessary to cause such a level rise (nominally 6 in.) would require the melter plenum pressure to rise to about 14 in. w.g., which would exceed the 10 in. w.g. melter design pressure limit long before reaching the glass spillover pressure.

   Following Independent Oversight's discussion of this observation with the HA Team Lead and the ORP representative, the HA Team revisited the evaluation. Although the reconsideration addressed pressurization exceeding the melter design pressure and potential failure of the gas barrier, it did not address how such failure would adversely affect other melter components, such as the integrity of the outer melter shell (potentially exceeding design pressure) due to the physical connections between the shells. It also discounted degradation of the outer shell integrity due to spillage of molten glass into the annulus based on conclusion that the glass would not burn through the outer shell, as previously discussed. This reevaluation did not consider other possible failure modes, such as stresses and potential widening of the refractory gap due to pressurization in the internals induced by differential thermal expansion of melter components, as well as local effects in areas surrounding the molten glass.

10. **Lack of evaluation of flammability for all expected operating states.** The HA Team's evaluations did not fully address flammable or explosive gas generation or dilution. First, the Team did not recognize that dilution flow design was incomplete and the dilution air flow rates are unverified assumptions for hydrogen (H_2) mitigation (*Flowsheet Bases, Assumptions, and Requirements*, Assumption 2.13.1). Second, the Team did not address the normal higher temperature melter conditions relative to pyrolysis and nitrogen oxide (NOx) generation above 600º C coupled with excess water addition, bridged cap, and/or feed addition supplying H_2 (sugar and NOx scavenging hydroxide, thereby increasing H_2). The generation rates of H_2 and other flammable reactants at idle plenum temperature (about 1000º C) are much higher than at 600º C. A calculation (24590-LAW-RPT-M-09-001, Rev 0) was provided as the basis for concluding that no gasses would be released at flammable or auto-ignition threshold conditions, on melter leakage or failure, unless more than twice the sugar was added. However, the study did not involve data at temperatures over 661º C, and it also cautions that omitting the heterogeneous gas phase mixtures from calculations may result in unsafe lower flammability limit predictions, if the first explosion limit is the determining factor. This caution was provided without considering that the generation rates of reactants and H_2 could be considerably higher at the 1000º C idle temperature. The reference also acknowledges the lack of specific empirical evidence to validate the flammability of the offgas. The Team did not recognize that neither the process flowsheet nor the flammability calculations demonstrated control of explosives and flammables for certain potential gas mixtures and for the upper range of expected melter conditions.

11. **Inadequate consideration of unmitigated events.** Several high pressure events considered by the HA Team assumed the availability of C5V ventilation and the function of the 10 in. w.g. overpressure protection device. This assumption is contrary to the requirement to evaluate unmitigated events.

12. **Metallic oxides and metals at the bottom of melter robbing current from Joule heating**. This event was dismissed as an undetectable age-related failure. However, if undetected, it could cause

localized heating and allow local glass hotspots to amplify high local temperatures due to the higher glass conductivity at the higher temperature, imposing stresses on the melter structure. Subsequent glass leakage could result in a secondary, consequent failure mode.

13. **Canister match-up to the bellows assumed as "all or nothing."** The HA Team did not evaluate the possible hazards due to an alignment mismatch in which partial engagement would allow a canister to be hung, jammed or misaligned.

14. **Orifice effects to regulate pressure not evaluated.** A regulating orifice's function of managing dynamic flow and pressure could alter or fail when the orifice changes shape, is blocked, or when the fluid no longer flows at predicted rates. Such conditions were not reviewed where an orifice is present in a line to establish dynamic pressure control during normal gas flow or liquid flow, particularly in the melter system. For example, the pour equalizer line with associated orifice manages flow and pressure and provides a dynamic pressure balance in the melter during the pours, as well as when a canister is not engaged. Various conditions (e.g., blockage, orifice corroding away, or pressure excursion in the melter) could result in an inadvertent pour by changes in the assumed dynamic conditions, such as a change in pressure leading to unexpected, excessive, or inadequate glass pour flow.

15. **Concrete-glass reaction.** The HA did not address concrete-glass reactions that could result in toxins, hydrogen generation, or steam explosion effects of chemical reaction, as well as potential structural stress effects on concrete structures due to steam explosion, or explosive spalling by glass thermal mass. HA Team discussions identified that the pour cave concrete is covered with cooling panels and a steel floor plate, possibly precluding this interaction, but this potential hazards control function was not identified in the HA documentation.

16. **Hazards to workers associated with maintenance work on the melter lid not adequately evaluated.** The HA Team dismissed this hazard because the system would be ungrounded. However, if there were already an unrevealed electrical short, the maintenance worker on the lid would be the path to ground as the second short.

B. Hazards that were not identified include:

1. **Improper locking of melter wheels.** The HA Team did not address the potential to impose excessive structural stresses due to improper (or no) locking of melter wheels. As Independent Oversight staff understand from discussions with the HA Team Lead, only one or two wheels would be locked to meet thermal performance and structural requirements; however, seismic considerations require all wheels to be locked. The actual or expected wheel locking may also be a contradiction in the melter design assumptions. The team did not question the actual wheel lock design strategy.

2. **NOx flammability hazard.** The HA Team considered the NOx hazard only as a potential toxic release from the melter. Other potential hazards of NOx, such as flammability and flash point, were not mentioned, nor were the added flammability effects of increased partial pressures of CO and H_2 generated at the higher melter idle and operating temperatures. There is a potential for a flame front or conflagration initiating within, or when gas exits the system and contacts the richer oxygen environment in the presence of plenum gases or glass melt. Further discussions with subject matter experts resulted in acknowledgement of the potential for gaseous flame front or conflagration (deflagration) hazard. Additional impacts may include rapid contraction after flame-off, potentially causing further conflagration and pressure excursion, as well as a transient involving both high and low pressure post-event contraction, either within the melter or outside the melter plenum after breach

of the melter or increased air in-leakage.

3. **Pyrolysis and aggressive reactants.** The HA Team dismissed the H_2 auto-ignition reaction by stating that the plenum runs below 500º C. However, idle temperature in the plenum is up to 1000º C. H_2 is provided by water, whenever feed or other water source can flow. (See List A, Item 10, above.) Therefore, the HA did not address the potential for pyrolysis (or other aggressive reactions) under the expected high temperature conditions. The melter plenum conditions (idle or upset) support pyrolysis, resulting in free H_2 and O_2 along with the other reactive free radicals, NOx, CO, and energetics in the melter, available to contribute to deflagration reactions. No evaluation of flammability, deflagration, or detonation front pressures or temperatures was conducted with data over 661^o C, even though normal operation of the melter plenum may reach 1000^o C routinely at idle conditions.

4. **Electrical fields, voltages, currents, bonding, protection, and grounding for the melter.** The HA Team did not examine the electrical profile for electrical leakage, heating, or other effects and mechanisms that may present electrical vulnerabilities in a current-carrying liquid. The electrical vulnerabilities may include areas of high potential difference, glass-to-Inconel or glass-to-metal continuity points, pour cave metal dam grounding, brick-to-metal joints subject to heatup, and glass foam and leakage (such as pour stream or uncontrolled leakage) contact points. For example, the HA Team did not consider the possibility of the glass in the pour stream providing an electrical current path to the canister, causing an atypical electrical hazard that could cause failure or cause bias in indicators by changing ground potential.

5. **Asymmetric failure of bubblers.** The HA Team did not evaluate the possibility of bubblers failing in a way that selectively heats areas of the glass pool (e.g., all bubblers failing on one side, or one bubbler remaining working). The electrical heating effects of the glass induction heating on melter structure would be uneven due to non-homogenous glass thermal conductivity. Joule heating could occur through the portions of the melter with the hottest self-amplifying electrical current path, with the outer melter structure then subject to non-homogeneous thermal stresses. This asymmetric temperature profile could cause larger stresses than those assumed in the thermal and structural design of the melter shell.

6. **Knife edge function.** The HA Team neither explored the knife edge function, nor assumed its failure. Its function is to cut off the glass flow and prevent glass hair from building up and blocking canister removal. It appeared that the HA Team discussed the function of the knife edge air stream only in terms of cooling of the canister internals.

7. **Blocked drains in the annulus and air gap.** The HA did not consider the possibility of a drain blockage filling the annulus or air gap with water; this would be a latent failure mode contributing to a rapid steam expansion event since the refractory face would remain sufficiently cool only in the absence of glass leakage. Water buildup due to blocked drains could also carry current introduced by glass, adding energy to the mix.

8. **Material bursts from the upper internals of the melter.** Excessive pressure or pH shock could blow a local burst of radioactive material downstream. The HA did not evaluate or bound such an event, which could inadvertently actuate sensors or cause exposures.

9. **Raised elevator interlock logic.** A raised canister elevator gives a permissive to pour, on the assumption that a canister is in place. The HA Team discussed this gap in interlock logic but did not document it in the spreadsheet as an error trap or control logic gap.

10. **Electrical or galvanic corrosion effects on bi-metallic joints.** Since several items in the melter lid and structure (including controls and instrumentation) are bi-metallic connections, their relative electrical potentials are vulnerable to accelerated galvanic corrosion, particularly since heating results from electrical currents. These joints were not evaluated, nor were the bonding and grounding of the system.

11. **Potential for steam implosion because of steam occluding inlet air due to high steam volume generation rate in an idled plenum.** The HA did not consider the potential for rapid depressurization in such conditions as the following. Generation of steam at the typical end-of-heel rinse operation of the slurry tank, concurrent with other steam generation (e.g., from air film cooler steam cleaning), may be sufficient to take the place of the design non-condensable air inlet flow. The steam additions may provide volumetric steam generation that occludes air inlet flow due to steam formation and associated pressure generation in the melter. Melter documentation indicates that up to 10 gallons per minute (gpm) of liquid water could be added via the feed system. The normal feed input could be about 6 gpm (or more) water during the final feed vessel heel rinses. If liquid feed continues and allows water to enter a steam environment, the interaction could result in condensation and rapid depressurization due to absorption of the steam heat of vaporization.

12. **External effects on the melter system.** The nodes defined for the melter did not include the entire melter system, such as bi-metallic effects, thermal shock to the outside of the melter, and structural risks due to external effects (e.g., variable heating, water impingement, and explosion front from industrial events such as welder rig bottle gas explosion).

13. **Evaluation of component material performance.** The HA Team did not evaluate the performance of materials of components that would be exposed to the melter environment (gas or liquid) during the life of the melter. Some materials serve well in high temperature as long as pH limits are managed. Other materials serve well in caustic or acidic environments but do not tolerate high temperature. Also, as previously mentioned, materials consisting of bi-metallic connections may form galvanic cells and cause accelerated corrosion when exposed to the alternating current conditions of Joule heating. Independent Oversight did not observe any evaluation of the melter materials and their interactions with the various process fluids or each other, or any review of the electrical profile of the melter.

C. Hazards analysis process weaknesses include:

1. **Lack of examination of vulnerabilities associated with variations of physical phenomena through the range of expected melter conditions.** The HA Team generally did not examine, even on a qualitative level, the physical phenomena through the full range of expected melter conditions in order to identify and evaluate the potential vulnerabilities. Examples include: the melter glass foaming characterization, which is altered by several drivers, such as temperature profiles, varying reaction surface area, effects of included gasses, and other operational activities that could exacerbate foaming vulnerabilities (see List A, Item 9, above); the generation rates of flammable or explosive gas mixtures through the expected melter temperatures exceeding 1000^{o} C (see List A, Item 10, above); and the pressures and stresses on the melter structure, which vary with the head of liquid glass and other dynamic operating conditions. These are also examples of concerns demonstrating that consequences at the full expected ranges could involve non-linear changes in phenomena.

2. **Lack of checking assumptions and reference information.** The HA Team did not check the assumptions on which some of their key conclusions and inferences were based regarding melter conditions or events. These assumptions in relevant technical documents (e.g., *Flowsheet Bases, Assumptions, and Requirements*) may call into question whether the analysis on which the HA Team

rests its judgment adequately bounds the melter conditions for the scenario being evaluated, as well as whether design limits exist for a specific parameter. Examples include flammability analysis (see List A, Item 10 and List B, Item 3, above); and assumptions about structural performance (e.g., melter wheels locked or not; see List B, Item 1, above). Further, in evaluating certain potential events, reference to the values of controlling parameters (e.g., design limits, expected operational ranges of temperatures, gas dilution ratios, and feed flows) would have been of value in guiding the HA Team's judgments. While reference to both qualitative and quantitative technical information is consistent with DOE-STD-3009-94 guidance on conducting a largely qualitative evaluation, the HA Team discussions included only limited use of such technical bases.

3. **Inconsistency in event evaluations with respect to addressing unmitigated consequences.** On numerous occasions when addressing the consequences of events, various HA Team members asserted that there would be no consequences, because certain active systems or components would be in operation when the event started. Such assertions miss the key purpose of the HA, which is to analyze unmitigated events. For example, the HA Team implicitly assumed that a control would stop feed flow after a pressure excursion that exceeded the melter design pressure and that could cause structural failure and release of glass. The unmitigated accident would not have the feed flow stop. In many cases, lengthy, unfocused discussions ensued about whether or not certain preventive or mitigative features might have failed or not, coincident with various manifestations of the event. The questions and discussions on several specific What-If events indicated that the HA Team appeared to have difficulty in characterizing those events properly, and that additional direction and guidance could have been beneficial.

4. **Hazards identification list not used directly as input to the What-If evaluations.** The HA Team first generated a hazards identification list for the melter process system before performing the What-If evaluations. However, this list was not directly used as input to the What-If evaluations, with the intent that the Team would revisit the list later at the completion of the What-If evaluations. Typically, however, hazards identification not only precedes hazards evaluation, but it serves to provide initiation points for the evaluation. The essentially reverse method that was used in this case, which is explicitly recognized in BNI's Hazards Analysis Handbook for simpler HAs or for those performed early in the design process, assumes that the HA Team has a good knowledge of the hazards before performing the hazards identification. For the relatively complex melter process system, not using a thoroughly prepared hazards identification list as the basis for the What-If evaluations may have resulted in weaknesses of the HA in identifying and evaluating hazards. In all cases, iterations between the hazards identification and hazards evaluation phases are likely necessary to ensure completeness, as noted in the BNI Hazards Analysis Handbook. The HA Team Lead stated that an iteration was intended, but that there was no intent to cross-reference the results. (Independent Oversight staff did not observe the hazards identification checklist process or any iteration of the checklist with the What-If process.)

5. **Hazards not required to be explicitly documented on HA What-If spreadsheets.** Contrary to the example provided by DOE-STD-3009-94 in Table 3-1, *Example process hazard analysis worksheet*, the What-If spreadsheets used to guide the evaluations did not contain any heading or explicit instructions requiring identification of all of the hazards associated with each scenario. The HA Team Lead indicated that the Team intended to check the results of the What-If analysis on the spreadsheet against the Hazard Identification Checklist provided in Appendix A of the BNI Hazards Analysis Handbook to make sure that all of the hazards had been identified. However, since the spreadsheets did not specifically require such identification, this approach may not be optimal for ensuring the required systematic identification of all of the hazards.

6. **Lack of review of lessons learned.** The HA Team's evaluations did not appear to be augmented by a systematic review of lessons learned from the experience of other major melters to identify the causes of events and to evaluate the vulnerabilities of the LAW melter to those causes. The BNI Hazards Analysis Handbook (Section 3.2.1) explicitly calls out lessons learned as one element of data gathering to support hazard identification and evaluation. The Team generally was unaware of the DOE report, *Waste Vitrification Systems Lessons Learned*, which documents numerous types of events, causes, as well as corrective actions for several melters. The diverse examples of melter problems discussed in the report include cracks in the refractory, melt leakage, feed tube and discharge orifice clogging, and melter pressure excursions.

5.0 CONCLUSIONS

BNI had developed a sufficiently detailed plan for performing a system-by-system HA to meet the DOE requirements and guidance for developing the DSA for WTP's LBL facilities. BNI also developed a procedure and guidance for this effort and initiated concerted efforts toward completing the HAs. The HA for the LAW melter system is one of the early HAs for a WTP system of significant complexity, which was conducted following BNI's new HA procedure and guidance. The HA Team members represented appropriate disciplines, and the team meeting discussions appeared to be open and free from undue constraints.

In observing the melter system HA, the Independent Oversight staff identified several significant weaknesses in the HA Team's process for identifying and evaluating hazards, as summarized in Section 4 of this report. Independent Oversight recognizes that the HA Team's meetings and development of the HA spreadsheet for a particular system are an intermediate step (yet a key one) toward completing the HA report on which Chapter 3 of the DSA will be based. However, addressing the weaknesses presented here could increase the confidence that the hazards associated with the facility are systematically identified and evaluated, as required by DOE regulations and BNI's procedure.

Based on Independent Oversight's and other comments on the HA activities, BNI paused in conducting the HAs to improve its HA process. BNI is also considering revisions to the HA guidance documents and providing additional training for the professional staff conducting the HAs.

6. OPPORTUNITIES FOR IMPROVEMENT

This Independent Oversight review identified the following opportunities for improvement. These potential enhancements are not intended to be prescriptive or mandatory. Rather, they are offered to the site to be reviewed and evaluated by the responsible line management organizations and accepted, rejected, or modified, as appropriate, in accordance with site-specific program objectives and priorities.

1. Review and revise the melter system HA, as appropriate, specifically to address the hazards that may not have been identified or that were not adequately evaluated, as discussed in Section 4 (Lists A and B) of this report.

2. Correct the HA process and methodology deficiencies (Section 4, List C) that resulted in not identifying hazards comprehensively, or not adequately evaluating the identified hazards.

3. Review and correct, as appropriate, the other WTP HAs (completed or in progress) to ensure that hazards are comprehensively identified and adequately evaluated using the revised process and

methodology.

4. Improve various technical aspects of hazards evaluation by enhancing HA guidance to:
   - o Ensure that undetected or undetectable failures (including potential latent flaws) are considered together with initiating events in aggregate, as a single event, not as two (or multiple) independent events.
   - o Ensure that all credible failure modes are consistently identified and evaluated and that all potentially limiting event parameters (the "weak links") are identified and considered in all evaluations.
   - o Ensure that key event conditions are clearly identified to ensure a complete and thorough evaluation of the event and identification of the necessary controls.
   - o Provide more detailed HA guidance on the consideration of multiple and/or dependent failures (common cause and common mode system and component failures) that may be essential in evaluating unmitigated consequences (e.g., availability or unavailability of the melter offgas system, fans, etc.).
   - o In evaluating events, ensure that all of the various operational modes and conditions are considered in each case.
   - o Ensure that end-to-end event scenario and failure assumptions are considered, exploring not only the ends, but also the spectrum of conditions between the ends; for example, melter gas plenum temperatures up to normal idle temperature (1000º C), not just up to normal (500º C) operation; failure of several bubblers, not just the case where all bubblers fail; and partial attachment of the canister, not just the cases where the canister is fully attached or detached.
   - o Ensure that, in addition to the system nodes, the entire system for which an HA is being performed is evaluated for potential external effects and conditions; and that the performance of materials and their interactions with various process fluids or each other are also evaluated for the life of the system.
   - o Revise HA What-If spreadsheet format to explicitly require identification of the specific hazards associated with each event. Include form, type, location, magnitude, and supporting references, as required by the BNI procedure.
   - o Revise HA spreadsheet headings for the event description and consequences to explicitly indicate *unmitigated* events and consequences, in order to keep that requirement in the forefront of the HA Team's considerations.

5. Ensure that judgmental statements and assumptions are sufficiently challenged, and that there is sufficient technical basis and adequate rationale for conclusions on a given event scenario through the requisite spectrum of potential conditions. (See discussion of HA process weaknesses in Section 4, List C, Items 1 and 2.)

6. The HA Team members must be allowed adequate advance preparation for evaluating potential events associated with the subject system node, and the relevant technical basis information must be readily available and consulted to validate assumptions made during HA discussions.

7. Include a formal, detailed description of the scope and boundaries (not just a brief annotation) of each node of the system in the hazard evaluation documentation, and make it available as part of HA preparation.

8. To aid in identifying preventive and mitigative controls for complex event scenarios, consider laying out the possible stages of event progression to identify potential controls systematically at each event stage.

9. Use and consider, as appropriate, the system limitations and bounding requirements specifically called out in, *Flowsheet Bases, Assumptions, and Requirements*, Bechtel National, Inc., 24590-WTP-RPT-PT-02-005. (See discussion of HA process weaknesses in Section 4, List C, Item 2.)

10. Ensure that applicable lessons learned from other similar melter process systems are reviewed and taken into consideration. In particular, thoroughly and formally evaluate the DOE Report, *Waste Vitrification Systems Lessons Learned*, March 1999, and document how the problems, lessons learned, and conclusions/recommendations are being addressed for WTP.

11. Ensure that events identified during the HA discussions that represent significant programmatic project risks related to the mission (e.g., loss of the melter) and are thus required to be identified and managed by DOE Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, are flagged and tracked for appropriate review and follow-up through WTP's Risk Management Plan. Also, capture all aspects of the evaluation of such events that would be valuable in identifying the controls necessary for project risk management.

Appendix A
Supplemental Information

Dates of Review

Onsite Review: October 1-18, 2012

Office of Health, Safety and Security Management

Glenn S. Podonsky, Chief Health, Safety and Security Officer
William A. Eckroade, Principal Deputy Chief for Mission Support Operations
John S. Boulden III, Director, Office of Enforcement and Oversight
Thomas R. Staker, Deputy Director for Oversight
William E. Miller, Deputy Director, Office of Safety and Emergency Management Evaluations

Quality Review Board

William Eckroade
John Boulden
Thomas Staker
William Miller
Michael Kilpatrick
George Armstrong
Robert Nelson

Independent Oversight Site Lead

William E. Miller

Independent Oversight Reviewers

Shivaji Seth – Lead
Mary Miller
Donald Prevatte

Appendix B
Documents Reviewed and Observations

Documents Reviewed

- 24590-WTP-GPP-RANS-NS-0005, *Hazards Analysis Procedure*, Rev 0, July 24, 2012
- 24590-WTP-GPP-RANS-NS-0002, *Hazards Analysis Handbook*, Rev 0, July 24, 2012
- 24590-LAW-3YD-LMP-00001, *System Description for the System LMP Low Activity Waste Melter*, Rev. 003, April, 29, 2010
- 24590-LAW-3YD-LOP-00001, *System Description for the LAW Primary Offgas (LOP) and Secondary Offgas/Vessel Vent (LVP) Systems*, Rev. 3, July 27, 2010
- 24590-LAW-RPT-M-09-001, *LAW Melter Off-gas Data Summary for Flammable Species*, Rev. 0
- 24590-WTP-PSAR-ESH-01-002-01, *Preliminary Documented Safety Analysis to Support Construction Authorization; General Information*
- 24590-WTP-PSAR-ESH-01-002-03, *Preliminary Documented Safety Analysis to Support Construction Authorization; LAW Facility Specific Information*
- 11-WTP-470, *Proposed Changes to the Waste Treatment and Immobilization Plant (WTP) Regulatory Construct to Support Project Transition to Commissioning and Operations*, U.S. Department of Energy Letter to Mr. F.M. Russo, Project Director, Bechtel National, Inc., December 22, 2011
- 24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document Volume II*
- 24590-WTP-RPT-PT-02-005, *Flowsheet Bases, Assumptions, and Requirements,* Rev. 6, June 23, 2011
- *Waste Vitrification Systems Lessons Learned*, U.S. Department of Energy, March 1999
- Current Schedules for DSA and Hazards Analyses Development prepared by Bechtel National, Inc.
- LAW Melter Hazards Analysis, Meeting Handout, 2 pages, (provides brief overview, including scope, boundary of analysis, and a list of the nodes of analysis)
- Low Activity Waste Facility Melter Hazards Analysis Agenda (Daily)

Observations

- LAW Melter System HA Team Daily Meetings and Debriefs with the HA Team Lead
- LAW Facility Field Walkdown