HSS Independent Activity Report - Rev. 0	Report Number: HIAR-WTP-2013-05-13
Site: Hanford Site	Subject: Office of Enforcement and Oversight's Office of Safety and Emergency Management Evaluations Activity Report for Waste Treatment and Immobilization Plant Low Activity Waste Melter Off-gas Process System Hazards Analysis Activity Observation

Dates of Activity :	05/13/13 thru 06/28/13	Report Preparer:	James O. Low

Activity Description/Purpose:
The Office of Health, Safety and Security (HSS) staff observed a limited portion of the start of the hazard analysis (HA) for the Waste Treatment and Immobilization Plant (WTP) Low Activity Waste (LAW) Primary Off-gas System (LOP). The primary purpose of this HSS field activity was to observe and understand the revised HA approach implemented by Bechtel National, Inc. (BNI), the contractor responsible for the design and construction of WTP for the U.S. Department of Energy (DOE) Office of River Protection (ORP). A secondary purpose was to understand the design and potential failure modes of the LAW melter process (LMP) and associated off-gas systems.

BNI has committed to conduct system-by-system HAs as part of developing the documented safety analysis (DSA) for the WTP LAW, Balance of Facility, and Analytical Laboratory nuclear facilities (collectively known as "LBL") in accordance with DOE-STD-3009-94. This HSS field activity is part of a planned multi-phase review (Ref. 1) that will focus on the technical adequacy of BNI-issued LAW HA reports (used as inputs for the LAW DSA) and subsequent submittal of the LAW DSA and technical safety requirements for ORP review and approval.

Previously, HSS observed the initial LMP HA in October 2012, which was based on the "What-If" analysis technique (Ref. 3) and also conducted a limited observation (Ref. 2) of BNI's LMP HA resumption (in March 2013), which introduced the Hazards and Operability (HAZOP) analysis technique to preparing the HA for relatively complex LBL systems. The LMP HA was suspended by BNI on May 6, 2013, to allow for startup of the LOP HA on May 13, 2013. The suspension of the LMP HA limited the ability of the HSS team to follow-up on BNI disposition of HSS-identified deficiencies (Ref. 3) in the initial LMP HA.

In accordance with the procedures, the HAZOP process was executed by a chartered Safety Design Integration Team (SDIT), which was led by the SDIT Chair. (Note: In previous HSS reports, the SDIT was referred to as the HA Team and the SDIT Chair was referred to as the HA Team Leader.) The team consisted of core team members from Nuclear Safety (chair, scribes), and subject matter experts (SME) from Production Engineering, Plant Engineering, and Operations. The team was supplemented by other SMEs, including an engineer from Controls and Instrumentation (C&I) and Nuclear Safety personnel as available.

Generally, the initial HAZOP process being executed by the SDIT followed the sequence below:

- Complete initial activities, including discussions of the system scope, review of the three-dimensional model of the facility, review of the system flowsheet and consequence estimates for potential hazardous material releases, and a facility walk down.
- Review, revise, and complete the hazard identification checklist.
- Select applicable guidewords and deviations to develop HAZOP matrix tables for the system subnode being evaluated.
- Brainstorm possible events (deviations from normal operations that result in consequences) for analysis.
- Document the identified hazardous event as Insight software event records.

Following the initial process and identification of possible events, the majority of the SDIT effort was directed toward completion of the Insight software event records for the possible events identified in the HAZOP matrix table for the subnode.

The HSS team observed the initial startup activities, hazard identification, development of the subnode HAZOP matrix tables, and HAZOP analyses by the LOP SDIT for subnode 1a (LOP film cooler) and 1b (LOP submerged bed scrubber, or SBS). The HAZOP identified LOP system process upsets in components, such as the film cooler and SBS, and hazardous events that could lead to one or more of the pre-defined types of undesirable consequences (e.g., uncontrolled release of radiological or hazardous materials). The subsequent process focused on describing the identified hazard events and characterizing the event parameters, such as causes, likelihood, consequences, methods of detection, and candidate (preventive and mitigative) controls necessary to complete the Insight event record.

BNI planned to complete the HA for both LOP and Secondary Off-gas/Vessel Vent (LVP) systems in 18 working days

(ending June 6, 2013) using the HAZOP technique. However, due to slower than expected progress, only one subnode was substantially completed (subnode 1a – film cooler) during the observation period. Subnode 1b (SBS) was partially completed to the extent that process deviations related to pressure, flow, and temperature parameters were analyzed. Additional time for HSS observation was added during the period in an effort for the HSS team to observe all salient parts of BNI HA protocols being executed.

At the conclusion of the HSS observation period (June 28, 2013), 13 subnodes comprising the balance of the LOP and LVP systems remained to be analyzed; BNI estimated the LOP HA activity was 15% complete. Due to time limitations, the HSS team was unable to observe the process for identification of candidate design basis accidents and beyond design basis accidents. The HSS team also did not observe the implementation of the cross-check of consistency between the hazard identification checklist and Insight event records. Given the limited activities observed for only the major portions of two subnodes of the technically complex LOP/LVP systems, this HSS observation constituted a narrow sample of a complex, lengthy HA process.

Result:
Summarized below are the preliminary observations on BNI's implementation of the revised HA methodology (HAZOP) for the LOP HA. These are based substantially on the observation of one SDIT's HA activity primarily led by a single Chair, although the HSS team did conduct brief observations of another HA by a second SDIT under the leadership of a different Chair.

Overall, the BNI procedure, handbook, and guide provide a systematic, comprehensive approach to the execution of the HA process, including detailed instructions for completing the Insight software event records. At the start of the HSS observation, the guidance included both an HA handbook and desk instruction. During the observation period, BNI implemented a number of changes to the procedure and handbook, including incorporation of the desk instruction into the handbook. The guidance also included an Insight software user's guide and an extensive hazard identification checklist form with accompanying instructions (which was not utilized for LOP). The guidance did not include detailed steps for performing the HAZOP process, allowing the SDIT Chair latitude in conducting this portion of the analysis.

For hazard identification analysis observed by the HSS team, the SDIT identified appropriate hazards associated with the LOP system subnodes and included them in the hazard evaluation. The HSS team did not identify additional hazards that would need to be developed into a new hazard event record. The radiological and hazardous material at risk and worker consequence information was sufficient to start the HA and appeared to be appropriately conservative. However, some of the qualitative consequence estimations were not always supported by reports or analyses that could be referenced as a defensible technical basis. The HSS team noted that BNI technical organizations were developing analyses needed to provide a technical basis for the consequence estimates.

Considering that the LOP system HA is BNI's second application of the HAZOP technique for developing the DSA for LBL facilities, this technique presents several challenges. The challenges to applying the revised HA methodology include the following:

- BNI expectations for executing the HAZOP process allow significant variation in application by the SDIT Chairs. For example, wide variation exists among the SDIT Chairs in the use of piping and instrumentation diagrams (P&IDs) and in the level of systematic analysis when identifying the specific deviation being analyzed. In fact, this concern was recognized to some extent by BNI toward the end of the HSS observation period. The HSS team observed the BNI HA process leader providing additional technical clarification to the SDIT Chairs on HA methods for conducting unmitigated HA (i.e., requirements to define physically meaningful scenarios), as well as the need to analyze abnormal events that are not necessarily bounding.
- Over the course of the observation period, BNI's use of the HAZOP process improved, including better engagement of the SDIT members in the discussion of events, individual and team use of drawings and sketches, and use of references. When the LOP SDIT used P&IDs, the SDIT discussion was generally well focused and guided, and event record documentation proceeded efficiently. The HSS team noted that this practice became more frequent over the observation period. However, the LOP SDIT generally did not use P&IDs collectively (e.g., projecting the P&ID or sketch on the wall for the SDIT to use during discussion) to promote common understanding of the hazard event's initial conditions and the subsequent hazard event progression. Likewise, contrary to typical HAZOP practice, the LOP SDIT Chair did not always establish the safety function, operating condition, and analysis boundary of the subnode being analyzed before commencing the hazard event analysis.
- DOE-STD-3009 guidance on hazards analysis calls for consideration of all modes of operations (e.g., startup, shutdown, maintenance). Operating modes have been identified and documented for LMP SDIT analysis of the melter; however,

the HSS team did not observe identification of operating modes by the LOP SDIT.

- While the SDIT Chairs have varying levels of experience with the HAZOP process, the core team members participating in the various SDITs have very limited training in this technique. The HSS team previously noted and communicated this observation regarding the adequacy of SDIT training and experience in its observations of the LMP HA in March 2013 (Ref. 2). Recognition of the need for training on the HAZOP process is evolving, and LOP SDIT performance may be improved by a 4-day HAZOP methodology class scheduled for initial delivery in July 2013. BNI management was open to further changes to their HA handbook guidance that may result from the HAZOP training class. The HSS team also noted that the BNI Safety Analysis Manager is developing an SDIT Chair qualification standard (i.e., Master Task List) to better define the leadership and facilitation tasks needed for facilitating SDITs.
- The HA analysis process used by the LOP SDIT focused on development of unmitigated hazard scenarios, which emphasize worst case hazard events. The resulting candidate control sets for the hazard events appear to be skewed toward mitigative rather than preventive controls based on the assumed failures of multiple system components. This practice may complicate later LOP SDIT activities to effectively identify the controls that are closest to the hazard event cause and thus more effective.
- Availability of full-time support by a C&I engineer increased the LOP SDIT's understanding of Integrated Control Network (ICN) and Programmable Protection System (PPJ) functions and enhanced the transparency of the resulting hazard event records. However, the lack of full-time support from the chemical process engineering SME inhibited the SDIT from arriving at clear conclusions regarding all of the potentially hazardous events (with consequences and candidate controls) involving off-gas flammability and off-gas explosion hazards.
- Use of the Insight software tool provided form and structure to the HA process. Insight software is generally an effective tool that contributes to thoroughness and consistency of hazard event analysis and documentation. For example, Insight software provides the ability to develop and use libraries of causes and potential candidate controls from which the SDIT may pick. It also allows the copying of similar hazard events to support efficient analysis of new events. However, the HSS team observed some potential limitations with the use of the tool.
  - In some instances, over attention by the LOP SDIT to completing Insight software hazard event records (attention to the wording) diverted the attention of the team from fully clarifying the sequential hazard event progression and causes.
  - The sequence of hazard event progression is not a required input for the Insight software tool, which may lead to subsequent omission of interconnections with candidate controls.
  - The format of the Insight software cause and control sections in the hazard event record allows multiple causes to be entered. For event records with multiple causes, there is no clear relationship between a candidate control and the cause it is intended to address, which could lead to some difficulty for subsequent reviewers to understand the logic for candidate controls documented by the LOP SDIT.
  - Documentation of the specific system damage mechanism or failure modes/locations is not required by Insight software. Consequently, some hazard event record descriptions are not clear with respect to the specific failure mode or physical failure locations of structures, systems, and components (SSCs), as the LOP SDIT tended to default to simply listing "failure" of an SSC.
  - The hazard event analysis, as documented in Insight, identified unmitigated system effects (USE) (i.e., effects in the HA analysis node that can affect other SSCs that are outside the LOP HA analysis scope). However, the process for tracking the handoff of the LOP's SDIT-derived USEs to other affected SDITs is unclear at this point in the process and was not observed.
- Hazards were analyzed based on unmitigated hazard event sequences, which led the LOP SDIT to identify generally reasonable sets of causes and candidate controls using this worst case analysis approach. However, the HSS team identified the following potential concerns with the interim results of the analysis. The exceptions are identified as potential concerns since the analysis process is incomplete until the HA reports are completed, internally reviewed, approved by BNI, and thus ready for DOE review. Nonetheless, the potential concerns could lead to weaknesses in the final HA reports. These potential concerns involve event records with unmitigated high consequences to the facility worker or collocated worker.
  - Potential Concern 1: Non-mechanistic failures were assumed for several hazard events such that the described sequence of events did not lead directly to the identified cause. An unclear sequence description may adversely impact subsequent identification of candidate controls.

    For example, the event description for event record LOP01A-3-001 (primary guideword pair of Off-gas Flow/Unbalanced) postulates an event sequence in which "low or no flow of Plant Service Air (PSA) would insufficiently cool the offgas resulting in a thermal failure of the film cooler or associated piping resulting in a

release of radioactive and chemically hazardous material (offgas). Failure of the film cooler or associated piping on the first melter train overwhelms the primary offgas system on the second melter train (starves the second melter), causing loss of depression and offgas release from the second melter." The event description is unclear as to the severity and type of the failure that would lead to the postulated release of nitrogen oxides, although an implicit assumption is complete (or nearly complete) severing of the film cooler or piping, such that the exhausters are unable to maintain offgas vacuum/flow. This failure mechanism appears to be incredible, based on off-gas temperatures and materials of design. In addition, the event description does not describe the sequence of failures in the PSA system (and lack of response) that lead to the over-temperature condition or the sequence of events leading to the failure of the second melter.

- Potential Concern 2: Multiple event sequences and release locations were combined in several hazard events. Different event sequences and different locations may require different candidate controls.

  For example, the event description for event record LOP01A-3-005 (Off-gas Pressure/High) postulates that the "film cooler or associated piping to the SBS plugs resulting in a release of radioactive and chemically hazardous material (offgas) due to pressurization and failure." The record identifies the melter gallery and the process cell as the affected locations, but the described event sequence, which combines several potential event sequences, does not specify whether the locations are or can be affected simultaneously. Different postulated sequences, depending on the plug location, lead to releases in different locations, and different controls may apply. If the blockage of both film coolers occurs internal to the melter, then the event could result in an internal melter pressurization event. Blockage in the SBS downcomer (which is part of subnode 1a) could challenge the melter overpressure protection controls in the subnode, leading to a different sequence of events and a different set of controls. Also, a postulated release in the melter gallery, which is normally unoccupied during operation, is likely to have a different set of candidate controls than a release in the process cell.

- Potential Concern 3: The development and documentation of the HAZOP matrix table for the subnode 1a (film cooler) was not performed in sufficient detail to lead to full analysis of all process parameter deviations that could potentially affect the off-gas system performance.

  For example, in analyzing subnode 1a (film cooler), the SDIT did not systematically use the P&ID to identify potential deviations in the operating conditions within the subnode. The SDIT did not address failures of the differential pressure detector (second plenum probe PDT-1411), which is connected to the standby film cooler through an instrument line and flexible hose. The failure of the hose will result in a false high differential pressure indication to the melter off-gas control system, and the SDIT did not evaluate the sequence of events and consequences of this false indication. Similarly, potential failures of the PSA control air valves PV-1105 or PV-2205 (e.g., failing closed) and the resulting consequences were not analyzed.

- Potential Concern 4: Some hazard events did not identify all of the related causes, and the hazard events did not always have a clear relationship between identified causes and subsequent candidate controls.

  For example, LOP01-1-001 (Off-gas Composition/Flammability) postulates "melter off-gas compositions at lower flammability limit result in fire within the film cooler and piping, resulting in high temperature failure of the piping and a release of radioactive and chemically hazardous material." In analyzing the hazard event, the SDIT identified "equipment failure - loss of dilution air" and "process failure - excess batch organics" as the causes. This list of causes for an off-gas fire in the LOP system omitted some possible causes that could lead to a greater than 25% composite lower flammability limit condition in the LOP system. Additional causes include: (1) over-addition of water (which lowers combustion temperature, creates additional nitrogen oxides, reduces air inflow, and causes off-gas surges); (2) excessive rate of addition of feed (sucrose included); and (3) reduction of dilution air (different event from the air system failure as recorded in the event record) as potential causes. These causes could lead to the need for additional candidate controls. This event record also identified the ICN film cooler high temperature alarm as a method of detection, without identifying an associated candidate preventative control.

Additional examples related to the potential concerns were informally transmitted (e-mail dated July 8, 2013) to the ORP Safety Basis Review Team Leader for his use.

HSS Participants	References
1.lead) James O. Low	1. – DOE/HQ HS-45, Plan for the Independent Oversight Review of the Hanford Site Waste

	Treatment Plant Low Activity Waste Facility Documented Safety Analysis Development, April 22, 2013.
2.David Odland	2 – DOE/HQ HS-45 Report Number: HIAR-WTP-2013-03-18, Activity Report for Follow-up of Waste Treatment and Immobilization Plant Low Activity Waste Melter Process System Hazard Analysis Activity Review.
3.Mary Miller	3 – DOE/HQ HS-40 Letter, JS Boulden III to SL Samuelson, *Independent Oversight Review of the Hanford Site Waste Treatment & Immobilization Plant Low Activity Waste Melter Process System Hazard Analysis Activity*, dated December 21, 2012.

Were there any items for HSS follow up? ☒Yes ☐No

HSS Follow Up Items

1. When available, review BNI actions in response to the observations and potential concerns identified in this and the previous reports related to LAW HAs.
2. When issued, review the Insight software documentation generated for the LAW melter and off-gas systems.
3. Conduct independent review of the draft and final Hazard Analysis Report (HAR) appendices for the LMP, LOP, and LVP systems for the disposition of the potential concerns and other identified deficiencies, as well as overall conformance to DOE-STD-3009 requirements.
4. Perform focused observations of HA development that directly affects LMP and LOP performance, e.g., LAW ICN/PPJ systems and LAW facility (natural phenomena hazards and facility-based HA). These observations may lead to additional independent reviews of HAR appendices for these systems.
5. Perform focused observations of BNI control selection team processes for the above specified systems.