CONF-960282--1

LA-UR-96- 0428

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: Use of Hazard Assessments to Support Risk-Based Decision Making in the US Department of Energy Stockpile Stewardship (SS-21) Program

AUTHOR(S): Stewart R. Fischer
Herbert Konkel
Mark Rainbolt

SUBMITTED TO: Symposium on Risk Management
February 27-28, 1996
New Orleans, Louisiana

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Title: Use of Hazard Assessments to Support Risk-Based Decision Making in the US Department of Energy Stockpile Stewardship (SS-21) Program

Authors: Stewart R. Fischer, Herb Konkel, and Mark Rainbolt

Prepared for presentation at the Risk Management Symposium; Risk Management and Decision Making (Session 14)

Date: January 1995

UNPUBLISHED

DISCLAIMER

Use of Hazard Assessments to Support Risk-Based Decision Making in the US Department of Energy Stockpile Stewardship (SS-21) Program

by

Stewart R. Fischer, Herb Konkel, and Mark Rainbolt
Probabilistic Risk & Hazard Analysis Group
Weapon Engineering Group
Los Alamos National Laboratory

ABSTRACT

This paper summarizes the nuclear explosive hazard assessment activities performed to support the US Department of Energy (DOE) Stockpile Stewardship (SS-21) Integrated Safety or "Seamless Safety" program. Past practice within the DOE Complex dictated the use of a significant number of post-design/fabrication safety reviews to analyze the safety associated with operations on nuclear explosives and to answer safety questions. These practices have focused on reviewing-in or auditing-in safety vs incorporating safety in the design process. SS-21 was proposed by the DOE as an avenue to develop a program to "integrate established, recognized, verifiable safety criteria into the process at the design stage rather than continuing the reliance on reviews, evaluations and audits." The cornerstone of the SS-21 design process is the hazard assessment, which is performed concurrently with process and tooling design. The hazard assessment is used as the key management tool to guide overall risk management associated with the nuclear explosive activity through supporting risk-based decisions made with respect to process design.

INTRODUCTION

In response to considerable criticism from the Defense Nuclear Facility Safety Board (DNFSB) regarding its Nuclear Explosive Safety Study (NESS) process and in recognition of the large uncertainty in the response of high explosives (HE) to various insults, the US Department of Energy (DOE) initiated the Seamless Safety "SS-21," or Integrated Safety Process, program to design safety into a nuclear explosive operation. In December 1993, the DOE formally initiated the SS-21 program; a demonstration project was started, based on the B61-0 Center Case Disassembly, to demonstrate, in part, the feasibility of performing concurrent hazard assessments (HAs) as part of an engineering design and development

effort and then to evaluate the use of the hazard assessment to guide risk-based process design changes and to provide an indication of the risk reduction or gain in safety achieved.

The goal of the SS-21 program is to "integrate established, recognized, verifiable safety criteria into the process at the design stage rather than continuing the reliance on reviews, evaluations and audits." As part of the SS-21 process, HAs are performed concurrently with process design and development to identify dominant hazards and focus risk-reduction efforts.

The effectiveness of the SS-21 process was demonstrated recently through the conduct of HAs for both the W69 and B61-0 Center Case Section disassembly processes as documented by Fischer.[1-3] Concurrent HAs were performed during process design and development to identify hazards and direct risk-reduction initiatives. These HAs also were used to identify and document weapon- and process-specific hazards and safety-critical operating steps. Both HAs focused on identifying accidents that had the potential for worker injury, public health impact, facility damage, toxic gas release, and dispersal of radioactive materials. A comparison of the old, or baseline, and new, or SS-21, process risks provided a semi-quantitative estimate of the risk reduction gained via the SS-21 or Integrated Safety Process.

CHARACTERISTICS OF NUCLEAR EXPLOSIVE OPERATIONS

Nuclear explosive operations that are carried out under US DOE purview can be characterized as being dominated by "hands-on" activities. The types of operations performed at the Pantex Plant or at the Nevada Test Site primarily involve manual tasks. These tasks are generally relatively simple, but their successful completion depends on human performance. Few credible accident sequences involve complex multiple failure events. The production workers are the principal population at risk for most credible accident sequences (excluding inadvertent nuclear detonation). All process activities are governed by procedural and administrative controls, and the use of energy sources within the process facilities that could interact with the nuclear explosive are severely restricted. The risk associated with nuclear explosive process-related hazards is clearly dominated by human performance. As a result of the importance of human behavior in nuclear explosive operations, DOE orders require that considerable

attention be paid to training, personnel assurance programs, procedure development, and incorporating human reliability into HAs.

SUMMARY OF THE INTEGRATED SAFETY PROCESS PER EP401110/A

Before the SS-21 program was implemented, nuclear explosive process design and development were design- and schedule-driven, and any risk assessments, if performed, were done after the process was complete. Process reviews conducted by the DOE focused on nuclear detonation and did not address worker risk or plutonium dispersal. As part of the SS-21 Demonstration Project, a joint effort was undertaken by the primary weapons laboratories to develop procedural guidance in the form of an Interagency Engineering Procedure, "EP401110/A—Integrated Safety Process for Assembly and Disassembly of Nuclear Weapons," to address the DOE requirement that a formal process be developed to ensure that only efficient, effective, and safe nuclear weapon assembly and disassembly operations are used. This acceptable process

- addresses established, verifiable "safety criteria;"
- ensures a complete integration of weapon, personnel, operating procedure, operating facility, equipment and layout, and tooling to form a safe, efficient, and effective operating environment;
- is jointly developed by and concurred with the responsible design agencies and the Pantex Plant; and
- is subjected to formal HAs performed concurrently with process development and resulting in a final Hazard Assessment Report (HAR).

The process HAR coupled with the facility Safety Analysis Report (SAR) and other key documents defines the safe operating envelope and establishes the design basis for a particular nuclear explosive operation.

The Safety Criteria have several purposes.

1. Prevent the application of unauthorized and unanalyzed energy from sources external to the nuclear weapon, or any component of a nuclear weapon, to prevent the release of energy from sources internal to the nuclear weapon. Energy sources include but are not limited to
   a. mechanical energy,
   b. electrical energy,
   c. thermal energy,
   d. electro-mechanical energy, and
   e. potential/kinetic energy (e.g., lifting, transportation, etc.).
2. Allow no single-point failure in an operation that could cause
   a. energy sources within the weapon, including self-contained energy sources, to be activated or released;
   b. radioactive exposure or contamination above thresholds set in the operating procedures;
   c. injury to personnel, the environment, or the public; and
   d. loss of facility operability.
3. Mitigate personnel exposure to radiation and hazardous substances to "As Low As Reasonably Achievable" (ALARA) levels. Levels include, but are not limited to
   a. less than 500 mrem (neutron quality factor of 20) per worker-year as a goal,
   b. OSHA limits, and
   c. those required by specific programs.

The overall philosophy of the SS-21 process is to achieve the highest level of safety and to provide defense in depth. The purpose of the SS-21 process is to produce safe, efficient, and effective operations that are driven by design not by review. The principle of defense in depth includes such items as

- using conservative design margins and quality assurance;
- designing processes to eliminate accident scenarios;
- using configuration management across the board;
- ensuring the use of highly trained and qualified personnel;
- ensuring facility and operational readiness;
- using controlled, conservatively developed, and tested procedures; and
- using safety analysis to evaluate the entire process

At the highest level, all DOE nuclear explosive operations must meet qualitative safety standards to prevent unintended nuclear detonation, fissile material dispersal, or loss of control. These standards require positive measures to minimize

- the possibility of accidents, inadvertent acts, or authorized activities that could lead to fire, HE deflagration, or unintended HE detonation;
- the possibility of fire, HE deflagration, or HE detonation given accidents or inadvertent acts; and
- the possibility of deliberate unauthorized acts that could lead to HE deflagration or HE detonation.

PURPOSE AND SCOPE OF THE EP401110/A HAZARD ASSESSMENT

The scope of the HA conducted in support of the SS-21 program, as delineated in EP401110/A, addresses the requirements in DOE Albuquerque Supplemental Directive 5610.11A, which directs that the HA must address all aspects of worker and public safety and environmental protection. The HA, which addresses all nuclear explosive operations and associated activities, must identify all hazards using a step-by-step review of the entire operation. Human reliability and human factors analyses are performed and should be used to determine accident-sequence likelihoods. For accident sequences resulting in high consequence (HE detonation, HE deflagration, nuclear detonation, and fire), the likelihood assessment should be detailed and thorough. For the high-consequence accident sequences, sufficient analytic detail, including uncertainty analyses, must be provided. The HA must identify and

categorize safety-significant or safety-class systems, structures, and components and identify operational safety controls. Finally, accident sequences deemed to be credible must be compared with the facility SAR to demonstrate that the SAR design-basis accidents are bounding.

The HA provides the basis for the HAR as well as for the Nuclear Explosive Hazard Assessment (NEHA). The NEHA focuses on the high-consequence accident sequences and is provided to the DOE Nuclear Explosive Safety Study Group (NESSG) during their review and scrutiny of the proposed process. The HA identifies the dominant accident sequences for a wide range of accident types. The identified accident sequences can be ranked by importance and reviewed by the NESSG to determine the acceptability of the process. The HAR establishes the bases for administrative controls and for the identification of positive measures. The HAR also is used to support the identification of safety-critical tooling and procedure steps as discussed in Fischer.[1] The HAR, of the which the NEHA is a subset, provides a thoroughly documented safety basis for the specific nuclear explosive operation and thus can be used to support change control activities. That is, the HAR can be maintained as a "living document" to support the evaluation of future changes and risk-reduction measures.

EP401110/A HAZARD ASSESSMENT ACTIVITIES

As directed in the engineering procedure, SS-21 Process is managed by a Project Team that in turn establishes various task teams to conduct the process design and development activities as shown in Fig 1. Figure 1 shows a typical SS-21 Project Management organization for a Los Alamos process with the HA Team broken out in detail. Task teams include Tooling, Facility, Procedures, Layout, Personnel, and Hazard Assessment Teams that are composed of knowledgeable representatives from Pantex and the design laboratories. As delineated in the engineering procedure and as shown in Fig. 2, the SS-21 Process involves seven phases or steps: a Tasking Phase, a Project Planning Phase, a Criteria Development Phase, a Concepts Development Phase, a Design Development Phase, an Implementation and Verification Phase, and a Readiness Phase. As shown in Fig. 2, the SS-21 Process requires that HAs be performed concurrent with the Concepts Development, Design Development, and Implementation and Verification

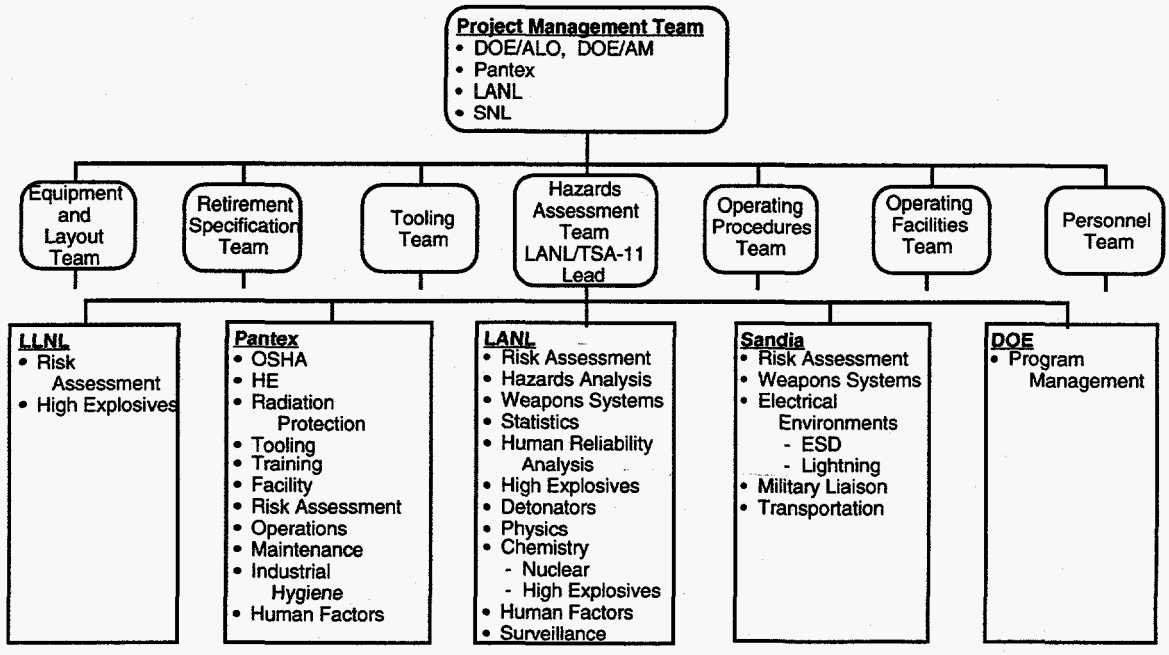

Fig. 1. Integrated Safety Program project team organization.

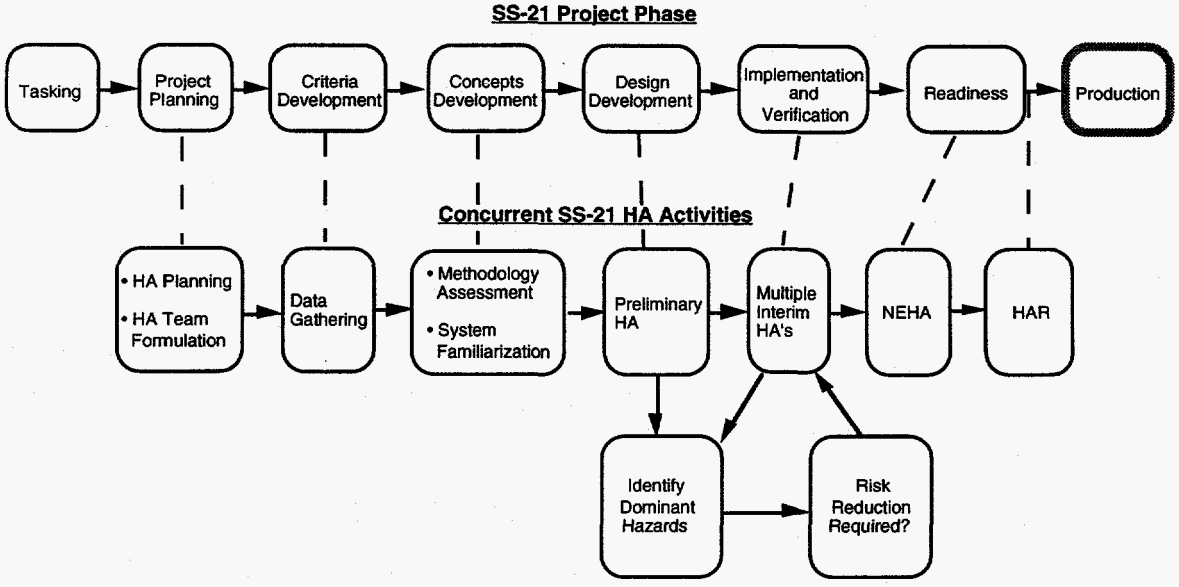

Fig. 2. Integrated safety process HA activities.

Phases. A preliminary HA is conducted for the Design Development Phase. Interim HAs are performed in support of the Implementation and Verification Phase. A final HA is conducted and documented in a HAR after the Implementation & Verification Phase. As mentioned previously, the HAR is maintained as a living document for use in the change control process. In particular, changes to the approved operating procedures must be evaluated using the HAR.

During the Criteria Development and Concepts Development phases, the HA Task Team evaluates the weapon design, the baseline process flow, and the operating facilities and, based on these evaluations, formulates an analysis plan and identifies the techniques they expect to use in HA. The team seeks out weapon requirements data, operational requirements data, facility safety documents, and subject matter experts. The task team identifies and communicates requirements for walk-throughs and videotaping sessions.

During the Design Development Phase, HA Task Team performs a Preliminary Hazard Assessment to identify risks that are independent of the details of the assembly or disassembly operation. For example, areas of concern include but are not limited to weapon-specific safety attributes (e.g., hydrogen buildup), facility-induced hazards (e.g., crane failure during lift), external events (e.g., facility response to seismic events), and the relative risk importance of different types of assembly or disassembly process activities (e.g., vacuum fixture lifting of HE). The task team provides documentation of their findings, both positive and negative, with suggestions for risk reduction as an initial input to all task teams participating in the Design Development Phase.

During the Design Development and Implementation and Verification Phases, HA Task Team performs multiple HAs of the process as it stands at various stages of the development based on walk-throughs and discussions with production technicians and engineers. The task team provides documentation of their findings, both positive and negative, with suggestions for risk reduction as input to all task teams participating in the Implementation and Verification Phase. The Task Teams and Project Team evaluate the identified dominant accident sequences and evaluate the need for further risk-reduction measures.

After the Implementation and Verification Phase and before the Readiness Phase, HA Task Team prepares a draft listing of process hazards or potential accident scenarios to guide readiness review activities. A formal HAR is prepared after the NESS study is complete to reflect the hazards based on the process used for the "pilot" lot. The HAR documents the weapon-specific hazards and clearly identifies safety-critical operating steps. The HAR also identifies existing and new hazards for the facility and ranks the risks involved for the entire weapon-specific operation at the Pantex Plant under normal environment conditions.

EP401110/A Hazard Assessment Methodology

As shown in Fig. 2, the HA Task Team conducts HAs at multiple steps in the SS-21 process to identify dominant accident sequences and to identify weapon-specific hazards for given operations. The HAs are performed concurrently with Operating Procedure, Operating Facility, Equipment and Layout, and Tooling design and development Task Team activities. Per engineering procedure guidance the HA, as a minimum, consists of the following tasks.

A. **Data Gathering.** Review of all applicable safety, design, and test documents, facility SAR and National Environmental Protection Act documentation; review of applicable Nuclear Explosive Operating Procedures (NEOPs); process observations at Pantex; and technical exchanges.

B. **Hazards Assessments.** Perform operational analysis and scenario development as follows.

   i. **Operational Analysis.** Modeling of all operations covered by applicable NEOPs; identification of weapon locations and configurations; preparation of process flow diagrams; and evaluation of hazards at each process step.

   ii. **Scenario Development.** Development of accident sequences; identification of accident environments; evaluation of weapon response, including thresholds.

C. Scenario Evaluation. Screening of accident sequences; grouping of scenarios by consequence; risk ranking of scenarios; formal analysis of high explosive detonation/deflagration and nuclear detonation accident sequences.

D. Documentation. Preparation of a HAR that documents the results of the HA process.

Figure 3 reflects the Los Alamos risk or hazard analysis process used for conducting a comprehensive HA concurrent with process design and development to meet the intent of the Integrated Safety Process and the needs of the NESSG) as delineated in Supplemental Directives 5610.10 and 5610.11. The details of the HA methodology are documented by Fischer[1,2] and Bott.[4] This HA process has been demonstrated to be effective in helping reduce risk associated with nuclear explosive operations through concurrent involvement in process design as shown in Fig. 2.

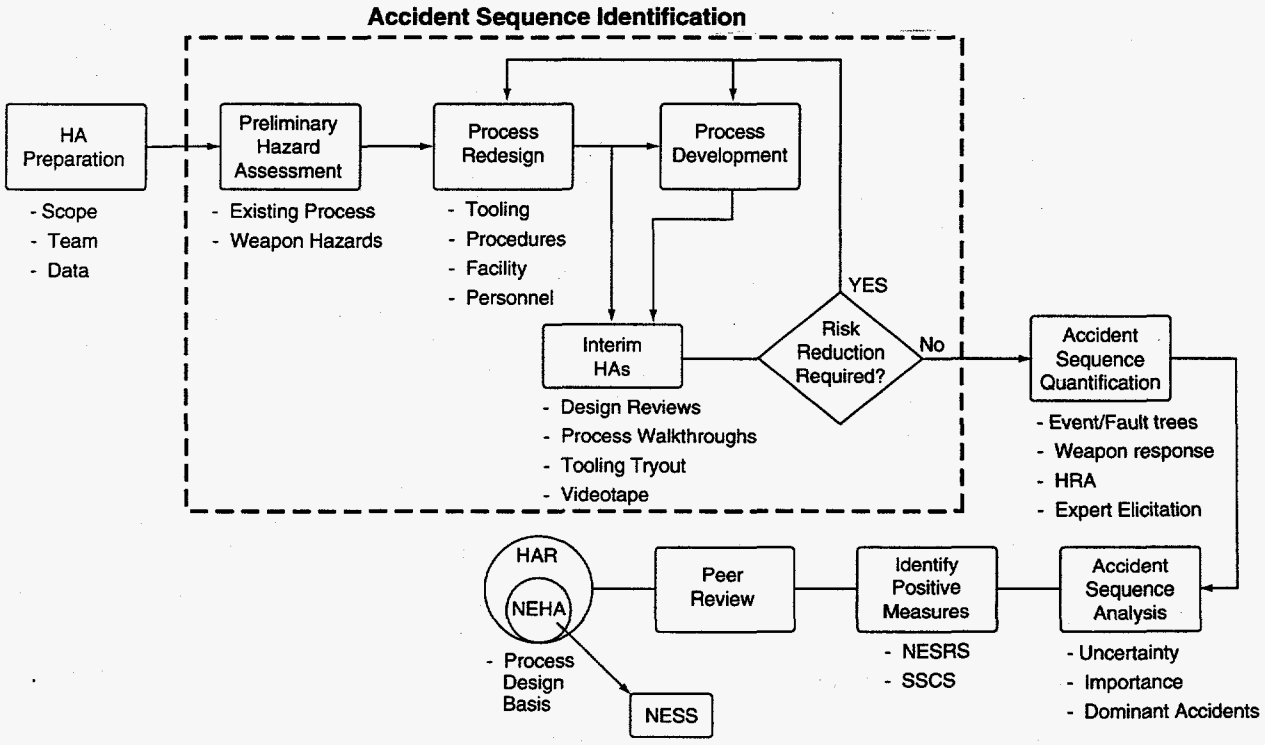

Fig. 3. Los Alamos SS-21 HA process.

SS-21 Risk Management Process

The HA identifies dominant hazards or accident sequences. However, consistent with the SS-21 process, the decision to implement risk-reduction changes to the design/process is made outside the HA Task Team. If changes are made, the HA Task Team evaluates those changes from a risk perspective. As shown in Fig. 3, there is a feedback loop in the HA process associated with the decision whether process changes are necessary to achieve the desired reduction in risk. Decisions to make process changes can be made by the individual Task Teams (i.e., Tooling, Procedures, Facility Task Teams, etc.) or by the Project Team. Process changes typically considered might include

- procedure or administrative changes,
- modification of existing tooling,
- additional tooling or changes in supporting equipment,
- modifications of the facility or facility support systems,
- personnel changes,
- changes in allowed inventory of explosive or fissile material, and
- modifications to the process flow.

Most process changes that result in a reduction in risk are identified through joint walk-throughs conducted as part of the SS-21 development process. These walk-throughs involve the Task Teams, which are composed of system engineers, assembly engineers, risk analysts, technicians, tooling engineers, radiation protection engineers, and other discipline specialists. Changes often are made by direct discussion and communication amongst the team of people involved. During these process walk-throughs, the risk analyst plays the role of the "devils advocate" by being very pessimistic and asking "What if?" questions to stimulate discussion. Most operations and design personnel are success-oriented and often find it difficult to think about how things might fail.

In some instances during process walk-throughs using weapon training units, potential insults to the nuclear explosive may be identified, and no one really knows whether the insult poses a problem.

The risk analyst typically will analyze the situation further in more detail, often consulting experts, to determine if there is a potential concern. If a concern arises, these items are discussed with the SS-21 Project Teams and individual Task Teams, and corrective action is taken as needed.

In general, no specific risk acceptance criteria other than engineering judgment are employed, nor do they exist at present, to guide risk-related decisions with respect to whether corrective action is required. The key concerns weighed by the SS-21 Task and Project Teams with respect to whether a change should be implemented include such items as likelihood of occurrence, consequence, time required to implement the change, schedule impact, cost to implement change, availability of resources to perform the change, the reduction in likelihood achievable, the reduction in consequence achievable, possible regulatory exposure, liability issues, etc.

Clearly, a nuclear explosive operation involves some risk, and the HAs typically identify numerous potential accident sequences with undesirable consequences. These potential sequences are ranked by likelihood and presented to the SS-21 Project Team and later to the DOE NESS group for their deliberations with respect to the acceptability of the process. The SS-21 safety philosophy encourages taking action to reduce or eliminate hazards regardless of likelihood. This philosophy stems, in part, from the recognized uncertainty in the response of HE to various insults. Experience to date shows that the B61 and W69 SS-21 programs have resulted in significant reductions in risk consistent with this philosophy.

RESULTS AND CONCLUSIONS

The mere conduct of a formal HA using standard AIChE methods with process videotapes, procedures, and a knowledgeable HA Team can lead to numerous procedure, tooling, and process flow modifications. Similarly as discussed above, team walkthroughs using a trainer with opportunity for "hands on" testing of tooling also can lead to the identification of potential problems and of procedure and tooling changes.

For the W76 disassembly process, the formal HA resulted in over 60 specific procedure changes (wording of steps, cautions/notes added, additional steps, etc.), tooling modifications, and process flow changes. One invaluable side benefit is the increased knowledge about the process hazards gained by the people involved in the HA. For the B61, preliminary team walk-throughs identified several potential concerns with respect to abrasion of HE that might result in a detonation. To better understand these issues, the HA Team held extensive discussion with HE experts. These concerns were later addressed in meetings with the SS-21 Task Teams and resulted in tooling changes. Consistent with the SS-21 philosophy, any change that can be undertaken to reduce risk is implemented given the available resources.

As documented by Fischer,[3] HAs can be conducted in parallel with process development, and the SS-21 process can result in a significant reduction in process risk. To gain the most benefit from the involvement of risk analysts in process development, it is essential that HA personnel be involved early on during process design and development. The quality of the HA and the success in identifying process hazards is dependent on the quality of the HA Team and their expertise, commitment, and involvement. However, it must be recognized that risk-reduction efforts involve "risk tradeoffs." For instance, in the B61 process, eliminating manual manipulations of HE resulted in the introduction of hazards associated with drops of turning fixtures onto HE. Finally, there are clearly inherent risks associated with work on nuclear explosives, and there will always be a dominant accident sequence!

REFERENCES

1. S. R. Fischer, H. Konkel, T. F. Bott, S. W. Eisenhawer, L. DeYoung, and J. Hockert, "Use of Hazard Assessments to Achieve Risk Reduction in the US Department of Energy Stockpile Stewardship (SS-21) Program," Los Alamos National Laboratory document LA-UR-95-1670 (May 1995).

2. S. R. Fischer, D. A. O'Brien, J. Martinez, and M. LeDoux, "Use of Quantitative Hazard Analysis to Evaluate Risk Associated with US Department of Energy Nuclear Explosive Operations," Los Alamos National Laboratory document LA-UR-96-49 (January 1996).

3. S. R. Fischer, H. Konkel, T. Bott, S. Eisenhawer, J. Auflick, K. Houghton, K. Maloney, L. DeYoung, and M. Wilson, "An Evaluation of the Effectiveness of the US Department of Energy Integrated Safety Process (SS-21) for Nuclear Explosive Operations Using Quantitative Hazard Analysis," Los Alamos National Laboratory document LA-UR-96-31 (January 1996).

4. T. F. Bott and S. W. Eisenhawer, 1995, "A Hazard Analysis of a Nuclear Explosives Dismantlement," Los Alamos National Laboratory document LA-UR-95-1774 (May 1995).