LA-UR-96-3915

CONF-960912--9

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: Quantitative Hazard Assessment of a US Department of Energy Nuclear Explosive Operation

AUTHOR(S): David O'Brien
Stewart R. Fischer
Eric R. Gerdes

SUBMITTED TO: Probabilistic Safety Assessment Topical Meeting (PSA '96)
September 29–October 3, 1996
Park City, Utah

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

QUANTITATIVE HAZARD ASSESSMENT OF A US DEPARTMENT OF ENERGY NUCLEAR EXPLOSIVE OPERATION

by

David O'Brien, Stewart R. Fischer, and Eric R. Gerdes
Probabilistic Risk and Hazard Analysis Group
Engineering Science and Applications Group
Los Alamos National Laboratory

ABSTRACT

Quantitative hazard assessments (QHAs) are being used to support the US Department of Energy Integrated Safety Process (SS-21), Nuclear Explosive Safety Study Group, and Environmental Safety and Health initiatives. The QHAs are used to identify hazards associated with nuclear explosive operations involving tooling and procedural processes.

The SS-21 program was used to integrate the assessment of hazards with the process of improving the safety of nuclear explosive operations. Three assessments of the specific nuclear explosive surveillance process have been performed or are in progress.

- A rough-cut hazard assessment of the high-risk areas of operations to maximize safety improvements during subsequent process redesign (completed).
- A baseline hazard assessment of current operations to focus efforts on risk reduction and track overall improvement following process redesign (in progress).
- A rolling assessment of hazards present in conceptual and final solutions to improve safety (in progress).

Each of these QHAs has three primary objectives.

- To facilitate the integration of safety into the design of the nuclear explosive assembly/disassembly process through early identification of hazards
- To support the identification of possible initiating events and accident scenarios for the risk assessment of the nuclear explosive assembly/disassembly process
- To aid in meeting the Occupational Safety and Health Administration process safety management requirements for the nuclear explosive assembly/disassembly process

The specific nuclear explosive preliminary QHA (the rough-cut assessment) was used to focus the process design teams on problem areas. This paper will summarize the preliminary QHA and how it focused the design teams on the problem areas found by the assessment.

I. INTRODUCTION

The Integrated Safety Process (SS-21) program, which integrates environment, safety, and health (ES&H) and nuclear explosive safety requirements under a single program, uses quantitative hazard assessments (QHAs) to identify accidents that have the potential for worker injury and public health or environmental impact. The SS-21 program requires the hazard assessment to generate information to support the following requirements: evaluate the likelihood of accident sequences that have the potential for worker or public injury or environmental damage, identify safety-critical tooling and procedural steps, identify operational safety controls, identify safety-class/significant systems, structures

and components, identify dominant accident sequences, demonstrate that the facility Safety Analys Report (SAR) design-basis accident envelops process-specific accidents; and produce a Hazard Ana Report (HAR) that can be used to support future change control activities

To address this multitude of requirements being imposed on the process hazard assessment, Los Alamos National Laboratory has developed a QHA methodology that has evolved from hazard assessment efforts conducted at the Los Alamos Plutonium Facility. The methodology has now bee used to conduct several hazard assessments for the B61 and W69 dismantlement efforts[1-2] as well as the nuclear explosive surveillance program.

The Los Alamos QHA approach integrates traditional probabilistic safety assessment tools (fault trees, event trees, uncertainty analysis, importance measures, etc.) with qualitative hazard assessmen methods to develop an effective QHA methodology for nuclear explosive operations. This paper summarizes the results to date of a preliminary QHA on nuclear explosive operations and its effect c the process redesign now in progress.

II. PROGRAM GOALS

The SS-21 process is based on the principle that the real benefit of a QHA is in facilitating risk reduction during process design and development. By providing importance measures for basic eve the analyst can estimate which events contribute the most to the accident frequency. Tooling and process designers then would be able to implement design and procedure changes or initiate positive measures to minimize the likelihood of the important base events from occurring. This iterative risk reduction process forms the basis for the SS-21 process.

The overall philosophy of the SS-21 process is to reduce the risk of nuclear explosive operations an acceptable level and to provide defense in depth against potential accident scenarios. The goal o process is to produce safe, efficient, and effective operations that design in safety features to reduce likelihood of accident scenarios, that is, provide safety features that are driven by design not by revi The principle of defense in depth includes such items as

- using conservative design margins and quality assurance,
- designing processes to eliminate accident scenarios;
- employing 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
- employing safety analysis to evaluate the entire process.

Among the accident cases to be considered are the following

- Accidents, inadvertent acts, or authorized activities that could lead to fire, high explosive (HE) deflagration, or unintended HE detonation
- Fire, HE deflagration, or HE detonation given accidents or inadvertent acts
- Deliberate unauthorized acts that could lead to HE deflagration or HE detonation
- Personnel death, injury, or accidents that may result in lost worker time

III. LANL QUANTITATIVE HAZARD ASSESSMENT PROCESS

As mentioned, to address the hazard assessment requirements being promulgated, Los Alamos used a QHA methodology that provides a systematic approach to identifying hazards associated with nuclear explosive assembly/disassembly activities and for assessing qualitatively, or quantitatively, the risk associated with those hazards. A QHA is performed to answer three questions.

- What can happen?
- How likely is it (frequency estimate)?
- What is the impact (consequence estimate)?

A QHA is a formal, systematic, and in-depth method for evaluating a set of possible accident scenarios associated with an activity. Frequency estimates of occurrence for all scenarios are assessed along with estimates of the damage level. Each accident scenario is assigned a "risk rank" based on the estimates of the frequency of occurrence and the consequence level. The entire set of accident scenarios then can be sorted in several ways—by the severity of the risk rank, by consequence level, or by disassembly activity.

The primary objectives of the QHA are

- to facilitate the integration of safety into the design of the assembly/disassembly process through early identification of hazards;
- to support the identification of possible initiating events and accident scenarios for the risk assessment of the assembly/disassembly process; and
- to aid in meeting the Occupational Safety and Health Administration (OSHA) process safety management requirements for the assembly/disassembly process.

Figure 1 shows the integrated hazard assessment process developed at Los Alamos to support the SS-21 and Department of Energy (DOE) Nuclear Explosive Safety Study (NESS) activities. A brief description of the activities shown in Fig. 1 is presented below:

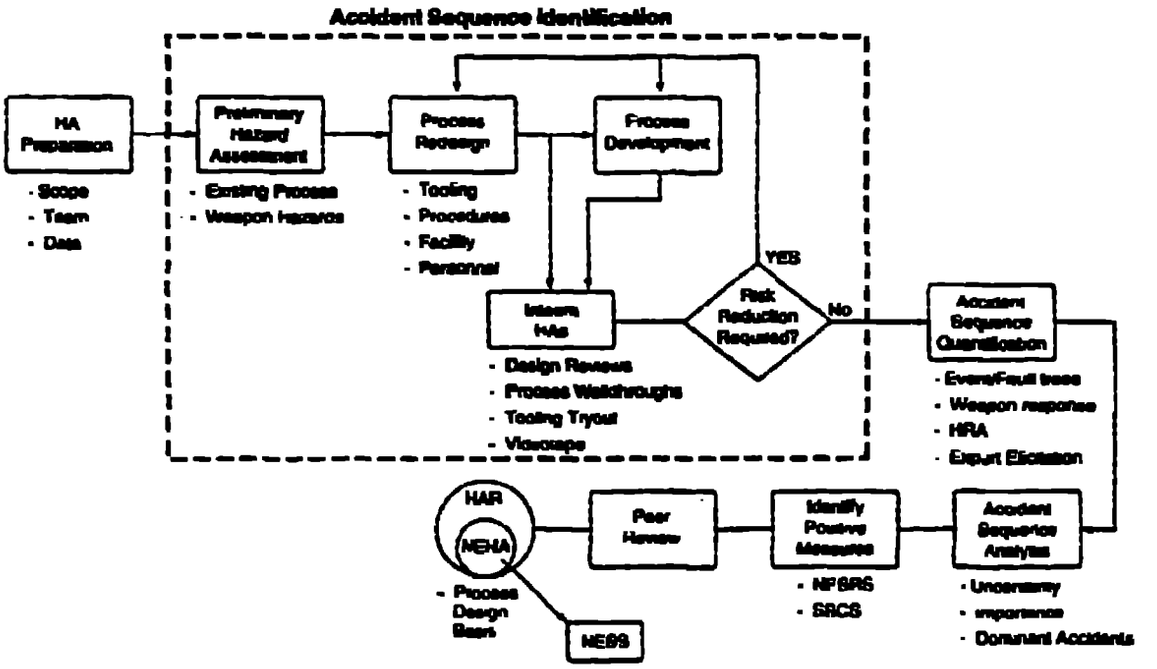

Figure 1. Integrated Hazard Assessment Process

A. HA Preparation

The success of a QHA relies heavily on the composition and competency of the analysis team, availability of information about the process, the hazards associated with the individual component facilities in which the process takes place, and the skills and training of the personnel performing process operations. Each member of the HA team must be knowledgeable in one or more aspects of specific disassembly process being studied. Process information should be collected and organized manner to facilitate its use during the QHA consistent with the maturity of the process design. Init when only conceptual information about procedures, the facility, and tooling and equipment design available, the QHA focuses on the identification and minimization of activities with the potential to significant risks.

B. Accident-Sequence Identification

Several hazard assessments are performed as part of the SS-21 process: a preliminary hazard assessment of the existing process, interim hazard assessments of conceptual process improvement a final hazard assessment of the final process. The steps for accident-sequence identification are essentially the same for each assessment. The basic steps performed during the HA process are

1. flow charting the process,
2. initial accident-sequence identification,
3. detailed accident-sequence identification, and
4. full process evaluation.

1. Flow Charting the Process. As the process matures, procedures can be used to develop a b diagram of the process that focuses the analysis activities. Examples of top-level process flow cha

e analyzed nuclear explosive operations are shown in Figs. 2 and 3. Information related to tooling hould be evaluated to identify possible failure modes or possible misapplications that could create ontribute to an accident. Incident information should be analyzed to identify unusual occurrences ircumstances that need to be considered in determining what types of accidents are likely or credib uclear explosive component hazard information should be summarized in a manner that supports I eam evaluation of the possible consequences of the response of the component to the types of stimu at can result from postulated unusual occurrences or circumstances. Facility information should b nalyzed to identify facility responses to natural phenomena and external events that could affect th afety of disassembly operations, possible faults in facility support systems that could cause or prev mitigation of accidents, and possible effects of concurrent operations on the safety of disassembly perations. Personnel skills and training information should be reviewed to identify situations in w lack of required skills or training deficiencies may increase the likelihood that operators will take nappropriate action and to support estimation of the probability that operators will take appropriate ction under both normal and unusual circumstances.

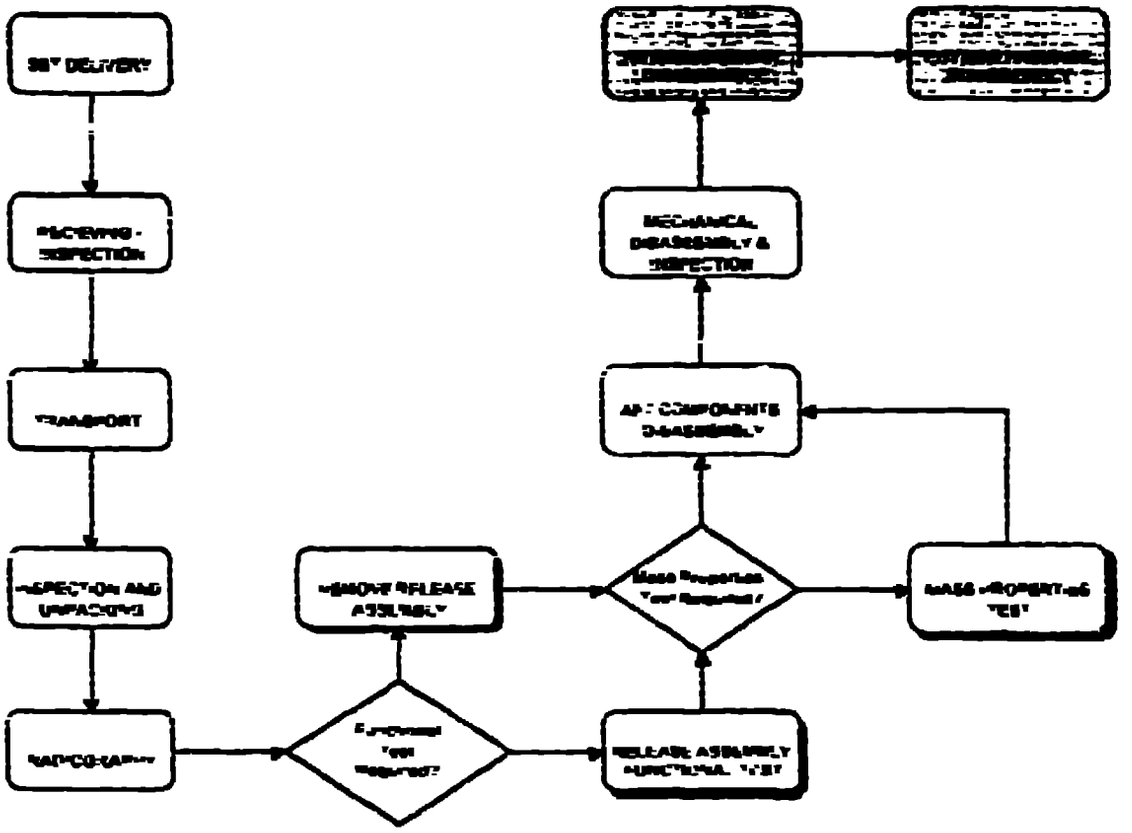

Figure 2. Nuclear Explosive Disassembly Process Flow Chart

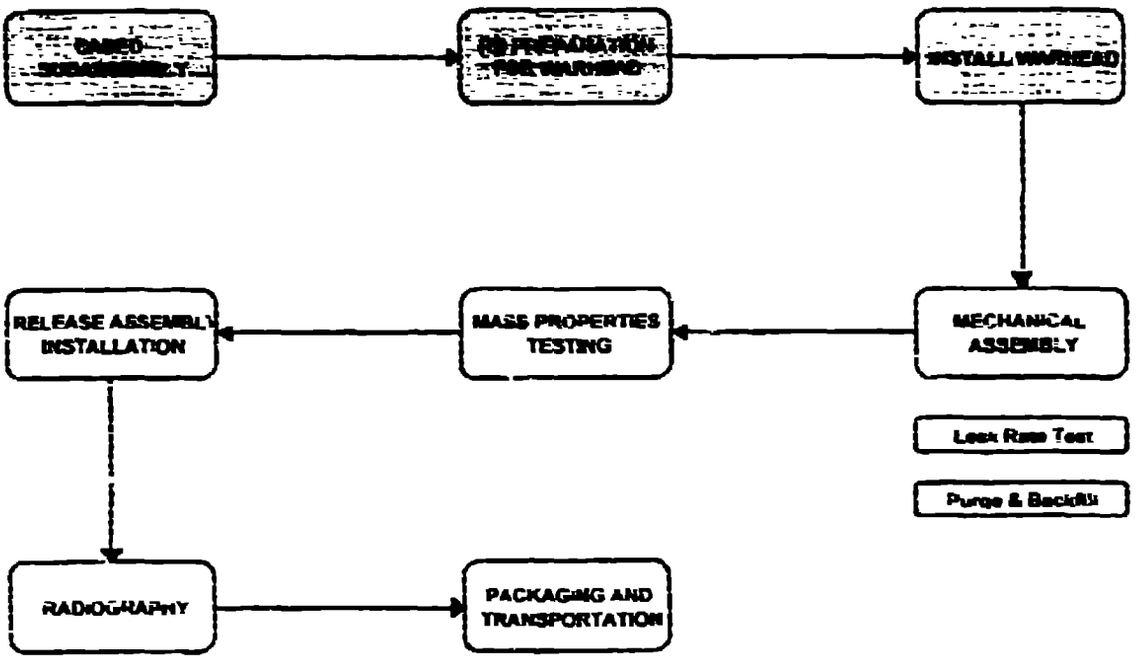

Figure 3 Nuclear Explosive Assembly Process Flow Chart

2. Initial Accident-Sequence Identification. During the initial accident-sequence identificat phase, the team members should review the procedure steps associated with each "block" of the p to identify potential hazards and possible human errors or equipment failures that could be initiati events in an accident scenario involving these hazards. Actual walkthroughs or videotapes of a walkthrough of the process combined with traditional hazard analysis techniques, such as the use "what if" questions or guide words, can be used to assist the QHA team in this process. The team should develop accident scenarios for all cases where there is an initiating event with consequenc public health and safety, the environment, or facility employees. The accident scenarios can be categorized by their consequences using a table such as Table 1

The hazard assessment focuses on identifying accident scenarios by asking the fundamental q "What can go wrong?" To guide the hazard assessment, a process flow chart needs to be develop using actual procedures. For each activity, three complementary techniques are used to identify s things that can go wrong. First, historical incidents are reviewed to identify activities where prob have been encountered during the assembly or disassembly process for this or similar nuclear explosives. Second, a predefined set of possible hazards is reviewed for applicability. Hazard assessment team members also are encouraged to think of things that could go wrong that would stimulate the identified energy sources to release energy or to otherwise expose workers or the pu hazardous material.

Table 1. Consequence Severity Categories

Category	Definition (Bounding Consequences)	
	Worker	Facility
A Catastrophic	Loss of Life as a result of chemical, physical (e.g., explosion), or nuclear-related hazard. • Lethal chemical >> ERPG-3	Significant Facility Damage or contamination resulting in loss of facility for future use.
B High	Severe Injury/Permanent Disability • Exceed lifetime occupational radiation limits • Physical injury resulting in permanent disability • Chemical exposure > ERPG-3	Moderate to Significant Facility Contamination and Damage • Repair and cleanup possible but quite expensive
C Moderate	Lost Time Accident but No Disability • Chemical exposure < ERPG-3 • Exceed annual/quarterly worker radiation dose limits • OSHA reportable injury	Facility Contamination Minor Facility Damage • Repair and cleanup possible at moderate expense
D Low	No Significant Impact: Minor or No Injury • Minor recordable injury • Chemical exposure < ERPG-1	Minor or No Facility Contamination • Minor facility damage
E No Hazard	No Impact to Worker	No Facility Damage

3. Detailed Accident-Sequence Identification. A more detailed review of the process is conducted following the review of accident scenarios. The process used is similar to the HAZOP process,[1] which involves combining a series of "guide words" and "parameters." The parameters include activities, items, and environmental conditions. The activities include everything that is to be accomplished in the procedure steps encompassed within the study node. The guide words are used to ensure comprehensiveness, not to limit the analysis. Thus, any useful "what if" question not suggested by the guide words should be considered in the analysis. In fact, when such questions are identified, the analyst should take the time to determine whether additional guide words are appropriate.

After the things that could go wrong have been identified, it is necessary to determine their possible causes. What could cause the operator to fail to remove the MCXXXX? What could cause the operator to select a part other than the MCXXXX for removal? The specific causes need to be developed in sufficient detail to obtain estimates of the probability of the event. In some cases, it may be possible for a postulated event to have been caused by, or made possible by, a contributing event at a previous study node. In such cases, the analyst should reexamine the results of the analysis of that study node to determine whether such a contributing event could have occurred to estimate its probability.

It is during this stage that the preliminary QHA is done as part of the Baseline Hazard Assessment (second block of Fig. 1).

4. Full Process Evaluation. After preliminary evaluations of a process have been conducted and the results passed to those redesigning the process, a full examination of the process may begin. A detailed spreadsheet following all the steps of a process is developed and used to document all possible accident sequences. The spreadsheet is completed through a thorough examination of written

procedures, walkthroughs/demonstrations, and videotapes of the process. This usually requires several days of meetings between process engineers, hazard analysts, and subject matter experts.

C. Accident-Sequence Quantification/Categorization

As an aid in determining which process steps require action for risk reduction, a categorization scheme has been established based on both the likelihood of an event occurring and its frequency for occurrence. This categorization is performed only on the final, complete list of accident scenarios developed from the checklist. The likelihood for each accident sequence should be estimated using likelihood categories ranging from Normal (Category I) to Improbable (Category V), with associated probabilities assigned by the hazard team members. Similarly, the consequence for each accident sequence should be estimated using categories like those listed in Table 1. A risk rank matrix such as Table 2 then should be used to provide a consistent estimate of their overall significance (i.e., risk rank from 1 to 4). Consensus recommendations should be developed for reducing risks for significant accident scenarios and transmitted to the various SS-21 task teams.

D. HA Documentation

Depending on the hazard assessment performed, a variety of documents is prepared to transmit results to those responsible for the process. For the preliminary hazard assessment (performed before the walkthrough), this is simply a table of numbers of accident sequences from the initial accident identification. As the process continues, monthly progress reports are submitted to management identifying high-risk areas that, at least to that point in analysis, will require action. Also, formal presentations are provided to the management to present these findings and to discuss conceptual approaches to solutions that will address risk management concerns.

Following the completion of spreadsheets for the baseline process flow or revised spreadsheets to reflect process improvements (the interim hazard assessment effort), a formal hazard assessment document is prepared. When the final process design has been developed and the associated risks have been reduced to the maximum extent practicable, the results of the hazard assessment are documented in a Nuclear Explosive Hazard Assessment (NEHA) and HAR. This should include, at a minimum, a brief description of the dominant risk accidents and their associated frequencies and consequences, the methodology used to identify and quantify these accidents, and the risk reduction recommendations made to the SS-21 teams and the disposition of these recommendations. Additionally, a peer review of the entire hazard assessment should be conducted before finalizing documentation.

Table 2 Risk Rank Matrix

Severity of Consequence	Likelihood of Postulated Accident				
	I	II	III	IV	V
A	1	1	2	3	3
B	1	2	3	3	4
C	2	3	3	4	4
D	3	4	4	4	4
E	NH	NH	NH	NH	NH

IV. CONDUCT OF PRELIMINARY NUCLEAR EXPLOSIVE HAZARD ASSESSMENT

For the preliminary hazard assessment (the second block of Fig. 2), only the existing process was analyzed. In addition, to date, the accident-sequence identification has only identified potential accidents and their worst possible consequences. The intent is to refine the analysis to provide more detailed understanding. However, the analysis to date has provided insight into which portions of the process could be changed to provide the most risk reduction by reducing the largest number of potential accidents in the nuclear explosive's most vulnerable configuration.

Before the conduct of the hazard assessment, an extensive data-gathering effort was undertaken, in particular to evaluate nuclear explosive response in the disassembly accident environments and to obtain information on past operating incidents. After viewing a videotape of the disassembly/assembly process and reviewing the procedure steps, the hazard assessment team members used the guide words and comparable historical events and drew from their experience and training to develop "what if" questions. These were recorded by the team member serving as scribe and examined by the team under the leadership of the hazard assessment team leader. In cases where the events postulated in response to the "what if" questions could pose a hazard, they were developed into a postulated accident sequence by the hazard assessment team and then documented.

The developed accident scenarios, along with the scenario consequences, were discussed in detail by the team. To facilitate future evaluation of the identified accident sequences, each sequence was assigned a keyword—industrial accident, radiation dose, explosion, and equipment or facility damage. The team determined the consequence severity for each of the two risk attributes—Worker Safety and Facility Damage—using Table 1. The hazard assessment team noted those parts of the process where the nuclear explosive became more vulnerable to drops, impact, and electrostatic discharge (ESD) (noted by the shaded areas of the respective process flow charts in Figs. 2 and 3. This would facilitate estimating, based on numbers of potential accidents and vulnerability of the nuclear explosive, where efforts at process redesign should occur.

V. RESULTS OF PRELIMINARY HAZARD ASSESSMENT

The results of the preliminary hazard assessment to date are shown in Tables 3 and 4 for the disassembly and assembly processes illustrated in Figs. 2 and 3. The shaded areas in these tables indicate the portion of the process where the nuclear explosive is more vulnerable to drops, impact, and ESD. It should be noted that those potential accidents which could cause a Facility Category A or B consequence also would cause a Worker Category A or B consequence. However, these are not counted in the total for Worker Category A or B consequences at present.

Table 3. Potential Process Related Accidents for Nuclear Explosive Disassembly Operations.

Major Activity	Potential Process Related Accidents			
	Facility Category A	Facility Category B	Worker Category A or B	Worker Category C
Inspection and Unpacking	1	7	3	3
Release Assembly Removal	3	16	10	0
All Components Disassembly	1	6	0	6
Mechanical Disassembly & Inspection	18	29	10	20

Table 4. Potential Process Related Accidents for Nuclear Explosive Assembly Operations.

Major Activity	Potential Process Related Accidents			
	Facility Category A	Facility Category B	Worker Category A or B	Worker Category C
[redacted]				
Mechanical Assembly	51	84	36	61

The hazard assessment team recommended, based on the number of potential accidents and nuclear explosive vulnerability, that the process redesign teams concentrate on those areas of the process shown shaded in Figs 2 and 3 (and Tables 3 and 4). The major initiators in these areas are drops, impacts, and ESD. By reducing the potential for drops, impacts, and ESD by redesigning tooling and procedures, the process risk will be reduced. In addition, the hazard assessment team will be providing the process design teams additional information as the baseline hazard assessment progress to redesign the other process areas to reduce the likelihood of the identified potential accidents.

VI. FUTURE WORK

The hazard assessment team will be completing the preliminary QHA on the baseline process by the end of September 1996 while providing continuous feedback via monthly memos and briefings to the process design teams on any additional problem areas discovered. This preliminary QHA will provide a risk ranking of potential accidents using Table 2 and estimates of the likelihood and consequences of the identified potential accidents. In addition, hazard assessment team members are participants on the various process design teams. This will allow the process design teams to be kept abreast of information from the baseline hazard assessment as well as provide feedback on concepts developed by the teams

REFERENCES

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

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

3 Center for Chemical Process Safety, "Guidelines for Hazard Evaluation Procedures," American Institute for Chemical Engineers (1992).