LA-UR-96-1948

CONF-960912--16

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: A Discussion of the Use of Hazards Assessment and Probabilistic Safety Analysis Techniques for Nuclear Explosive Operations

AUTHOR(S): Terry F. Bott
Stephen W. Eisenhawer
Stewart R. Fischer

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

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

A Discussion Of the Use of Hazards Assessment And Probabilistic Safety Analysis Techniques for Nuclear Explosive Operations

Submitted to the International Topical Meeting on
Probabilistic Safety Assessment
September 29- October 3, 1996
Park City, Utah

Terry F. Bott, Stephen W. Eisenhawer and Stewart Fischer
Probabilistic and Hazards Assessment Group, TSA-11
Los Alamos National Laboratory
Los Alamos, New Mexico

ABSTRACT

The results of a hazard analysis and a probabilistic safety analysis for the same system, a nuclear weapon dismantlement process, are discussed. The probabilistic safety analysis was begun as a pilot project to investigate the feasibility of performing this type of analysis on a nuclear weapon process. During the course of the pilot study, it was decided that a hazard assessment should be performed on the same system. Thus, the hazard assessment and the probabilistic safety analysis proceeded in parallel on the same process and using many of the same resources. This gave the authors a unique opportunity to apply both hazard assessment and probabilistic safety assessment techniques to the same system. In this paper, the authors examine the two methods, including relative strengths and weaknesses, differing technical expertise requirements, and optimal methods for combining the two approaches to achieve an efficient analysis.

I. INTRODUCTION

Los Alamos National Laboratory performed a pilot safety study to explore the use of probabilistic safety analysis (PSA) techniques in nuclear weapons safety and to assess the adequacy of models and data for producing quantitative estimates of the frequency of nuclear weapons accidents.[1] Shortly after the inception of the pilot study, the DOE began an initiative identified as "SS-21."[2] This initiative was intended to integrate safety analysis with weapon-handling process design so that the benefits of safety analysis were realized during the design of procedures and tooling for the weapon dismantlement process. This effort was wider in scope than the pilot study because it addressed worker safety issues as well as nuclear safety issues. The pilot study used what will be termed a PSA approach to analysis; the approach used in the SS-21 study will be termed a hazard analysis (HA) approach. The intent of the HA approach was to identify and address significant safety issues during the process design through identification of positive measures or procedural changes, whereas the intent of the PSA was to identify and quantify the dominant accident sequences leading to a specific class of accident outcome.

These circumstances resulted in two parallel efforts on the same process with considerable overlap in scope but differing approaches. The principal investigator and a lead analyst for the pilot study also participated in the SS-21 study, so there was overlap of personnel between the two studies. This provided an unique opportunity for exploring techniques for integrating the HA approach with the analytical methods associated with the PSA approach.

II. THE HAZARD ANALYSIS APPROACH

The HA approach used in the SS-21 study is a systematic evaluation of the weapons dismantlement process. Experts in weapons design and processing (the subject experts) provided expertise on the weapon hazards, responses to abnormal environments, and process details. A small set of the safety assessment experts (the normative experts) provided the safety analysis expertise required to produce a systematic and well-documented analysis. A few follow-up meetings were held to work out difficulties, but these were restricted in scope and number by the difficulty of assembling the entire team time after time. The HA approach used in this analysis included the identification of accident sequences, the identification of preventive and mitigative features, and estimates of accident-sequence frequencies and consequences by a team of process and weapons experts. The team was headed by normative experts familiar with HA techniques and expert elicitation. Other members of the team included weapons engineers for both the nuclear and nonnuclear portions of the weapon, weapons processing experts, and process design specialists. Before the team meeting, the normative experts spent several weeks studying safety studies and other documents to become familiar with the weapon and the dismantlement process.

The team was convened at the dismantlement plant. The format of the team meeting included reading the procedure simultaneously with viewing a video of the dismantlement process. At each step in the process, the video was halted, and accident initiating events were elicited from the team. Potential safety problems were noted, and possible improvements were documented. For each accident initiating event that was identified, one or more accident sequences were constructed by the team members. The team's consensus on the relative frequency of the accident sequences and their likely consequences was elicited. The frequencies were expressed as order of magnitude estimates. The consequences were binned according to broad classes of outcomes. An initial attempt was made to elicit the frequency of an entire accident sequence as one estimate, but this proved intractable for the experts, so each accident sequence was broken into an initiating event, accident progression events, and a weapon response.

Information on each accident sequence was entered on a spreadsheet, including a description of the initiating event and accident progression, the weapon response, all the probability and frequency estimates, and the consequence class. The accident-sequence frequency estimates were converted to qualitative ranges at the conclusion of the hazard team meeting. The risk ranking for each accident sequence was estimated based on the accident-sequence class and consequence class according to a set of combinatorial rules. The result of the analysis was a matrix of accident sequences that could be ordered by frequency, outcome, or a combination of both.

III. THE PROBABALISTIC SAFETY ASSESSMENT APPROACH

The PSA approach uses so-called normative experts familiar with PSA techniques to collect and analyze data on the process. Experts in the subject are treated more as consultants than partners in the analysis. The PSA approach to the safety analysis began with a study of the weapon design, the process procedures, previous safety studies, and an operational history of weapon processing collected in the form of unusual occurrence reports (UORs). Based on this information, a fault tree was constructed whose cut sets were accident sequences for the process. This fault tree is called the accident sequence logic diagram (ASLD) and is an extension of the master logic diagram (MLD) concept.[3] The ASLD was updated and expanded continuously during the next several months as new accident sequences were identified from a further study of historical records or interviews with subject excerpts of various types.

Based on an examination of the accident sequences identified on the ASLD, a set of event trees was constructed that modeled the accident progression for all the accident sequences on the ASLD. The process of constructing the event trees expanded the number of separate accident sequences over that identified by the HA because many more possible branches in the accident progression were constructed. For the purposes of the pilot study, no quantitative estimates of accident consequence were required, but qualitative accident outcome bins similar to those used in the SS-21 study were used.

The accident-sequence frequencies were estimated using a variety of sources. Many initiating-event frequencies were estimated based on surrogate data from other sources or were developed using an operational data base that used the UORs as event data and nuclear weapon processing records for population data.[4] Human reliability analysis contributed many others.[5] Conditional probabilities for accident progression events, which appear as branches on the event tree, were estimated from a variety of analyses, including structural analysis, geometric considerations, and weapon response estimates. The weapon response estimates used a limited test data base along with an extensive expert elicitation.[6] Uncertainty was included for each probability or frequency estimate. Probability distributions for the frequencies of the accident sequences that contributed 99% of the total estimated frequency for each accident consequence category were generated with Monte Carlo simulation.

IV. DISCUSSION OF THE APPROACHES

A discussion of using these two methods for accident analysis and arriving at similar results is very instructive. The discussion indicates that the two approaches, when integrated, produce a superior result with more efficient use of resources than the exclusive use of either approach.

A. Initiating Event Identification

The HA team approach was an excellent way to identify initiating events in the process itself. The process and weapons experts were efficiently utilized by using the video to walk through the dismantlement process, which allowed time for discussion. However, using this method requires some careful handling. The subject matter experts tend to be success oriented and must undergo a considerable attitude change to begin looking for faults and failures. Human error is a particularly sensitive topic with the technicians on the HA team, and the subject must be treated with care. When the normative experts gained the trust of the technicians, the technicians got into the spirit of the HA and identified many potential accidents either from their personal experience with the relative difficulty of a procedure or from "close calls" or incidents they had witnessed in the past.

The PSA methodology added a new dimension to initiating-event identification through the ASLD. The ASLD is developed by first identifying possible energy sources that can affect the process. This approach naturally includes events external to the process itself, which are very difficult to identify with a process-oriented approach. In addition, the ASLD imposes an order and logic on the search for initiating events that enhance the probability of identifying initiating events. The ASLD had been developed before the first meeting of the HA team and was brought to the team meeting. In the team context, the ASLD served as a prompt for ensuring that all types of potential accidents, including those that the subject experts had ignored based on preconceived notions of likelihood, were considered.

An important aspect of the PSA analysis is the time spent observing live process operations. The luxury of this type of observation is not available to the HA team but can be used by a small team of normative experts. The normative experts were able to observe many dismantlement processes on weapons trainers by experienced technicians. This provided the opportunity for the analysts to stop the technicians during operations and ask questions, redo steps, and even try things themselves to determine such things as alerting factors for human errors and the difficulty of reading component identification numbers. This information was not always readily available in the HA team setting because the technicians either could not remember or had never paid attention to that aspect of the work.

The HA normally would be preceded by a study of historical incidents . This was already available from the ASLD constructed for the PSA, allowing the HA to focus immediately on the process. Here having an ASLD to use as a prompt for the HA proved to be a very useful addition to traditional HA techniques. The HA team approach, when supplemented by the ASLD, was very effective at rapidly identifying initiating events.

B. Accident-Sequence Development

Most of the important accident sequences were identified using the HA approach. Accident-sequence development by HA is rapid but relatively incomplete compared with PSA analysis because it tends to identify only one path on each event tree, whereas the PSA can look at all paths. The HA approach to accident-sequence development is excellent for outlining the types of accidents that can occur and providing a rapid view of the important steps in accident progression.

Some important results of accident-sequence analysis were more completely realized in this study when event-tree analysis was used. The HA approach is less systematic in developing accident sequences that can result from a single initiating event because of accident progression branching. In the HA approach used in this study, the one or two most important branching sequences were identified, whereas many more were identified using event-tree modeling. This may not be an important consideration when there is only one consequence of interest for an accident. However, it becomes important when several different accident consequences of widely varying importance are possible. Event-tree development is also important for risk reduction. In several instances, accident sequences that were identified only by event-tree development provided significant risk-reduction opportunities that were missed using the less-detailed HA accident sequences.

Qualitative understanding of the accident sequences also was enhanced by event-tree development. The thought processes involved in event-tree construction helped place the different steps in the accident progression in much better focus than was possible using team elicitation. For example, the importance of the orientation of the high explosive when it strikes an objects as well as the characteristics of the striking surface were highlighted by event-tree development. The importance of these parameters was much less clear during the team elicitation. The event trees also provided an improved qualitative understanding of the relative importance of dependence between events. As an example, the event trees clearly outlined the dependencies between a airplane crash into the plant, the probable disablement of fire fighting systems in the vicinity of the crash, and the probable fire resulting from the crash.

HA is an effective method for identifying the dominant accident sequences. The experience of this study demonstrated the utility of event-tree development in producing a more comprehensive accident sequence set for a subset of the accidents identified through HA.

1. Accident-Sequence Screening. The HA is a very effective tool for identifying accident sequences with consequences so low that they are not of interest. It also can be used to identify any accidents among a group of related accident sequences that have a much lower frequency for some reason. When this is the case, the low-frequency accident sequences can be absorbed into the higher frequency accident sequences and reduce the calculational effort. Screening is an extremely important function in PSA because it can significantly narrow the field of accident sequences that must be quantified. The key to using the HA to screen is to carefully record the judgments of the experts concerning the consequences and the relative likelihood of accidents. In many cases, the analysts noted similarities between different accident sequences that the subject experts had constructed. Often, one of the accidents would be considered much less likely to result in a particular consequence than another related accident because of some difference in weapon configuration or insult energy. In these cases, several accident sequences forming a logical grouping could be consolidated into one accident represented by the most likely member.

2. Frequency and Probability Estimates. Many of the best estimates for accident sequences made in the HA captured the basic nature of later, more detailed estimates. The relative frequency of many of the accident sequences in the PSA was little different than values estimated during the HA. Many of the initial human error probabilities made during the HA using rules of thumb were well within reasonable uncertainty bounds of the value estimated using the Technique for Human Error Rate Prediction (THERP).[7] The main advantage to performing the more detailed PSA calculations was that the PSA values are better documented. Quantifying a problem invariably leads to a more thorough consideration of the details and a much more thorough understanding.

The weapons engineers used in the HA had a general feeling about the sensitivity of the high explosives to certain classes of insults but did not have the detailed knowledge of this specialized field that was required to differentiate between more subtle distinctions in insult type or energy. The PSA expert elicitation and test analysis showed that the weapons engineers were less conservative than the high explosive experts in their estimates. The high explosive experts tended to have wide uncertainty bounds on their estimates that they could express numerically, whereas the weapons experts had less quantitative feel for their uncertainty, which they expressed more as a lack of knowledge than numerical bounds. The high explosives experts used in this analysis were intelligent and thoughtful. Some wished to consider their responses in private for some time before committing themselves to a response. Others preferred to talk through the thought process they followed in formulating a response to a question and discuss their internal models of the problem in detail. In either case, much of the most valuable information elicited by the interviews would have been much more difficult to gather in a group environment.

3. Uncertainty Estimates. The HA approach usually does not make any attempt to quantify uncertainty. The results of this analysis are best estimates that are binned in frequency and consequence classes without any uncertainty statements. The PSA techniques treat uncertainty explicitly by estimating uncertainty bands for each of the frequency and probability estimates used in the quantification of accident frequency. These individual uncertainties are propagated through the analysis to the final frequency result using a Monte Carlo simulation. This simulation provides a probability distribution of the frequency. This uncertainty is no better than the uncertainty estimates of the individual frequency and probability estimates and does include model or phenomenological uncertainties that usually dominate this type of analysis. Nevertheless, the uncertainty capabilities of the PSA provide some additional insights into the meaning of the PSA frequency estimates.

C. Level and Type of Effort

1. Use of Subject Experts. The HA and PSA approaches use experts much differently. The HA brings together a variety of experts in an interactive format. The experts make judgments as a group about accident initiating events, accident progression, and consequences. To control the size of the group, the experts used in the HA approach were more generalists. Specialists in such areas as tooling design and change control were brought in on an as-needed basis.

The PSA used more specialists as experts. A prime example is the high explosive response data base. This base was constructed entirely independently of the weapons process personnel. The experts were consulted using a formal elicitation process that took up to two days and, in some cases, several visits to complete. The data collected from the experts were organized, interpreted, statistically analyzed, and then checked with the experts for correctness.

2. Documentation. The documentation of the HA includes an explanation of the entries on the accident-sequence matrix, including preventive and mitigative features; additional controls are identified as well. Some rationalization for the team decisions is entered on the matrix. Many of the reasons for the frequency and consequence estimates in the HA are simply declared to be engineering judgments.

Documentation in the PSA approach is quite detailed and is designed to defend the analysis. The probabilities and frequencies in the PSA approach must have a traceable provenance for credibility. In many cases, this requires a detailed explanation of a calculation, such as the complete human response analysis (HRA) event trees and THERP table references for a human error probability estimate. In other cases, reference to a data base and some justification of why the data are appropriate is required. The effort required to document in this manner is very great and consumes a considerable fraction of the total PSA effort. However, the result is a substantial data repository for future work.

The extensive documentation of a PSA can be turned to advantage by treating the study as a reference basis for future studies of a similar type. Many of the detailed probability calculations in the PSA can be used in their entirety in later work. For example, an HA performed at a later time could reference many of the detailed and traceable estimates in a PSA study instead of relying on new estimates by the HA team. In this way, the advantages of PSA documentation can be coupled with the rapidity of the HA approach. This approach ib being used currently for the analysis of the disassembly of a different weapon.

V. CONCLUSIONS

The use of HA or PSA approaches to safety assessment depend on the objective of the study. For many purposes, an HA approach is preferred, whereas in some cases, a PSA may be justified. An integration of both approaches is ideal and is essentially the approach described in DOE Standard 3009.[8] In the case reported here, the HA achieved a rapid and effective survey of the process safety and identified numerous improvements and controls for the safety process. The PSA produced a more complete identification of accident sequences and risk-reduction measures. Future integrated studies of weapons processes that are similar to the one in this study can benefit from the models and database developed in the PSA.

The HA method produces a comprehensive assessment of the safety of the process. The HA requires less effort than a PSA approach, with the greatest saving being in the documentation of the results. The probabilistic study required a substantial investment in analytical resources for many accident sequences that turned out to be insignificant from a risk perspective because screening of insignificant sequences is difficult. The HA techniques were excellent for forming an overview of the process safety concerns and including the process experts in the analysis. Much additional information was gained by the use of PSA techniques in identifying and developing accident sequences. Using these techniques did not increase the effort involved in accident-sequence identification as much as expected and provided a valuable supplement to the HA team approach.

For analyses where the results will be scrutinized closely, an integrated approach is recommended. This approach would begin with a HA team accident analysis to scope the problem and reduce the number of accident sequences that are considered by rapidly identifying accident sequences and screening out impossible, low-consequence, or relatively lower frequency sequences. PSA techniques then can be used to provide more detailed models for the reduced set of accident sequences that survive the screening process and provide a defensible and traceable quantitative data base for accident-sequence frequency estimates with relatively little additional effort. In this way, resources are concentrated on accident sequences that have a high potential of being significant contributors to the risk. In addition, the documentation provided by a previously completed PSA study can be used to produce a high-quality safety analysis in a relatively short time by using the HA team approach to identify accident sequences and extending the results of the PSA to the new study. In this manner, the team is used to do what it does best, i. e., identify accident sequences, and the frequencies of these sequences are quantified rapidly using well-documented estimates from previous work.

REFERENCES

1. T. F. Bott and S. W. Eisenhawer, "A Hazard Analysis of a Nuclear Explosives Dismantlement," *Proc. 1995 ASME International Mechanical Engineering Congress and Exposition*, PVP-Vol. 320, SERA-Vol. 5, American Society of Mechanical Engineers (November 1995).

2. S. R. Fischer, H. Konkel, T. Bott, S. W. Eisenhawer, L. DeYoung, and J. Hockert, "USDOE Stockpile Stewardship (SS-21) Program," *Proc. 1995 ASME International Mechanical Engineering Congress and Exposition*, PVP-Vol. 320, SERA-Vol. 5, American Society of Mechanical Engineers (November 1995).

3. D. R. MacFarlane et al., "Risk Assessment for Hanford High-Level Waste Tank 241 SY-101," Los Alamos National Laboratory document LA-UR-93-2730 (1993).

4. S. W. Eisenhawer and T. F. Bott, "Initiating Event Frequencies for Nuclear Weapons Dismantlement Hazard Analysis," *Proc. International Topical meeting on Probabilistic Safety Assessment*, September 29–October 3, 1996.

5. T. F. Bott, "A Human Reliability Analysis Nuclear Explosives Dismantlement," *Proc. 1995 ASME International Mechanical Engineering Congress and Exposition*, PVP-Vol. 320, SERA-Vol. 5, American Society of Mechanical Engineers (November 1995).

6. S. W. Eisenhawer, T. F. Bott, and T. R. Bement, "Detonation Probabilities of High Explosives," *Proc. 1995 ASME International Mechanical Engineering Congress and Exposition*, PVP-Vol. 320, SERA-Vol. 5, American Society of Mechanical Engineers (November 1995).

7. A. Swain and H. Guttmann, "Handbook of Human Reliability Analysis with an Emphasis on Nuclear Power Plant Applications," US Nuclear Regulatory Commission report NUREG-1278 (August 1983).

8. U.S. Department of Energy, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," DOE-STD-3009-94 (July 1994)