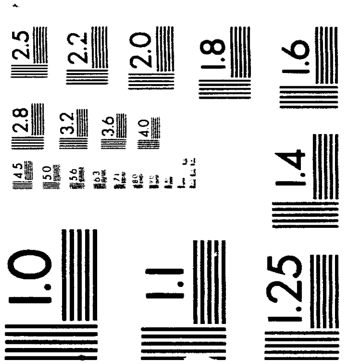
2.5
2.2
2.0
1.8
1.6
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
1.4
1.0
1.1
1.25

1 of 1

LA-UR 93-3625

Conf-940312--37

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: PROBABILISTIC RISK ASSESSMENT OF DISASSEMBLY PROCEDURES

AUTHOR(S): D. A. O'Brien, T. R. Bement, B.C. Letellier

SUBMITTED TO: PSAM II

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

FORM NO. 836 R4
ST. NO. 2629 5/81

PROBABILISTIC RISK ASSESSMENT OF DISASSEMBLY PROCEDURES

D. A. O'Brien, T. R. Bement, B. C. Letellier

Los Alamos National Laboratory, MS F684
Los Alamos, NM 87545

1. Background and Charter For The Study.

The purpose of this report is to describe the use of Probabilistic Risk (Safety) Assessment (PRA or PSA) at a Department of Energy (DOE) facility. PRA is a methodology for i) identifying combinations of events that, if they occur, lead to accidents, ii) estimating the frequency of occurrence of each combination of events and iii) estimating the consequences of each accident.

Specifically, the study focused on evaluating the risks associated with disassembling a hazardous assembly. The PRA for the disassembly operation included a detailed evaluation only for those potential accident sequences which could lead to significant off-site consequences and affect public health. The overall purpose of this study was to investigate the feasibility of establishing a risk-consequence goal for DOE operations.

2. Methodology

The methodology outlined in Figure 1 was used to estimate the risk to the population surrounding the plant. The following summarizes the analysis process:

1. Written procedures and other applicable documentation were obtained and reviewed. These included disassembly procedures currently in use and records of the engineering and development of the hazardous assembly.
2. A two-day HAZards and OPerability analysis (HAZOP) was conducted. Unresolved issues raised during the HAZOP meeting were addressed by experts who developed the hazardous assembly.
3. A two-day site visit was conducted where all disassembly operations were observed. There were several opportunities for discussions with engineers and technicians responsible for disassembly operations.
4. Following the site visit, a number of deterministic calculations were done. These were done as part of an initial attempt to identify those accidents that could be ruled out and those that could clearly lead to significant off-site impact.
5. Event trees and fault trees were then constructed for those operational accidents that have potential off-site consequences.
6. Probabilities for failure (errors) and their associated uncertainties were determined or

estimated for both the event trees and the fault trees.

7. Fault tree and event tree equations were solved using the Set Equation Transformation System (SETS).[1] The associated calculations of propagated uncertainties for the errors were done on the sequence cut sets using the Top Event Matrix Analysis Code (TEMAC).[2] This gave the accident frequency with its associated uncertainty.
8. The consequence analysis modeled the atmospheric transport of accident-caused hazardous material as well as the resulting ground contamination and the latent cancer fatalities (LCFs). Weather variations and source term uncertainties were taken into account. This gave the likelihood of an effect (contamination or LCFs) with the associated uncertainty *given an accident*.
9. The accident frequency and likelihood of an effect were then combined probabilistically to give the final frequency of an effect with an associated uncertainty.

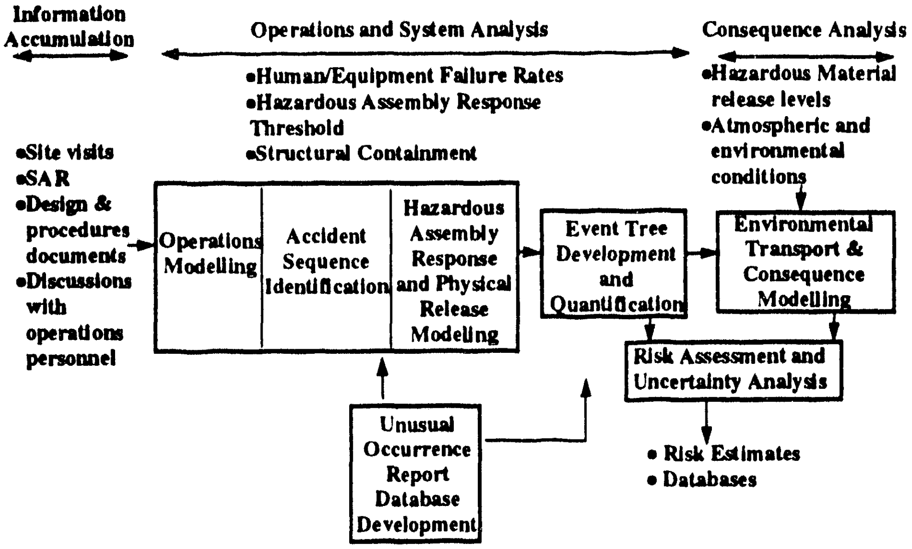
Information Accumulation
Operations and System Analysis
Consequence Analysis
•Human/Equipment Failure Rates
•Hazardous Assembly Response Threshold
•Structural Containment
•Hazardous Material release levels
•Atmospheric and environmental conditions
•Site visits
•SAR
•Design & procedures documents
•Discussions with operations personnel
Operations Modelling
Accident Sequence Identification
Hazardous Assembly Response and Physical Release Modeling
Event Tree Development and Quantification
Environmental Transport & Consequence Modelling
Risk Assessment and Uncertainty Analysis
Unusual Occurrence Report Database Development
• Risk Estimates
• Databases

Figure 1. Outline of PRA methodology used for analysis of disassembly operations.

3. HAZards and OPerability (HAZOPs) Analysis

A HAZOP is a systematic method for identifying operations that have serious accident potential. A HAZOP is performed by having an interdisciplinary team of experts systematically examine a process and its procedures to attempt to identify the effects of departures from standard procedures. Experts then determine if the departures will create hazardous conditions. Identification is also made of actions or systems that mitigate the consequence.

Each step in the disassembly procedures was reviewed by the HAZOP team. Also, a training videotape showing correct disassembly was reviewed. Tables like Table 1 were developed for each procedure, listing all steps and hazards. The hazards included impact, fire, chemical, electrical, and radiological. Each of the potentially hazardous steps were then used, after screening, as event tree headings for accident-sequence identification.

4. Event and Fault Tree Development

Event trees were used to quantify the possibility of off-site consequences caused by disassembly accidents. Unlike reactor "accident-sequence analysis", where event trees are developed for each accident initiator and each branch on an event tree represents an accident mitigating system, the event trees in this study were developed around the normal disassembly procedures. The entry points (corresponding to the usual initiating events) for the event trees were the beginning of specific procedures and not the occurrence of an accident. All of the probabilities obtained by solving these trees were on a per disassembly basis rather than on a time or frequency basis and were converted to yearly frequencies by multiplying by the number of disassemblies each year.

Table 1. Sample Hazardous Operations Analysis table.

Step No.	What If..;	Direct Consequence	Increased Vulnerability	Protection or Mitigation	Interactions with Other What Ifs	Disposition
W	Hoist failure; handling; lifting and rotating	Dropping assembly	Refer back to T- same	Well protected by case; front section	---	Revisit
X	Electrical bonding failed; result susceptible to static discharge	Low-energy components could fire	Common squibs; vulnerable to firing	Low-energy--contained and protected	---	Revisit
Z	Front dropped on center	None	None	Well sealed center; protected	None	None

Each operation identified by the HAZOP was represented by a top event on an appropriate event tree (an illustration of this is given in Figure 2). The top events were developed further by constructing fault or human error trees. In some cases, the human error trees were developed to feed information into fault trees. An example of a fault tree feeding into a top event (from Figure 2) is shown in Figure 3, where a human error, Failure to Electrically Bond, is further developed in a subsequent human error tree, Figure 4. In developing the human error trees, the procedural steps were broken down into fundamental human actions for which some kind of failure rate could be estimated. **It should be noted that the trees presented in this paper are for illustration purposes only and do not represent the actual trees developed.**

5. Human Error Estimation

Several branches of the event trees and basic events in the supporting fault trees involve human actions that can lead to human errors. These human activities were modeled using human error trees, which were developed using the methods described in Swain and Guttmann.[3] The process of developing the trees involves breaking down the procedural steps into those fundamental actions for which typical failure-rate data can be obtained from data bases or estimated in some other reasonable manner. These trees themselves are relatively simple, with binary branching corresponding to success or failure of each activity. However, in a few cases, multiple branching is used to include recovery actions. In these cases it is necessary to account for the fact that different levels of recovery can occur depending on how many previous errors have occurred.

In general, a branch to the right (labeled by a lower case letter) by convention will correspond to a failure to properly complete an activity. A branch to the left (labeled by an upper case letter) corresponds to successful completion of an activity. Depending on what the activity is, a "failure" to complete a procedural step in some cases might actually lead to a less hazardous condition. Therefore, terminating branches of the trees are labeled with an "s" or "f" to indicate whether that sequence is considered an overall "success" or "failure".

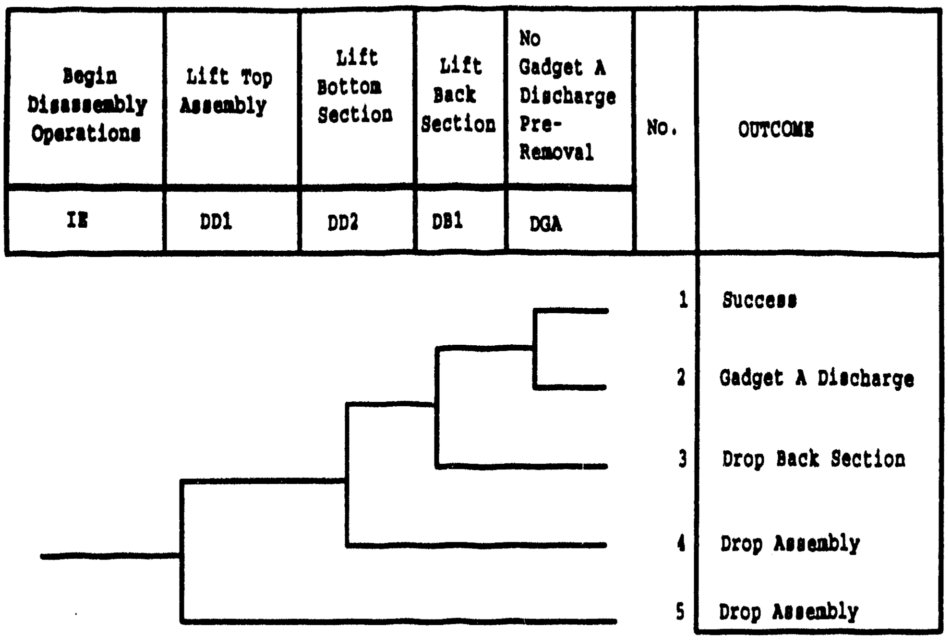

Figure 2. Sample Event Tree.

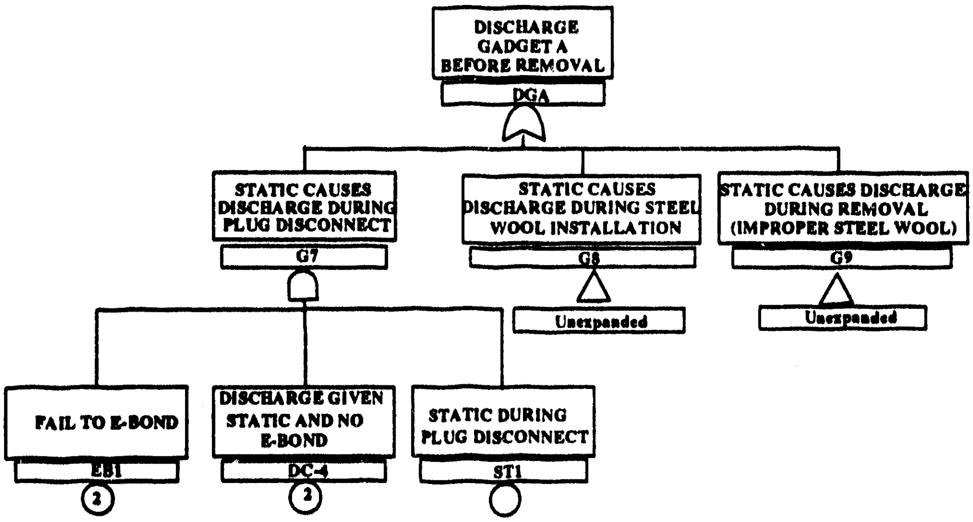
DISCHARGE GADGET A BEFORE REMOVAL
DGA
STATIC CAUSES DISCHARGE DURING PLUG DISCONNECT
G7
STATIC CAUSES DISCHARGE DURING STEEL WOOL INSTALLATION
G8
Unexpanded
STATIC CAUSES DISCHARGE DURING REMOVAL (IMPROPER STEEL WOOL)
G9
Unexpanded
FAIL TO E-BOND
EB1
2
DISCHARGE GIVEN STATIC AND NO E-BOND
DC-4
2
STATIC DURING PLUG DISCONNECT
ST1

Figure 3. Sample Fault Tree.

6. Integration of Risk Sources - Consequence Analysis

The Sandia National Laboratory "ERAD" code was selected for use in this study. It is a constant weather, flat terrain model with a sophisticated detonation plume-rise description, and a Monte Carlo particulate transport package. The code assumes that the atmosphere conditions vary only with altitude.

Account is taken of the variation of particle settling rate with particle size, and treats the stochastic nature of particulate diffusion under unstable atmospheric conditions. ERAD outputs land contamination and integrated air concentration data on a grid extending down wind from the source point. A post processor was used to plot contours of contamination level and potential inhaled dose (for an assumed ICRP standard human, breathing at 330 cc/sec). Plumes were tracked to any distance necessary to bound the regulatory action limit contour of 100 mrem for inhalation and .2 µci for deposition, typically 80 to 100 km. This analysis was repeated for 60 typical weather profiles for the area, and the resultant "potential inhaled dose" contours were combined with appropriate weather probabilities, accident probabilities, and population data to produce expected area contamination and population radiological exposures (person-rem) per disassembly operation.

Each set of 60 weather profiles with a single source term yields 60 consequence values which can be expressed as a cumulative distribution function (CDF). Each CDF can be subtracted from one (1) and expressed as a complimentary CDF (CCDF). If the CCDF is multiplied by the accident frequency, the resulting exceedance function (EF) gives the unconditional frequency of a consequence at least as severe as a specified value.

Randomly chosen source-term values were paired with randomly chosen accident frequencies to yield 40 EFs. Figure 5 shows a hypothetical example of 40 EFs for a consequence metric. From this set of EFs, one can determine the expected value (mean) and range of likely values (the 5th and 95th percentiles) of the exceedance frequency over a range of consequences.

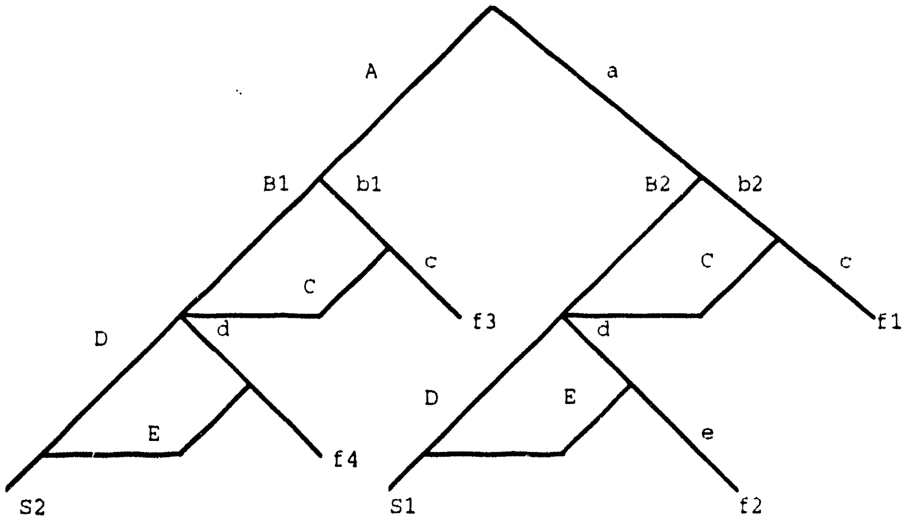

Figure 4. Human error tree for electrical bonding.

7. Risk of Disassembly Operations and Risk Reduction Measures

Using the actual trees developed for this study, the risk of the disassembly procedure was found to be very small. The expected individual risk for latent cancer fatality was calculated to be 3.5 x10^{-12} per individual per year. This is many orders of magnitude less than the Secretary of Energy goal for nuclear facilities of 2 x 10^{-6} per individual per year (which equates to less than a 0.1% increase in an individuals risk of cancer).

The true benefit of the PRA approach, though, is in risk reduction. By providing importance measures for basic events, the analyst can determine which events contribute the most to the accident frequency. Plant operators may then be able to implement positive measures to minimize the likelihood of the important base events from occurring. This is clearly an iterative process in which plant operators are heavily involved.

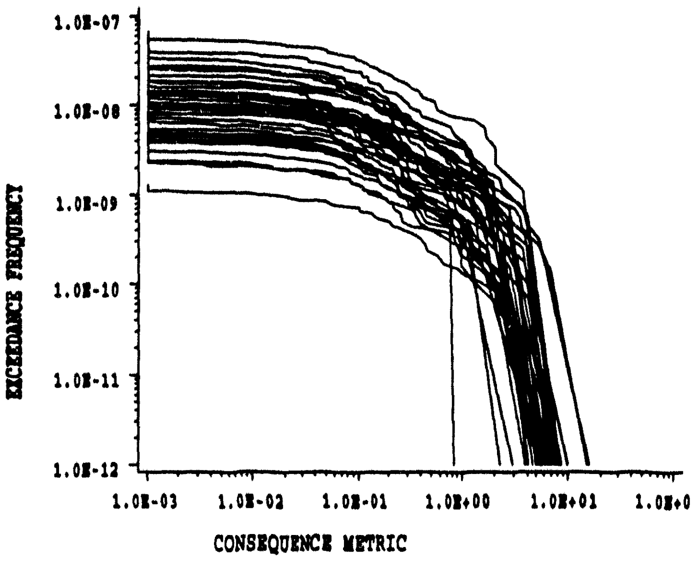

Figure 5. Generic example of 40 Exceedance Frequency vs. Consequence curves.

8. Conclusions

Several conclusions were drawn from this study:

- ❑ PRA can provide a rigorous, systematic approach to safety assessment for DOE operations,
- ❑ PRA can be used to evaluate total risk and provide a consistent framework for risk management,
- ❑ Though the uncertainties in the final numbers are large, qualitative interpretations of results are valuable in identifying
  - the safety benefits (gains) of proposed positive measures,
  - the relative risks posed by various parts of the process or procedure,
  - areas needing further study which will have the greatest effect on reducing uncertainty.

Finally, the analysts concluded that the establishment of a DOE risk criteria (regulatory criteria) was premature.

9. References

1. D. W. Stack, "A SETS User Manual for Accident-Sequence Analysis," Sandia National Laboratories report SAND 83-2230, NUREG/CR-3547 (January 1984).
2. R. L. Iman and M. J. Shortencarrier, "A User's Guide for the Top Event Matrix Analysis Code (TEMAC)," Sandia National Laboratories report SAND 86-0960, NUREG/CR-4598 (August 1986).
3. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report)," NUREG/CR-1278-F.

DATE
FILMED
2/4/94

END