APPLICATION OF PROBABILISTIC METHODS TO ACCIDENT ANALYSIS AT WASTE MANAGEMENT FACILITIES

I. Banz
Westinghouse Electric Corporation
Carlsbad, NM 88220

ABSTRACT

Probabilistic risk assessment is a technique used to systematically analyze complex technical systems, such as nuclear waste management facilities, in order to identify and measure their public health, environmental, and economic risks. Probabilistic techniques have been utilized at the Waste Isolation Pilot Plant (WIPP) near Carlsbad, New Mexico, to evaluate the probability of a catastrophic waste hoist accident. A probability model was developed to represent the hoisting system, and fault trees were constructed to identify potential sequences of events that could result in a hoist accident. Quantification of the fault trees using statistics compiled by the Mine Safety and Health Administration (MSHA) indicated that the annual probability of a catastrophic hoist accident at WIPP is less than one in 60 million. This result allowed classification of a catastrophic hoist accident as "not credible" at WIPP per DOE definition. Potential uses of probabilistic techniques at other waste management facilities are discussed.

INTRODUCTION

Probabilistic risk assessment (PRA) is an analytical technique to assess the risk of a particular facility by integrating the diverse aspects of its design and operation. In achieving this objective, probabilistic risk assessments serve many purposes. An assessment of facility-specific risk provides both a measure of potential accident risks to workers and the public, and insights into the adequacy of facility design and operation. Information developed in the assessment could help in making decisions about the allocation of resources for safety improvements by directing attention to the features that dominate facility risk. The models developed in a PRA provide a basis for evaluating alternative design changes to improve safety.

The Nuclear Regulatory Commission (NRC) is relying increasingly on PRA techniques to supplement its more traditional analytical methods for determining whether nuclear power plants are safe.[1] Although NRC's 1975 Reactor Safety Study[2] was the first application of PRA to nuclear power plant risks, NRC did not significantly use PRA until after the March 1979 accident at the Three Mile Island nuclear power plant. At that time, both a presidential commission and a special NRC inquiry group that investigated the accident recommended that NRC use PRA techniques in safety analyses. PRA, they said, was the best available tool to identify how serious accidents could occur and to make decisions regarding possible corrective or preventive actions.[3]

Since the completion of the Reactor Safety Study in 1975, the NRC has been exploring ways of systematically applying probabilistic analysis to nuclear power plants. As a result, the use of PRA techniques has been rapidly becoming more widespread in the nuclear community. As stated by H. Lewis in 1981, "The Three Mile Island incident illustrates graphically how important it is to quantify both the probability and the consequences of an accident, and to generate some public awareness of these issues . . . This is an issue that goes to the heart of many regulatory and safety decisions, where one must have some measure of the risks one is willing to accept on as quantitative a basis as the expert community can provide."[4]

These same probabilistic techniques can be used to analyze systematically other complex technical systems, such as nuclear waste management facilities, in order to identify and measure their associated public health, environmental, and economic risks. Probabilistic methods provide a means to mathematically quantify risk on the basis of calculated probabilities of component and human failures, both singly and in combination. Three basic questions should be addressed in a PRA:

- What could go wrong?
- How likely is it that this will happen?
- If it happens, what are the consequences?

In performing such an analysis, an attempt is made to quantify probabilities and consequences as accurately as possible in order to determine realistic mathematical expressions of risk. When risks have been quantified in a consistent manner, they can be compared in order to determine which risks appear to be the greater, and what the major contributors to risk are. This information can then be used by decision-makers to determine whether changes to the facility are necessary to improve safety.

DESCRIPTION OF PROBABILISTIC METHODS

Probabilistic assessments can be performed to varying levels of detail. A simple analysis may involve the calculation of accident probabilities, while a more complex analysis may include evaluation of both probabilities and consequences (and thus risk) of accident events. A simple probabilistic analysis can be useful in determining which accident events are deemed credible and therefore necessitate evaluation of consequences. An example of such an analysis performed for the Waste Isolation Pilot Plant (WIPP) is described in the following section.

A probabilistic analysis begins with a systematic search for contributors to risk. Two specific

methods to define the contributors and to graphically display their interrelationships are event tree analysis, which identifies the sequences of events that may result in an accident, and fault tree analysis, which determines how failure of a system may occur.[5]

Event tree analysis begins with an attempt to identify all conceivable events that could precipitate an accident. These events are referred to in PRA terminology as "initiating events." Next, all significant sequences of events that could follow each initiating event are developed.

The construction of fault tree diagrams is a method of system modeling that displays the various ways that a system can fail. This analysis may consider component failures, human error, maintenance and testing activity, potential system interactions, and common-cause contributors. The example presented in this paper illustrates the use of a fault tree in evaluating the probability of a hoist system failure.

Although probabilistic techniques are useful tools in identifying significant risk contributors, large uncertainties exist since, by their nature, PRAs identify and assign probabilities to events that rarely occur. These uncertainties are not unique to PRA but reflect incomplete knowledge about facility systems, human behavior, and accident processes. Some of the uncertainties include: potentially significant accident sequences that could be overlooked, continued uncertainties in relatively unexplored areas such as human behavior and external causes of accidents, and uncertainties resulting from the absence of actual experience or data from a severe accident.

To account for these uncertainties, a variety of techniques may be employed, such as propagation of probability distributions through each branch (or sequence) of the fault and event trees. The probability distribution for each component of the accident sequence reflects the level of uncertainty in the probability assigned to that component. In the simple analysis described below, conservative assumptions were employed in assigning probabilities to events to account for uncertainties in data and modeling.

APPLICATION OF PROBABILISTIC TECHNIQUES AT WIPP

A simple fault tree analysis was performed to evaluate the probability of a catastrophic hoist accident at WIPP near Carlsbad, New Mexico.[6] In addition, probabilistic calculations have been performed at WIPP to analyze the probability of a spontaneous ignition in a waste container and subsequent fire propagation to adjacent containers. Also, probabilistic techniques will be employed in the assessment of long-term repository performance, as required by the Environmental Protection Agency in their recently promulgated regulations on storage and disposal of high-level and transuranic waste (40 CFR 191).[7] The Catastrophic Hoist Accident Analysis is summarized below to illustrate the application of probabilistic methods at WIPP.

Catastrophic Hoist Accident Analysis

Radioactive waste will be transported from the surface to an underground facility at WIPP. The proposed waste transport system is a counterbalanced multi-rope friction hoist that operates a single conveyance in a vertical engineered shaft. The WIPP hoist system will carry two primary types of radioactive waste. Contact-handled transuranic (CH TRU) waste will be handled as unshielded boxes or drums; remote-handled (RH) TRU waste will be contained in canisters that are carried in shielded casks. The analysis described here evaluated the probability of a catastrophic waste hoist accident involving a hoisting system malfunction that has the potential to cause an uncontrolled release of radioactive material from the conveyance cargo.

Methodology

Abstracts of 814 hoisting accidents compiled by the Mine Safety and Health Administration (MSHA) for the period 1978 to 1984 (the latest year for which statistics were available) were reviewed. Those hoisting incidents that could be applicable to the WIPP project were identified. On the basis of the MSHA records and considering the proposed design and operation of the waste transport system, accident scenarios for the WIPP hoist were postulated in three primary categories:

- o cable break
- o overtravel into headframe
- o overtravel into sump

These postulated scenarios were considered to be mutually exclusive, independent events, which collectively represent all incidents capable of causing a catastrophic hoist accident.

The WIPP hoist configuration was schematically portrayed as a multi-component system with parallel (standby) redundancies designed to protect the system from failure (Fig. 1). A probability model was developed to represent the hoisting system and to determine the probability of a catastrophic hoist accident. Fault trees were constructed to identify the sequences of events that could potentially lead to a catastrophic hoist accident. Figure 2 depicts the fault tree that was developed to identify six sequences resulting in an overtravel into the headframe while CH TRU waste is being transported on the hoist. A total of 18 event sequences were identified using five fault trees (Table I).

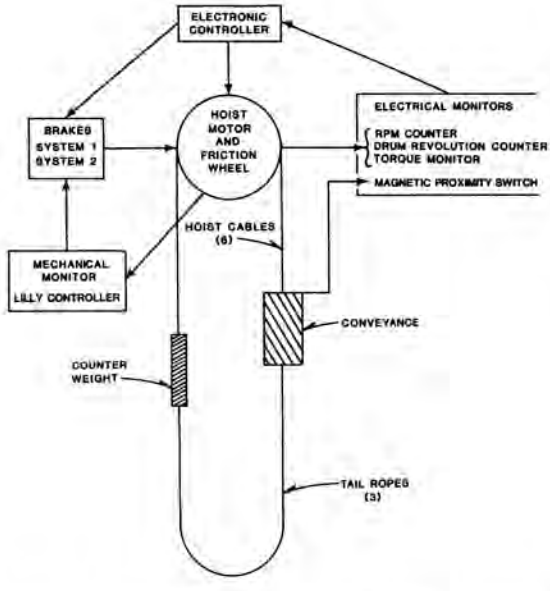

Fig. 1. Components of the WIPP Hoist System.

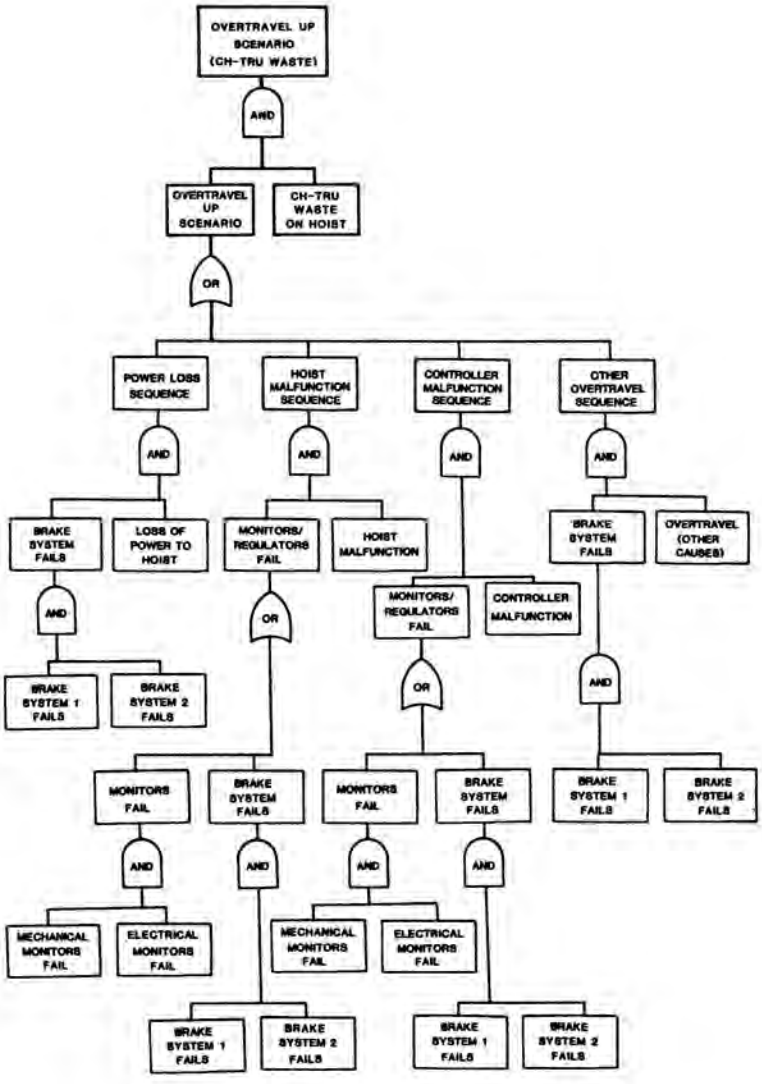

Fig. 2. Fault Tree for Overtravel Up Scenario (CH TRU Waste).

TABLE I

Sequences of Events Postulated to Cause a Catastrophic Hoist Accident at WIPP

Sequence	Scenario	Waste	Initiating Event	Redundancy Failure	Redundancy Failure
1	Cable Break	CH TRU	Cable Break	Cable Break	Cable Break
2	Overtravel Up	CH TRU	Power Loss	Brake System 1	Brake System 2
3	Overtravel Up	CH TRU	Hoist Malfunction	Electrical Monitor	Mechanical Monitor
4	Overtravel Up	CH TRU	Hoist Malfunction	Brake System 1	Brake System 2
5	Overtravel Up	CH TRU	Controller Malfunction	Electrical Monitor	Mechanical Monitor
6	Overtravel Up	CH TRU	Controller Malfunction	Brake System 1	Brake System 2
7	Overtravel Up	CH TRU	Other Overtravel	Brake System 1	Brake System 2
8	Overtravel Down	CH TRU	Electrical Malfunction	Electrical Monitor	Mechanical Monitor
9	Overtravel Down	CH TRU	Controller Malfunction	Brake System 1	Brake System 2
10	Cable Break	RH TRU	Cable Break	Cable Break	Cable Break
11	Overtravel Up	RH TRU	Controller Malfunction	Electrical Monitor	Mechanical Monitor
12	Overtravel Up	RH TRU	Controller Malfunction	Brake System 1	Brake System 2
13	Overtravel Down	RH TRU	Power Loss	Brake System 1	Brake System 2
14	Overtravel Down	RH TRU	Hoist Malfunction	Electrical Monitor	Mechanical Monitor
15	Overtravel Down	RH TRU	Hoist Malfunction	Brake System 1	Brake System 2
16	Overtravel Down	RH TRU	Controller Malfunction	Brake System 1	Brake System 2
17	Overtravel Down	RH TRU	Electrical Malfunction	Electrical Monitor	Mechanical Monitor
18	Overtravel Down	RH TRU	Other Overtravel	Brake System 1	Brake System 2

Results

Statistics generated from MSHA abstracts on hoisting accidents were used to estimate annual rates of occurrence needed to quantify the model. The fault trees were quantified using simple logic relationships (AND, OR).[8] Results show that the annual probability of a catastrophic hoist accident at WIPP from all 18 postulated failure scenarios is less than one in 60 million.[6]

Table II describes the dominant hoist accident sequences. Almost 80 percent of the hoist accident probability results from a sequence in which a power loss occurs while CH TRU waste is being transported down the shaft, and both brake systems subsequently malfunction. An additional 14 percent results from an analogous sequence in which a power loss and subsequent brake failure occur while RH TRU waste is being transported down the shaft. Note that since the hoist conveyance loaded with CH TRU waste weighs less than the counterweight, a power loss and subsequent brake failures will cause the conveyance to move up the shaft. A load of RH TRU waste weighs more than the counterweight, and thus will travel down the shaft.

Based on this result, it was determined that a catastrophic hoist accident is not a credible event at WIPP, as defined in DOE-AL Order 5481.1A,[9] and need not be considered a design basis event.

SUMMARY AND CONCLUSIONS

Probabilistic risk assessment is a valuable analytical technique for evaluating facility design and operations for the purpose of assessing risk to workers and members of the public from the operation of a waste management facility. A fault tree technique has been utilized at WIPP to calculate the probability of infrequently occurring events, such as a catastrophic hoist accident. The technique provides insight into the adequacy of the facility design and operations and to the need for further analysis of these events.

Probabilistic techniques can be utilized effectively at other waste management facilities to serve a variety of purposes, including the following:

- to provide a measure of risks to the public;
- to provide insight into the adequacy of facility design and operation;
- to aid in making decisions about the allocation of resources for safety improvements by directing attention to the features that dominate facility risk;
- to evaluate alternative design changes to improve safety;
- to aid in training personnel;
- to evaluate the sensitivity of accident event probabilities to changes in decision parameters.

Probabilistic risk assessment can provide an objective rather than a subjective approach to accident analysis at waste management facilities.

REFERENCES

1. U.S. General Accounting Office, "Probabilistic Risk Assessment: An Emerging Aid to Nuclear Power Plant Safety Regulation," GAO/RCED-85-11, June 19, 1985.

2. U.S. Nuclear Regulatory Commission, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, October 1975.

3. "Three Mile Island: A Report to the Commissioner and Public (Rogovan Report)," NUREG/CR-1250, 1980.

4. H. W. LEWIS, "The Safety of Fission Reactors," Scientific American, March 1981.

5. Office of Nuclear Regulatory Research, USNRC, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, January 1983.

6. I. BANZ, S. G. BUCHBERGER, and D. G. RASMUSSEN, "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant," WTSD-TME-063, U.S. Department of Energy, July 1985.

7. Environmental Protection Agency, "Environmental Radiation Protection Standards for Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes," 40 CFR 191, 1985.

8. N. J. MCCORMICK, Reliability and Risk Analysis, Academic Press, 1981.

9. U.S. Department of Energy, Albuquerque Operations Office, "Safety Analysis and Review System for AL Operations," DOE-AL 5481.1A, September 1982.

TABLE II

Dominant Hoist Accident Sequences

Waste Type	Sequence	Annual Probability	Percent of Total
CH TRU	Overtravel Up: Power Loss, Brake System Failure	1.3E-8	76
RH TRU	Overtravel Down: Power Loss, Brake System Failure	2.3E-9	14
CH TRU	Overtravel Up: Hoist Malfunction, Brake System Failure	3.7E-10	2
CH TRU	Overtravel Up: Other Overtravel, Brake System Failure	2.6E-10	2
CH TRU	Overtravel Up: Hoist Malfunction, Electrical/Mechanical Monitor Failure	2.2E-10	1

Note: 1.3E-8 = 1.3×10^{-8}