Survey of Systems Safety Analysis Methods and Their Application to Nuclear Waste Management Systems

**P. J. Pelto
W. K. Winegardner
R. H. V. Gallucci**

November 1981

**Prepared for the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830**

**Pacific Northwest Laboratory
Operated for the U.S. Department of Energy
by Battelle Memorial Institute**

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the Department of Energy, nor any of their employees, nor any of their contractors, subcontractors, or 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.

The views, opinions and conclusions contained in this report are those of the contractor and do not necessarily represent those of the United States Government or the United States Department of Energy.

PACIFIC NORTHWEST LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
Under Contract DE-AC06-76RLO 1830

Printed in the United States of America
Available from
National Technical Information Service
United States Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22151

Price: Printed Copy \$ _____ *: Microfiche \$3.00

*Pages	NTIS
	Selling Price
001-025	\$4.00
026-050	\$4.50
051-075	\$5.25
076-100	\$6.00
101-125	\$6.50
126-150	\$7.25
151-175	\$8.00
176-200	\$9.00
201-225	\$9.25
226-250	\$9.50
251-275	\$10.75
276-300	\$11.00

3 3679 00059 5696

PNL-4072
UC-70

SURVEY OF SYSTEMS SAFETY ANALYSIS
METHODS AND THEIR APPLICATION TO
NUCLEAR WASTE MANAGEMENT SYSTEMS

P. J. Pelto
W. K. Winegardner
R. H. V. Gallucci

November 1981

Prepared for the
U.S. Department of Energy
Under Contract DE-AC06-76RLO-1830

Pacific Northwest Laboratory
Richland, Washington 99352

EXECUTIVE SUMMARY

This report reviews system safety analysis methods and examines their application to nuclear waste management systems. The safety analysis methods examined include expert opinion, maximum credible accident approach, design basis accidents approach, hazard indices, preliminary hazards analysis, failure modes and effects analysis, fault trees, event trees, cause-consequence diagrams, GO methodology, Markov modeling, and a general category of consequence analysis models. Previous and ongoing studies on the safety of waste management systems are discussed along with their limitations and potential improvements. The major safety methods and waste management safety related studies are surveyed. This survey provides information on what safety methods are available, what waste management safety areas have been analyzed, and what are potential areas for future study. The information developed should assist the process of implementing the use of consistent and cost-effective safety methods throughout the DOE Waste Management Program.

CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	iii
1.0 INTRODUCTION	1-1
2.0 SYSTEMS SAFETY ANALYSIS METHODS	2-1
2.1 SPECIFIC SAFETY ANALYSIS METHODS	2-2
2.1.1 Expert Opinion	2-2
2.1.2 Maximum Credible Accident Approach	2-3
2.1.3 Design Basis Accidents Approach	2-3
2.1.4 Hazard Indices	2-3
2.1.5 Preliminary Hazards Analysis	2-4
2.1.6 Failure Modes and Effects Analysis	2-5
2.1.7 Fault Trees	2-5
2.1.8 Event Trees	2-13
2.1.9 Cause-Consequence Diagrams	2-14
2.1.10 GO Methodology	2-18
2.1.11 Markov Modeling	2-18
2.1.12 Consequence Models	2-21
2.2 RISK ANALYSIS METHODS	2-22
3.0 APPLICATIONS TO NUCLEAR WASTE MANAGEMENT	3-1
3.1 HLW SAFETY APPLICATIONS	3-1
3.1.1 Short-Term HLW Management Activities	3-1
3.1.2 Long-Term Isolation of HLW	3-7
3.2 TRU WASTE SAFETY APPLICATIONS	3-12
3.3 LLW SAFETY APPLICATIONS	3-13

CONTENTS (cont.)

	<u>Page</u>
3.4 AIRBORNE WASTE SAFETY APPLICATIONS	3-15
4.0 ONGOING WASTE MANAGEMENT SAFETY ANALYSIS RESEARCH PROGRAMS	4-1
5.0 CONCLUSIONS AND RECOMMENDATIONS	5-1
REFERENCES	R-1
APPENDIX A - METHODS AND APPROACHES FOR RISK PREDICTION AND ASSESSMENT	A-1
APPENDIX B - A RISK ASSESSMENT METHOD FOR NUCLEAR FUEL CYCLE OPERATIONS	B-1

TABLES

2.1 Preliminary Hazards Analysis (PHA) for Example System	2-7
2.2 FMEA for Example System	2-8
2.3 Summary of Safety Analysis Methods	2-24
4.1 Waste Handling and Isolation Activities in Foreign Countries	4-2
5.1 Summary of Safety Analysis Methods	5-2

FIGURES

	<u>Page</u>
2.1 Example System	2-6
2.2 Fault Tree Logic Symbols	2-10
2.3 Fault Tree Event Symbols	2-11
2.4 Fault Tree for Example System	2-12
2.5 Event Tree for Example System	2-15
2.6 Symbols for Event Tree Segment of Cause-Consequence Diagram	2-16
2.7 Cause-Consequence Diagram for Example System	2-17
2.8 GO Operators	2-19
2.9 GO Model for Example System	2-20
3.1 Potential LWR Fuel Cycle Wastes	3-2

1.0 INTRODUCTION

Radioactive waste is generated in a variety of forms by operations in the nuclear fuel cycle. Numerous management systems have been devised to immobilize and isolate these wastes. Such systems include multisite processing, transportation and storage operations.

Evaluation of radioactive waste management systems is a complex process. Assessments of proposed systems involve consideration of technical feasibility, research and development needs, timing, cost, national and international policies, environmental impact, and safety. Safety has been a key consideration in evaluating waste management systems.

Waste management systems go through many stages of development before they become operational. These can be categorized as a conceptual stage, a detailed planning stage, a design stage, and ultimately a licensing and operational stage. Safety information is required for each of these stages of development. In the early stages a measure of the relative safety of a particular concept and its alternatives may be all that is required. However, in the licensing stage, detailed quantitative studies are needed to adequately assess the factors affecting the safety of the system. Consequently, a range of safety analysis tools is required depending upon the stage of development of the particular waste management system and the objectives and constraints of the safety analysis program.

This report reviews system safety analysis methods and examines their application to nuclear waste management systems. Previous and ongoing studies on the safety of waste management systems are discussed along with their limitations and potential improvements. The major safety methods and waste management safety related studies are surveyed. This survey provides information on what safety methods are available, what waste management safety areas have been analyzed, and what are potential areas for future study. The information developed should assist the process of implementing the use of consistent and cost-effective safety methods throughout the DOE Waste Management Programs.

This work was performed as a part of the Waste Management Safety Studies Program sponsored by the Department of Energy. The report is organized as follows. Section 2.0 describes the various systems safety analysis methods in use. Section 3.0 discusses the application of these methods to nuclear waste management systems. Section 4.0 briefly reviews ongoing work on the safety of waste management systems. The results are summarized and conclusions presented in Section 5.0.

2.0 SYSTEMS SAFETY ANALYSIS METHODS

The objectives of a safety assessment include:

- . Identifying potentially hazardous conditions or elements in a system or facility.
- . Quantifying the potentially hazardous conditions or elements (may be in terms of probability, consequences, or both).

In some safety applications, the quantification step is not required. In most applications, some degree of quantification is necessary for relative or comparative safety assessment. If an absolute measure of the safety of a single system is required, much more stringent requirements are placed on the safety assessment method used.

As outlined by Haasl (1974) there are basically four sources of information when analyzing the safety of a system or facility:

1. Experience
2. Testing
3. Analysis
4. Conjecture.

For most systems or facilities, a combination of the above sources of information is required to perform a safety analysis.

Systems safety analysis originated in the aerospace and defense industries. It is typically defined as a systematic process of identifying hazardous conditions existing in a system. As the use of systems safety analysis has evolved, more emphasis has been placed on quantifying the hazardous conditions. A broad range of methods has been developed to facilitate this process. These methods may be qualitative or quantitative. They may be inductive (what happens if?) or deductive (how can something happen?). They may be consequence-oriented or risk-oriented. The objectives and constraints of the safety program of interest may require one or a combination of the above safety assessment method categories.

The safety analysis methods discussed in this report include expert opinion, maximum credible accident approach, design basis accidents approach,

hazard indices, preliminary hazards analysis, failure modes and effects analysis, fault trees, event trees, cause-consequence diagrams, GO methodology, Markov modeling and a general category of consequence analysis models. Each of these methods is discussed separately in Section 2.1. Recent developments in the safety analysis have focused on risk analysis. Section 2.2 briefly describes how some of the above techniques can be combined to relate the probability of a hazardous condition to its consequence.

2.1 SPECIFIC SAFETY ANALYSIS METHODS

This section provides a brief description of the major safety analysis methods applicable to waste management systems.

2.1.1 Expert Opinion

Expert opinion is a broad safety assessment technique in which a recognized body of experts provides overall safety judgments or specific inputs (Greenborg, et al., 1978). These judgments or inputs can be formally or informally solicited. Such mechanisms as review committees, workshops, surveys and questionnaires can be used.

The Delphi method is one of the formal techniques for obtaining expert opinion. A series of questionnaires are given individually to a group of experts. Subsequent questionnaires utilize feedback from the earlier questionnaires and permit the experts to comment on the group consensus. The process continues until agreement is reached or it is concluded that useful results will not be generated. The Delphi method originated at the RAND Corporation in 1948 and has been used extensively for forecasting, long-range planning, urban and regional planning, and in defining a large variety of social goals (Dalkey and Helmer 1963; Gordon and Helmer 1964; Helmer 1966).

A major advantage of expert opinion is the ability to obtain safety information or judgments which cannot be obtained by analytic methods. Subjective judgment can be documented in a systematic manner. This approach also has many weaknesses. Experts often have strong differences of opinion and may be perceived to represent special interest groups. Experts may have a tendency of stepping beyond the bounds of real expertise.

2.1.2 Maximum Credible Accident Approach

The maximum credible accident approach is a formalized approach for safety analysis in which engineering judgment is used to survey possible accidents or accident categories (Ott, 1976). Based on an intuitive estimate of their probabilities, the surveyed accidents are subdivided into credible and non-credible accidents. The noncredible accidents are not analyzed in detail. A maximum credible accident is defined and quantified. This accident represents the upper bound of the accident potential of the particular operation under study and can be used as a basis to design specific protective systems. The consequences of the maximum credible accident have been used to provide safety comparisons of different systems or operations.

An advantage of the maximum credible accident approach is its simplicity and the ease in which safety comparisons can be made. A major weakness is the subjective nature of the subdivisions between credible and noncredible accidents.

2.1.3 Design Basis Accidents Approach

The design basis accidents approach is a refinement and extension of the maximum credible accident approach. A series of accidents including low-probability accidents with major consequences are postulated and used as the explicit basis for design or analysis (Ott, 1976). These design basis accidents are determined based upon engineering judgment about the accidents to be included or not included in the safety analysis. Accidents of a lower probability than the maximum credible accident are generally analyzed.

An advantage of the design basis accidents approach is that engineering judgment is applied to a specific set of accidents which can be reviewed and discussed. It is more comprehensive and avoids the more individual judgments used in the maximum credible accident approach. A major weakness is the subjective nature of the selection of the accidents.

2.1.4 Hazard Indices

Hazard indices are comparative tools used in place of a more comprehensive safety assessment method because of study limitations (Voss 1979). A primary use of hazard indices is to aid in the comparative safety assessment of alternative conceptual systems for which there is little available design information.

Many different types of hazard indices have been proposed by many researchers. Their traditional use is to study a system which processes, transfers, and/or stores a potentially hazardous material. For radioactive material the indices use one or more of the following parameters: radioactive material quantity, specific activity, decay properties, chemical and physical form, packaging, toxicity, time behavior and pathways to man. A typical hazard measure, HM, is defined for radionuclide i :

$$(HM)_i = \frac{Q_i}{(MPC_W)_i}$$

where Q_i is the radioactivity in curies of radionuclide i and $(MPC_W)_i$ is the maximum permissible concentration of radionuclide i in drinking water, curies/m³. The total HM of a mixture of radionuclides is the sum of the $(HM)_i$'s. Other hazard indices add more parameters to account for the decay properties, packaging, and pathways to man. Section 3.1.2 discusses several types of hazard indices in more detail.

Hazard indices offer a simple mechanism to make safety comparisons. They require little detailed information and are primarily useful in analyzing conceptual systems or as a first step in a more rigorous safety analysis. The limitations of the hazard indices approach include either the inability or difficulty to take into account the radionuclide physical form and insolubility, the facility design, and the transport pathways.

2.1.5 Preliminary Hazards Analysis

A preliminary hazards analysis (PHA) is a qualitative assessment of the hazardous conditions and potential accidents within a system (Lambert, 1973; Roberts, 1981). A PHA is performed early in a system's life cycle and is usually presented in tabular format. This table contains the following information:

- 1) Subsystem/component identification
- 2) Potential hazard condition
- 3) Possible effects
- 4) Existing preventive and control measures.

To illustrate the concept of the PHA, consider the example system shown in Figure 2.1. Table 2.1 presents a PHA for this example system.

A PHA offers a convenient formal process to perform a qualitative safety assessment in the conceptual stages of a system design or as a first step in a more rigorous safety analysis. A PHA allows the establishment of initial design and procedural safety requirements to control the identified potential accidents. A limitation of a PHA is its qualitative nature and the fact that attention is usually focused on one hazard or component at a time. Experience has shown that accidents are frequently the result of a sequence of events.

2.1.6 Failure Modes and Effects Analysis

A failure modes and effects analysis (FMEA) is an inductive analysis that systematically analyzes component failure modes and identifies the resulting effects on the systems (Lambert, 1973; Roberts, 1981). An FMEA is similar to the PHA in structure, but is much more detailed and can be quantitative. Emphasis is placed upon identifying the problems which result from hardware failure. Typically, a columnar format is employed in an FMEA. Specific entries include:

- 1) Component identification
- 2) Failure rate
- 3) Failure mode
- 4) Effect on the system
- 5) Severity Class
- 6) Compensating provisions.

Table 2.2 presents an FMEA for the example system given in Figure 2.1.

An FMEA provides a systematic examination of the hazardous conditions in a system and is simple to apply. The FMEA is more detailed and quantitative than the PHA, but it has the same disadvantage in that it considers only one failure at a time and not multiple failures.

2.1.7 Fault Trees

Fault tree analysis is a deductive logic technique which diagrammatically models the various combination of basic failure events which contribute to some overall failure event (Lambert 1973; Roberts, 1981; USNRC 1975; Smith et.al.,

EXAMPLE SYSTEM

This hypothetical system consists of a tank containing a liquid under pressure. If released this liquid will react with air to form a hazardous particulate. The tank is surrounded by a normally vented structure containing a spray air cleaning system and a ventilation isolation system. The spray air cleaning system and the ventilation isolation system need electric power to function. In the case of power failure an emergency power system is available

FIGURE 2.1 Example System

TABLE 2.1 Preliminary Hazards Analysis (PHA) for Example System

<u>Subsystem or Component</u>	<u>Potential Hazard Condition</u>	<u>Effect</u>	<u>Existing Preventive and Control Measures</u>
Valve	Failure of valve (primary and external causes)	Release from tank	Valve maintenance and inspection; ventilation isolation system; spray air cleaning system.
Tank	Failure of tank (primary and external causes)	Release from tank	Tank maintenance and inspection; ventilation isolation system; spray air cleaning system.
Spray air cleaning system	Failure of system (primary and external causes)	No cleaning of air in the event of a release from the tank	Maintenance, testing and inspection; ventilation isolation system.
Ventilation Isolation System	Failure of system (primary and external causes)	Release of particulate in the event of a release from the tank	Maintenance, testing and inspection
Building structure	Failure of structure (primary and external causes)	Release of particulate in the event of a release from the tank	Structure maintenance and inspection
Off-site electric power	Failure of power (primary and external causes)	Failure of spray air cleaning and ventilation isolation systems	Emergency power system

TABLE 2.2 FMEA for Example System

Component	Failure Rate	Failure Mode	Effect on the System	Class	Compensating Provisions
Valve	Probable	Fails closed	None	Safe	
	Reasonably probable	Fails open	Release from tank	Critical	Ventilation isolation system; spray air cleaning system
Tank	Reasonably probable	Leaks	Release from tank	Marginal	Ventilation isolation system; spray air cleaning system
	Remote	Ruptures	Release from tank	Critical	Ventilation isolation system; spray air cleaning system
Spray air cleaning system	Reasonably probable	Fails to function	None unless combined with release from tank	Marginal	Ventilation isolation system
Ventilation isolation system	Reasonable probable	Fails to function	None unless combined with release from tank	Marginal	
Building Structure	Remote	Containment failure	None unless combined with release from tank	Marginal	
Off-site electric	Probably	Fails to function	Fails spray air cleaning and ventilation isolation system	Marginal	Emergency power system

1976). A fault tree begins at the TOP with the definition of this ultimate failure event, which is expanded downward through subsequent levels of contributing failures until an appropriate level of basic failure events has been reached. These contributory failures are combined by logical AND and OR gates at the appropriate levels. Fault trees are normally used to model events having binary failure states (total failure vs. total success), as opposed to those having partial failures. The symbols used in fault trees are shown in Figures 2.2 and 2.3.

The means by which the TOP event can occur are known as "cut sets," the combination of basic events leading to the TOP. Of particular importance, especially in evaluating failure probabilities associated with the TOP event, is the concept of a minimal cut set--one in which return of any one of the basic failure events to a success mode precludes the occurrence of the TOP event. By assigning probabilities to the basic failure events, the probability of the TOP event can be found from the Boolean sum of the probabilities for each of the minimal cut sets.

Fault trees are often used to model system failure in terms of failure of its basic components. Component malfunctions are divided into two types: failures and faults. Failures are malfunctions which require repair (or replacement) of the component to correct the malfunction. Faults are malfunctions that can be corrected without maintenance of the component in question. Repair refers to the reversal of a basic event state from failed to unfailed.

Although traditionally used to model system failures, fault trees can also be used to model accident sequences, where the TOP event becomes some consequence of those sequences. Usually, this involves combining several system fault trees which contribute to the overall consequence. When a consequence fault tree is constructed for each of the various consequences of the accident sequences, the complete analysis is equivalent to a complete event tree analysis (with conditional fault trees) covering all initiating events, or to a corresponding cause-consequence analysis. Figure 2.4 presents a fault tree for the example system presented in Figure 2.1.

Fault trees are an established and widely accepted technique for systems safety analysis. FTA can identify potential accident scenarios from combinational

Output

Inputs

AND Gates

Coexistence of all inputs required to produce output.

Output

Inputs

OR Gates

Output will exist if at least one input is present.

INHIBIT Gates

Input produces output directly when conditional input is satisfied.

DELAY Gates

Output occurs after specified delay time has elapsed.

FIGURE 2.2 Fault Tree Logic Symbols (Aerojet Nuclear Co. 1975)

RECTANGLE

A Fault Event resulting from the combination of more basic faults acting through logic gates.

CIRCLE

A basic component fault - an independent event.

DIAMOND

A Fault Event not developed to its cause.

TRIANGLE

A connecting or transfer symbol.

HOUSE

An event that is normally expected to occur or to never occur. Also useful as a "trigger event" for logic structure change within the fault tree.

FIGURE 2.3 Fault Tree Event Symbols (Aerojet Nuclear Co. 1975)

FIGURE 2.4 Fault Tree For Example System

events. Fault trees can be used both qualitatively and quantitatively. Their deductive nature is an advantage in that no assumption of initiating or critical events is necessary. Fault trees can be best applied to systems whose components exhibit an absolute behavior (total failure vs. total success). It is more difficult to model systems whose components can have partial failures. FTA requires a detailed knowledge of the system of interest and the analysis can be complex and expensive. The analyst must anticipate all the significant events, or important system failure modes may be missed.

2.1.8 Event Trees

Event tree analysis is an inductive logic technique which sequentially models the progression of events, both success and failure, leading from some initiator to a series of logical outcomes (USNRC 1975; Lambert, 1973). An event tree begins with some initiating failure, usually on a component level, and maps out a sequence of events, usually on the system level, to form a set of branches, each of which represents a specific accident sequence whose outcome, or consequence, corresponds directly to the events contained in the sequence. Like fault trees, event trees are normally used to model events having binary failure states, these events usually corresponding to total success or failure of a system.

Each accident sequence leading to a particular undesired consequence is somewhat analogous to a cut set on a fault tree. Whereas, a cut set represents a combination of failures leading to the TOP event, an accident sequence represents a combination of sequential events (successes and/or failures) leading to a particular consequence. This suggests a possible equivalence between event trees and consequence fault trees, i.e., fault trees whose TOP events correspond to consequences of accident sequences. Complete event tree analysis requires identification of all possible and distinct initiating events and development of an event tree for each. There tends to be an extensive overlap of consequences among the various trees.

Event trees, using system successes and failures as the basic events at the branching points, tend to view overall consequences to a limited degree of resolution, that being the system level. Fault trees, both those for system failures as well as for consequences, tend toward a greater degree of resolution, that being the component level. To obtain true equivalence between

event trees and consequence fault trees, it is necessary to resolve the system failures on the event tree to their contributing component failures. The usual technique involves development of a system fault tree for each branching point, the events on this tree being conditional upon what has occurred earlier in the event tree sequence. The formal combination of event trees with conditional fault trees forms the basis of cause-consequence analysis and is examined in the next section. Figure 2.5 presents an event tree for the example system presented in Figure 2.1.

Event trees provide a logical framework for modeling specific accident sequences given an initiating event. Event trees typically model the safety system responses to an initiating event. If failure data is available at the system level they can be quantified directly. Usually the systems shown on an event tree need to be resolved to the component level by developing a fault tree for each branching point. A disadvantage of event trees is that there is no formal procedure to develop the required key initiating events and no formal construction procedures for the event tree. Event trees also suffer from the limitation that the identification of all potential accident sequences cannot be assured.

2.1.9 Cause-Consequence Diagrams

Cause-consequence analysis is a formalized combination of event tree and conditional fault tree analysis (Aerojet 1975; Nielsen 1971). The event tree is used to map out the sequence of events leading to the various consequences. The causes of these events, usually system failures, are modeled by conditional fault trees. Cause-consequence diagrams are basically event trees with the conditional fault trees directly attached to the branching points. The fault tree symbolism is the same, while the event tree symbolism is somewhat formalized (see Figure 2.6). As with an event tree, cause-consequence diagrams begin with an initiating event except that now this event may be expanded into its contributory failures. The combination of event trees with conditional fault trees, although not formalized into cause-consequence diagrams, formed the basis of the Reactor Safety Study (USNRC 1975). Figure 2.7 presents a cause-consequence diagram for the example system presented in Figure 2.1.

*VALVE FAILURE IS PICKED AS INITIATING EVENT

FIGURE 2.5 Event Tree For Example System

BRANCHING OPERATOR

Output is "yes" if condition is met; "no" otherwise.

DELAY OPERATOR

Indicates the amount of time delay required for output event to result from the input event.

DIRECTOR

Indicates the direction of event flow.

EVENT DESCRIPTOR

Describes the event present at specified position in chart.

CONSEQUENCE DESCRIPTOR

Describes the consequence. A terminal Symbol.

Inverse AND Gate

All outputs occur if the input occurs.

FIGURE 2.6 Symbols For Event Tree Segment of Cause-Consequence Diagram (Aerojet 1975)

FIGURE 2.7 Cause-Consequence Diagram For Example System

Cause-consequence analysis incorporates both fault tree and event tree analysis and utilizes the advantage of each technique. A complete problem can often be divided into manageable segments. A disadvantage is the lack of formal construction procedures and the potential difficulty of developing the key initiating events. A complete analysis may require cause-consequence diagrams for several initiating events and many individual fault trees.

2.1.10 G0 Methodology

The G0 methodology is a combined simulation and logic technique which models both hardware and logic operations on an overall flow chart (Gateley 1968). It is basically a success tree approach. (A success tree is analogous to a fault tree except that success rather than failure events comprise its makeup at all levels, including the TOP.) A G0 flow chart consists of "events" linked by hardware and logic operators to form some overall sequence of operation. Each "event" corresponds to the occurrence of output from a G0 operator and can occur in several states, each corresponding to an occurrence time for an output. Up to 128 states are possible, with 0 representing premature or spurious operation while the highest state represents a failure to operate (operation delayed over the entire mission time). As mentioned, the G0 operators correspond to both hardware, such as electrical components, and logic gates. Each is normally represented by a circle whose included numeral represents the type of operator. Figure 2.8 shows some of the more commonly used G0 operators. Figure 2.9 presents a simplified G0 model for the example system presented in Figure 2.1.

Being essentially a logic technique with additional capability to directly assimilate hardware operation, the G0 methodology possesses the capabilities of fault and event trees plus the capacity to model time-dependency through the various event states. These event states may also be used to simulate partial failures, alleviating the limitation of binary failure states prevalent in fault and event tree analysis. A major disadvantage of G0 is its complexity.

2.1.11 Markov Modeling

Markov modeling is a mathematical inductive analysis procedure which reduces a system of many stochastic processes, effects, and paths to a single stochastic relationship characterized by a series of discrete time processes.

Operator

Characteristic

1	Success/failure state
2, 10	Up to 10 inputs allowed
3	Initiates spurious signal
5	Initial input on flow chart
6, 7	Output only if both inputs are present
8	Adds/subtracts an integer to/from input value
9	Output determined by (S1-S2); NAND/exclusive OR gate
12	Mutually exclusive outputs
14	Output is linear combination of inputs
15	Output only if input within specified limits

FIGURE 2.8 GO Operators (Gateley 1968)

FIGURE 2.9 GO Model For Example System

As described by Rasmuson (1979), Markov models are functions of two random variables - the state of the system, and the time of observation. Any Markov model is defined by a set of probabilities P_{ij} which define the probability of transition from any state i to any state j . Another important feature of any Markov model is that transition probability P_{ij} depends only on states i and j and is completely independent of all past states except the last one, state i .

A Markov process can be specified by a set of differential equations and their associated initial conditions. Because of the basic Markov assumption that only the last state is involved in determining the probabilities, the analysis always yields a set of first-order differential equations. The constants in these equations can be specified by constructing a transition-probability matrix.

Markov models provide a quantitative assessment for stochastic system models. They can be resolved to either the component or system level. The method will only model discrete random processes that are independent of previous states. Markov models present a communication problem in that the approach is highly technical and difficult to describe to the non-technical person.

2.1.12 Consequence Models

The safety assessment methods discussed in the preceding sections deal primarily with identifying accidents and quantifying their probability of occurrence. For systems dealing with the processing, transfer, and/or storage of hazardous material, an assessment of the consequence of a potential release is a key aspect of any safety analysis. The analysis of the consequences of a potential release is usually accomplished in two stages. The amount and physical/chemical characteristics of the material released are estimated. Then the various pathways through the environment and the resulting consequences to man and the environment are examined. Both of these stages require appreciation of the basic laws of science and engineering to develop models of the important process.

The first stage of the consequence analysis is very specific to the system studies and general models have not been developed. The type of information required includes volatility, solubility, and frangibility data for the form of hazardous material in the system under study, the degree of confinement system failure, and transport and deposition of the release within the facility. The basic sources of required information are existing experimental data; test programs; engineering analysis; and engineering judgment.

Several general models exist for analyzing the transport of radioactive material in the environment and the consequences to man. Major pathways include atmospheric, groundwater, and surface water transport. The output of these models is combined with dose models which calculate the resultant dose to man. Streng (1976) and Raymond (1977) review the strengths and limitations of calculational models and computer programs for evaluating the dose assessment of radioactive releases.

A detailed discussion of the various consequence models is out of the scope of this study. Specific models are discussed in Section 3.0 as applicable.

2.2 RISK ANALYSIS METHODS

Recent developments in the safety assessment area have focused on risk analysis. A risk analysis is a systematic method drawing on the safety analysis methods described in Section 2.1 to relate the probability of a hazardous condition to its consequences. Appendix A presents a general discussion of the methods and approaches for risk assessment.

The most general definition of risk is that it is some function of the probability and the consequences of a release sequence. A frequently used definition of risk is the product of the anticipated frequency of a release sequence and its consequences. That is, risk is the mathematically expected consequence of a release sequence. In general a risk analysis of a system consists of the following basic steps: (1) Definition of the inventory of hazardous material and its containment/confinement barriers; (2) Identification of potential failure modes; (3) Estimation of the probability and amount of hazardous material released by the potential failure modes; (4) Analysis of the consequences of the hazardous material released; and (5) Estimation of the system risk.

The safety methods described in Section 2.1 can be combined in several ways to analyze each of these steps. Appendix B presents a detailed risk assessment method developed at PNL for analyzing nuclear fuel cycle operations (Pelto 1977; Smith et al. 1976).

As indicated in this section, various degrees of sophistication of safety analysis methods and output are possible. Safety analysis programs have different objectives and different constraints on time (when the work must be completed) and cost. They, therefore, differ in breadth and precision of analysis. Some programs involve existing systems with a great deal of applicable system definition and safety-related data. Safety/risk analyses of these systems can be performed in considerable depth and with good accuracy, if time and cost constraints are not severe. On the other hand, studies made during conceptual phases of system design preclude detailed analysis. Other things being equal, the later in the system life-cycle the study is performed, the more information is available and the greater the accuracy of the results. However, the sooner the analysis is made, the easier it is to effect any safety-related changes in the system under study or the conceptual design. A tradeoff is involved between the timeliness and the depth of accuracy of the analysis. Other programs require a tradeoff between the cost and the depth and accuracy of analysis. A variety of analytic methods and data retrieval systems is needed to satisfy the particular requirements of different safety analysis programs. Table 2.3 presents a summary table of selected characteristics of the various safety assessment methods discussed in this section.

TABLE 2.3 Summary of Safety Analysis Methods

	Quali- tative	Quanti- tative	Inductive/ Deductive	Compara- tive	Syste- matic	Compre- hensive	Com- plex	Failure/ Success Oriented	Repro- ducible	Scru- table	Pictorial	Models Sequential Action	Models Partial Failures	Models Time Dependence
Expert Opinion	yes	somewhat	N.A.	somewhat	somewhat (Delphi Method)	no	no	failure	no	somewhat	no	N.A.	N.A.	N.A.
Maximum Credible Accident	yes	yes	N.A.	yes	somewhat	somewhat	no	failure	somewhat	somewhat	no	N.A.	N.A.	N.A.
Design Basis Accident	yes	yes	N.A.	yes	somewhat	somewhat	no	failure	somewhat	somewhat	no	N.A.	N.A.	N.A.
Hazard Indices	no	yes	N.A.	yes	N.A.	no	no	N.A.	yes	somewhat	no	N.A.	N.A.	somewhat
PHA	yes	no	inductive	N.A.	yes	somewhat	no	failure	yes	yes	somewhat	no	no	no
FMEA	yes	somewhat	inductive	N.A.	yes	yes	somewhat	failure	yes	yes	somewhat	no	no	no
Fault Tree Analysis	yes	yes	deductive	N.A.	yes	yes	yes	failure	yes	somewhat	yes	somewhat	no	no
*Event Tree Analysis	yes	yes	inductive	N.A.	yes	somewhat	somewhat	failure	yes	yes	yes	yes	no	no
Cause-Conse- quence Analysis	yes	yes	both	N.A.	yes	yes	yes	failure	yes	somewhat	yes	yes	no	no
GO Methodology	no	yes	both	N.A.	yes	yes	yes	success	yes	no	yes	yes	yes	yes
Markov Models	no	yes	inductive	N.A.	somewhat	N.A.	yes	success	somewhat	no	yes	yes	yes	yes
Consequence Analysis	no	yes	N.A.	yes	somewhat	yes	yes	N.A.	somewhat	no	no	N.A.	N.A.	somewhat

*Excludes conditional fault trees. These are included with event trees as cause-consequence analysis.

3.0 APPLICATIONS TO NUCLEAR WASTE MANAGEMENT

Nuclear waste management operations are divided into two steps: 1) the short-term operating steps and 2) long-term storage or isolation. Figure 3.1 provides a schematic of the potential wastes from the LWR fuel cycle (Pelto et. al. 1977). The following categories of waste are considered in this report: 1) High-level wastes (HLW); 2) Transuranic wastes (TRU); 3) Low-level wastes (LLW); and 4) Airborne wastes. The methods described in Section 2.0 have been applied to these waste streams with varying degrees of detail. This section summarizes representative applications of safety assessment methods to the processing and storage/isolation of the above waste streams.

3.1 HLW SAFETY APPLICATIONS

HLW operations are divided into short-term operational activities and long-term waste isolation.

3.1.1 Short-Term HLW Management Activities

For HLW, short-term operational steps include liquid storage, solidification and canning, interim storage, and the emplacement operations at a geologic repository.

A report prepared by Oak Ridge National Laboratory (1970) analyzed the consequences of an airborne and a groundwater release from a HLW storage tank. Worst case analyses were performed and used to compare acid versus neutralized waste. A hydrogen explosion was postulated to initiate an airborne release. No probabilities were estimated and the large consequences illustrated the need for a reliable hydrogen control system. The type of waste did not affect the airborne consequences. A leak in a tank was postulated to release radioactive waste solutions to the soil beneath the tank. A procedure for determining the consequences was developed using an ion exchange column model. A specific site was analyzed (a shale formation). No probabilities were estimated. A need for actual tests of seepage and dispersion was noted.

FIGURE 3.1 Potential LWR Fuel Cycle Wastes

A report prepared by the Atlantic Richfield Hanford Company (1973) described a preliminary safety analysis of a water basin storage concept for solidified HLW. Safety considerations were categorized as normal, abnormal, and accident conditions and potential releases were postulated for each category. A maximum credible accident was defined as a massive canister failure in the receiving cell. The ventilation and filtration systems are assumed to function. This accident results in a first year bone dose to an individual at the exclusion zone boundary of .15 rem. Other lower-probability-higher-consequence accidents were discussed but not quantified. This report is a good example of the maximum credible accident approach.

McGrath (1974) reviewed waste management strategies and discussed risk and risk reduction. Detailed analyses were not performed, but an interesting approach was presented based on an expected risk criterion. Using this criterion and postulating upper limit consequences for liquid waste storage, waste solidification, and solid waste storage, he estimated permissible upper limit accident probabilities. The conclusion was that the most stringent safety requirements apply to liquid waste storage. A series of potential accidents was also postulated for these operations. No formal attempt was made to quantify them. Input needs for a total risk evaluation were identified and a systems approach for the evaluation of HLW risks was proposed.

Smith and Kastenbergh (1975) gave a background discussion on risk analysis and waste management and performed a brief risk analysis for extra-terrestrial disposal and interim surface storage. The release scenarios analyzed were simply postulated directly and the results indicate, within the assumptions used, that the risks of these management schemes are small compared with that of natural background radiation. Engineering judgment was used to obtain the release fractions. Limitations on the analysis included the small number of postulated accident events, the lack of failure data, and the lack of definitive design information.

Winegardner et. al (1976) and Pelto et. al (1977) applied the fault tree method described in Appendix B to a conceptual high-level waste management system. This system consisted of operations involving 1) liquid storage; 2) solidification; 3) water basin storage; 4) rail transport; and 5) retrievable surface storage.

Dominant failure sequences for the accidental release of radionuclides were identified for the various activities of the reference system. Dominant sequences were defined as those with the highest mathematical product of probability and consequences, the latter in terms of quantities of waste released. The initial assessment revealed that dominant scenarios that could conceivably have significant public health and safety impact were highly improbable, e.g., on the order of 10^{-6} per year of operation.

Accidental releases of radioactive material initiated by both process operating events and events external to the plant (e.g., earthquake) were found to contribute to total system risk. Except for the mechanically or electrically induced interruption of cooling water to stored liquid and solidified waste, postulated release scenarios contributing the bulk of the risk generally involved sequences initiated by external events.

Dominant scenarios with conceivable significant public health and safety impact were associated with the passive storage activities rather than with the relatively active modes of solidification and transportation. This appears to be due primarily to the large radionuclide inventories associated with the storage activities. Dominant scenarios were associated with airborne pathways.

This study identified several areas of information needs. These were placed in the following closely-related categories: 1) Additional information on the probability of breaching containment/confinement barriers versus the severity of the breach; 2) Data on the quantity, transport mechanism, and the chemical-physical form of the radioactive material released from failed barriers; 3) More information on system characteristics and interactions in the accident environment; and 4) More information characterizing the solidified high-level waste form.

Wingender (1976) applied a modified version of the fault tree approach described in Appendix B to a HLW tank farm and vitrification plant. Results are presented in terms of both curies released and inhalation radiation dose to a maximum individual. The expected release (probability times dose) was .02 mrem/year for the tank farm and .07 rem/year for the vitrification plant. The study did not present the detailed probability data used or the release fraction assumptions. One can assume that there was some uncertainty and this should have been addressed in the study. It is not clear from the analysis whether severe external events were addressed.

J. J. Cohen et. al (1977) performed a safety study utilizing a systems approach for the handling, storage, transportation, and disposal of solidified HLW. Failure modes, probabilities of failure, and the severity of consequences were determined for each step. Event tree methodology was used to determine potential failure modes. The best data available and engineering judgment were used to evaluate probabilities and consequences. Results were presented in expected curies per megawatt year. Two major accident types were determined to dominate -- drainage of the interim storage pool and a transportation accident. This study contains several major weaknesses. Event tree methodology is used to display accident sequences. No detailed event tree analysis was performed. A few representative accident sequences were postulated directly. No detailed reference system was postulated. The normalized approach used does not indicate the consequences of individual contributing events. The probability analysis has several technical holes and seems to neglect common-cause failures and dependencies. Oston et. al. (1979) provided follow-on information for this study.

The U.S. Department of Energy (1980) has completed the Environmental Impact Statement of Commercially Generated Radioactive Wastes. A supporting document was prepared (DOE 1979) which provides the technical backup for the impact statement. The safety aspects of the HLW operations are analyzed in this document along with the other types of waste streams. The accident analysis basis consisted of developing a spectrum of representative accidents. Accident frequencies and source terms were estimated and the accident scenarios classified into three groups: minor, moderate, and severe. The main emphasis

of the accident analysis was those with a potential for offsite releases. Several accidents which could expose plant workers were identified.

Detailed facility descriptions of HLW processing and interim storage operations were given. Representative accidents were postulated for liquid HLW storage, vitrification, and solidified HLW storage, transportation of HLW, and handling of HLW canisters at a repository. The accidents were realistically postulated and low-probability-high-consequence accidents were not directly considered. This study also quantified routine effluents and occupational exposure for HLW operations.

Waite (1980) and Waite and Kaczmarzsky (1981) analyzed the safety aspects of the repository operational phases. These include construction, operation, transportation, decommissioning, and postclosure. This study utilized the results of the commercial waste management impact statement (DOE 1979) and conceptual repository designs. Routine and accidental radiological dose exposures were estimated. Occupational and population doses were considered. Routine occupational exposures were assessed by 1) specifying each task associated with operations of the repository, 2) estimating the duration of each task, 3) characterizing the radiological conditions surrounding each task and 4) establishing the number of workers for each task. The estimated occupational external dose was 290 person-rem. Only two operational accidents were described - venting a leaky fuel assembly and a hoist drop accident. No estimates were given on the probabilities of occurrence. This study is very preliminary and more detailed work using specific repository designs should be performed.

A report prepared by the Nuclear Energy Agency Organization for Economic Cooperation and Development (NEA 1981) performed a survey safety analysis of the nuclear fuel cycle. HLW operations were included. HLW systems were briefly described and potential safety problems identified. This report is a good example of the use of expert opinion. Some of the safety problems discussed include extended loss of cooling situations for storage operations and the design of process control systems and air cleaning systems and their behavior in abnormal situations for solidification operations. The study recommended additional work in these and other related areas.

3.1.2 Long-Term Isolation of HLW

Present programs in the U.S. and elsewhere for commercial HLW are aimed at isolation in deep geologic formations. Research into the safety of waste disposal has been conducted in several countries. The Electric Power Research Institute sponsored a study (The Analytic Sciences Corporation 1979) which reviewed ten major safety studies of HLW geologic isolation. These are summarized in this section along with some additional studies.

Claiborne and Gera (1974) analyzed potential failure mechanisms and their consequences for a repository in bedded salt in New Mexico. Causes of containment failures examined included drilling through the geologic disposal formation, impact of a meteorite, volcanic activity, a fault intersecting a repository, sabotage, nuclear warfare, increase in salt dissolution rates, and waste disinterment by erosion of the overburden. The primary conclusion was that a serious breach of containment for such a repository is only a very remote possibility. Consequence estimations were made only for a meteorite impact. Probability estimates were given for meteorite impact and for faulting. Other events were analyzed qualitatively. This study formed the basis for later work. Some weaknesses are the lack of detailed geologic and hydrologic data and the failure to address self-induced failure due to the presence of the repository.

De Marsily, et. al (1977) reviewed previous investigations in the U.S. and characterized the effects of various geologic parameters on the migration of radionuclides through rock. A simplified transport model was used and the transport of ^{129}I , ^{239}Pu , and ^{237}Np was analyzed (these were assumed to be the major radionuclides of interest). The effect of two leaching models was examined. Sorption phenomena (ion exchange, filtrations, etc.) were found to be the most important factors in confining radionuclides with long half-lives. The analysis performed in this study is incomplete. More accurate data and models are necessary.

Girardi et. al (1977) used fault tree methodology for assessing the failure probabilities of salt domes and bedded salt as a function of time. Engineering judgment was required to generate much of the failure data.

Exhumation of waste by man was identified as the most likely cause of failure during the first 10,000 years. Groundwater contact with the waste is the most likely failure cause after 10,000 years. A simplified and conservative consequence model was developed for direct release of waste into a surface river. Leach rate, therefore, was a dominant parameter. The projected radiological doses were small. This study was of a scoping nature. The fault tree model used requires failure rate data not readily available. The rigorous application of fault tree analysis to repository failure analysis has been questioned by several researchers.

Hill and Grimwood (1978) described potential mechanisms that would release waste from a repository and analyzed the consequences of groundwater circulation through the buried wastes. Probabilities for a meteorite impact, a volcano, and seismic activity were estimated. No probability estimates were made for the potential of groundwater circulation due to lack of site-specific information. Waste transport is modeled by the same set of equations used by Burkholder (1975). This model takes into account the differential transport of radionuclides within the same decay chain and improves the transport calculations for the ^{234}U , ^{230}Th , ^{226}Ra decay chain. The peak individual whole body dose occurs at 10^4 years and is 5 mrem. This study presents a preliminary assessment and serves primarily to provide input for the development of more sophisticated models. The effects of uncertainty in the data base used needs to be investigated.

Burkholder et. al (1975, 1976) developed a transport model and applied it to investigate the incentives for separating and eliminating various elements from radioactive waste prior to final geologic storage. Groundwater contact with the waste was assumed. No probability values were given. For the cases considered, the incentives for removing selected radionuclides from the HLW were small because the hazard from the HLW is already small. The geosphere transport model is one-dimensional and models the differential transport of radionuclides within the same decay chain. The method of solution is analytical. Biosphere transport and dose models were taken from earlier generic models used for nuclear power plant effluents. An extensive sensitivity study was performed on the important geologic parameters. ^{14}C

was found to contribute the maximum 50 year accumulated individual dose. This study used a higher initial inventory of ^{14}C and radium than the studies described earlier. It is the most complete generic study of groundwater intrusion into a HLW repository. No probability estimates are given for the scenario.

A report prepared by Kärn-Bränsee-Säkerhet (1978) described a risk assessment study for a HLW repository in Sweden. Circulation of groundwater was concluded to be the only important release mode. The transport of radionuclides through rock was modeled by the transport model developed by Burkholder (1975). A compartment-type biosphere model was used. The well water scenario was found to result in the highest individual dose. The predicted doses were very small. This study was site specific and offers some improvements over those discussed in previous sections. In situ tests were performed to validate the nuclide migration models and retardation factors. The study emphasized the potential for engineered barriers to insure long-term safety. The reference design utilizes costly engineered systems. Potential improvements include testing the proposed leaching behavior of vitrified HLW. The study also could be improved by investigating sudden disruptive events more rigorously.

Berman et. al (1978) have developed and applied a methodology for long-term general assessment of mined disposal of nuclear wastes. The objectives were to construct a flexible and efficient model for generic and potential repository sites. The models developed were used to study the effects of different parameter values on the isolation effectiveness of a given repository. Only the escape of radionuclides by transport in ground water was considered. Bedded salt and shale emplacement media were considered. Computer models were developed to quantify the geosphere and biosphere transport and the resulting dose. The geosphere model can model flow through many underground pathways. The predicted doses were quite similar for both repositories (shale and bedded salt). A three-million-year time frame was considered and ^{99}Tc was the critical radionuclide. The doses were small and normalized to a GWe-yr basis. Radionuclide release via well water was not considered in detail. Inhalation pathways were not addressed.

Logan and Berbano (1978) developed a methodology for evaluating the environmental adequacy of proposed waste management alternatives. The model was applied for demonstration purposes to a reference repository in bedded salt. The model used incorporates fault tree analysis, a release model, an environmental model and an economic and health effects model. Fault trees are used to organize release events and compute their likelihood. Disruptive events analyzed included meteorite impact, volcanic activity, and faulting. On a probabilistic basis the volcanic release event was found to be dominant. A conservative approach is used throughout. Some potential errors exist in the expression used for the probability function and in the groundwater transport model. Logan et. al (1980) used a revision of this model to examine the effect of actinide partitioning and transmutation (P-T) on waste repository risk. P-T was found to have only limited effectiveness in reducing long-term risk.

Campbell et. al (1978), Dillon et. al (1978), and Iman et. al (1978) summarized research performed to develop analytical risk assessment methods for use by the NRC in licensing waste repositories. No overall risk assessment was performed, but various aspects of the methods developed were demonstrated. External release events were modeled on a probabilistic basis. Self-induced release events are deterministically modeled using numerical simulation techniques. A three-dimensional ground water transport code was developed and a multicompartment environmental transport model was used. The models developed are detailed and are highly dependent on assumptions made by the user which may be very difficult to justify or validate. Campbell et. al (1980) and Iman (1980) describe refinements to these models.

B. L. Cohen (1977) performed a simplified assessment of the long-term risks from the mined disposal of HLW. The approach used avoided all the complex and detailed modeling on which other studies are based. Cohen examined the HLW from a 400 GWe-yr installed capacity of nuclear electricity. He used the BEIR Report to derive the number of cancers resulting from ingestion of all of the HLW. Cohen then multiplied the calculated number of cancers by the average probability of an atom of waste being ingested by man. A value of 4×10^{-13} /yr was estimated by comparing the amount of radium in the soil to

the observed concentration of radium in surface waters. The resultant risk versus time curve was integrated from the time waste is first assumed to reach man out to one million years. Only about 0.4 deaths are predicted. Several criticisms have been made of this study. One is that waste may more likely be released from a repository than natural radium from rock and soil. Concentration of radionuclides other than radium in the food chain is ignored. No assessment is made of the possible long-term buildup of radionuclides in the environment.

Silviera et. al. (1980) summarize the work conducted at PNL to develop and improve methods to assess the long-term effectiveness of isolating nuclear wastes in geologic formations. This work started in 1976 in the Waste Isolation Safety Assessment Program (WISAP) and continues in the Assessment of Effectiveness of Geologic Isolation Systems (AEGIS) Program. This approach consists of eight steps. First, information is acquired on the geologic, hydrologic and engineered systems of the proposed repository site. A conceptual description of the existing regional geologic and hydrologic systems is developed. Computer codes to model groundwater flow patterns are applied. Plausible natural disruptive events or human activities that could breach the geologic isolation systems are evaluated. Computer codes are applied to model natural disruptive events and their influence on the repository. Groundwater flow paths of the future hydrologic system are modeled by computer code. Radionuclide transport to the accessible environment is modeled by computer codes. Radiation dose cases are applied to estimate the potential impact on individuals and populations. Cole and Bond (1980) summarized the application of the release consequence methodology to four hypothetical repository sites.

Arthur D. Little, Inc. (1977a; 1977b; 1977c; 1977d) performed a study for the EPA which characterized the source terms for HLW disposal, examined the effectiveness of engineering controls, and assessed migration pathways and accidental pathways. For the analysis of migration potential a simplified geosphere model was selected. Diffusive transport to the aquifer and direct convective transport to the aquifer were modeled. Dose commitments were estimated and were typically below that due to natural background. Principal

radiation dose effects were from strontium-90, iodine-129, radium-226, neptunium-237 and plutonium-239 and -240. Ten descriptive events were postulated including such events as shaft seal failure, future drilling, fault movement, and meteorite impacts. Probability estimates were made. No consequence calculations were performed for the disruptive events. Background information for some of this work is given in a report of an ad hoc panel of earth scientists (EPA 1977).

Voss (1979) examined and critiqued thirteen hazard indices. These ranged from the total radioactivity Q to the hazard measure HM (see Section 2.1.4) to the hazards available HA. HA has been developed to account for pathways to man. Voss applied seven of these indices to HLW and spent fuel. The hazards indices were shown to provide useful qualitative comparisons. Some of the simple indices are more useful (e.g. Q and HM). Not enough information is typically available to quantify the more complicated ones (e.g. HA). The HLW and spent fuel comparison showed that solidified HLW may be potentially less hazardous than packaged spent fuel. This study is primarily a methods demonstration study.

3.2 TRU WASTE SAFETY APPLICATIONS

TRU waste management operations are also divided into short-term operational activities and long-term waste isolation. The same methods discussed under short-term HLW are applicable to TRU waste. It is anticipated that commercial TRU waste will be disposed of in a geologic repository. The HLW geologic isolation safety studies discussed earlier are also applicable to TRU waste. For these reasons, TRU waste safety applications were not reviewed in detail. Three recent studies are summarized below.

The Environmental Impact Statement of Commercially Generated Radioactive Wastes supporting documents (DOE 1979) analyzed the TRU waste management operations. Waste streams examined include fuel residue from a fuel reprocessing plant (FRP), failed equipment and noncombustible waste from an FRP and a mixed oxide fuel fabrication plant (MOX FFP), combustible and compactable waste from an FRP and a MOX FFP, and wet waste particulate solids from an FRP and a MOX FFP. Reference facility descriptions were given and a list of representative accidents was postulated. Processing, packaging,

storage, transportation, and disposal operations were examined. The frequencies and consequences of the representative accidents were quantified. Routine effluents and occupational exposure were also estimated. The potential radiation exposures from the waste management operations were small. The accident analysis given was not complete. The accidents were realistically postulated and low-probability-high-consequence accidents were not directly considered.

Pelto and Voss (1979) performed a comparative assessment of the waste management safety implications of a once-through fuel cycle and a coprocessed UO_2 - PuO_2 fuel cycle. The TRU waste streams were considered. Hazard indices were developed for routine releases, occupational exposure, and accidental releases. The safety aspects of the TRU wastes were found to be small when compared to the HLW. This study was primarily a methods demonstration study.

A report prepared by the Nuclear Energy Agency Organization for Economic Cooperation and Development (NEA 1981) performed a survey safety analysis of the nuclear fuel cycle. Fuel cladding waste and plutonium contaminated solid wastes were included. Areas for further work include improved methods for plutonium content determination and the development of designs to minimize the production of TRU wastes. A comprehensive safety analysis of the TRU waste management system was recommended.

3.3 LLW SAFETY APPLICATIONS

LLW waste management operations consist of processing, packaging, transportation and disposal. Most of the current safety work examines LLW burial grounds. Four recent studies are summarized below.

Macbeth et. al. (1979) evaluated alternative methods for the disposal of LLW. A comparative analysis of four basic alternatives to shallow land burial of solid LLW was performed. These included deeper burial, disposal in mined cavities, disposal in engineered structures and ocean disposal. Several factors were evaluated for comparison, including those important to safety, namely waste compatibility, safeguards and environmental effects. The general approach involved definition of a reference disposal facility and a reference inventory of radioactive LLW. The operational phase as well as post-disposal

short and long-term effects were considered. Potential health effects from waste transportation were also included in the analysis. In addition to radiological effects, those from non-radiological sources, such as industrial accidents, were evaluated. Little variation was evident among the alternatives regarding waste compatibility and safeguards. Greater variation existed for the environmental effects, especially between Eastern and Western sites. Overall, the safety considerations were dominated by the transportation aspect.

Little (1981) described a computer program for LLW transport and risk assessment. A computer code PRESTO (Prediction of Radiation Effects from Shallow Trench Operations) has been developed to evaluate possible health effects from shallow land burial trenches. The generic model assesses radionuclide transport and the resulting exposure and health effects to a static local population over a 1000-year period. Natural radionuclide transport processes, such as groundwater transport, as well as direct human exposure scenarios, such as intrusion, are considered. Doses to both the individual and the population are calculated as well as cumulative health effects (fatalities) for the population over the 1000-year period. Data bases are under development for the shallow burial sites at Barnwell, SC; Beatty, NV; and West Valley, NY.

Rodgers and Onishi (1981) are developing an LLW site evaluation methodology. The overall effort focuses on three areas: land-use evaluation, environmental transport modeling, and long-term scenario development, including long-range climatology projections. A four-step methodology is proposed, consisting of the following:

1. land use suitability assessment
2. land use - ecosystem interaction determination
3. biotic and abiotic simulation of containment transport in the environment
4. sensitivity analysis.

Specific modeling techniques are suggested for use in these steps, including the BIOTRAN meteorological model, the Agricultural Runoff Management (ARM) model for hydrology, and the Sediment and Radionuclide Transport (SERATRA) model for migration.

Kahle and Rowlands (1981) performed a site specific safety analysis of trench subsidence and potential stabilization methods for the Sheffield LLW disposal site. The geology, hydrology, and meteorology were specified for the actual site, providing a better data base than that typically used for generic analyses of this type. Actual data was available on trench subsidence and was used to develop an overall model. The following mechanisms were identified as causing subsidence and settlement: piping and settlement of trench backfill soil into voids, consolidation of the trench backfill soil, and deterioration of the wastes and containers by corrosion and biodegradation. Several trench stabilization techniques were investigated: dynamic consolidation, compaction by pile-driving, surcharging, surface compaction by heavy equipment, compaction grouting using soil-cement, and grouting using soil-cement and acrylamide. Of these, surcharging was found to be least hazardous for exposing waste to the environment, and for exposing workers and equipment to waste.

3.4 AIRBORNE WASTE SAFETY APPLICATIONS

Airborne waste management operations consist of separation, processing, packaging, transportation, and disposal. Carbon-14, krypton-85, and iodine-129 are the major radionuclides of interest. Three recent studies are summarized below.

Christensen et. al. (1980) performed a preliminary safety evaluation of a commercial-scale krypton-85 encapsulation facility. A catastrophic failure of the high pressure vessel during an encapsulation run was assumed to be the maximum credible accident. No detailed analysis was made of other potential release sources and no probability calculations were performed. The consequences of this maximum credible accident were analyzed. The explosive characteristics of vessel rupture were quantified. Engineered safety features to contain vessel fragments and krypton-85 released were proposed. Further safety evaluations of the probability and consequences of a more comprehensive list of accidents are necessary.

Evans et. al. (1980) performed a preliminary comparison of the various alternatives for the collection and fixation of carbon-14, krypton-85, and iodine-129 and for transportation and storage/disposal of the resulting

waste forms. Evaluation parameters included simplicity, reliability, safety, cost, state-of-the-art, and material handling. A numerical rating system was devised and a relative numerical rating on a scale of 1 to 10 was assigned to candidate processes. These values were subjective and based upon engineering judgment. The safety parameter was given a weight factor of 2 (cost was 1.5 and state-of-the-art was 3). This rating system permits qualitative safety comparisons of different processing options for each radionuclide. For example, ion implant was assigned a value of 16 and encapsulation was assigned a value of 10 for krypton fixation. Safety comparisons between radionuclides typically overlapped. No specific safety recommendations were made in this study. More detailed safety analyses of specific accidents are required.

Mellinger et. al. (1980) examined the radiological consequences arising from the trade-offs for krypton-85 waste management alternatives. A representative system using cryogenic distillation and storage in steel cylinders was selected as the basis for this study. For the case of krypton-85 recovery, both public and occupational radiation exposures were evaluated. Radiation doses occur to workers in the recovery and storage facilities during operations and maintenance activities and from accidental releases. Doses to the general public occur from non-recovered krypton-85, from the release of residual krypton-85 at the end of the storage period and from possible accidents. These radiation exposures were compared with the radiological consequences from the total continuous atmospheric release of krypton-85. Occupational exposures were primarily due to maintenance activities. Public radiation exposure from accidents was estimated by postulating a list of representative accidents. The frequencies and consequences of these accidents were quantified. The results of this study indicated that it makes little difference to the magnitude of the world population dose whether krypton-85 is captured and stored or chronically released to the environment. This study illustrates the difficulty in comparing routine and accidental radiological exposures on the same basis. Also (as the study points out) comparisons of radiation exposures to very large populations at very low dose rates with much higher exposures to a small number of occupationally exposed workers may be misleading. External events (e.g. earthquake) were not considered in the accident analysis.

4.0 ONGOING WASTE MANAGEMENT SAFETY ANALYSIS RESEARCH PROGRAMS

Major research programs on all phases of nuclear waste management are currently being conducted in the United States and in other countries. The Department of Energy, the Nuclear Regulatory Commission, and the Environmental Protection Agency are conducting major research and development programs. This section briefly discusses ongoing safety related waste management research activities in foreign countries and in the United States.

The International Program Support project being conducted by Pacific Northwest Laboratory under U.S. Department of Energy sponsorship assembles and consolidates openly available information on foreign and international nuclear waste management programs and technology (Harmon and Kelman 1981). This review is conducted annually and includes information on safety research and development programs. Table 4.1 presents a summary of waste handling and isolation activities in foreign countries (DOE 1980). The last column identifies countries performing detailed safety-risk analysis.

The Department of Energy nuclear waste management program is described in the Nuclear Waste Management Program Summary Document (DOE 1980). Research and development is being carried out for defense nuclear waste, commercial nuclear waste, and spent fuel. Waste treatment technology, transportation, and terminal isolation research and development programs have been established. Safety analysis activities are being performed in each of these areas to support such areas as technology development and environmental impact statement preparation. A large effort to develop and apply safety analysis models to assess the safety of a geologic repository is in progress.

The Nuclear Regulatory Commission has specific regulatory responsibilities for high level waste, low level waste, uranium recovery and mill tailings, spent fuel storage, and transportation. Safety analysis work is being performed in each of these areas to support the development of appropriate regulations and regulatory guidance. NRC's program in these areas encompasses those activities associated with the safety and environmental reviews required

TABLE 4.1. Waste Handling and Isolation Activities
in Foreign Countries (DOE 1980)

	TRANS- PORTATION	INTERIM STORAGE	SHALLOW LAND BURIAL	GEOLOGIC ISOLATION	SEABED ISOLATION	AIRBORNE WASTE IMMOBILIZATION	SAFETY/ RISK ANALYSIS
Austria				X			X
Belgium	X			XX		X ^(a)	X
Canada		XX		XX		X	X
Denmark				X			
France	XX	X	X	XX	XX	X	XX
Federal Republic of Germany	XX			XX		XX	XX
India				X			X
Ispra							XX ^(b)
Italy				X			
Japan	XX			X	XX	X	X
Netherlands				X			X
Spain		X		X			
Sweden		XX		XX			XX
United Kingdom	X	X		X	XX	XX	XX
USSR	X	X	X	X			

a) Eurochemic/NEA program — Mol, Belgium

b) Joint Research Centre of CEC — Ispra, Italy

X) R&D activities underway.

XX) U.S. interest in cooperative program
is already identified.

for the licensing of these activities. NRC is also conducting a large effort to develop and apply safety analysis models to assess the safety of a geologic repository.

The Environmental Protection Agency has primary responsibility for establishing radiation protection guidance and for interpreting existing guides for other Federal agencies. The radioactive waste management activities include high level waste, uranium recovery operations (mill tailings), and all other wastes. The primary objective of EPA's waste management program is to develop environmental standards for the management and disposal of these wastes. EPA is conducting a research program in support of these activities and various safety assessments are being conducted. EPA is also conducting a large effort to develop and apply safety analysis models to assess the safety of a geologic repository.

5.0 CONCLUSIONS AND RECOMMENDATIONS

This report has reviewed the major system safety analysis methods and examined their application to nuclear waste management. Table 5.1 presents the methods summary table given earlier with a new category - previous application to waste management. As seen from the table, the maximum credible accident, design basis accident, hazard indices, and consequence analysis approaches have been used extensively in waste management safety analyses. These are the more deterministic and simpler approaches. The more complicated probabilistic approaches have not been used as extensively. Each of the methods described was found to be useful and applicable to waste management systems. As discussed earlier, a range of safety tools is required depending upon the stage of development of the particular waste management system and the objectives and constraints of the safety analysis program. The risk assessment approach described in Appendix B incorporates many of these safety analysis tools and provides a systematic technique for a detailed safety analysis of a nuclear waste management system.

Many safety analyses have been performed on nuclear waste management systems using the methods discussed in this report or similar methods. The results of those safety analyses indicate that suitable methods are available but their detailed application is limited by the lack of input data. Safety analysis methods will require refinements and improvements but the basic principles have been well established. The lack of input data has often necessitated the use of conservative assumptions.

Some specific information needs for improving waste management safety analyses and therefore their usefulness, can be placed in the following closely-related categories: (1) Additional information on the probability of breaching containment/confinement barriers versus the severity of the breach; (2) Data on the quantity, transport mechanism, and the chemical-physical form of the radioactive material released from failed barriers; (3) More information on system characteristics and interactions in the accident environment; and (4) More information characterizing the waste form. Research programs are addressing some of these areas. Stronger coordination of the process development research and development with the anticipated safety program requirements would assist in obtaining this information.

TABLE 5.1 Summary of Safety Analysis Methods

	<u>Quali- tative</u>	<u>Quanti- tative</u>	<u>Inductive/ Deductive</u>	<u>Compara- tive</u>	<u>Syste- matic</u>	<u>Compre- hensive</u>	<u>Com- plex</u>	<u>Failure/ Success Oriented</u>	<u>Repro- ducible</u>	<u>Scru- table</u>	<u>Pictorial</u>	<u>Models Sequential Action</u>	<u>Models Partial Failures</u>	<u>Previous Applications To Waste Management</u>
Expert Opinion	yes	somewhat	N.A.	somewhat	somewhat (Delphi Method)	no	no	failure	no	somewhat	no	N.A.	N.A.	some
Maximum Credible Accident	yes	yes	N.A.	yes	somewhat	somewhat	no	failure	somewhat	somewhat	no	N.A.	N.A.	many
Design Basis Accident	yes	yes	N.A.	yes	somewhat	somewhat	no	failure	somewhat	somewhat	no	N.A.	N.A.	many
Hazard Indices	no	yes	N.A.	yes	N.A.	no	no	N.A.	yes	somewhat	no	N.A.	N.A.	many
PHA	yes	no	inductive	N.A.	yes	somewhat	no	failure	yes	yes	somewhat	no	no	some
FMEA	yes	somewhat	inductive	N.A.	yes	yes	somewhat	failure	yes	yes	somewhat	no	no	some
Fault Tree Analysis	yes	yes	deductive	N.A.	yes	yes	yes	failure	yes	somewhat	yes	somewhat	no	some
*Event Tree Analysis	yes	yes	inductive	N.A.	yes	somewhat	somewhat	failure	yes	yes	yes	yes	no	some
Cause-Conse- quence Analysis	yes	yes	both	N.A.	yes	yes	yes	failure	yes	somewhat	yes	yes	no	few
GO Methodology	no	yes	both	N.A.	yes	yes	yes	success	yes	no	yes	yes	yes	few
Markov Models	no	yes	inductive	N.A.	somewhat	N.A.	yes	success	somewhat	no	yes	yes	yes	few
Consequence Analysis	no	yes	N.A.	yes	somewhat	yes	yes	N.A.	somewhat	no	no	N.A.	N.A.	many

*Excludes conditional fault trees. These are included with event trees as cause-consequence analysis.

Areas requiring methods refinement and development include improvements in the analysis of occupational exposure, uncertainty, common-cause failures, and operator error. In addition an improved comparative safety method to support decision making for such areas as alternative processing methods and alternative waste forms would be useful.

REFERENCES

- Aerojet Nuclear Company. 1975. Methods for Reliability and Safety Engineering, MAP-0015, Idaho Falls, Idaho.
- The Analytic Sciences Corporation. 1979. Status Report on Risk Assessment for Nuclear Waste Disposal, EPRI NP-1197, Reading, Massachusetts.
- Arthur D. Little, Inc. 1977a. Technical Support of Standards for High-Level Radioactive Waste Management. Task A Report Assessment of Migration Pathways, EPA 520/4-79-007A, Cambridge, Massachusetts.
- Arthur D. Little, Inc. 1977b. Technical Support of Standards for High-Level Radioactive Waste Management. Task B Report Engineering Controls, EPA 520/4-79-007B, Cambridge, Massachusetts.
- Arthur D. Little, Inc. 1977c. Technical Support of Standards for High-Level Radioactive Waste Management. Task C Report Migration Pathways, EPA 520/4-79-007C, Cambridge, Massachusetts.
- Arthur D. Little, Inc. 1977d. Technical Support of Standards for High-Level Radioactive Waste Management. Task D Report on Assessment of Accidental Pathways, EPA 520/4-79-007D, Cambridge, Massachusetts.
- Atlantic Richfield Hanford Company. 1973. Retrievable Surface Storage Facility Water Basin Concept Conceptual System Design Description, ARH-2799, Richland, Washington.
- Berman, L. E. et al. 1978. Analysis of Some Nuclear Waste Management Options, UCRL-13917, The Analytic Sciences Corporation, Reading, Massachusetts.
- Burkholder, H. C. et al. 1975. Incentives for Partitioning High-Level Waste, BNWL-1927, Pacific Northwest Laboratory, Richland, Washington.
- Burkholder, H. C. et al. 1976. "Incentives for Partitioning High-Level Waste," Nuclear Technology, 31:202.
- Campbell, J. E. 1978. Risk Methodology for Geologic Disposal of Radioactive Waste: Interim Report, SAND78-0079, Sandia Laboratories, prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-0458.
- Campbell, J. E. et al. 1980. Risk Methodology for Geologic Disposal of Radioactive Waste: Transport Model Sensitivity Analysis, NUREG/CR-1377, Sandia National Laboratories, Albuquerque, New Mexico.
- Christensen, A. B. et al. 1980. Preliminary Safety Evaluation of a Commercial-Scale Krypton-85 Encapsulation Facility, ENICO-1055, Exxon Nuclear Idaho Company, Incorporated, Idaho Falls, Idaho.

- Claiborne, H. C. and G. Gera. 1974. Potential Containment Failure Mechanisms and Their Consequences at a Radioactive Waste Repository in Bedded Salt in New Mexico. ORNL-TM-4639, Oak Ridge National Laboratory, Oak Ridge, Tennessee.
- Cohen, B. L. 1977. "High-Level Radioactive Waste from Light Water Reactors," Reviews of Modern Physics, 49:1.
- Cohen, J. J. et al. 1977. Determination of Performance Criteria for High-Level Solidified Nuclear Waste, NUREG-0279, Lawrence Livermore Laboratory, Livermore, California.
- Cole, C. R. and F. W. Bond. 1980. Summary of Four Release Consequence Analyses for Hypothetical Nuclear Waste Repositories in Salt and Granite, PNL-3548, Pacific Northwest Laboratory, Richland, Washington.
- Dalkey, N. C. and O. Helmer. 1963. "An Experimental Application of the Delphi Method to the Use of Experts." Management Science. 9(3).
- de Marsily, G., E. Ledoux, A. Barbreau, and J. Margot. 1977. "Nuclear Waste Disposal: Can the Geologist Guarantee Isolation?," Science, 197(4303):519-527.
- Dillon, R. T., R. B. Lantz, and S. B. Pahwa. 1978. Risk Methodology for Geologic Disposal of Radioactive Waste: The Sandia Waste Isolation Flow and Transport (SWIFT) Model. SAND 78-1267, Sandia Laboratories, prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-0424.
- Evans, A. G. et al. 1980. Management of Radioactive Waste Gases from the Nuclear Fuel Cycle - Volume 1 Comparison of Alternatives. NUREG/CR-1546, E. I. duPont de Nemours & Co., Savannah River Plant and Laboratory, Aiken, South Carolina.
- Gateley, W., et al. 1968. GO-A Computer Program for the Reliability Analysis of Complex Systems," KN-67-704, Kaman Sciences Corp., Colorado Springs, Colorado.
- Girardi, F., G. Bertozzi, and M. D'Alessandro. 1977. Long-Term Risk Assessment of Radioactive Waste Disposal in Geological Formations. Commission of the European Communities, EUR 5902.e, Ispra, Italy.
- Gordon, T. J. and O. Helmer. 1964. Report on a Long-Range Forecasting Study. Rand Paper P-2982, Rand Corporation, Santa Monica, California.
- Greenborg, J., et al. 1978. Waste Isolation Safety Assessment Program Scenario Analysis Methods for Use in Assessing the Safety of the Geologic Isolation of Nuclear Waste. PNL-2643, Pacific Northwest Laboratory, Richland, Washington.
- Haas, D. F. 1974. "Fault Tree Analysis." Course notes, Joint Center for Graduate Studies, Richland, Washington.

- Harmon, K. M. and J. A. Kelman. 1981. Summary of Non-U.S. National and International Radioactive Waste Management Programs 1981. PNL-3881, Pacific Northwest Laboratory, Richland, Washington.
- Helmer, O. 1966. Social Technology. Basic Books, New York, New York.
- Hill, M. D. and P. H. Grimwood. 1978. Preliminary Assessment of the Radiological Protection Aspects of Disposal of High-Level Waste in Geologic Formations. NRPB-R69, National Radiological Protection Board, Harwell, United Kingdom.
- Iman, R. L. et al. 1978. Risk Methodology for Geologic Disposal of Radioactive Wastes: Sensitivity Analysis Techniques. SAND78-0912, Sandia Laboratory, prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-0394.
- Iman, R. L. et al. 1980. Risk Methodology for Geologic Disposal of Radioactive Waste: Small Sample Sensitivity Analysis Techniques for Computer Models, NUREG/CR-1397, Sandia National Laboratories, Albuquerque, New Mexico.
- Kärn-Bränsle-Säkerhet. 1978. Nuclear Fuel Safety Project, Handling of Spent Nuclear Fuel and Final Storage of Vitrified High-Level Reprocessing Waste. Stockholm, Sweden.
- Kahle, R. and J. Rowlands. 1981. Evaluation of Trench Subsidence and Stabilization at Sheffield Low-Level Radioactive Waste Disposal Facility. NUREG/CR-2101, Ralph Stone and Company, Inc., Los Angeles, California.
- Lambert, H. E. 1973. Systems Safety Analysis and Fault Tree Analysis. UCID-16238, Lawrence Livermore Laboratory, University of California, Livermore, California.
- Little, C. A. et al. 1981. "The PRESTO Low-Level Waste Transport and Risk Assessment Code," in Proceedings of the Symposium on Waste Management at Tuscon, Arizona.
- Logan, S. E. and M. C. Berbano. 1978. Development and Application of a Risk Assessment Method for Radioactive Waste Management. EPA 520/6-78-005, U.S. Environmental Protection Agency, Washington, D.C.
- Macbeth, P. et al. 1979. Evaluation of Alternative Methods for the Disposal of Low-Level Radioactive Wastes. NUREG/CR-0680, Ford, Bacon, & Davis Utah, Inc., Salt Lake City, Utah.
- McGrath, P. E. 1974. Radioactive Waste Management Potentials and Hazards from a Risk Point of View. KFK-1992, Gesellschaft für Kernforschung mbH, Karlsruhe, Germany.
- Mellinger, P. J. et al. 1980. ⁸⁵Kr Management Trade-offs: A Perspective to Total Radiation Dose Commitment. PNL-3176, Pacific Northwest Laboratory, Richland, Washington.

- Nielsen, D. S. 1971. "The Cause/Consequence Diagram Method as a Basis for Quantitative Reliability Analysis." Presented at the ENEA/CREST Meeting on Applicability of Quantitative Reliability Analysis of Complex Systems and Nuclear Plants in its Relation to Safety, Munich.
- Nuclear Energy Agency Organization for Economic Cooperation and Development. 1981. Safety of the Nuclear Fuel Cycle. A State-of-the-Art Report by a Group of Experts of the NEA Committee in the Safety of Nuclear Installations.
- Oak Ridge National Laboratory. 1970. Siting of Fuel Reprocessing Plants and Waste Management Facilities. ORNL-4451, Oak Ridge, Tennessee.
- Oston, D. A. et al. 1979. Aspects of Nuclear Waste Management. Volume 1. Pre-emplacement Risks. UCRL-15167 (Vol. 1), The Analytic Sciences Corp., Reading, Massachusetts.
- Ott, K. O. 1976. Risk-Assessment Methodology for Fast Breeder Reactors. ANL-76-39, Argonne National Laboratory, Argonne, Illinois.
- Pelto, P. J., T. H. Smith, J. W. Bartlett. 1977. "Risk Assessment Methods for Nuclear Waste Management Systems." In Proceedings: A Workshop On Issues Pertinent to the Development of Environmental Protection Criteria for Radioactive Wastes, ORP/CSD-77, February 1977, The U.S. Environmental Protection Agency, Office of Radiation Programs, Washington, D. C.
- Pelto, P. J. and W. K. Winegardner. 1977. "A Risk Assessment Method for Nuclear Fuel Cycle Operations." In ANS Transactions, Vol. 26, June 1977, 23rd Annual ANS Meeting, New York, NY.
- Pelto, P. J. and J. W. Voss. 1979. Comparative Techniques for Nuclear Fuel Cycle Waste Management Systems. PNL-3153, Pacific Northwest Laboratory, Richland, Washington.
- Rasmuson, D. et. al. 1979. Common-Cause Failure Analysis Techniques: A Review and Comparative Evaluation. TREE-1349, EG&G Idaho, Idaho Falls, Idaho.
- Raymond, J. R. 1977. Workshop on Transport Modeling for Nuclear Waste Repositories. PNL-SA-7468, Pacific Northwest Laboratory, Richland, Washington.
- Roberts, N. H. et. al. 1981. Fault Tree Handbook. NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D. C.
- Rogers, J. C. and Y. Onishi. 1981. "Development of a Comprehensive Management Site Evaluation Methodology" in Proceedings of the Symposium on Waste Management at Tucson, Arizona.

- Silviera, D. J. et. al. 1980. Assessment of Effectiveness of Geologic Isolation Systems. A Short Description of the AEGIS Approach. PNL-3398, Pacific Northwest Laboratory, Richland, Washington.
- Smith, C. F. and W. E. Kastenbergl. 1975. "On Risk Assessment of High Level Radioactive Waste Disposal." Nuclear Engineering and Design 39:293-333.
- Smith, T. H., P. J. Pelto, P. L. Stevens, G. D. Seybold, W. L. Purcell, L. V. Kimmel. 1976. A Risk-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accidental Release Sequences in Nuclear Fuel Cycle Operations. BNWL-1959, Pacific Northwest Laboratory, Richland, Washington.
- Strengel, D. L., et. al. 1976. Review of Computational Models and Computer Codes for Environmental Dose Assessment of Radioactive Releases. BNWL-B-454, Pacific Northwest Laboratory, Richland, Washington.
- U.S. Department of Energy. 1979. Technology for Commercial Radioactive Waste Management. DOE/ET-0028, Washington, D. C.
- U.S. Department of Energy. 1980. Final Environmental Impact Statement, Management of Commercially Generated Radioactive Waste. DOE/EIS-0046-F, Washington, D. C.
- U. S. Department of Energy. 1980. Nuclear Waste Management Program Summary Document. DOE/NE-0008, Washington, D. C.
- U.S. Environmental Protection Agency. 1977. State of Geological Knowledge Regarding Potential Transport of High-Level Radioactive Waste From Deep Continental Repositories, Report of an Ad Hoc Panel of Earth Scientists. EPA/520/4-78-004, Washington, D. C.
- U.S. Nuclear Regulatory Commission. 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400, Washington, D. C.
- Voss, J. W. 1979. Safety Indices and Their Applications to Nuclear Waste Management Safety Assessment. PNL-2727, Pacific Northwest Laboratory, Richland, Washington.
- Waite, D. A. 1980. "Occupational Safety in Mined Geologic Repositories," in Proceedings of the 1980 National Waste Terminal Storage Program Information Meeting. Office of Nuclear Waste Isolation, Battelle Memorial Institute, Columbus, Ohio.
- Waite, D. A. and M. M. Kaczmarzky. 1981. "Radiological Impacts of Commercial Waste Management," in Proceedings of the Symposium on Waste Management at Tucson, Arizona.
- Winegardner, W. K. et. al. 1976. "Systems Safety Evaluation", in Quarterly Progress Report Research and Development Activities Waste Fixation Program, January through March 1976. BNWL-2080, Pacific Northwest Laboratory, Richland, Washington.
- Wingender, H. J. 1976. Methodology and Application of Probabilistic Risk Analysis. ERDA-tr-308, NUKEM, Hanau, Germany.

APPENDIX A

METHODS AND APPROACHES
FOR RISK PREDICTION AND ASSESSMENT

W. K. Winegardner

APPENDIX A

METHODS AND APPROACHES FOR RISK PREDICTION AND ASSESSMENT

A.1	INTRODUCTION	A-1
A.2	DEFINITIONS/BACKGROUND	A-1
A.3	PREDICTING RISK	A-3
A.3.1	Identification of Possible Accident Scenarios	A-3
Experience		A-4
Analysis		A-5
Conjecture/Other Considerations		A-12
A.3.2	Assigning Consequences and Probabilities to Scenarios	A-13
Qualitative Assignment		A-13
Quantitative Assignment		A-15
Probabilities		A-15
Consequences		A-17
Combining Probabilities and Consequences		A-20
Failure Data		A-26
A.4	ASSESSING RISK	A-28
A.4.1	Approaches	A-28
Cost Benefit		A-28
Revealed Preferences		A-30
Expressed Preferences		A-30
Natural Standards		A-31
Other Approaches		A-31
A.4.2	Quantitative Values	A-33
A.5	REFERENCES	A-34

APPENDIX A

METHODS AND APPROACHES FOR RISK PREDICTION AND ASSESSMENT

A.1 INTRODUCTION

Predicting the possibility of loss, i.e., predicting risk, is being emphasized as a major part of an attempt to better manage technological hazards. This report was prepared to compile a list of methods that are being used in this effort. Summary descriptions of several of the systematic processes that appear to be most frequently used are also included. Mention is also made of some of the efforts related to the formidable technical and societal undertaking of examining the question of acceptable risk. The compilation of methods is preceded by a background section that defines risk and briefly reviews the uses and scope of risk assessment.

The literature references and summary reviews compiled in the report were generated as background and support information for risk studies being conducted at the Pacific Northwest Laboratories (PNL). There is no intent to imply that predictive methods, let alone techniques for judging acceptability, have been developed that are widely accepted. It is hoped that this paper will encourage the reader to study the references in greater depth, thus providing an even better understanding of the utility and limitations of the various methodologies currently available. The report was written as part of the Waste Management Safety Studies Project being performed for the Office of Nuclear Waste Management in the U.S. Department of Energy.

A.2 DEFINITIONS/BACKGROUND

A first dictionary definition of risk is given as the "possibility of loss or injury: PERIL" (Webster's New Collegiate Dictionary, 1975). Rowe (1977) defines risk as". . . the potential for realization of unwanted, negative consequences of an event . . . risk at the general level, involves two major components: (1) the existence of a possible unwanted consequence

or loss, and (2) an uncertainty in the occurrence of that consequence which can be expressed in the form of a probability of occurrence." In summary, prediction of risk requires consideration of both the probability and consequences of events. As suggested by the above definitions, events are thought of only in terms of potential negative impact.

Predicting risk has become popular because the technique can be used to comprehensively and systematically evaluate complex systems as well as compare the possibility of loss for basically different systems and activities. It was this latter property that led to the proposal by Farmer (1967, 1967a) to replace the maximum credible accident approach with one that considers probability as well as consequences for the assessment of nuclear reactor hazards (also see Nicholson, 1970). In addition to the contexts of comprehensiveness and comparisons, efforts to estimate the likelihood and severity of failures can also be used to predict how systems will fail, thus identifying where remedial measures should be the most effective.

The ultimate incorporation of risk concepts into decision making, i.e., complete risk assessment, frequently requires more than predicting probabilities and consequences. For example, risk predictions can logically define where remedial measures will be the most effective. However, the cost of adding a standby or protective system may far exceed that associated with any expected incremental benefit. Further, the predicted risk may already be judged as acceptable, irrespective of any expected additional benefit, or even judged to be unacceptable, no matter what remedial measures are proposed. In other words, complete risk assessment can involve determining the value of the predictions to those affected. Otway and Pahner included the determination of social values (risk evaluation) along with quantification (risk estimation) in their two-stage definition of risk assessment. It is also interesting to note that Lowrance (1976) uses these two very different activities, measuring risk (measuring or quantifying the probability and severity of harm) and judging the acceptability of that risk, to define safety--"a thing is safe if its risks are judged to be acceptable." Using the above definitions, risk and safety assessment essentially become the same process.

A.3 PREDICTING RISK

Usually there are collections of continuing processes, single events, and combinations of events associated with an activity that can conceivably result in loss. What actually will happen is subject to chance (it is only when the mission is complete that it is possible to determine the frequency of undesired events). Risk prediction then includes the following tasks (1) identification of the potentially harmful processes and events, i.e., the possible accident scenarios and (2) assigning probabilities and consequences to these scenarios. Some of the methods and techniques that have been used in these two tasks are discussed in the following sections.

A.3.1 Identification of Possible Accident Scenarios

Each activity, system, or product has inherent hazards, i.e., conditions with the potential for harm. Once the safety analyst has obtained an understanding of the activity in question, his next task is to identify these hazards and the events which can turn the hazards into accidents. Frequently there are myriad such causative events and their identification can be a massive undertaking. Emphasis should be on comprehensiveness rather than on considerations of likelihood or severity. The analyst should be asking "How can it fail?" rather than "Is it credible?" or "How bad can it be?"

Risk "measurement" provides an invaluable background for the identification, in a collectively exhaustive manner, of hazards and causative events. Such an undertaking inherently requires consideration of the entire spectrum of possible factors, from the chronic to the rare. The work is performed against a probabilistic backdrop where it is assumed that anything is possible. Resources available to the analyst to aid in the identification of hazards and accident scenarios include experience and analysis. Open-mindedness and conjecture are also important to a comprehensive identification process.

Experience

Experience is the primary method of identification of hazards and the events that can turn hazards into accidents. Further, inference from direct experience can be the most accurate. It is regrettable but obvious that the more failure information and data there is, the better the predictions of accident scenarios and their probability and consequences will be. For example, underground coal mining results in a relatively large number of accidents. Extensive compilations of fatality and injury experience are available. Predictions of how coal miners will die and the probability of fatal accidents can be made with alarming accuracy.

The vast amounts of failure data that have been compiled for various industries and activities can never be overlooked by the analyst. Existing information exchange programs will be discussed later in the report. Information from past experience has been used to construct tables that can be used as checklists. Hammer (1972) includes an extensive appendix that can be used as such a checklist, i.e., as an aid to the comprehensive identification of hazards and events that can transform the hazard into undesired consequences. Hammer (1972) also notes that "specifications, standards, codes, and safety regulations are excellent sources of information on hazards and methods for their elimination or control for systems, hardware, procedures, and personnel."

Identification of failure modes by testing is obviously important. Many components and products are amenable to failure testing, i.e., destructive or nondestructive testing. As indicated by Lowrance (1976) "an impressive repertoire of tests have been developed by such organizations as the American Society for Testing and Materials, Underwriters Laboratories, the engineering societies, the military, and the government agencies."

When considering effects of exposure, experimenting on human subjects and on nonhuman organisms as well as epidemiological investigations can all be viewed as tests to provide new insights into potentially harmful accident scenarios. Lowrance (1976) also notes that reviewing inadvertent and occupational exposure can provide extremely valuable information.

Analysis

The past may never reveal all possible hazards and failure modes, even for established activities. Further, activities can be so complex that any standardized test to failure of the entire system is impractical. Results of tests of selected key components would not be totally satisfactory because of complex interrelationships and dependencies. Finally, the activity may only be in the development or early planning stages. In such cases experience and testing can be supplemented with analyses to aid in the identification of hazards and failure modes.

Different authors have classified the methods of analysis in different ways. Lambert (1975) and Vesely et. al (1981) categorize the methods in terms of inductive and deductive analysis. As stated in the first of these references, ". . . inductive analysis involves postulating a possible state of components and/or subsystems and determining its overall effect on the system . . . [deductive analysis] involves postulating a possible state of the overall system and identifying those component states that may contribute to its occurrence." Hammer (1972) classifies the methods in terms of periods in development of a system; initial, detailed analyses, and operating safety analyses, and then includes a fourth category, termed quantitative safety analyses.

No effort will be made in this paper to redescribe all of the methods presented by Hammer (1972), Lambert (1975) and Vesely et. al (1981). Some general comments, however, are in order. As the titles suggest, several of the analysis techniques presented by Hammer (1972) focus on assessment considering a fundamental parameter. For example, "Mapping" focuses attention on problems that could develop because of the locations or proximity of components, lines, and hazards while "Energy Analysis" centers on potential problems arising from sources of available energy. Other techniques of this type include "Mission Analysis," "Environmental Analysis," "Critical Analysis" (emphasis on critical components in pieces of equipment), "Interface Analysis" (focus on incompatibilities between units of a system that could cause problems), "Flow Analysis" (emphasis on flow of fuel, energy, or both), "Link Analysis" (focus on transmission of information), and "Procedures (task) Analysis."

Many systems, products, and situations may require a more comprehensive method for the identification process than the methods just described that focus on a selected parameter. In fact, there are many situations where narrowing the focus could result in oversight and actually be harmful. Two frequently used broad and more all-encompassing techniques are termed Preliminary Hazards Analysis (PHA) and Failure Modes and Effects Analysis (FMEA). PHA is used during the conceptual stages of system design. Very little information is available concerning design features or procedures. The objective is to identify potential hazards inherent to the system and describe the effects of possible accidents. FMEA is performed at the design stages and emphasis is on the identification of problems that could result from hardware failure.

Although a narrative PHA is sometimes used, both PHA and FMEA are usually presented in a columnar format. Specific entries for a PHA include columns for describing the hazard, triggering events or causes that can transform the hazard into an accident, the effect or consequences, and corrective or preventive measures. A sample PHA using the columnar format is shown in Figure 1 (from Lambert, 1975). The use of the checklists such as those presented by Hammer (1972) can supplement experience and aid in assuring that the PHA process is comprehensive. Obviously the PHA should be superseded as design and procedural information becomes available.

As indicated earlier, FMEA is performed at the design stages and focuses on hardware failures, i.e., on the ways components can fail. Specific entries for columns of a FMEA include descriptions of the component, its failure modes, causes of failure, possible effects, and again, actions to reduce failures and consequences. The formats for both PHA and FMEA can be more comprehensive than indicated above. For example, columns and information could be included to list failure probability, qualitatively categorize hazards, to identify responsible organizations, and to identify tests and research and development needs. A portion of a FMEA of a shutdown heat removal system is shown in Figure 2 (from Bertucio, 1978). Additional information concerning basic steps and procedures that should be undertaken to conduct a PHA or FMEA are presented by Hammer (1972), Wang et. al (1979) and Vesely et. al (1981).

Hazardous element	Triggering event 1	Hazardous condition	Triggering event 2	Potential accident	Effect	Corrective measures
1. Strong oxidizer	Alkali metal perchlorate is contaminated with lube oil	Potential to initiate strong redox reaction	Sufficient energy present to initiate reaction	Explosion	Personnel injury; damage to surrounding structures	Keep metal perchlorate at a suitable distance from all possible contaminants
2. Corrosion	Contents of steel tank contaminated with water vapor	Rust forms inside pressure tank	Operating pressure not reduced	Pressure tank rupture	Personnel injury; damage to surrounding structures	Use stainless steel pressure tank; locate tank at a suitable distance from equipment and personnel

FIGURE 1. Sample Preliminary Hazards Analysis (Lambert, 1975)

PART ASSEMBLY OR PROCESS				P/N		PREPARED BY		DATE		
						R. C. Bertucio		2/25/76		
ITEM NO.	PART, ASSEMBLY OR PROCESS NUMBER	PART, ASSEMBLY OR PROCESS NAME	PART, ASSEMBLY OR PROCESS FUNCTION	FAILURE MODE(S)	FAILURE CAUSE(S)	PROBABILITY	CRITICALITY	FAILURE EFFECT(S)	CORRECTIVE ACTION OR PREVENTIVE ACTION	PART, ASSEMBLY OR PROCESS INTERFACING AND REMARKS
1.1	Reactor Vessel		Provides support for fuel assemblies. Contains sodium	Leakage, rupture	Corrosion, erosion, thermal shock, excessive loads			Sodium fills guard vessel. Decay heat removal possible.		Failure not critical unless there is a coincident failure of guard vessel.
2.1	Shutdown Heat Removal System Piping, Valving, and Components		Includes piping, drainvalves, vent valves, manual isolation valves	External leakage, rupture (represents total unavailability of a SHRS loop due to leakage of all components)	Bending fatigue, creep strain, thermal or mechanical loads, weld failure, thermal shock, thermal stresses, and corrosion			Sodium spills into cell. Loop drained and repaired; unavailable for decay heat removal		If the system is at negative pressure at the point of leak, gas enters the coolant.
2.2	FM Pump			Fails to operate	Loss of electrical power supply. Short circuit in MG set. Windings fail. Loss of cooling to windings. Structural failure of MG set.			Loss of forced convection in SHRS loop. Heat transport by natural circulation.	Redundant EM pumps would protect against random independent failures of the pump.	Option 2, 3, and 4 would possibly not naturally circulate if there was pony motor flow. ΔP would close checkvalve.
2.3	SHRS Checkvalve		Prevent reverse flow in loop during normal operation	Fails to open	Contamination, mechanical distortion			Prevents flow in SHRS loop. No decay heat removal capability.	Positive pressure from pump head will very often open stuck valve, thereby reducing true failure rate.	
3.1	PHTS Piping Valving, and Components			Leak, rupture	Bending fatigue, creep strain, thermal or mechanical loads, weld failure, corrosion, nozzle weld failures.			Sodium spills into PHTS cell. Loop drained and repaired.		Loop unable to provide pony motor flow through core.
	PHTS Pump			Seal leakage, failure	Thermal cycling, fatigue, wear, corrosion			Sodium leaks into cell. Pump drained and repaired.		Loop unavailable to provide pony motor flow through core.
				Bearing seizure	Wear, corrosion, contamination			No forced convection in PHTS loop.		Loop unavailable to provide pony motor flow through core.
				Shaft failure, structural failure of pump internals	Thermal shock; excessive loading.			No forced convection in PHTS loop.		Precludes pony motor operation.

PROBABILITY NUMBERS
 64
 32
 1

CRITICALITY NUMBERS
 5
 4
 3
 2

FIGURE 2. Sample Failure Mode and Effects Analysis (Bertucio, 1978)

A limitation of PHA or FMEA in the identification process is that attention is usually focused on one hazard or component at a time.^(a) Experience has shown that accidents are frequently the result of a sequence of seemingly unrelated events. Several events must occur in combination for the accident to occur. Complex interrelationships can be involved. A deductive method of analysis that has been used to identify potential accident scenarios from combinational events is termed fault tree analysis (FTA).

FTA is a formalized logic technique that graphically models the various combinations of possible conditions or events that could result in undesired consequences. Fault tree construction starts with the careful definition of the system and of the undesired event. The safety analyst, thinking "How could this top event happen?" and using and/or logic gates, systematically diagrams backward to identify the events that could cause the top, undesired events to occur. As the diagram grows, step-by-step, combinations of events are added. The process stops when the analyst defines events that for one reason or another, are not developed further, usually because the events are either not amenable to further resolution or where it appears there is no need for additional definition. These latter events are termed primary events. As indicated by Lambert (1977), the tree becomes "... a Boolean logic model that depicts the parallel and sequential combinations of [primary] events that cause a top event to occur." At the minimum the tree is a qualitative graphic model and can be used for displaying what has been considered in the assessment. Identification of how the system can fail results from the identification, by algorithms, of cut sets, the primary events and combinations (sets) of primary events whose occurrence can cause the top undesired event. The cut sets, paths to the top of the tree, are the potential accident scenarios. An excellent discussion of fault tree construction fundamentals and the technique for cut set determination has been presented by Vesely et al. (1981).

(a) Hammer (1972) states that "[In FMEA] each failure is considered individually, as an independent occurrence with no relation to other failure in the system except the subsequent effects that it might produce." Failure of two components at the same time can be considered, but considering the tabular format, the number of such combinations could rapidly become unmanageable. An inductive technique that specifically includes consideration of double failures is the Double Failure Matrix (DFM), a method for use with relatively simple systems (Vesely et al., 1981).

A sample fault tree, developed for illustrative purposes rather than as an effort to accomplish realism or comprehensiveness, is shown in Figure 3. Review of Figure 3 will show that the seven primary events reduce to five cut sets; three one primary event cut sets and two, two primary event cut sets. The former represent those single failures which cause the top event, the latter, double failures which together cause the undesired event.

FTA is an excellent method for identification, in a collectively exhaustive manner, of accident scenarios consisting of combinational events. However, it must always be remembered that the analysis focuses on a specific undesired event. Definition of this event is extremely important. Broad definitions, resulting from the desire for comprehensiveness can result in an overwhelming analysis. Large systems can be divided into subsystems but there are pitfalls that must be recognized associated with interrelationships interfaces. As indicated by Smith, et. al (1977), a complex web of events can be involved in an accident scenario and "a potential weakness of any systems safety method exists in the process of uncoupling the web of events, performing independent calculations on these segments, then recoupling. Interactions among the uncoupled portions of the web are easily overlooked." A constant awareness of interfaces and clear definitions are needed to assure that important failure scenarios are not overlooked in analyses that will be integrated.

A specific potential problem associated with FTA concerns the fact that the primary events of fault trees are treated as independent events. Obviously there are single causes that can degrade or negate the independency presumed for redundancy. Even supposedly redundant components installed in widely separated locations or buildings can be affected, e.g., by manufacturing or installation errors or by a site related phenomenon such as an earthquake. As systems have become more complex, the need for the identification of such causes, termed common causes, has become more important. As a result, techniques to supplement and complement FTA have been developed to aid in the search for those common causes that can significantly impact safety, reliability and risk predictions. For example, primary events of fault trees can be assessed for potential susceptibility, e.g., components

TOP EVENT = $(P_1) \text{ OR } (P_2 \text{ AND } P_3) \text{ OR } (P_4) \text{ OR } (P_5 \text{ AND } P_6) \text{ OR } (P_7)$, i. e., TOP EVENT IS COMPRISED OF FIVE CUT SETS (PATHS TO TOP OF TREE)

[] ABNORMAL SYSTEM STATE

⌋ OR GATE

⌋ AND GATE

○ PRIMARY EVENT

FIGURE 3. Sample Fault Tree Cut Set Identification

with the same x-y coordinates or having the same manufacturer can be identified. Methods for representation of dependencies within fault trees have been developed. Checklists have been developed that can aid in the search for common links (e.g., see Woodward and Baloh, 1978, Rasmuson et. al, 1979. and Putney, 1981). Hagen (1979) has prepared a review of common cause failure that includes an extensive bibliography.

Conjecture/Other Considerations

When the risk predictor or safety analyst is faced with a new problem, there is really no recognized standard method to fall back on. Further, experience gained in other areas may not be totally applicable. There will always be instances where the only thing the analyst can do is supplement experience and methods by predictions based on conjecture. In fact, there can always be a danger in placing too much reliance on the use of formal methods and techniques. The use of the latter should never override the questioning nature of the analyst. The identification process should never become one of just filling out a form or drawing a tree. Whether accident scenarios are a list of 50 single events developed by a panel of experts or a list of 10,000 combinations of events developed by computerized FTA, there should always be a nagging concern about the list being complete, especially when common cause scenarios are considered. In fact, the analyst is probably the most vulnerable when it is assumed that all of the scenarios have been identified. Clark (1977) notes that "it is indeed ironic that our confidence in prediction and control of the known serves to increase our vulnerability [by diminishing the ability to respond to the inevitable undefined hazard]." The completeness problem is inherent in the predictive nature of the work and is mentioned primarily from the standpoint that it must be recognized. The analyst has to be willing to live with and admit uncertainty. As suggested above, contrary assumptions can even be another mechanism for increasing the chance for loss.

Efforts have been made to provide insights into the completeness problem. One approach, based on assumptions about the unknown sequences, is presented by Smith, et. al (1977). Smith et. al (1977) notes that "the accuracy of the estimate of total risk is probably limited more by uncertainties in evaluating identified sequences than by omission of sequences." Another potential analytical approach involving a Bayesian framework has been

suggested by Kaplan and Garrick (1979); "information about the frequency of such events [events not yet imagined] is contained in the fact that none of them have occurred yet; . . . this information can be quantified as for any other event" (also see Parry and Winter, 1981).

Finally, whether formal techniques or conjecture are used, the identification of potentially harmful causative events should be done by several people with inter-reaction between those involved. It is, of course, first necessary to know and understand the activity or technology, the mission, and what constitutes failure. Ideally, the safety analysts should not be the same ones that also defend the activity. Temporary team members not totally familiar with the activity but who are not afraid to ask questions can also prove to be invaluable in the identification of hazards and failure scenarios.

A.3.2 Assigning Consequences and Probabilities to Scenarios

The search for potential accident scenarios ultimately results in a list. If the effort is being performed solely to identify weak links, then the work can stop with the list (but remembering the nagging concern about completeness). However, a risk or safety related evaluation is rarely this simple. Questions frequently arise concerning the need for remedial measures or alternatives. If it is decided that corrective or preventive measures are needed, questions then arise concerning what to do first. Assuming the usual case of limited resources, coupled with the identification of myriad scenarios, it becomes necessary to prioritize or rank the scenarios that comprise the list. Assessment of the consequences and probabilities associated with the list of scenarios can aid in answering questions related to repair and choices. There are methods that can be used to aid in assigning measures of importance to the individual failure scenarios as well as to assess the overall level of risk involved. This section of the report discusses the qualitative and quantitative methods that are used to order the list of failure scenarios in terms of consequences, probability, or both, i.e., in terms of risk.

Qualitative Assignment

Qualitative methods usually focus on consequences. Indices of consequences are frequently developed, e.g., as previously indicated, columns can be added to the formats of PHA or FMEA to categorize hazards. In

general, items are ranked with an index based on relative terms. Hammer (1972) indicates that four categories sometimes used in FMEA are catastrophic (failure results in death or injury or prevents performance of mission); critical (degradation of system beyond acceptable limits could cause death or injury if corrective action is not immediately taken); major (degradation of system beyond acceptable limits but can be counteracted/controlled); and minor (failure does not degrade performance beyond acceptable limits).

Assigning a category such as catastrophic or critical to a component failure mode-possible effect scenario will not always be easy or a clear cut choice. As a result, some FMEA proceed beyond the initial columnar format. For example, rankings are developed for certain system components that can be especially critical to the mission. These criticality rankings are generally expressed as probabilities but may be indicated in other ways, e.g., designation in categories from 1 to 10.^(a) This expanded FMEA is termed Failure Modes Effects and Criticality Analysis (FMECA) and is discussed in greater detail by both Lambert (1975) and Hammer (1972). The rankings can be used to determine which components should be safeguarded as well as where remedial measures can be applied most effectively. Little, if anything, is done in either FMEA or FMECA to combine probabilistic and consequence considerations.

Another use of indices as comparative tools is the development of values related to the maximum potential for loss, established guides, and combinations of these two. Voss (1979) presents a list of 13 indices that have been developed for the assessment of nuclear waste management activities. A frequently used index is developed from the quotient of the total radioactivity and the recommended concentration guides for radionuclides in air and water. This basic index has been modified in several ways to account for factors such as radioactive half-life, waste form release characteristics, and period of concern (also see Smith, Cohen and McKone, 1980).

(a) One criticality number is calculated from the number of failures of a specific type expected during each million operation in a critical mode.

Quantitative Assignment

Efforts such as those described in the preceding section can provide insights and can be especially valuable in preliminary evaluations or in placing maximum possible consequences in perspective. However, even with sophisticated indices, it is an admittedly subjective technique. As a result, in an effort to remove as much of the judgmental aspect as possible, modern systems safety related assessment appears to be focusing more and more on the development of quantitative methods, especially those that ultimately result in a prediction of risk. To repeat, such a prediction requires consideration of probability and consequences.

Probabilities

Evaluation of probabilities is of key importance to risk evaluation. The interpretations of probability and descriptions of the underlying mathematical methods and concepts of probabilistic assessment would require an entire textbook and are obviously beyond the scope of this paper. There are numerous texts that provide extensive discussions of the various topics involved; Shooman (1968) and Hahn and Shapiro (1967) are examples. In addition, fundamental material necessary for understanding the use and limitations of applications related to risk predictions has been presented by Vesely et. al (1981), Apostolakis (1974), Lambert (1975), Fussell (1975), Kaplan and Garrick (1979) and Rothbart et. al (1981). Before proceeding, however, one particular aspect of interpretation should be noted. Uncertainty is an inherent and dominant factor in the quantitative assessment of failure scenarios. The safety analyst is frequently faced with the assessment of low probability scenarios and the attendant lack of "statistically significant" data because there have not been enough "trials". Apostolakis (1978) and Kaplan and Garrick (1979), argue that in such a situation the subjectivistic interpretation of probability is the appropriate framework for assessment (also see Worledge, 1979 and Parry and Winter, 1981). Kaplan and Garrick (1979) define probability as a "numerical measure of a state of knowledge, a state of confidence" and note that "when one has insufficient data, there is nothing else one can do but use probability." The foregoing definition, i.e., probability as a measure of the degree of belief, is, of course, the subjectivistic interpretation, and interpretation long debated and not always accepted (see Easterling, 1981 and Hoos, 1980).

Although underlying theory is extensive and frequently complex, application can be relatively straightforward. In general, when combination events are involved, events are systematically related in a logic diagram or structure that depicts the system. Then from the diagram, the laws of probability theory, and failure data input, probabilistic attributes of the system can be calculated. Fault trees are probably the diagrams most frequently used. As previously indicated, primary events are related to each other with and/or logic gates. The initial step in the quantitative evaluation of a fault tree is the representation of the top event in terms of the primary events, i.e., the identification of the cut sets. The notion of cut sets and the rules of symbolic logic (combination of the and/or gates using rules for combination of unions and intersections) can be merged to provide a systematic method of analyzing the probabilistic behavior of the tree. Several quantitative probabilistic reliability characteristics can be calculated or approximated (see Fussell and Arendt, 1979 and Wang, et. al, 1979). In general, probabilities of the top event and the cut sets that make up the top event are derived in terms of primary event probabilities. These calculations are usually based on the assumption of small probabilities and a constant-hazard ("failure rate") model. Cut sets consisting of combinations of repairable primary events only, non-repairable primary events only, or mixtures of both types can be assessed. Components associated with primary events can be on-line or standby. Unavailability (probability of being unavailable) contributions from pre-existing failures, failures on demand, and testing and maintenance downtime can be handled (see Smith et. al, 1977, and Vaurio and Sciaudone, 1979). Some of the computer codes presently being used for cut set identification and probabilistic analysis have been listed by Fussell and Arendt (1979) and Vesely et. al (1981).^(a)

(a) It is noted in the text that the probabilistic calculations are usually based on a constant-hazard model. The "failure rate", λ , in any time period remains constant throughout the mission, i.e., is the same in the first and last week of the mission. This assumption of constant rate leads to relatively simple results, e.g., reliability becomes $e^{-\lambda t}$, failure probability $1-e^{-\lambda t}$, and mean time to failure (MTTF), $1/\lambda$. The capability of one of the computer codes discussed in the references, FRANTIC, has recently been enhanced to permit the evaluation of time dependent hazard models (e.g., evaluation of burn-in or wear-out), see Vesely et. al. (April 1981) concerning FRANTIC II. An electronic instrument for simulating reliability of complex systems has even been developed that permits comparison of the theoretical predictions from FTA with "experimental" observations (see Rothbart, et. al, 1981).

Output of FTA is usually the probabilistic ranking of the cut sets that make up the top event. Such a ranking permits identification of primary events and combinations of primary events that significantly contribute to the undesired event. Measures of importance and their probabilistic meaning are discussed by Fussell (1975) and Lambert (1975).

The sample fault tree presented earlier has been evaluated in Figure 4 using arbitrarily assigned probability values. Review of Figure 4 will reveal that for every ten trips home, one tow-in could be predicted. The most likely reason is incapacitation of the only available driver, a one event cut set. The sample tree can be used to illustrate other points. As previously indicated, diagramming of the tree stops when the analyst defines events that are either not amenable to further resolution or where it appears there is no need for additional definition. Obviously the tree shown in Figures 3 and 4 could be developed still further, e.g., these are numerous reasons why the starter or battery might fail or the driver might become incapacitated. Judgment is needed in developing details of any tree. In the sample tree, failure data may be available only for installed starter or battery assemblies, thus indicating a good place to stop. On the other hand, the analysis indicates that perhaps additional details may need to be developed concerning the "primary" reason for driver incapacitation. The tree could have also shown additional details concerning tire failures. For example, failure of one tire could have been detailed as an OR gate consisting of four primary events each having a probability of 10^{-3} ; right front tire failure, right rear tire failure, etc.

Consequences

Ranking of failure scenarios in terms of consequences would appear to be a relatively straightforward process. Mortality and morbidity immediately come to mind as indicators of accident consequences. Further, there is usually little difficulty in evaluating many types of loss in terms of dollar costs. For example, property damage (replacement costs of equipment, vehicles, and property), reconstruction costs, medical fees, and loss of production and earnings can all be reduced to dollar values. However, consequence assessment can become much more than a search of tables of fatality and injury data or making cost calculations using normal

$$\text{TOP EVENT} = P_1 + P_2 P_3 + P_4 + P_5 \cdot P_6 + P_7 = (10^{-2}) + (10^{-3})(10^{-4}) + (6 \times 10^{-6}) + (4 \times 10^{-3})(10^{-5}) + 10^{-1} \approx 10^{-1}$$

FIGURE 4. Sample Fault Tree Probabilistic Assessment

accounting techniques. Calculation of fatalities and injuries from the accidental release of radionuclides is an excellent example of the complexity that can be involved. In this latter calculation, methods and techniques are needed to predict the amount of radioactivity released as the result of the particular accident scenario in question (the source term); to predict the amount of radioactivity transported via the various potential pathways (airborne, waterborne, direct dose); to predict dosimetry; and ultimately to predict health effects. Prediction of health effects includes late as well as early somatic effects and even genetic impacts. Such predictions can involve consideration of fatalities and injuries that are not even concurrent with the accident and even future generations. Finally, there are subjective components associated with human loss that can contribute significantly to complexity. Pain and suffering are obvious components and can even become more important than material loss.

Despite the controversial nature of some of the above considerations, methods have been and are being developed to aid in their assessment. Streng et. al (1978) has presented a review of current methodologies used for analysis of environmental consequences of releases of radionuclides. Little and Moller (1979) describe the capabilities of several models to accurately predict either pollutant concentrations in environmental media or radiological dose to human organs. The BEIR reports (1972, 1977 and 1980) are frequently cited references containing information and insights into the conversion of radiation dose into somatic and genetic effects. The last of the latter three reports also reflect the range of opinions that can develop from the efforts to quantify issues where there is incomplete data and a large degree of uncertainty (also see Pochin, 1978). Health effects of electricity generation, including those of air pollution, are discussed by Lave and Freeburg (1973) and Newkirk (1976). "Value of Life" concepts are discussed in several papers of the Engineering Foundation Workshop (1975) (also see Hirshleifer, et. al, 1974, and Linnerooth, 1975).

It is not always necessary to completely develop the indicators of consequences. Adequate comparisons can often be made using "secondary" indicators, especially if the primary purpose is to find and rank weak links. For example, ranking of accident scenarios involving release of radioactivity using radiation dose or even quantities of radioactivity released as indicators may prove to be sufficient for screening studies.

Combining Probabilities and Consequences

Prediction of risk requires coupling the scenario with the probability and consequence measure of that scenario. As indicated by Kaplan and Garrick (1979) "The output of a risk analysis therefore should always boil down one way or another to specifying a set of triplets:

$$R = \{ \langle s_i, p_i, x_i \rangle \} \quad , \quad i = 1 \dots n \quad (3.1)$$

Where s_i is a scenario identification or description

p_i is the probability of that scenario

x_i is the consequence or evaluation measure of that scenario,
i.e., the measure of damage.

This set of triplets, is equivalent to a risk curve and can be plotted as such graphically by simply setting

$$R(x) = \sum_{x_i \geq x}^n p_i \quad (3.2)$$

(where the sum is over all values of i for which $x_i \geq x$.)

For analytical purposes, therefore, we may also say that this set, $\{ \}$, of triplets, $\langle \rangle$, is the risk, R ."

As suggested above, results of a risk assessment are frequently presented in the form of an integral probability curve or "risk curve." An ordinate value is the probability associated with a consequence of level x or greater. The consequence indicator is plotted on the abscissa. A sample risk curve is shown in Figure 5. Risk can also be expressed as the mathematical product of probability and consequences, i.e., the mathematically expected value of the consequences. However, as indicated by Kaplan and Garrick (1979), "this operation reduces the whole [risk] curve to a single number which is a pronounced loss of information since many vastly different curves with enormously different significance could have the same expected value. In contrast, the point of view that risk is probability and consequences would say that the risk is the whole [risk] curve. . ." (also, see Okrent, 1979).

FIGURE 5. Sample Risk Curve

Methods have been developed which aid in the simultaneous investigation of probability and consequences, i.e., closely couple the probability and consequence analyses. One approach, presented by Smith, et. al (1977) is based on fault tree analysis (also see Pelto and Purcell, 1977 and Seybold, 1977). This approach differs from conventional FTA in that the top event of the fault tree is defined in such a way that a spectrum of consequences can be considered. In addition to probability values, consequence indicators are assigned for each primary event. The approach was developed for the evaluation of uncontrolled release of radioactive material from the confinement/containment barriers of waste management systems. Uncontrolled release of radioactive material from the system barriers, rather than failure of any one barrier component, is postulated as the top, undesired event. As in conventional FTA, using and/or gates, all conceivable and physically meaningful combinations of events which could lead to release are systematically identified. A to/through method follows the flow of radioactive material in reverse sequence from its passage through the final barrier back to the initiating events that led to its flow through the initial barrier (material must move to each barrier and pass through it for release to occur). The risk relationship used is expressed as mathematically expected consequence (product of probability and consequences indicators) but other risk expressions can be accommodated.

Event trees are another technique for coupling consequence and probability investigation. Event trees are inductive logic diagrams that begin with a given initiating event and depict various sequence of events that result in multiple outcome states. In business applications the trees are termed decision trees and are used to evaluate the various outcomes of business and investment decisions. In risk/safety related assessments, a consequence is associated with each outcome of the tree. The tree becomes a diagram illustrating the alternative consequences of a specified initiating event. Event trees are especially suitable for predicting outcomes in terms of the success or failure of a series of standby and/or protection systems. Probability values are assigned at branch (success/failure) points of the tree. One method of constructing safety related event trees is to develop the most likely progression of events resulting from the initiating event. An alternative to this progression is then considered by branching the tree. This alternative, a mutually exclusive output, is developed to termination

and also branched.^(a) Each time a new branch is added the process of development to termination and branching is repeated until the desired level of detail has been achieved (frequently when the last in series of backup, protective systems has been considered). A sample event tree is shown in Figure 6. Again the sample tree was drawn primarily for illustrative purposes. In this case arbitrary values have been assigned to consequences. Additional information concerning event trees is presented in the Reactor Safety Study (1975) as well as by Lambert (1975) and Fleming, et. al (1975).

The probabilities associated with event tree branch points can be determined by FTA. For example, a fault tree could be constructed with jumper cable failure as the top event and the probability calculation for this undesired event used in Figure 6 as the value for P_c . Combinations of event trees and fault trees were used extensively in the Reactor Safety Study (1975). Event trees were used to define the accident progression, i.e., to define outcomes of an initiating event. The binary gates of the trees frequently represented success or failure of an engineered safety system. FTA was then often used to develop the probability of safety system failure used in the analysis of the event tree. A diagrammatical method that uses fault trees in combination with event trees for describing/analyzing failure sequences in complex systems, termed cause-consequence analyses (CCA), is described by Burdick and Fussell (1976). The cause portion of the diagram is a fault tree with the top event being a failure that can result in several outcomes or consequences depending on the effectiveness of various standby, protection systems. An event tree is used to define the outcomes, i.e., comprises the consequence portion. The probability of the initiating event is determined from the "cause" fault tree. Again, additional supplementary fault trees can be used in determining probabilities for the various event tree branch points. A schematic of a simplified cause-consequence diagram is shown in Figure 7. A computer program that determines system risk using cause-consequence diagrams is described by Arendt, et. al, (1978).

^(a)The most likely path and the alternative are mathematical complements.

FIGURE 6. Sample Event Tree

FIGURE 7. Simplified Cause Consequence Diagram

Failure Data

Failure data is a fundamental input for predicting the risk of potential accident scenarios. Although the analyst should use the best numbers available, only "order of magnitude" precision is usually needed. As indicated by Vesely et. al (1981) "Extreme precision is not required (and is not believed!) in a fault tree evaluation; it is the order of magnitude size of the failure rate that is of concern, i.e., is the failure rate 10^{-6} per hour or 10^{-5} per hour." Some of the sources of failure data are listed below.

Component failure rate data are included in the Reactor Safety Study (1975) and compilations have also been developed by Melvin and Maxwell (1974), Garrick, et. al, (1967), and Balfanz (1973). Data for electronic, electrical, and mechanical equipment are presented including failure rate data for static and dynamic components, equipment, instruments, and mechanical, pneumatic, and hydraulic parts. There are also large data exchange programs, e.g., the Government Industry Data Exchange Program (GIDEP).^(a) The GIDEP program contains failure information generated when significant problems are identified on parts, components, processes, fluids, materials, or safety and fire hazards. The failure data bank includes an alert system in which participants are notified of problems as well as techniques to query all other participants on specific problems. Other sources of failure data and additional references are listed in Land, et. al (1980) and Wang, et. al (1979). Land, et. al (1980) also presents a compilation of the failure data used to predict reliability of a fossil fueled plant.

Information presented thus far is primarily related to hardware. The safety analyst is frequently faced with scenarios involving human factors and natural phenomena. Apostolakis (1974) discusses both of these factors and lists several related references. Some human error analyses were presented in the Reactor Safety Study (1975). These analyses have been expanded by the Statistics, Computing, and Human Factors Division, Sandia Laboratories into a handbook to aid in the evaluation of the effect of human error (Swain and Guttman, 1980). Fleming, et. al (1975) includes sections concerning human operator reliability and earthquake

(a) Application for GIDEP participation made through Officer in Charge, GIDEP Operations Center, Corona, California, 91720.

analysis in their description of a methodology for the systematic probabilistic analysis of the High Temperature Gas-Cooled Reactor. Several of the natural phenomena have been investigated or are under review, e.g., a technique is being developed for applying regional seismic histories to analysis of risk from earthquakes (see Probabilistic Safety Analysis V, 1979). Dunlap and Wiedner (1971) present information concerning the probability of a tornado strike, and Hawkins (1963) and Brown (1960) discuss meteorite impacts.

Efforts to evaluate the probabilities and consequences associated with four unlikely potential accident scenarios are included in a series of UCLA reports. Ayyaswamy et. al (1974) discuss dam failure; Solomon, et. al, (1974) airplane crashes; Simons, et. al (1974) toxic chemical spills; and Solomon, et. al, (1974) meteorite impacts. Cottrell (1975) provides a bibliography and compilation of articles on the protection of nuclear power plants from "tornadoes and high winds, floods and high waves, earthquakes, plane crashes, sabotage and diversion, acts of war, and other disasters." Clarke, et. al, (1976) presents quantitative information to aid in the assessment of the risk transporting hazardous materials. Aircraft, truck, and train accidents are discussed. Information concerning the frequencies and consequences (number of fatalities) of hurricanes, tornadoes, floods, earthquakes, and aircraft, marine, motor vehicle, railroad, mining and fire/explosion catastrophes has been tabulated by Coppola and Hall (1981). Rowe (1977) also includes an extensive data base concerning man-made and natural catastrophes. Finally, the publication Nuclear Safety frequently presents summaries of failure data, e.g., information has been presented concerning the following:

Aircraft Impact	Vol. 15 No. 3 Vol. 17 No. 3
Flooding	Vol. 15 No. 4
Pressure vessels/piping	Vol. 15 No. 4 Vol. 17 No. 5
Emergency Power Systems/Prime Movers	Vol. 16 No. 2 Vol. 20 No. 2
Human Reliability	Vol. 16 No. 3 Vol. 17 No. 3 Vol. 21 No. 3
Air-cleaning Systems	Vol. 16 No. 4 Vol. 18 No. 5 Vol. 20 No. 2

Turbine Generators	Vol. 16 No. 4
	Vol. 19 No. 6
	Vol. 20 No. 3
Nuclear Plant Fires	Vol. 20 No. 3
Reactor Containment	Vol. 21 No. 5
Valves	Vol. 22 No. 2

A.4 ASSESSING RISK

As suggested earlier, complete risk assessment can involve a judgment of the acceptability of the predicted risk. It is this judgmental aspect that must ultimately be used as a major part of the effort to come to grips with what at times seems to be an almost bewildering array of risks from technological activities. However, as indicated by Levine (1978), "Quantitative levels of acceptable risk have not yet been established in the United States regarding any human endeavor." Further Fischhoff, et. al (1979) noted that "Of late, many hazard management decisions are simply not being made . . . in part because there are no clear criteria on the basis of which to decide. . . The decisions that are made are often inconsistent . . . Frustration over this state of affairs has led to a search for clear, implementable rules which will tell us whether or not a given technology is sufficiently safe." Obviously, such a search is a formidable technical as well as societal undertaking. This section of the report describes approaches being used in this undertaking and lists references concerning quantitative values that have been proposed to provoke discussion in concrete terms.

A.4.1 Approaches

Fischhoff, et. al (1979) note that the four most frequently used approaches used in efforts to find the above "clear, implementable" rules are cost-benefit analysis, natural standards, revealed preferences, and expressed preferences.

Cost-Benefit

Cost-benefit analysis is an evaluation to determine if the estimated dollar value of the incremental benefits from a proposed action can be expected to be commensurate with the incremental costs of implementing the action. In its usual form, the ratio of estimated benefits to estimated costs is used as a major criterion in determining whether or not to proceed.

Some common pitfalls that can lead to incorrect interpretation of this ratio are discussed by Giant and Ireson (1964). The concept is appealing, especially if it can be expanded such that all advantages and disadvantages of an action are enumerated, evaluated probabilistically, and expressed in terms of dollar cost. Risk, in the form of expected dollar gain or loss, is easily incorporated in such an expanded concept. Risk reduction or increase from the action is simply listed as an advantage or disadvantage. Proposed actions are then taken only when it can be shown that the ratio of the total, expected, incremental dollar advantage to the total, expected, incremental dollar disadvantage exceeds unity.

In a more narrow application of the concept, use is made of a benefit-cost (or cost-benefit) ratio where the lone benefit considered is the incremental reduction in risk (the cost is the dollar cost of the system or component needed to achieve the reduction). Such ratios can provide rationale for implementation of safety measures as well as suggest a point of diminishing returns in their application (see Burnham, 1973, and O'Donnell and Mauro, 1979). O'Donnell and Mauro (1979) have also used the ratios to compare the investment costs to reduce mortality rates in nuclear and nonnuclear operations. In another variation of this application, costs of risk reduction are plotted against risk values. Assuming that expenditures generally follow a law of diminishing returns, the shape of the cost-risk curve can then be used as an aid to decision making. Judgment is required in establishing a point on the curve that corresponds to an acceptable level of cost effectiveness of risk reduction (see Rowe, 1977, pages 76-78).

Although conceptually straightforward, extension of cost-benefit concepts to include risk is not a trivial undertaking. Efforts to cover the spectrum of advantages and disadvantages can be involved. Aggregation of markedly different values is required with the goal of expressing all values in the common unit of dollars. Questions concerning uncertainty and intertemporal equity can become significant. Complicating factors are discussed further in the 1977 BEIR report as well as by Fischhoff et. al (1979), Hirshliefer et. al, (1974) and Van Horn and Wilson (1976). A comprehensive list of risk benefit analysis literature has been compiled by Clark and Van Horn (1976).

Revealed Preference

In this approach historical risk data is used to reveal patterns of acceptable risk-benefit tradeoff. It is an empirical approach, based on recorded data, that attempts to identify what has been traditionally accepted by society. The work of Starr (1969) is probably the classic example. His efforts assume that accident records are adequate for revealing consistent patterns of fatalities in the public use of technology and that historically revealed social preferences and costs are sufficiently enduring to allow their use for predictions. Starr's conclusions include the following ". . . the public is willing to accept voluntary risks roughly 1000 times greater than involuntary risk . . . risk of death from disease appears to be a psychological yardstick for establishing the level of acceptability of other risks . . . acceptability of risk appears to be crudely proportional to the third power of the benefits (real or imagined) . . .". An expanded replication of Starr's work is presented by Fischhoff et. al (1979). Drawbacks to the revealed preference approach are also discussed by Fischhoff et. al (1979) as well as by Okrent and Whipple, (1977) and Otway and Cohen (1975). The validity of the above quantitative results are also examined in the latter of these three references. Rowe's use of historical review/data to develop risk preferences based on what society seems willing to accept is another example of the revealed preference approach (1977).

Expressed Preferences

In this approach public preference is determined by asking people, e.g., people are asked directly what levels of risk are acceptable to them. Access to public preference is obtained through questionnaires, opinion polls, and psychometric surveys concerning their perceptions and evaluations of risk (e.g., see Fischhoff et. al, 1979, Fischhoff et. al, 1978a, Maynard et. al, 1976, Lindell and Earle, 1980, and Slovic, 1978, 1980). Information obtained can be used almost directly or incorporated in formal decision methodologies, e.g., utility methods (see Hendrickson et. al, 1976 and Otway and Edwards, 1977). The appeal of the approach is that timely input can be obtained through widespread public involvement. On the other hand, people's actions have been found to contradict what they say (see Okrent and Whipple, 1977). Other criticisms of this approach include the possibility that safety issues are too complicated for the

majority to understand and that for some issues people simply haven't found preferences. In the latter case, the way people are asked can then have a significant effect on their response. Additional problems with this approach are discussed by Fischhoff et. al, 1979 and Griesmeyer and Okrent, 1980.

Natural Standards

As noted by Fischhoff, et. al, (1979), "A shared flaw of the approaches described above is that all of them are subject to the existing limitations of society and its citizens. . . . Rather than examining (recent) historical time for guidelines [polling people, or reducing risks to dollar values], one might look to geological time, assuming that the optimal level of exposure to pollutants to that characteristic of the conditions in which the species evolved." Use of this "natural standards" approach in an effort to establish criteria is illustrated by the recent investigation of the rationale of the suggestion that geologic repositories for high-level nuclear waste impose no greater risk than that due to naturally occurring uranium ore deposits (Wick and Cloninger, 1980). Attractive features as well as drawbacks to the approach, including the problem of consideration of new substances for which there is no geologic tolerance record, are listed by Fischhoff, et. al (1979).

Other Approaches

In addition to Fischhoff, et. al (1979), guides to aid in judging acceptability are discussed by Lowrance (1976), Rowe (1977), Okrent and Whipple (1977), Cohen (1977), Griesmeyer and Okrent (1980), Fischhoff et. al (1978), Mitra et. al (1981), and Richmond (1980). Abstracts of articles, reviews, symposiums, reports, etc., that cover numerical risk analysis, with specific consideration given to those involved in formulating and utilizing numerical risk criteria, have been compiled by Miller and Hill, 1981.

The following nine general guides are listed and discussed by Lowrance (1976, especially see Chapter 3): reasonableness; custom of usage; prevailing professional practice; best available practice, highest practicable protection, and lowest practicable exposure; degree of necessity or benefit;

the Delaney principle (food additives not safe if found by test to induce cancer); no detectable adverse effect; toxicologically insignificant levels; and the threshold principle. Obviously, many of the above offer little specific guidance and when they do, e.g., the Delaney principle, the guidance can be highly controversial. Lowrance (1976) notes that the above general guidelines are usually supplemented by several empirical criteria, namely exposure relative to natural background, occupational exposure precedent, public referenda and polling, and comparison with accustomed hazards.

Okrent and Whipple (1977) recommend risk criteria that result from coupling interpretation of past political decisions, i.e., revealed preferences, with subjective evaluations of achievable levels of safety relative to cost.

In efforts related to development of acceptable risk criteria for nuclear waste management, Cohen (1977) listed seven approaches to the development of environmental, health, and safety criteria: custom of usage; structured expert panel, unstructured expert panel, decision analysis, dictate, individual technical analysis, and public poll. Using a systematic selection procedure, it was determined that multi-attribute decision analysis techniques coupled with the use of structured panels as value sources showed the greatest promise. A discussion of the application of decision analysis techniques to the generation of acceptable risk criteria is presented in Chapter 8 of this reference.

Griesmeyer and Okrent (1980) list and discuss the following approaches; professional judgment, cost benefit and cost effectiveness considerations, comparison with background hazards, public preferences, and comprehensive analysis of various options.

Finally, a de minimus concept (limit materials present to such minute amounts so as to be considered relatively harmless to man and his environment) is discussed by Richmond (1980). "Once we determine a de minimus value for a given material, we would be able to dispose of or release the material without any unique handling or precautions, or for that matter, regulatory considerations. The real problem, obviously is how small is small enough."

Quantitative Values

Obviously, none of the approaches listed above has provided an adequate solution to the problem of defining acceptable risk. However, they have, in conjunction with other ideas, served as input to facilitate judgments, and discussion of the problem has proceeded beyond approaches. An investigation into the feasibility of developing and then using risk criteria to judge the safety of nuclear power plants is described by Mitra, et. al (1981). Several numerical safety goals have been proposed.

A recent example is the quantitative goals for nuclear power plants proposed by Griesmeyer and Okrent (1980d) to "help stimulate discussion and evaluation in concrete terms." The safety goals are expressed in the form of a set of quantitative decision rules which include:

- Limits placed on the frequency of occurrence of certain hazardous conditions (hazard states) within the reactor
- Limits placed on the risk of the individual of early death, or delayed death due to cancer arising from an accident
- Limits placed on the overall societal risk of early or delayed death
- An "as low as reasonably achievable" approach applied with a cost-effectiveness criterion that includes both economic costs and a monetized value of preventing premature death
- A small element of risk aversion applied to infrequent accidents involving large numbers of early deaths compared to a similar number of deaths caused by accidents each involving one or two deaths.

In addition to their effort, Griesmeyer and Okrent reviewed ten previously presented quantitative proposals including those by Adams and Stone (1967), Bowen (1975), Farmer (1967a), the Atomic Energy Control Board of Canada (AECD, 1978), Kinchin (1978, 1979), the Construction Industry Research and Information Association of the U.K. (CIRIA, 1977), Okrent and Whipple (1977), Comar (1979), Nuclear Safety Analysis Center (NSAC, 1980, 1980a), and the Atomic Industrial Forum (AIF, 1980, 1980a).

Not mentioned in this review were the efforts of Gibson (1976) and Rowe (1977). The latter includes comparison of predicted risk with an appropriate risk "referent", defined as "a specific level of risk deemed acceptable by society or a risk evaluator . . . "

The risk referents for a specific project are obtained by adjusting absolute values developed from historical data. Absolute values are tabulated for injuries and morbidity, property damage, insured losses, and reduction in life expectancy, as well as for fatalities (see Table 17.10 of Rowe, 1977). Proposed risk criteria have also been tabulated by Miller and Hall (1981).

REFERENCES

AECB (1978), Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants, Report of the Inter-Organizational Working Group, Atomic Energy Control Board, Canada, AECB-1149, November 1978.

AIF, (1980), Statement on the Use of Probabilistic Risk Assessment in the Regulatory Process, Atomic Industrial Forum Committee on Reactor Licensing and Safety, June 1980.

AIF, (1980a), Atomic Industrial Forum Presentation before the Advisory Committee on Reactor Safeguards, USNRC, July 1, 1980.

Adams, C. A. and C. N. Stone, (1967), Safety and Siting of Nuclear Power Stations in the United Kingdom, IAEA Symposium on the Containment and Siting of Nuclear Power Plants, Vienna, April 1967.

Apostolakis, G. E., (1974), Mathematical Methods of Probabilistic Safety Analysis, UCLA-ENG-7464, University of California, Los Angeles, CA, September 1974.

Apostolakis, G. E. (1978), Probability and Risk Assessment: The Subjectivistic Viewpoint and Some Suggestions, "Nuclear Safety," May - June 1978.

Arendt, J. S., et. al., (1978), EXCON - A Computer Program for System Risk Assessment, JBFA-129-78, JBF Associates, Inc., Knoxville, Tennessee, October 1978.

Ayyaswamy, P., B. Hauss, T. Hseigh, A. Moseati, T. E. Hicks, and D. Okrent, (1974), Estimates of Risk Associated with Dam Failure, UCLA-ENG-7423, University of California, Los Angeles, CA, March 1974.

Balfing, H. P., (1973) Failure Rate Compilation, AEC-TR-7564, W. J. Grimes and Co., Washington, D.C., December 1973.

BEIR, (1972), The Effects on Populations of Exposures to Low Levels of Ionizing Radiation, Report of the Advisory Committee on the Biological Effects of Ionizing Radiations, National Academy of Sciences--National Research Council, Washington, D.C., 1972.

BEIR, (1977), Considerations of Health Benefit-Cost Analysis for Activities Involving Ionizing Radiation Exposure and Alternatives, EPA 520/4-77-003, Report of the Advisory Committee on the Biological Effects of Ionizing Radiations, National Academy of Sciences--National Research Council, Washington, D.C., 1977.

BEIR, (1980), The Effects on Populations of Exposure to Low Levels of Ionizing Radiation, Report of the Committee on the Biological Effects of Ionizing Radiations, National Academy of Sciences--National Research Council, 1980.

Bertucio, R. C., (1978), Large LMFBF Shutdown Heat Removal System Reliability Trade-off Study, WARD-SR-3045-7, Westinghouse Electric Corp., Madison, Pennsylvania, 1978.

Bowen, J. H., (1975), The Choice of Criteria for Individual Risk, For Statistical Risks, and for Public Risk, Risk-Benefit Methodology and Application: Some Papers presented at the Engineering Foundations Workshop, September 22 - 26, 1975, Asilomar, CA, UNCL-ENG-7598, University of California, Los Angeles, CA.

Brown, H., (1960), The Density and Mass Distribution of Meteoritic Bodies in the Neighborhood of the Earth's Orbit, Journal of Geophysical Research, June 1960.

Burdick, G. R., and J. B. Fussell, (1976), Report V, On the Adaptation of Cause-Consequence Analysis to U. S. Nuclear Power Systems Reliability and Risk Assessment, "A Collection of Methods for Reliability and Safety Engineering," ANCR-1273, Aerojet Nuclear Co., Idaho Falls, Idaho, April 1976.

Burnham, J. B., (1973), Risk Protection, Power Generation, and Fiscal Responsibility, "Power Engineering," May 1973.

CIRIA, Rationalization of Safety and Serviceability Factors in Structural Codes, Construction Industry Research and Information Association, London, Report 63, July 1977.

Clark, E. M., and A. J. Van Horn, (1976), Risk-Benefit Analysis and Public Policy: A Bibliography, BNL-22285, Brookhaven National Laboratory, Upton, N.Y., November 1976.

Clarke, R. K., J. T. Foley, W. F. Hartman, and D. W. Larson, (1976), Severities of Transportation Accidents, SLA-74-0001, Sandia Laboratories, Albuquerque, NM, July 1976.

Clark, W. C., (1977), Managing the Unknown, "Managing Technological Hazard: Research Needs and Opportunities," Institute of Behavioral Science, University of Colorado, Boulder, Colorado, 1977.

Cohen, J. J., (1977), Determination of Acceptable Risk Criteria for Nuclear Waste Management, UCRL-52404, Lawrence Livermore Laboratory, Livermore, CA, October 1977.

Comar, C. L., (1979), Risk: A Pragmatic De Minimis Approach, "Science," 203, p. 319, 1979.

Coppola, S. and R. E. Hall, (1981), A Risk Comparison, NUREG/CR-1916, U.S. Nuclear Regulatory Commission, Washington, D.C., February 1981.

Cottrell, W. B., (1975), Protection of Nuclear Power Plants Against External Disasters, ORNL-NSIC-117, Oak Ridge National Laboratory, Oak Ridge, Tennessee, April 1975.

Dunlap, J. A., and K. Wiedner, (1971), Nuclear Power Plant Tornado Design Considerations, "Journal of the Power Division, Proceedings of the American Society of Civil Engineers," March 1971.

Easterling, R. G., (1981), Letter to the Editor, Bayesianism, "Nuclear Safety," July - August 1981.

Engineering Foundation Workshop, (1975), Risk-Benefit Methodology and Application: Some Papers Presented at the Engineering Foundation Workshop, September 22 - 26, 1975, Asitmar, California, UCLA-ENG-7598, University of California, Los Angeles, CA, December 1975.

Farmer, F. R., (1967), Reactor Safety and Siting: A Proposed Risk Criterion, "Nuclear Safety," November - December 1967.

Farmer, F. R., (1967a), Siting Criteria--A New Approach, "Containment and Siting of Nuclear Power Plants," Vienna: International Atomic Energy Agency, 1967.

Fischhoff, B., P. Slovic, and S. Lichtenstein, (1978), Weighing the Risks, "Environment," May 1979.

Fischhoff, B., H. Christoph, R. E. Kasperson, and R. W. Kates, (1978), Handling Hazards, "Environment," September 1978.

Fischhoff, B., P. Slovic, S. Lichtenstein, S. Read, and B. Combs, (1978a), How Safe is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits, "Policy Sciences," 8, 1978.

Fleming, K. N., P. N. Roabe, G. W. Hannamon, W. J. Houghton, R. D. Pfremmer, and F. S. Dombek, (1975), HTGR Accident Initiation and Progression Analysis, Status Report, Vol. II, Area Risk Assessment Methodology, GA-A13617, Vol. II, General Atomic Co., San Diego, CA, October 1975.

Fussell, J. B., How to Hand Calculate System Reliability and Safety Characteristics, IEEE Transactions on Reliability, Vol. R-24, No. 3, August 1975.

Fussell, J. B., and J. S. Arendt, System Reliability Engineering Methodology: A Discussion of the State of the Art, "Nuclear Safety," September - October 1979.

Garrick, et. al., Reliability Analysis of Nuclear Power Plant Protective Systems, HN-190, Holmes and Narver, Co., May 1967.

Gibson, S. B., The Use of Quantitative Risk Criteria on Hazard Analysis, Journal of Occupational Accidents, 1976.

Grant, E. L., and W. G. Iveson, (1964), Some Aspects of Economy Studies for Government Activities, "Principles of Engineering Economy," 1964.

Griesmeyer, J. M., and D. Okrent, (1980), On the Development of Quantitative Risk Acceptance Criteria, "An Approach to Quantitative Safety Goals for Nuclear Power Plants," NUREG-0739, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1980.

Griesmeyer, J. M., and D. Okrent, (1980a), Risk Management and Decision Rules for Light Water Reactors, "An Approach to Quantitative Safety Goals for Nuclear Power Plants," NUREG-0739, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1980.

Hagen, E. W., (1979), Common-Mode/Common Cause Failure: A Review and a Bibliography, NUREG/CR-0566, Oak Ridge National Laboratory, Oak Ridge, Tennessee, May 1979. (Also see "Nuclear Safety," March - April 1980).

Hahn, G. J., and S. S. Shapiro, (1967), Statistical Models in Engineering, John Wiley and Sons, Inc., New York, NY, 1967.

Hammer, W., (1972), Handbook of System and Product Safety, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1972.

Hawkins, G. S., (1963), Impacts on the Earth and Moon, "Nature," February 1963.

Hendrickson, P. L., C. L. McDonald, and A. H. Schilling, (1976), A Review of Decision Methodologies for Evaluating Regulatory Actions Affecting Public Health and Safety, BNWL-2158, Pacific Northwest Laboratory, Richland, WA, 1976.

Hirshleifer, J., T. Bergstrom, and E. Rappapirt, (1974), Applying Cost-Benefit Concepts to Projects Which Alter Human Mortality, UCLA, ENG-7478, University of California, Los Angeles, CA, November 1974.

Hoos, I., (1980), Risk Assessment in Social Perspective, Proceedings of the 15th Annual Meeting of the National Council on Radiation Protection and Measurements, NCRP, Washington, D.C., March 15, 1980.

Kaplan, S., and B. J. Garrick, (1979), Notes for a Workshop on Risk, Reliability and Decision Under Uncertainty, Pickard, Lowe and Garrick, Inc., Irvine, CA, June 1979.

Kinchin, G. H., (1978), Assessment of Hazards in Engineering Work, "Proc. Instn. Civ. Engrs.," 64, pt. 1, pp. 431-438, 1978.

Kinchin, G. H., (1979), Design Criteria, Concepts and Features Important to Safety and Licensing, Proc. of Inter. Meeting on Fast Reactor Safety Technology, Seattle, WA, 1979.

Lambert, H. E., (1975), Fault Trees for Decision Making in Systems Analysis, UCRL-51829, Lawrence Livermore Laboratory, Livermore, CA, October 1975.

Lambert, H. E., and G. Yadigarov, (1977), Fault Trees for Diagnosis of System Fault Conditions, "Nuclear Science and Engineering," Vol. 62, 1977.

Land, R., L. Reyes, and F. T. Burns, (1980), Extension and Validation of Fault Tree Analysis for Reliability Prediction, EPRI, AP-1510, Electric Power Research Institute, Inc., Palo Alto, CA, September 1980.

Lave, L. B., and L. C. Freeburg, (1973), Health Effects of Electricity Generation from Coal, Oil and Nuclear Fuel, "Nuclear Safety," September - October 1973.

Levine, S., (1978), The Role of Risk Assessment in the Nuclear Regulatory Process, "Nuclear Safety," September - October 1978.

Lindell, M. K., and C. E. Timothy, (1980), Public Attitudes Toward Risk Tradeoffs in Energy Policy Choices, PNL-3402, Battelle, Human Affairs Research Centers, Seattle, WA, June 1980.

Linnerooth, J., (1975), The Evaluation of Lifesaving: A Survey, IIASA RR-75-21, International Institute for Applied Systems Analysis, Roxenburg, Austria, 1975.

Little, C. A., and C. W. Miller, (1979), The Uncertainty Associated With Selected Environmental Transport Models, ORNL-5528, Oak Ridge National Laboratory, Oak Ridge, Tennessee, November 1979.

Lowrance, W. W., (1976), Of Acceptable Risk, William Kaufmann, Inc., Los Altos, CA, 1976.

Maynard, W. S., S. M. Nealey, J. A. Hebert, and M. K. Lindell, (1976), Public Values Associated With Nuclear Waste Disposal, BNWL-1997, Battelle, Human Affairs Research Centers, Seattle, WA, June 1976.

Melvin, J. A., and R. B. Maxwell, (1974), Reliability and Maintainability Manual, Process System, AECL-4607, AECL, Chalk River, Canada, January 1974.

Miller, B., and R. E. Hall, (1981), Index of Risk Exposure and Risk Acceptance Criteria, NUREG/CR-1930, U.S. Nuclear Regulatory Commission, Washington, D.C., January 1981.

Mitra, S., R. Hall, and A. Coppola, A Study of the Implications of Applying Quantitative Risk Criteria in the Licensing of Nuclear Power Plants in the United States, NUREG/CR-2040, U.S. Nuclear Regulatory Commission, Washington D.C., May, 1981.

NSAC, (1980), A Proposed National Nuclear Safety Seal, Nuclear Safety Analysis Center, Electric Power Research Institute, March 1980.

NSAC, (1980a), Nuclear Safety Analysis Center Presentation Before Advisory Committee on Reactor Safeguards, USNRC, July 1, 1980,

Newkirk, N. W., (1976), Environmental Effects of Energy Production and Utilization in the U.S. Volume 2: Public Health Effects, UCRL-51930, Lawrence Livermore Laboratory, Livermore, CA, June 1976.

Nicholson, H. M., (1970), Quantitative Safety Analysis, Introduction, "Nuclear Engineering and Design," North-Holland Publishing Co., 1970.

O'Donnell, E. P., and J. J. Mauro, (1979), A Cost-Benefit Comparison of Nuclear and Non-Nuclear Health and Safety Protective Measures and Regulations, "Nuclear Safety," September - October 1979.

Okrent, D. and C. Whipple, (1979), An Approach to Societal Risk Acceptance Criteria and Risk Management, UCLA-ENG-7746, U. of California, Los Angeles, CA, June 1977.

Okrent, D., Risk-Benefit Evaluation for Large Technological Systems, "Nuclear Safety," March - April 1979.

Otway, H. J., and J. J. Cohen, (1975), Revealed Preferences: Comments on the Starr Benefit-Risk Relationships, RM-75-5, International Institute for Applied Systems Analysis, Austria, March 1979.

Otway, H. J. and W. Edwards, (1977), Application of a Simple Multi-Attribute Rating Technique to Evaluation of Nuclear Waste Disposal Sites: A Demonstration, RM-77-31, International Institute for Applied Systems Analysis, Austria, June 1977.

Otway, H. J., and P. D. Pahnner, (1976), Risk Assessment, "Futures," April 1976.

Parry, G. W., and P. W. Winter, (1981), Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis, "Nuclear Safety," January - February 1981.

Pelto, P. J. and W. L. Purcell (1977), MFAULT: A Computer Program for Analyzing Fault Trees, BNWL-2145, Pacific Northwest Laboratory, Richland, WA, November 1977.

Pochin, E. E., (1978), Why Be Quantitative About Radiation Risk Estimates? National Council on Radiation Protection and Measurements, Washington, D.C., July 1978.

Probabilistic Safety Analysis V, (1979), EPRI-NP-1275, Science Applications, Inc., Palo Alto, CA, December 1979.

Putney, B. WAMCOM, Common-Cause Methodologies Using Large Fault Trees, EPRI NP-1851, Science Applications, Inc. Palo Alto, CA, May 1981.

Rasmuson, D. M., G. R. Burdick, and J. R. Wilson (1979), Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation, TREE-1349, EG&G Idaho, Inc., Idaho Falls, ID, September 1979.

Reactor Safety Study (1975), WASH-1400, United States Nuclear Regulatory Commission, Washington, D.C., October 1975.

Richmond, C. R., (1980), Risks in Perspective: Natural, Occupational, and de minimus, CONF-8010118-1, Presented to the 68th National Safety Congress and Exposition, Chicago, IL, October 23, 1980.

Rothbart, G., R. Fullwood, S. Basin, J. Newt, and J. Escalera, Verification of Fault Tree Analysis Vol. 1 Experiments and Results, Vol. 2 Technical Description, EPRI NP-1570 Vol. 1 and Vol. 2, Science Applications, Inc., Palo Alto, CA, May, 1981.

Rowe, W. D., (1977), An Anatomy of Risk, John Wiley and Sons, New York, NY, 1977.

Seybold, G. D., (1977), RAFT: A Computer Program for Fault Tree Risk Calculations, BNWL-2146, Pacific Northwest Laboratory, Richland, Washington, November 1977.

Shooman, M. L., (1968), Probabilistic Reliability: An Engineering Approach, McGraw Hill, Inc., New York, NY, 1968.

Simmons, J. A., R. C. Erdmann, and B. N. Haft, (1974), The Risk of Catastrophic Spills of Toxic Chemicals, UCLA-ENG-7425, University of California, Los Angeles, CA, May 1974.

Slovic, P., (1978), The Psychology of Protective Behavior, "Journal of Safety Research," Vol. 10, No. 2.

Slovic P., (1980), Images of Disaster: Perception and Acceptance of Risks from Nuclear Power, Proceedings of the 15th Annual Meeting of the National Council on Radiation Protection and Measurements, National Council on Radiation Protection and Measurements, Washington, D.C., March 15, 1980.

Smith, C. F., J. J. Choen, and T. E. McKene, (1980), A Hazard Index for Underground Toxic Material, UCRL-52889, Lawrence Livermore Laboratory, Livermore, CA, June 1980.

Smith, T. H., P. J. Pelto, D. L. Stevens, G. D. Seybold, W. L. Purcell, and L. V. Kimmel, (1977), A Risk-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accident Release Sequences in Nuclear Fuel Cycle Operations, BNWL-1959, Pacific Northwest Laboratory, Richland, WA, January 1977.

Solomon, K. A., R. C. Erdmann, T. E. Hicks, and D. Okrent, (1974), Airplane Crash Risk to Ground Population, UCLA-ENG-7424, University of California, Los Angeles, CA, March 1974.

Soloman, K. A., R. C. Erdmann, T. E. Hicks, and D. Okrent, (1974), Estimate of the Harards to the Nuclear Reactor from the Random Impact of Meteorites, UCLA-ENG-7426, University of California, Los Angeles, CA, March 1974.

Starr, C. (1969) "Social Benefit Versus Technological Risk." Science. Volume 165.

Streng, D. L., J. K. Soldat, and E. C. Watson, (1978), A Review of Methodology for Accident Consequence Assessment, NUREG/CR-0545, PNL-2633, Pacific Northwest Laboratory, Richland, WA, September 1978.

Swain, A. D., and H. E. Guttman, (1980), Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Draft), NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., October 1980.

Van Horn, S. J., and R. Wilson, (1976), The Status of Risk-Benefit Analysis, BNL-22282, Brookhaven National Laboratory, Upton, NY, December 1976.

Vaurio, J. K., and D. Sciaudone, (1979), Unavailability Modeling and Analysis of Redundant Safety Systems, ANL-79-87, Argonne National Laboratory, Argonne, IL, October 1979.

Vesely, W. E., F. F. Galdberg, N. H. Roberts, and D. F. Haasl, (1981), Fault Tree Handbook, NUREG-0492, United States Nuclear Regulatory Commission, Washington, D.C., January 1981.

Vesely, W. E., F. F. Goldberg, J. T. Powers, J. M. Dickey, J. M. Smith, and R. E. Hall, (1981), FRANTIC II--A Computer Code for Time Dependent Unavailability Analysis, NUREG/CR-1924, U.S. Nuclear Regulatory Commission, Washington, D.C., April 1981.

Voss, J. M., (1977), Safety Indices and Their Application to Nuclear Waste Management Safety Assessment, PNL-2727, Pacific Northwest Laboratory, Richland, WA, April 1977.

Wang, P. Y., J. Mavec, R. M. Wolosewicz, J. M. Calm, and P. S. Chopral, (1979), Reliability, Maintainability, and Availability Engineering for Integrated Community Energy Systems, ANL/CNSV-6, Argonne National Laboratory, Argonne, IL, December 1979.

Wick, O. J., and M. O. Cloninger, (1980), Comparison of Potential Radiological Consequences From a Spent Fuel Repository and Natural Uranium Deposits, PNL-3540, Pacific Northwest Laboratory, Richland, WA, September 1980.

Webster's New Collegiate Dictionary, (1975), G&C Merriam Co., Springfield, Massachusetts, 1975.

Woodward, W. S. and F. J. Baloh (1978), Common Cause Failure Assessment Specification for the CRBRP Reactor Shutdown System, CRBRP-ARD-0195, Westinghouse Electric Corp., Madison, Pennsylvania, July 1978.

Worledge, D. H., (1979), The Role of Event Trees in Reactor Accident Analysis, SRD-R-128, United Kingdom, Atomic Energy Authority, Culcheth, Warrington, England, 1979.

APPENDIX B

A RISK ASSESSMENT METHOD
FOR NUCLEAR FUEL CYCLE OPERATIONS

P. J. Pelto

APPENDIX B
A RISK ASSESSMENT METHOD FOR NUCLEAR FUEL CYCLE OPERATIONS

	<u>Page</u>
B.1 INTRODUCTION	B-1
B.2 RISK ANALYSIS METHOD	B-1
B.2.1 Preliminary Analyses	B-3
B.2.2 Release Sequence Identification	B-3
B.2.3 Preliminary Evaluation and Screening	B-4
B.2.4 Release Sequence Probabilities	B-7
B.2.5 Release Fractions	B-7
B.2.6 Use of Cutoffs	B-8
B.2.7 Computer Program	B-8
B.2.8 Detailed Analysis	B-10
B.2.9 Comparison of Methods	B-10
REFERENCES	B-12

B.1 INTRODUCTION

This appendix presents a summary of a specific risk assessment method developed at PNL (Pelto and Winegardner; Smith et al. 1976). In general, risk analysis of a nuclear related system consists of the following basic steps: (1) Definition of the inventory of radioactive material and its containment/confinement barriers; (2) Identification of potential failure modes; (3) Estimation of the probability and amount of radioactive material released by the potential failure modes; (4) Analysis of the consequences of the radioactive material released; and (5) Estimation of the system risk. Figure 1 shows the information flow and calculational steps for a risk analysis.

In performing a risk analysis potential release sequences ranging from the frequent to the unlikely are identified. These release sequences are evaluated in terms of consequences as well as probability. Knowing both the consequences and the probability, a risk expression can be generated. The most general definition of risk is that it is some function of the probability and the consequences of a potential release sequence. A frequently used definition of risk is the product of the anticipated frequency of a release sequence and its consequences. That is, risk is the mathematically expected consequences of a release sequence. Recognizing the subjective nature of risk and its perception by the public, many studies (USNRC 1975; McSweeney et al., 1975) have avoided the use of a specific risk expression and simply report curves of probability versus consequences.

The most comprehensive risk assessment to date has been the WASH-1400 study of light water reactors (USNRC 1975). Safety/risk analysis have been performed to various depths on other nuclear fuel cycle operations; however, none at the detailed level comparable to WASH-1400.

B.2 RISK ANALYSIS METHOD

A method for the identification and preliminary evaluation of potential accident releases sequences from nuclear fuel cycle operations is discussed in detail by Smith et al. (1976). The major elements of this method are given below.

FIGURE 1. RISK ANALYSIS CALCULATION FLOW (SMITH et al. 1974)

B.2.1 Preliminary Analyses

Several preliminary analyses are performed prior to the systematic identification of potential release sequences. The facility and its operation are described in sufficient detail for the purpose of the analysis. System bounds are established in space (physical boundaries of the system studied), time (time periods of interest for the safety analysis, i.e., mission time), and limit of resolution (degree of system detail considered). Preliminary hazards analyses are then performed to generate a list of hazardous elements in the system and qualitative information on the potential release mechanisms and design measures for prevention and control.

B.2.2 Release Sequence Identification

The next phase of the analysis is the use of more powerful inductive or deductive methods to systematically identify potential release sequences. Methods that may be applicable include: event trees alone; event trees with fault trees used to supply most of the branch probabilities; the similar cause/consequence analysis in which a fault tree feeds into an event tree through a common critical event and which fault trees again supply most of the branch probabilities; and various fault tree techniques.

Inductive methods, such as event trees, start with assumed initial failures. Additional component failures required to obtain a release (system failure) are then identified. Fault tree analysis is a deductive process. The analyst assumes the occurrence of an event selected as the top, undesired event, constituting system failure. He then systematically works backward to identify component faults which could cause or contribute to the undesired events.

The approach selected was the "to/through" fault tree method. This fault tree construction technique is similar to the leak path approach (Fullwood and Erdmann 1974). The top, undesired event (accidental release of radioactive material from the operation) is postulated. The analyst traces back in reverse sequence to determine how each containment barrier could have been breached. The initial material released during an accident must move to each barrier and pass through it for release to occur. This process continues until

initiating events have been reached. Figures 2 and 3 give a simplified illustration of the to/through fault tree technique. A sequence of events which negates the containment/confinement barriers and results in the occurrence of the top event is termed a release sequence. These sequences correspond to the familiar cut sets of fault tree analysis. The binary limitation of fault trees (i.e., faults must be "on-off") can be circumvented by treating each release sequence (cut set) separately and using a distribution of releases where necessary.

B.2.3 Preliminary Evaluation and Screening

Using this fault tree technique often requires the analysis of very large trees. It is neither feasible nor necessary to rigorously evaluate the large number of release sequences identified by the fault tree. The approach used is to separate the dominant sequences from the low risk sequences by a preliminary evaluation and screening process. Refined analysis can then be performed on these dominant sequences.

In nuclear risk analysis the significance of an accident sequence is measured by both its probability and its consequence. Therefore, the evaluation and screening process must be based on a calculation of risk, not just probability alone. This screening is based on a simplified risk expression and use of derived cutoffs (based on risk) on the probability and length of an accident sequence.

The risk of a release of radioactive material can be defined as a product of five terms, in appropriate units: (A) the probability of the release sequence; (B) the release magnitude; (C) measures of the physical, chemical and radiological characteristics of the released material; (D) a measure of the environment transport path efficiencies; and (E) a measure of the population distribution and habits. An (F) term for conversion from population dose to health or environmental effects, is optional, as is a (G) term, for conversion of risk to monetary units. As mentioned in Section B.1, other definitions of risk have been proposed. The effects of alternate measures of risk and their effects on the method discussed in this paper are considered by Smith et al. (1976).

FIGURE 2. BARRIER CONFIGURATION FOR EXAMPLE OF TO/THROUGH TECHNIQUE FOR FAULT TREE CONSTRUCTION (SMITH et al., 1976)

FIGURE 3. FAULT TREE REPRESENTING RELEASE FROM THE BARRIER SYSTEM OF THE PRECEDING FIGURE. THE ANALYSIS HAS BEEN SIMPLIFIED BY ASSUMING 1) ALL RADIOACTIVE MATERIAL IS INITIALLY CONTAINED WITHIN BARRIER 1; 2) THE TRANSPORT PATHS 2a→3a, 2a→3b, 2b→3a, and 2b→3b ARE ALL IDENTICAL; AND 3) THE TRANSPORT PATHS 1→2a AND 1→2b ARE IDENTICAL (SMITH et al, 1976).

When comparing and screening sequences within a fault tree for an operation at one site, the risk expression can be simplified. The E term (population density) is generally independent of failure sequence. Sequences with similar D (environmental transport) terms are grouped and compared only within a group. The C term (material characteristics) can be handled by grouping sequences with similar C terms, or by including C terms with the B terms for release magnitude. Under these conditions, screening and preliminary ranking of sequences can be conducted (for sequences with similar D terms) based simply on comparisons of the product of the A and B terms.

As indicated above the screening and ranking of the potential release sequences requires the probability of the release sequence (A term) and the release magnitude (B term). The basic steps in this procedure include: (1) identify the release sequence; (2) compare release sequence length against the derived cutoff; (3) calculate release sequence probability; (4) compare release sequence probability against the derived cutoff; (5) calculate release sequence release fraction; and (6) rank release sequences on the appropriate A x B comparisons.

B.2.4 Release Sequence Probabilities

The release sequence probabilities are calculated using available data and extensions of the WASH-1400 (USNRC 1975) equations. The probability calculations are based on the assumption of small probabilities and constant hazard rates (i.e., exponential failure distributions). Cut sets consisting of repairable components only, nonrepairable components only, or mixtures of both types can be evaluated. On-line or standby components, unavailability contributions from pre-existing failures, failures on demand, and testing and maintenance down-time can be handled.

B.2.5 Release Fractions

A release fraction is assigned to each basic event in the fault tree. The release fraction is defined as the amount of radioactive material passing through a containment/confinement barrier divided by the amount of material to which the barrier is exposed. For an initiating event the release fraction is the fraction of the total inventory of radioactive material initially

dispersed. Some basic events do not have a release fraction (e.g., fan fails) and a value of 1.0 (which results in no effect on the calculation) is assigned. Other basic events may have a distribution of releases and up to four distributed values can be assigned. Combining the release fractions and the total inventory of radioactive material available results in the estimated release of radioactive material for the release sequence.

Sources of information for assigning basic event probabilities, unavailabilities, and release fractions are operating data, test data, analysis and engineering judgment. Many events require use of engineering judgment because of the lack of operating experience, test information and analysis.

B.2.6 Use of Cutoffs

In the evaluation and screening process, cutoffs on release sequence length and probability are used to reduce the calculational effort required to evaluate large fault trees. These cutoffs are derived on a risk basis and are conservatively calculated. In calculating the probability cutoff, a reference release sequence is selected and its risk measure is calculated. The probability cutoff is calculated based on the question: "At what probability will even the release of the total system inventory result in negligible risk compared to the reference release sequence?" The release sequence length cutoff is calculated by conservatively assuming the n highest probability basic events compose a single release sequence. The cutoff value is that value of n which results in a probability less than or equal to the probability cutoff.

B.2.7 Computer Program

The identification, preliminary evaluation, and screening process is facilitated by a computerized procedure. A computer package consisting of three codes has been developed to assist in performing a preliminary risk assessment. Figure 4 illustrates the use of these codes in the screening procedure. The names of these programs and their functions are given below:

ACORN - draws a fault tree diagram based on the tree logic description input by the analyst (Carter 1977).

FIGURE 4. SCHEMATIC OF SCREENING PROCESS (PELTO AND PURCELL 1977)

MFAULT - identifies release sequences, calculates release sequence probabilities, and screens release sequences on the basis of derived cutoffs (Pelto and Purcell 1977).

RAFT - Calculates a risk measure and orders release sequences in terms of decreasing risk measure (Seybold 1977).

B.2.8 Detailed Analysis

The screening processes facilitates the determination of which release sequences are dominant risk contributors and warrant additional analysis. The output from the screening process generally does not result in a complete or suitable determination of the system risk. Areas which require further analysis are spectrum considerations (events which may have frequency versus severity distributions), identification of common cause failures and mathematical treatment of identified dependent events, and sensitivity and importance studies.

Detailed probability and consequence studies of the dominant release sequences should follow. These detailed studies can be performed using the release sequences directly or by performing a more detailed fault or event tree analysis.

B.2.9 Comparison of Methods

The fault tree analysis method employed by PNL has some advantages and weaknesses relative to other safety analysis methods, such as event tree and cause consequences analysis. No assumption of initiating or critical events is necessary in the fault tree method. This is an advantage for systems where the key initiators are not known. Other advantages include more direct treatment of common cause failures because all events appear on one fault tree, and potentially a more complete analysis can be conducted because the system is treated as a whole. One disadvantage of this approach is the required analysis of very large fault trees.

Event trees and cause-consequence analysis better facilitate and display the detailed analysis (particularly time phasing) of accidents involving a common initiating or critical event. Using these techniques, a complex problem can often be divided into manageable segments. A disadvantage is that there is no formal procedure to develop the required key initiating events. Difficulties often arise in the ordering and the treatment of dependencies of the branch operators (key events or decision points in the event trees or cause-consequence diagrams).

Most safety analysts will agree that there is no best method for performing a safety/risk analysis. Depending upon the system being evaluated a combination of approaches is often advantageous. One potential combination is suggested. A fault tree analysis method as described in this paper would be used to provide a comprehensive identification of potential accidents and to separate those that should be examined in more detail. Detailed analysis of such accidents could follow by means of event trees or cause-consequence analysis. If the key initiating events are known with confidence, the comprehensive type of fault tree analysis may not be necessary.

REFERENCES

Carter, J. L. 1977. ACORN: A Computer Program for Plotting Fault Trees. BNWL-2144, Pacific Northwest Laboratory, Richland, Washington.

Fullwood, R. R. and Erdmann, R. C. 1974. "On the Use of Leak Path Analysis in Fault Tree Construction for Fast Reactor Safety." Proceedings of the Fast Reactor Safety Meeting, USAEC, CONF-740401-P3, pp. 1493-1507.

McSweeney, T. I., Hall, R. J., et al. 1975. "An Assessment of the Risk of Transporting Plutonium Oxide and Liquid Plutonium Nitrate by Truck," BNWL-1846, Pacific Northwest Laboratory, Richland, Washington.

Pelto, P. J. and Purcell, W. L. 1977. MFAULT, A Computer Program for Analyzing Fault Trees. BNWL-2145, Pacific Northwest Laboratory, Richland, Washington.

Pelto, P. J. and Winegardner, W. K., 1977. "A Risk Assessment Method for Nuclear Fuel Cycle Operations." In ANS Transactions, Vol. 26, June 1977, 23rd Annual ANS Meeting, New York, NY.

Seybold, G. D. 1977. RAFT: A Computer Program for Fault Tree Risk Calculations. BNWL-2146, Pacific Northwest Laboratory, Richland, Washington.

Smith, T. H., Winegardner, W. K., Jansen, G., Williams, L. D. and McSweeney, T. I. 1974. "A Methodology for Risk Analysis of Nuclear Waste Management Systems." presented to the American Nuclear Society 20th Annual Meeting, BNWL-SA-4899, Pacific Northwest Laboratory, Richland, Washington.

Smith, T. H., Pelto, P. J., Stevens, D. L., Seybold, G. D., Purcell, W. L. and Kimmel, L. V. 1976. A Risk-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accidental Release Sequences in Nuclear Fuel Cycle Operations. BNWL-1959, Pacific Northwest Laboratory, Richland, Washington.

DISTRIBUTION

No. of
Copies

No. of
Copies

OFFSITE

Battelle Memorial Institute
Office of Nuclear Waste Isolation
Attn: Ms. Beverly Rawles
505 King Avenue
Columbus, OH 43201

L. Carter
Science Magazine
4522 Lowell Street, N.W.
Washington, D.C. 20016

R. C. Erdmann
Science Application, Inc.
2680 Hanover Street
Palo Alto, CA 94303

A. A. Churm
DOE Chicago Patent Group
9800 South Cass Avenue
Argonne, IL 60439

C. R. Cooley
DOE Nuclear Waste Management
Washington, D.C. 20545

27 DOE Technical Information Center

D. Egan
Environmental Protection Agency
Office of Radiation Programs
Washington, D.C. 20460

T. H. Smith
EG&G Idaho
P.O. Box 1625
Idaho Falls, ID 83415

G. B. Levin
EG&G Idaho
P. O. Box 1625
Idaho Falls, ID 83415

J. Malaro
NRC Office of Nuclear Regulatory
Research
Washington, D.C. 20545

E. F. Mastal
DOE Nuclear Waste Management
Washington, D.C. 20545

A. F. Perge
DOE Nuclear Waste Management
Washington, D.C. 20545

J. W. Rowen
DOE Operations and Traffic
Washington, D.C. 20545

K. Schmitz
DOE Nuclear Waste Management
Washington, D.C. 20545

No. of
Copies

No. of
Copies

V. G. Trice
DOE Operations and Traffic
Washington, D.C. 20545

J. W. Voss
Battelle Project Management
Division
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

E. Wahlquist
DOE Nuclear Waste Management
Washington, D.C. 20545

R. Williams
Electric Power Research Institute
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94304

Pacific Northwest Laboratory (contd)

P. J. Pelto (25)
R. E. Rhoads
J. V. Robinson (5)
W. K. Winegardner (5)
NWTP0 Library (3)
Publishing Coordination (2)
Technical Information (5)

ONSITE

3 DOE Richland Office Operations

H. E. Ransom
J. J. Schreiber
M. W. Shupe

2 Rockwell Hanford Company

R. E. Isaacson
D. E. Wood

2 Human Affairs Research Centers

J. Hebert
S. M. Nealey

57 Pacific Northwest Laboratory

T. D. Chikalla
D. A. Dingee
R. H. V. Gallucci (5)
K. M. Harmon
M. R. Kreiter
W. V. Loscutoff
R. W. McKee