1/36

A SURVEY OF RISK ASSESSMENT METHODS FROM THE NUCLEAR, CHEMICAL, AND AEROSPACE INDUSTRIES FOR APPLICABILITY TO THE PRIVATIZED VITRIFICATION OF HANFORD TANK WASTES

Prepared for

Nuclear Regulatory Commission
Contract NRC-02-97-009

Prepared by

M. Frank (Consultant)

Safety Factor Associates, Inc.
Encinitas, California

Edited by

M. Jarzemba
J. Weldy

Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas

August 1998

2/36

ABSTRACT

This document presents a summary of risk assessment methods derived from theory and practice in the nuclear, chemical, and aerospace industries which may be of use for regulatory decision making for privatization of vitrification operations at the Hanford Tank Waste Remediation System. The report begins by discussing components of risk assessment (e.g., trigger events, scenario development) and proceeds by discussing how these components are typically implemented in practice. A discussion of techniques that can be used for event consequence analysis (e.g., computer codes) and how to factor uncertainty into such analyses is also presented. The report then concludes by commenting on the overall usefulness of risk assessment as a regulatory tool.

3/36

CONTENTS

Section Page

CONTENTS (cont'd)

Section Page

FIGURES

Figure Page

TABLES

6/36

ACKNOWLEDGMENTS

This report was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-97-009. The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards, Division of Waste Management. The report is an independent product of the CNWRA and does not necessarily reflect the views or regulatory position of the NRC.

The author and editors wish to thank Ms. Laura Deere for her technical review and Dr. B. Sagar for his programmatic review of this document. Thanks are also extended to Ms. J. Gonzalez and Ms. L. Selvey for secretarial support and Ms. B. Long for her editorial review.

QUALITY OF DATA, ANALYSES, AND CODE DEVELOPMENT

DATA: No CNWRA-generated original data were used in this report.

ANALYSES AND CODES: No computer codes or analyses were used in this report.

7/36

1 INTRODUCTION

1.1 RISK ASSESSMENT, RISK MANAGEMENT, AND DECISION MAKING

Safety risk analysis is a process that involves risk assessment (RA) and risk management. Risk management for safety is a process that involves development of prioritized risk contributors, development of strategies to deal with the contributors, and selection of the "best" strategy. "Best," of course, is relative to the criteria (either explicit or implicit) that are used in making decisions about safety. Typically, a well-executed safety RA leads to the development of candidate risk reduction strategies for the improvement of safety. Table 1-1 provides the key definitions used in this document (Frank, 1995).

Making a decision on which candidate strategy to implement is often complex and difficult because it involves balancing safety with factors such as technical feasibility, cost, schedule, performance (waste throughput), and availability. Often other factors, which are not readily quantifiable, are also factored into a decision. Thus, a key element of managing risk to improve safety is making decisions.

As an illustration, a multicriteria decision process showing the role of risk assessment and decision making is exhibited in figure 1-1. At the time of a decision, a decision maker would evaluate each strategy in terms of decision criteria. In this figure, the example criteria are cost, performance, and safety. The values of these criteria are always uncertain. They are, therefore, expressed as probability distributions over the range of the possible criterion values. For example, the value of the cost criterion is usually expressed in dollars, and the value of the safety criterion can be expressed in frequency of release, frequency as a function of source term, or frequency as a function of dose (or all three).

Table 1-1. Risk definitions for this document

Term	Definition
Risk	Uncertainty associated with the achievement of any parameter, goal, criterion, or requirement associated with a decision.
Risk (Specific to safety)	Frequency of occurrence (with uncertainty) of undesired end states where the degree of severity of each end state is included.[1]
Risk Assessment	The process of developing a model that may be used to obtain risk.
Risk Management	The process of risk contributor prioritization, development of risk modification strategies, and decision making.
Risk Analysis	The combination of risk assessment and risk management.
Decision Making	Process of choosing among alternative courses of action.

[1] NRC definition of risk, including risk triplet and aggregate risk may be found in C.4.4.4 of NUREG-1489 (Nuclear Regulatory Commission, 1994a).

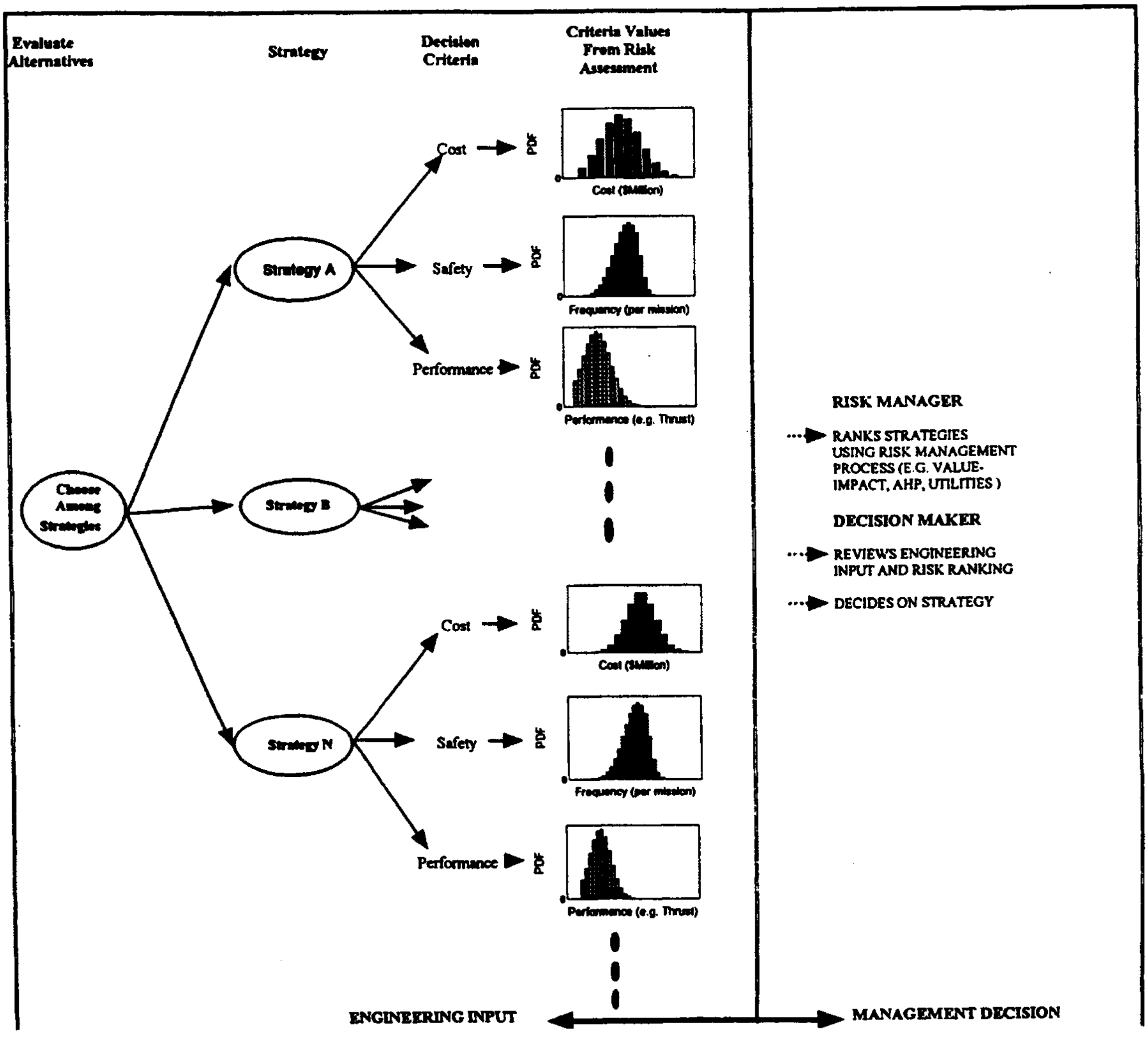


Figure 1-1. Relationship of risk assessment, risk management, and decision making

1.2 SCOPE OF THIS STUDY

This document is intended as a survey of RA methods, derived from RA theory and practice in the chemical, nuclear, and aerospace industries, that might be of use for regulatory decision making and promulgation of regulations for the Hanford Tank Waste Remediation System (TWRS) privatized vitrification project. It is not a method handbook, guidance document, tutorial, or manual.

The currently preferred approach for the Privatized Vitrification Project at Hanford is a phased development of remediation activities. It is currently intended that the Phase II facilities and processes would be licensed and regulated by the Nuclear Regulatory Commission (NRC). The survey behind this document assumed that the principle intent of licensing and regulation is to assure safety. This survey is limited to safety RA methods. Programmatic risk methods (project cost and schedule risk), cost-benefit, value-impact, and other decision analysis methods are not included. It is recognized, however, that some of the methods discussed in this report may also be applied in the arena of programmatic risks. From this point on in this report, the term risk is used to mean safety risk.

The literature about risk methods and techniques is vast. Those useful in the nuclear power industry, during interactions with the NRC, represent a small sample of the plethora of techniques used. A complete description of all of the individual RA methods is not feasible and not the intention of this survey. Rather, the intention of this report is to provide a general characterization of categories of fundamental risk methods, derived from the nuclear, chemical, and aerospace industries, that, may be applicable for regulatory purposes with respect to the Privatized Vitrification Project at Hanford. Detailed descriptions of individual techniques will not be provided in this report. An extensive reference list is provided for those who wish to learn more about individual techniques.

This document presents a survey of fundamental methods of RA. Some currently popular pseudonyms for RAs include, but are not limited to probabilistic risk assessment (PRA), integrated risk assessment (IRA), quantitative risk assessment (QRA), probabilistic safety assessment (PSA), integrated hazard analysis (IHA), enhanced hazard analysis (EHA), and integrated safety assessment (ISA). Each of these RAs is a compilation of fundamental methods specifically selected to meet the needs of a community of interest and/or a class of systems or facilities. These RAs vary in their objectives and emphasis on qualitative versus quantitative analysis and in comprehensiveness, detail, expertise required, and amount of effort to apply.

1.3 USE OF RISK ASSESSMENT IN NUCLEAR REGULATORY COMMISSION REGULATORY ACTIVITIES

The uses of RA depend on the decisions to be made. As described in section 1.1, decision making is essentially a prediction and selection activity. Based on best available information, the decision-maker tries to predict the outcome of each prospective strategy and then selects the one that "best" fits the criteria. The greatest benefit of RA is achieved as a predictor of potential risk significant scenarios rather than an after-the-fact safety analysis (although it has been and continues to be used for that also). Thus, RA is well suited to provide information to a decision-maker.

Assuring the safety of an operating system involves decisions regarding, for example, inherent safety features, engineered safety systems, administrative controls, and operation and maintenance philosophy. Engineered safety systems for the Privatized Vitrification Project may include such items as double-walled piping and redundancy of containment walls. Safety systems also may include features that prevent the vitrification system from undergoing severe temperature transients. These features would either prevent or mitigate an unwanted hazardous material release. A comprehensive RA discovers scenarios that might lead to release of hazardous materials despite the safety systems. Because of the predictive ability of RA, how to best prepare for a hazardous material release becomes a crucial decision.

Although a regulatory agency does not engage in design, it does have the responsibility for review and approval of aspects of design, operation, maintenance, and emergency preparedness that are essential for safety. A good example of the NRC function in this area is the promulgation of Regulatory Guides that provide information on how to best meet General Design Criteria [e.g., given in 10 CFR Part 50 (Nuclear Regulatory Commission, 1997b)]. RA gives a regulatory agency a tool for anticipating accidents and preparing regulatory strategies that will mitigate risk. Historically, RA methods have been shown to be useful in a variety of regulatory areas. Those areas that might apply to licensing and regulatory activities of privatized vitrification operations are listed as follows:

- Identify hazards
- Rank risk significance of systems and human actions
- Review and approve safety systems to meet safety criteria
- Review and approve limiting conditions of operation and allowed system outage times
- Review and approve the array of parameters to be monitored during operation
- Review and approve emergency operating procedures
- Review and approve emergency plans
- Evaluate residual risk after design is complete

Another use of RA, proposed many years ago and beginning to be used in the nuclear power arena, is a risk meter—a risk model that runs online is developed and continuously updated. The general idea is that, in addition to relying on set-points for limiting conditions of operation, the current risk status of the operating unit is monitored and the online risk is displayed. When the risk reaches a predetermined level, the system is either shut down or reconfigured to a safer one. These risk levels and actions can be incorporated into the technical specifications of the system. Because this risk meter method avoids the guesswork in attempting to determine if an abnormal reading on a specific parameter is risk significant during the operations phase, this technique is not limited to a regulatory tool.

1.4 FUNDAMENTAL CONCEPTS OF RISK ASSESSMENT

A particular property of RA for regulatory purposes may be called integration. RA has the ability to integrate all hazards (i.e., chemical, radiological, mechanical, electrical, thermal, etc.) into a cohesive picture of risk. It has the ability to integrate all components, subsystems, processes, software, and items related to safety of the system or facility into this picture. Once a risk model is developed, therefore, changes in the system or the hazards are reflected in a change in the risk of the entire system or facility.

RA allows analysis of the spectrum of effects or influences that a system can cause to its biological and physical environment and the occurrence frequency of each end state. Both the end states and their frequencies are treated as uncertain variables. The methods combine probability theory and decision theory with traditional engineering and scientific disciplines to develop structured, quantitative information suitable for aiding risk management decision making in the face of uncertainties. The outcome of an RA is a model of the perturbations, end states, scenarios, and frequencies of events, with uncertainties, that may be used to assess how to reduce risk and may be modified as conditions change. The usefulness of RA to achieve the property of integration and the detailed analysis of effects to the biological and physical environment derives from the following basic methodological characteristics (Frank, 1995):

- It is imperative that the RA methodology assemble a multitude of elements (or events) of a problem or situation into groups based on common properties. These events in turn, may be grouped and re-grouped according to higher level common properties.

- It is scenario based—string of events leading from some initial mishap to an undesired end state may be thought of as a scenario. Best estimate scenarios and realistic variations are developed. Conservative or bounding scenarios are also included, but their risk significance is moderated by the probability of occurrence.

9/36

- It is structured, logical, and organized such that prioritization of scenarios, elements, and failure modes, is readily obtained. The underlying reasons for the prioritization are explained.

- Because the path and causes of failure are developed, insights into viable risk reduction strategies are apparent.

- It allows identification and quantification of uncertainties associated with modeling of the physical, biological, and chemical aspects of events, the parameters of the models, and the frequency of events. Information from analysis, databases, testing, and judgement may be combined within the models. Uncertainties may be propagated throughout the risk model so that the result includes all significant contributing uncertainties.

A useful interpretation is to think of RA as a logical, structured thought process that has the above five characteristics. Any number of tools or methods, some of which are described in section 2, may be used.

A basis of RA is the development of scenarios. Scenarios may be thought of as strings of events that lead to a consequence or end state. Each scenario begins with a trigger event, sometimes called an initiating event, and ends with an end state (no damage or no significant effect are also valid end states). A trigger event is any abnormality, malfunction, or failure (whether it is human, hardware, software, or process) that causes a deviation from desired operation. The decision-maker defines the end states (e.g., dose to offsite populations). Between trigger events and end states are pivotal events which determine whether and how a trigger event propagates to an end state. One trigger event, one or more pivotal events, and one end state define each scenario. Pivotal events may be protective, mitigative, aggravative, or benign. A protective event reduces the likelihood of the trigger event producing an undesired end state. A mitigative event reduces the severity of the end states. An aggravative event increases the severity of the end state, the frequency of reaching undesired end states, or both. A benign event has little or no effect on the course of the scenario although it may have been a *priori* perceived as beneficial. A scenario, therefore, may be conceptually represented in figure 1-2.

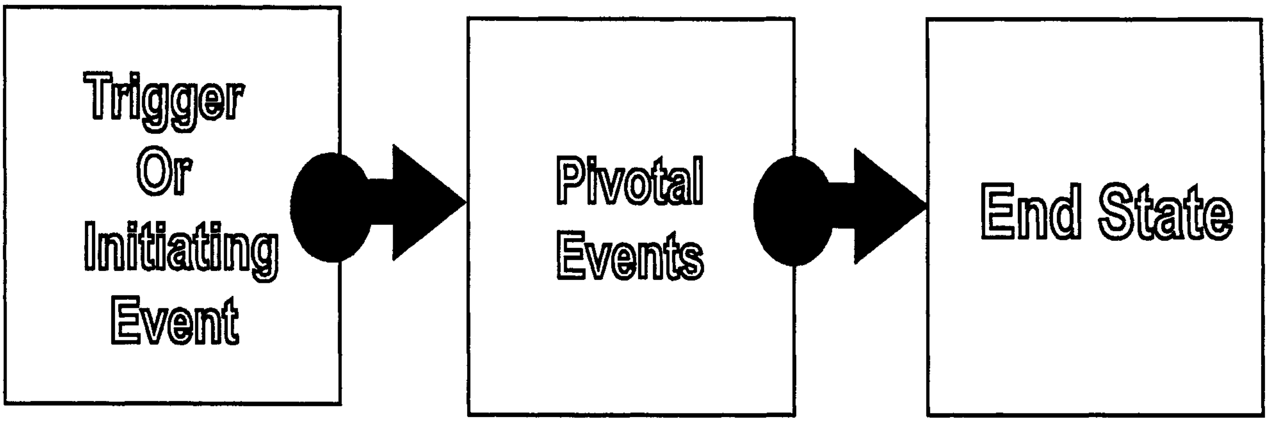


Figure 1-2. Conceptual representation of a scenario

2 METHOD SURVEY

This section provides an overview of the concepts of commonly used categories of RA methods that, may be applicable for regulatory purposes with respect to the Hanford Privatized Vitrification Project. A significant aspect of the selection of methods is that an RA of the vitrification process must include the ability to analyze both radiological and chemical hazards. A brief description of the intent of each category of methods is provided along with allusions to uses of the method and software available. The discussion makes extensive use of references.

Methods are categorized as follows:

- Event identification
- Scenario structuring
- Frequency and probability analysis
- Consequence analysis
- Uncertainty analysis
- Other topics

These categories are in consonance with the conceptual vision of RA described in section 1.4. Methods have been selected that would, aid in regulatory decision making and the promulgation of regulations. There has been no attempt to list or mention every RA method and technique.

2.1 EVENT IDENTIFICATION

Hazards may be thought of as a source of danger with the potential to cause personal injury, damage to the environment, or to the facility. Such hazards could also be thought of as giving rise to risk. Events that perturb a system from its normal state have the potential cultivate or release the hazard. As stated in section 1.4, scenarios, composed of initiating events, pivotal events, and end states, form the structure with which risk is analyzed. Early tasks of a risk analyst, when confronted with a new system to analyze, are to identify hazards, identify events that might act upon hazards, and structure these events into scenarios. This section describes methods of identification, and the next section describes methods of structuring scenarios.

Some of the more common methods in use are summarized in the next section in order of increasing comprehensiveness and structure. As the system or process becomes more complex, a more structured approach is needed to maintain order and increase comprehensiveness. On the other hand, the more structured approaches require more detailed information regarding the facility or system and, therefore, may not be appropriate at an early stage of system development.

Experience. The first documented use of this unstructured approach for safety assessment was by Pliny, the Elder (Raouf and Dhillon, 1994). An individual or group creates a list of hazards and events from background and experience. If by a group, it is done either during a group discussion or by a *posteriori* compilation of the ideas of individuals. An advancement of this method, is brainstorming, which is a more formal group activity in which creativity is encouraged, and no idea is discouraged. Another variation of this method is for experts to be interviewed by someone skilled at knowledge elicitation (Shisko, 1995). Experience-based methods are typically assisted by a survey of previous accidents or mishaps, usually embodied in a checklist. This method is effective for a small system or a small portion of a larger system in which interactions are not immediately apparent. The techniques of brainstorming are incorporated into the What If? Creative Checklist, and Hazard and Operability study (HAZOP) approaches described as follows:

What If? (American Institute for Chemical Engineers, 1985). A multidisciplinary team is assembled. Hazards are identified by reviewing a design. The design may be partitioned to decrease the complexity in thinking. The participants ask themselves What If questions to identify potential failure events or hazards, which are associated with potential causes and consequences. Sometimes safety systems are identified. The results are written in a list. Normally, the most severe consequences conceivable are associated with the event. This association is often assisted by a checklist, in which case the technique is called What If/Checklist (System Safety Society, 1993). This process is quite similar to the methods termed Preliminary Hazard Analysis and Hazard Analysis in the aerospace and defense industries [U.S. Department of Defense (MIL–STD–882b), 1984b; National Aeronautics and Space Administration, 1987a]. The differences between the two hazard analyses refer to the stage in the design at which the analysis is performed, not the completeness of the analysis.

Creative Checklist. A significant advance in the use of experience, What If? analysis and Checklists are embodied in the Creative Checklist approach—was developed to identify hazards in chemical process and storage facilities (Knowlton,1992). The principal steps of this approach include:

First, a system-specific checklist is created from existing generic checklists by brainstorming the perturbations, hazards, and events that might lead to an undesired damage state. The brainstorming is structured and greatly aided by using previously developed generic checklists. Such checklists, which generally consist of generic hazards based on energy, interactions, and environment, are already in the literature (Knowlton, 1992; American Institute for Chemical Engineers, 1985; Nuclear Regulatory Commission, 1983; European Space Agency, 1992). The created checklist for a specific system can contain human interactions and external influences (e.g., fires, earthquakes, floods) as well as component and subsystem related hazards.

Second, three matrices are created in which materials, equipment, and activities of the system/facility are associated with each item on the checklist. For example, at the intersection of each material/checklist item, the analyst marks if the material can have the hazard noted in the checklist. If it can, then this hazard/material combination is investigated. Equipment, components, and activities may not be known in the early stages of design development. In this case, only the material/checklist matrix is used. This approach can be applied when only a vague list of materials used in the process is known and it can continue to be applied as the equipment and activities in the process evolve. The Creative Checklist is a useful adjunct or companion method to Failure Mode and Effect Analysis (FMEA) and HAZOP because it to provides a broader, cross system and facility-wide perspective.

Failure Mode and Effect Analysis [American Institute for Chemical Engineers, 1985, 1992; (MIL–STD–1629); Orvis et al., 1981; National Aeronautics and Space Administration, 1987b). This method has been used as a tool for reliability studies in the aerospace, defense, chemical, and nuclear industries for more than 40 yr. It also has application to RA. This method is an extremely detailed, inductive-logic approach in which a design is reviewed, component by component, to determine failure modes of the component and the effect on the next higher level of assembly. That is, failure of a component is assessed with respect to its effect on the subsystem, and subsystem failures are assessed with respect to their effect on the system. For a specific portion of a facility or process (e.g., subsystem), it is a detailed method to identify specific failure modes, possible causes, and immediate effects. FMEA is not effective to identify

11/36

system interactions, common cause and other dependent failures, human interactions, environmental, and external influences. This method has its place in RA as an adjunct to a Creative Checklist, HAZOP, or Master Logic Diagram (MLD) to focus on a narrow but high-hazard aspect of a system or facility. An FMEA is typically in tabular format which is easily converted to a computerized spreadsheet. Typically, worst-case effects are assigned to each failure mode. Many checklists, spreadsheets and software aids have been developed to assist FMEA.

Hazard and Operability Study (Knowlton,1992; American Institute of Chemical Engineers, 1985, 1992). This method has been in use for two decades in the chemical industry. It is perhaps the most widely used method in the world for identifying hazards and how they can lead to undesired consequences. HAZOP is a team endeavor that was created to present a series of images to the team to stimulate the virtual experience of a system. This virtual experience makes it possible to predict potential problem areas in the design. The design is partitioned into parts, each of which is examined by a specific procedure as follows:

- The intention of each part is obtained. The intention is how the part is expected to operate.
- Next, deviations are discovered by systemic application of Guide Words. A deviation is a departure or perturbation of the Intention. As such, it is nearly identical to trigger events as defined in section 1.4.
- The third and fourth general steps are to identify causes and consequences of a deviation.

The key to a HAZOP study is the clear definition, interpretation, and use of Guide Words to stimulate images of how the system may deviate from its intended operation. The standard Guide Words are No or Not, Don't, More, Less, As Well As, Part of, Reverse, and Other Than. These are applied to the material used in the process and the function or action of the process.

Although developed for chemical process, transfer, and storage systems, HAZOP has been successfully applied in other industries. The identification of operational difficulties, as well as safety related hazards, emerges from this approach. Several commercially available software aids, including imbedded checklists and help menus, have been developed to assist the recording of a HAZOP. There is some controversy on the use of such software is a net benefit to the HAZOP process (Knowlton, 1992).

Master Logic Diagram. This logic tree approach was developed about 15 yr ago for nuclear RA (Nuclear Regulatory Commission, 1983) but has been successfully applied in aerospace RAs. An MLD, sometimes called an initiating event logic diagram, is a convenient method for checking that a set of initiating events are reasonably complete. It is a hierarchical depiction of ways in which system perturbations can occur. By a functional categorization of perturbations to the system that eventually leads down to a component characterization for each function, a team of analysts usually capture all but the most indiscernible events. An MLD starts with a top event that is an end state of interest to a decision maker (e.g., radioactivity release, toxic chemical release). Events that are necessary but not sufficient to cause the top event are enumerated in more detail as lower levels of the hierarchy are built. Typically, the top levels are functional failures (e.g., failure to contain, failure to control, failure to cool, etc.). The lower levels are subsystem and component failures that contribute to the functional failures.

These logic models are easily drawn using off-the-shelf commercial drawing or flow chart software.

2.2 SCENARIO STRUCTURING

Event identification methods, described previously, are capable of producing an enormous body of deviations, trigger events, hazards, and scenario fragments. They do not show clear sequences of events, from trigger events through pivotal events to end states, and they do not facilitate development of the likelihood of each scenario. Furthermore, the previous methods do not lend themselves to identification of common cause failure, system interactions, human and software errors, and quality assurance related defects. This is done within the context of scenario development. The general categories of scenario development discussed herein are

- Belief networks
- Simulation
- Dynamic tree methods

One of the keys to a feasible scope of work in an RA is judicious categorization of events. It should be readily apparent that all trigger events are actually categories of events. For example, table E.1.1.1 of the Hanford TWRS Environmental Impact Statement (EIS) lists accidents characterized by leaks, ruptures, and breaches. Both the frequency of occurrence and the severity of the accident are functions of the size of the leak, rupture, or breach. As its approximation, the EIS chose to combine all leaks into a single category.

All scenario development includes some fashion of categorization. One way to settle on the categorization of events is to decide on the resolution of accident severity below which differences can be ignored. Then, events are categorized if they produce differences in consequences that are less than the level of resolution that the analyst (or decision maker) cares about. Another commonly used way to settle on the categorization of events is based on whether pivotal events are significantly different. That is, if two trigger events may be described as reaching end states via the same set of pivotal events, then for purposes of defining scenarios, these two trigger events are of the same category. This is a powerful notion for a risk analyst because, by a judicious selection of trigger event and pivotal event categories, the risk model may be significantly simplified.

Scenario development is part of the art of RA in that, although there are standard techniques as described herein, the outward appearance (or representation) of a risk model usually varies greatly from one analyst to the next. Even though two risk models may be representationally different, if both are done conscientiously in accordance with the techniques described herein, their results should not significantly differ.

2.2.1 Belief Networks

Influence diagrams and decision trees are directed graph networks of lines connecting nodes that represents events or influences about a decision to be made (Howard and Matheson, 1984). The nodes represent random variables, decisions, and criteria for making a decision. The most widely used methods for structuring scenarios in RA are diagrams that use only nodes that represent random variables for events that may or may not occur. Examples of such methods are event trees, fault trees, scenario diagrams, event sequence diagrams, influence diagrams, and digraphs.[2] These RA methods may be thought of as a special

[2] Influence diagrams and digraphs will not be discussed because they are not currently in general use for RA, and provide no advantage over other methods discussed in this report.

12/36

case of the more general decision tree or influence diagram and have been given the name "belief networks" (Shachter and Peot, 1992). A similar use of belief networks is found in planning and controlling projects via Management Oversight and Risk Tree (MORT) and Program Evaluation Review Technique (PERT) charts (Event Analysis, Inc., 1985). MORT diagrams have also been applied for postaccident investigations.

Belief networks may use either inductive (e.g., event trees) or deductive logic (e.g., fault trees) for their construction. One of the features of an RA is that the exact diagrammatic form is not unique. Different analysts may select different forms to help themselves develop and display the model. Part of the creativity in performing an RA is the selection of the diagrammatic forms that perform both the model development and model presentation functions. The set of diagrams depends on the objectives and scope of the analysis as well as the audience for the results. Experience with many RAs helps the analyst make a good choice of diagrams. As will be described later, both inductive and deductive methods serve different purposes in a comprehensive RA and they complement each other.

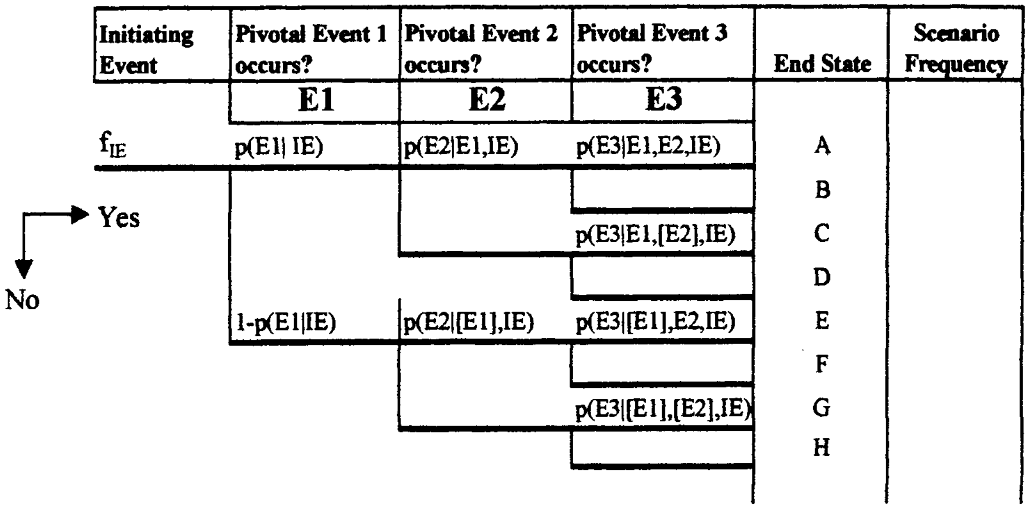
In safety and reliability RAs, the most commonly used belief nets are event trees, fault trees, and event sequence diagrams. Dependent events and common cause failures are often important to overall risk and are usually modeled in event trees and fault trees. Advanced methods for treatment of dependent events have been developed (Fleming et al., 1983; Mosleh, et al., 1988; Vaurio, 1994). Human actions and software errors, as well as hardware malfunctions, and physical and chemical process/phenomenological events are included in the scenarios.

Event Trees. An event tree is a succinct method of diagramming a large number of scenarios (Nuclear Regulatory Commission, 1975). As illustrated in figure 2-1, an event tree begins with an Initiating Event on the left and ends with End States on the right. Across the top are pivotal events that most influence how the initiating event can progress to one of the end states. In this example, a scenario is characterized by a line starting at the left under Initiating Event and proceeding horizontally and vertically along a solid line. The initiating event has a frequency of occurrence, f_{IE}, which may have units such as number of events per year. Each pivotal event is phrased as a yes/no question. If the answer is yes, the scenario proceeds to the next event on the right. If the answer is no, the scenario proceeds downward before going to the right. A number, such as $p(E1|IE)$, characterizes the fraction of occurrences for which the answer is yes or no. This is called the conditional probability of the event or branch point probability. Each scenario has an end state and a scenario frequency. Figure 2-1 shows a binary event tree. That is, each node has only two branches extending to the right. The sum of the two branch point probabilities must equal unity. The scenario frequencies, therefore, reflect the partitioning of the initiating event frequency such that the sum of the scenario frequencies equals the initiating event frequency.

A few practitioners develop event trees with more than two branches extending from a node. It can be mathematically demonstrated that a binary tree is perfectly general in that for each nonbinary event tree, an equivalent binary tree may be constructed.

Although it is traditional in nuclear power plant risk assessments to separate the events into three levels of analysis, there is no inherent reason and no advantage in risk analysis for doing so. Such separation is typically not done in other applications.

Software that aids the development and quantification of event trees is commercially available.



f_{IE} = frequency of initiating event

p(Ex|Ey) = conditional probability of event Ex given occurrence of event Ey

[Ey] = event Ey does not occur

Figure 2-1. Concept of an event tree

Event Sequence Diagram or Scenario Diagram. These diagrams are essentially flow charts that show the same information as an event tree. Their ability to display and communicate the flow of and dependency among events is somewhat clearer than an event tree (Nuclear Regulatory Commission, 1983). It is also better capable of displaying assumptions, design features, and procedures that influence or are involved with the scenarios. Typically, event sequence diagrams are used to communicate a series of complex scenarios, while event trees are used to quantify the frequency of scenarios.

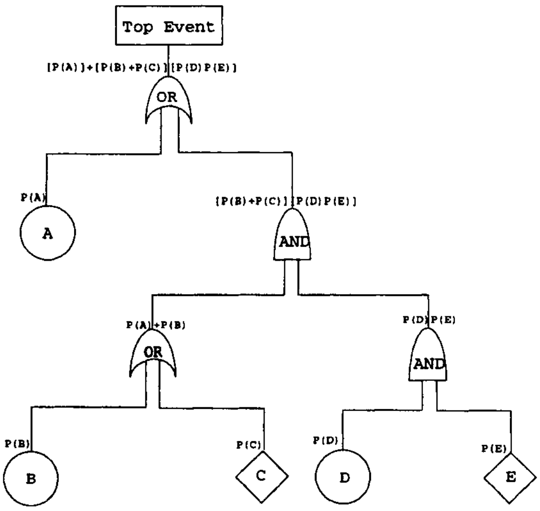
Fault Trees. Fault trees were originally developed in the early 1960s for aircraft system safety studies (Haasl, 1965). Constructing a fault tree involves deductive reasoning. Fault trees are often useful in developing the hierarchy of events. This technique is included in many hazard, safety, reliability, risk, and system engineering books and manuals (Orvis et al., 1981; American Institute of Chemical Engineers, 1985; Shisko, 1995; Shooman, 1990). However, the most comprehensive treatment of the background, theory, and practice is provided in Fault Tree Handbook (Vesely et al., 1981).

Constructing a fault tree involves deductive reasoning because it answers the question How can the top event occur? First, a top event, which is simply an undesired state of a system, is specified. The system is then analyzed in the context of its environment, operation, and items related to safety to find all credible ways that the top event can occur. In the process, all redundancies, controls, software, maintenance, inspection, and other human actions should be considered. A single fault tree is not necessarily a comprehensive description of all failures of a system because it is constructed for its top event, which should be a very specific statement about an undesired system state. A fault tree uses logical gates (AND, OR, NOT) to depict the relationships among events and the top event.

The lowest level of detail depicted in a fault tree is called a Basic Event. Each basic event may be assigned a probability of occurrence. Sometimes events are called undeveloped in that they may be broken down into more detail but the analyst has chosen not to do so. They are treated as if they are basic events. If a fault tree is constructed and analyzed correctly, it will provide the probability of the occurrence of the top event as a probabilistic combination of the basic event probabilities. Any fault tree has an equivalent Boolean equation that expresses the relationship of the events and the top event. In order to correctly obtain the probability of the top event as a function of those of the basic events, a fault tree has to be Boolean reduced to its prime implicants. In fault tree analysis, this is referred to as minterm form. This form is achieved by repeated use of the DeMorgan, Absorption, and Idempotency rules of Boolean algebra. Numerous commercial fault tree development and analysis packages are available to aid in construction, Boolean reduction, and quantification of the top event (see figure 2-2).

Combined Use of Inductive and Deduction Belief Networks. Because of the complementary nature of using both inductive and deductive reasoning processes, event trees and fault trees are often combined for system RA. This practice produces a more complete, concise, and clearer development and documentation of scenarios than using either one exclusively. This combination was first practiced in the Reactor Safety Study (Nuclear Regulatory Commission, 1975). In that study, fault trees were used to analyze the causes of system or subsystem failures depicted in event trees. This study was a powerful insight because it allowed categories of events (i.e., higher level events such as systems or functions) to be depicted in the event trees. Thus, event trees were used to generally give an overview of the scenarios leading to end states while fault trees were used to analyze causes of failures and development of the probabilities. That is, each event in an event tree was used as a top event of a fault tree.

A similar approach to the combined use of inductive and deductive belief networks was developed in the chemical industry and is called Cause-Consequence analysis (American Institute of Chemical Engineers, 1985). Both event tree/fault tree method and cause-consequence analysis use event trees and fault trees, both obtain accident sequences, both obtain scenario probabilities, and both claim an advantage in communication and documentation for the combination of fault trees and event trees. There is a small difference in diagram symbology between Cause-Consequence analysis and the event tree/fault tree method employed in the nuclear industry.



P(X) = Probability of Occurrence of Event X

Figure 2-2. Concept of a fault tree

Belief nets are most useful for processes that do not change significantly over time. They are generally used in applications where the consequences of an accident are similar if the accident occurs on the first day of operation or 10 yr later. The advantages of belief nets over the scenario development methodologies are that they are relatively simple to construct and can give a clear picture of how individual facility components and safety systems impact the safety of the entire facility. The main disadvantage of belief nets is that they do not model dynamic systems very well.

2.2.2 Simulation

Simulation is a completely different paradigm for RA than that described above. In RA using belief nets, the analyst thinks through a system and develops diagrams that explicitly depict scenarios. Standard event tree and fault tree computer codes take care of the analysis of the risk. In simulation methods, the analyst develops a mathematical model, which must be coded as software. A perturbation is introduced to the system (i.e., an initiating event) and the effect of that perturbation (i.e., end state) results from the simulation. Object-oriented programming is a common and powerful way to design such simulations.[3]

Alternative scenarios arise because of (i) variations in the perturbations, (ii) variations in the response of the system, and (iii) uncertainty in knowledge about the system. Variations in system response arise because some processes are inherently stochastic. The most mundane example of this is the time to failure of a component such as a pump. Although a particular class of pumps may exhibit a well-established mean time to failure, because of subtle and often unmeasured variations in the manufacture, handling, operating environment, etc., each pump will exhibit a somewhat different characteristics. The objective of a simulation method is to attempt to characterize the likelihood of alternative scenarios and the probabilities of end states by simulating the situation a large number of times (or trials). Sampling methods are used for this, the two most common are Monte Carlo (Rubinstein, 1981) and Latin Hypercube (Iman and Shortencarrier, 1984).

Over the last decade, the most extensive application of simulation methods has been with space nuclear power RAs (Lockheed Martin Corporation, 1997b). In this application, scenarios are considered dynamic because the response to an initial perturbation evolves over time because of component, phenomenological, and environmental interactions. For example, the potential for and amount of radioactive material released depends on the magnitude of previous explosions, fragment fields, and altitude of the vehicle. The fragment field, in turn, depends on the magnitude of the explosion and the altitude of the vehicle. Furthermore, explosions are inherently uncertain phenomena in that slight differences in conditions can cause significant differences in explosion overpressures. In this simulation approach, an entire set of physical, chemical, and biological processes are modeled. Scenarios include the abnormal trajectory of a space vehicle; its impact, explosion or both; the containment or release of radioactive material; the transport, dispersion, and deposition of released material; biological uptake of the material; and potential health effects. The analysis results in probability distributions (i.e., probabilities with uncertainties) of end states such as the amount and location of released material and number of latent cancer fatalities. Both Monte Carlo and Latin Hypercube simulation techniques were used.

[3] Frank and Epstein (1986) and Cacciabue and Amendola (1986) for early examples of such simulation used for nuclear safety and reliability.

Simulation methods offer a powerful technique for modeling dynamic systems at the expense of the ability to clearly visualize scenarios and the relationship of end states to initiating events and the associated phenomena. Belief nets allow representational clarity but may not be as accurate for dynamic systems.

2.2.3 Dynamic Tree Methods

Two emerging RA methods are the dynamic event tree method (Acosta and Sui, 1993) and the dynamic flowgraph method (Milici et al., 1996). These dynamic methods have similarities to both belief networks and simulation methods (Siu,1994; Devooght and Smidts,1993). Their usefulness arises from the ability to model dynamic scenarios, especially involving human actions, while maintaining some representational clarity. The dynamic event tree approach is characterized by branching at discrete time intervals during an accident progression. A dynamic event tree approach involves application of sets of information or rules for (i) defining a branching set, (ii) branching rules, (iii) system state, (iv) sequence expansion, and (v) quantification (Acosta and Sui,1993). The solution algorithm tracks forward in time.

The dynamic flowgraph method starts with a directed graph of the system. As in fault trees, the algorithm develops prime implicants of the system by parsing backwards in time through the directed graph, obtaining the prime implicants for the most recent time and then backtracking in time to discover how these prime implicants were caused (Milici et al., 1996).

These rules and algorithms are similar in concept to techniques used in object-oriented programming in which objects and their interrelationships behave according to well defined rules (such as equations-of-state). Both the simulation and dynamic tree methods tend to be both labor and computationally intensive for realistic problems. For complex systems for which dynamic interactions are crucial for understanding risk, useful results are obtainable (Siu,1994).

2.3 FREQUENCY AND PROBABILITY DEVELOPMENT

Once scenarios have been developed, a quantitative RA would require that each fundamental or basic event be associated with either a frequency or probability of occurrence. This would lead ultimately to the frequency of scenarios and the ability to make decisions using the likelihood of occurrence of end states as a factor in the decision.

Frequency is distinct from probability in the following way. A frequency is a rate of occurrence (i.e., number of failures per unit time) and may have a value greater than one. It is usually associated with initiating events. A function that associates an event, E, within a sample set, S, is called a Probability, P, if $p(S) = 1$ and $p(E) \geq 0$ and $p(E1 \bullet E2 \bullet E3 \bullet . . .) = p(E1) + p(E2) + p(E3) +. . .$ where none of the E intersect in the sample set. Thus, a probability is a number between zero and one inclusive. A conditional probability is a probability whose number depends on a previous event. Most of the numbers in a typical quantitative risk model are conditional probabilities.

The development of frequencies and probabilities is grounded in probability and reliability theory. Good overviews as well as detailed instruction, therefore, may be found in a number of textbooks and standards [Green and Bourne, 1972; Dhillon, 1988; Shooman, 1990; Martz and Waller, 1991; U.S. Department of Defense, 1991 (MIL–HDBK–217F); 1993 (MIL–STD–690)]. The PRA Procedures Guide (Nuclear Regulatory Commission, 1983) still provides a good overview of nuclear power plant applications in RA.

Consistent with the guidance of the Occupational Safety and Health Administration (OSHA) (Occupational Safety and Health Administration, 1991) and the U.S. Environmental Protection Agency (EPA) (U.S. Environmental Protection Agency, 1993a), the chemical industry has thus far de-emphasized quantitative RA. Methods suggested in these documents are qualitative, and were described previously in sections 2.1 and 2.2. In the chemical industry, risk management is driven by the amount and type of hazardous material that could potentially be released. Decision making regarding risk reduction strategies are generally not related to the likelihood of mishaps or the frequency of releases. California State and Los Angeles Risk Management and Prevention Program guidance documents (Lercari, 1988; Los Angeles County Fire Department, 1991) suggest a screening of hazards using a combination of probability and severity. However, this screening method is essentially identical to the simple severity versus likelihood matrix used in military applications in the 1970s [U.S. Department of Defense (MIL–STD–882b), 1984a]. In practice, this matrix is usually completed without a rigorous and mathematically sound development of the data, relying on guesses made by the analysts. Thus, methods of quantitative risk assessment and reliability data development used in the chemical industry (American Institute of Chemical Engineers, 1989a,b) are largely derivatives of and quite similar to those developed in the nuclear power and defense industries. These methods may be divided into four categories and will be discussed in the following section:

- Statistical
- Bayesian
- Judgement or opinion
- Analytical.

Applications of these methods are generally associated with frequency or probability of hardware failure modes and occurrence of physical, chemical, and biological (i.e., environmental) phenomena. Often, aspects of all four methods are used in a single analysis or even a single event. Analyses of software and human errors use different methods that will be summarized in section 2.6.

RA is essentially a prediction method in that it attempts to anticipate and develop the likelihood of scenarios before they happen. As such, it is particularly useful for rare scenarios. If an event or scenario occurs regularly, then a simple statistical analysis of the resulting trials would provide the frequency, and the RA methodology would not be needed. Therefore, the perspective of quantitative RA is naturally probabilistic. The complexity of the potential scenarios and the rare occurrence of events suggest that probabilities and frequencies have a good deal of uncertainty. In fact, data about hardware failure may be characterized as one of the following:

(1) Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (e.g., operational experience)

(2) Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (e.g., test data)

(3) Historical performance of successes and failures of a similar piece of equipment or similar category of equipment under conditions that may or may not be those under analysis (e.g., test data from other programs or data from handbooks or compilations)

(4) General engineering or scientific knowledge about the design, manufacture, and operation of the equipment or an expert's experience with the equipment.

15/36

For newer technology, systems, and equipment, items (3) and (4) are often the only source of information available. Uncertainty arises because of a number of factors, not the least of which is the applicability of the data to the equipment and conditions studied in the RA. Even for items (1) and (2), however, uncertainty may be significant. For example, the failure rate of a particular component in a nuclear waste processing system could be accurately known if a sufficient number of trials that demand the operation of the component were performed. Since such comprehensive experiments are rarely available, uncertainty in the failure rate is a given. Therefore, one perspective is to view the piece of equipment under study as a member of a population of similar pieces of equipment undergoing a variety of operating conditions and environments. Using this perspective, the failure rate or probability of a piece of equipment is represented by the range that characterizes this population. A probability distribution is the way risk analysts express such ranges. In a safety analysis, however, an upper limit or conservative estimate is often used for practicality.

Probabilistic information about the occurrence and characteristics of physical, chemical, and biological processes within a scenario are derived from judgment alone, analysis alone or, most commonly, a combination of the two. The complexity of the potential scenarios (as indicated in the previous sections) demand that we account for both natural variability of physical processes and the lack of knowledge of these processes. Variability refers to the inherent variation of a physical process over many similar trials or occurrences and is sometimes call aleatory uncertainty. Any particular scenario may or may not occur during any operating time interval, modeling of physical and chemical processes may be approximate, the experimental data may only be partially applicable, and the values of the parameters of the models may not be precisely known. This imprecision is known as epistemic uncertainty, and is discussed further in section 2.5.1.

2.3.1 Generic Data Sources

Two practical realities of RA are that (i) there is always some data[4] and (ii) there is rarely enough data of sufficient verisimilitude. Typically, therefore, RA is performed using a combination of data sources and methods. Compilations of data, otherwise known as generic data sources, play a major part in quantitative RA. Table 2-1 provides a list of some well-known data compilations that may be useful in vitrification process risk studies.

2.3.2 Statistical Methods

These methods involve traditional statistical sampling, data analysis, and uncertainty (or confidence interval) methods and are found in standard textbooks (Winkler and Hays, 1975; Green and Bourne, 1972).

When analyzing a set of sample data in the form of number of failures in a given number of hours, Poisson, Weibull, or Log-normal models are used to derive the associated failure rate in failures per unit time (Abernathy, 1983). A Binomial model is used when analyzing a set of sample data in the form of number of failures in a given number of attempts, trails, or tests. Statistical confidence intervals, which provide the range of failure probabilities that are consistent with the data, may be found for each of these distributions.

[4] As a minimum, the data resides in the minds of those who are designing, building, or operating the system.

Table 2-1. Some data sources used in risk assessment

Source	Comment
U.S. Department of Defense, Reliability Prediction of Electronic Equipment, MIL–HDBK–217F, Washington, DC, 1991	Standard reference for basic electronic component data as a function of military environment
Bellcore, Reliability Prediction Procedure, Issue 5	Similar to above but focuses on commercial equipment
Handbook of Reliability Prediction Procedures for Mechanical Equipment, NSWC–94/L07, 1994	—
W. Denson et al., Nonelectronic Parts Reliability Data, 1995, NPRD–1995, Reliability Analysis Center, Defense Technical Information Center, Rome, NY: 1995	Electrical and some mechanical equipment
Reliability analysis Center, Failure Mode/Mechanism Distributions 1997, FMD–97, Rome, NY: 1997	Provides fraction of total failure rates for a limited set of components in NPRD
Center for Chemical Process Safety, Guidelines for Process Equipment Reliability Data with Data Tables, American Institute of Chemical Engineers, New York, NY: 1989	Only generic chemical industry source
IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, IEEE-STD–500–1984, John Wiley and Sons, New York, NY: 1983	A standard reference based on collective engineering judgment
OREDA Committee Offshore Reliability Data Handbook, Hovik, Norway: 1984	Severe environment associated with offshore oil drilling and pumping equipment
C.H. Blanton et al., Savannah River Site Generic Data Base Development, WSRC–TR–93–262, Savannah River Site, Aiken, SC: 1993	This is a compilation of other generic data sources for RA on the Savannah River nonreactor nuclear and chemical process facilities
D.I. Gertman et al., Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), NUREG/CR–4639, Nuclear Regulatory Commission, Washington, DC: 1989	—
Reactor Safety Study: An Assessment of Accident risks in U.S. commercial Nuclear Power Plants, Appendix III, Nuclear Regulatory Commission, WASH–1400 (NUREG–75/014), Washington, DC: 1975	The first to include uncertainties and still useful if no other more recent sources are available
IREP Procedures Guide, section 5, Nuclear Regulatory Commission, NUREG/CR–2728, January 1983	An update of WASH–1400 values
K.N. Fleming et al., Classification and Analysis of Reactor Operating Experience Involving Dependent Events, Electric Power Research Institute (EPRI) EPRI–NP–3967, 1985	Common cause failure values and methods
A. Mosleh et al., Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR–1205, 1980	—
Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, EG&G, NUREG/CR–1205, 1980	—
Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants, EG&G, NUREG/CR–1363, 1980	—
Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants, EG&G, NUREG/CR–1740	—

Table 2-1. Some data sources in risk assessment (cont'd)

Source	Comment
U.S. Department of Energy, Hazard & Barrier Analysis Guidance Document, EH-33, Office of Operating Experience Analysis and Feedback, Washington, DC, 1996	Provides tools and methods for analysis of operating event at the U.S. Department of Defense (DOE) facilities
U.S. Department of Energy, Preparation Guide for U.S. DOE Nonreactor Nuclear Facility Safety Analysis Report, DOE-STD-3009-94	Specifically describes methods to be used for nonreactor nuclear facilities

The statistical treatment is useful if sample data (i.e., failures over trials or time) is available. However, different generic data sources such as in table 2-1 will often provide different failure probabilities and not the underlying sample data. A variety of methods have been developed for combining information from disparate generic data sources. The earliest use of a variety of data sources for RA was in the Reactor Safety Study (Nuclear Regulatory Commission, 1975). In this study, each data source was equally weighted, and the values were assumed to be lognormally distributed. The largest and smallest values among the data sources were assumed to define a 90-percent confidence interval. The median of such a distribution is easily found to be the geometric mean of the largest and smallest values.

Another approach was used in IEEE-STD-500 (Institute of Electrical and Electronic Engineers, 1984). In this study, much of the failure rate information was derived from expert judgement. The information included an upper limit, a lower limit, and a best estimate. In the earlier version of the standard, the listed values corresponded to the geometric means. For example, the upper limit displayed in the standard was the geometric mean of the experts upper limits. The lower limit and best estimate was similarly established. In the later version of the standard, a weighted maximum likelihood estimator was used for the best estimate, where the weighting factor of a particular source is inversely proportional to its variance.

Other methods, using the underlying assumption that either the underlying data or the failure rates are distributed lognormally among data sources, are used in Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) (Gertman et al., 1989) and the Savannah River generic data source (Blanton et al., 1993; Martz and Bryson, 1993).

2.3.3 Bayesian Methods

Often, uncertainty in the probability of failure is larger than that which can be inferred from the data only. This increased uncertainty arises because of such factors as differences in the component/equipment of interest from that in the data sources, partial applicability of the test situation to the actual operational situation, or differing environments, stresses, and operating conditions. These kinds of considerations are commonly accounted for, in RA, by introducing expert opinion or judgement to increase the uncertainty over that of a purely statistical analysis.

It is also the case that the uncertainty in a failure rate can be less than that which can be derived from a purely statistical analysis of the available data. This uncertainty arises when there is a large body of experience from similar hardware in similar environments but little experience with the specific piece of hardware. In this case judgement is used to reduce the otherwise overestimated uncertainty, owing to sparse data in the specific population being analyzed, by accounting for the experience of the similar or surrogate equipment.

The preferred method in RA for combining judgment with data is application of Bayes' Theorem. Bayes' theorem has been particularly useful in quantifying the frequency of rare events when there is insufficient sample data for a traditional statistical analysis.

Bayes' theorem provides a formal way to change an estimate of the probability of an event to take into account new data. Based on a prior estimate of the probability of an event using estimates of the probability of the data being measured occurring given that the probability of the event is a certain value. It is based on Eq. (2-1).

$$\mathbf{P(A_n / B) = \frac{P(A_n)*P(B / A_n)}{\sum_{m=1}^{N} P(A_m)*P(B / A_m)}} \tag{2-1}$$

where

P(A) — Prior estimate of the probability of A
P(B|A) — Probability of B assuming that A is a given value
N — Total number of possible values for A

This is best illustrated with an example. Suppose that an event is known to have a probability of occurrence of either 0.3 or 0.6 and estimated to have an 80-percent chance of having an annual probability of occurrence of 0.3 [$P(A_1)$] and a 20-percent chance of having an annual probability of occurrence of 0.6 [$P(A_2)$]. After 3 yr, the event has not occurred. If the annual probability of occurrence was 0.6, the probability of 3 yr of no events would be $(1-0.6)^3$, or 0.064 [$P(B|A_2)$]. If the annual probability of occurrence was 0.3, the probability of 3 yr of no events would be $(1-0.3)^3$, or 0.343 [$P(B|A_1)$]. Therefore, the new estimate of the annual probability of the event would be 0.3 with a 96-percent probability and 0.6 with a 4-percent probability.

There exists an extensive literature base that describes the use of Bayes' theorem in the following areas relevant to RA. Examples are

- General mathematical development (Martz and Waller, 1991)
- General background in applicability to RA (Apostolakis, 1978)
- Calculation of reliability from life testing (Bhattacharya, 1967)
- Combination of data and judgment to obtain failure rates (Apostolakis, 1981; Kaplan, 1986)
- Combining the opinion of experts when such opinion is expressed as probability distributions (Mosleh and Apostolakis, 1982)
- Calculating human error rates in RA (Apostolakis, 1986)
- Prediction of the number of future failures in a repairable system (Beiser and Rigdon, 1997)

- Decision making in the face of uncertainty (Berger, 1993)

Easy-to-use software is available to perform simple calculations using Bayes' theorem.

2.3.4 Obtaining Probabilities Using Judgment or Opinion

In addition to the use of judgment to augment data, another use of judgment is predicated on the reasonable notion that sometimes the data resides only within an expert's mind or the data can only be reasonably interpreted and used via the background and experience of an expert. The elicitation of knowledge, including but not limited to probabilities, is a large field of study and practice by itself. The literature contains books, reports, and papers from the fields of psychology, management science, decision theory, probability and statistics, and nuclear engineering (Cooke, 1991; Nuclear Regulatory Commission, 1987, 1993; Kahneman et al., 1982; Mosleh et al., 1987; Apostolakis, 1988). Of importance to RA is the construction of probability distributions that express the uncertainty in the probability of occurrence of an event, uncertainty in the severity of an event (e.g., earthquake severity, peak temperature, peak pressure), or uncertainty in the strength of a material (e.g., equipment or structural capacity). In some cases, there is even uncertainty in which event will occur (e.g., modeling uncertainty).

Although methods in the literature differ, a general procedure for a comprehensive knowledge elicitation session uses four-steps:

- Preparation by the risk analysts
- Knowledge elicitation session with the experts
- Scoring
- Combining judgments

Although a variety of specific techniques and analyses are used at each step, they can be described as follows.

Preparation includes identification of variables and parameters that are significant potential sources of uncertainty, development of questions to be asked of the experts, and identification of a moderator for the elicitation session. If elicitation is to be conducted to help develop a model as well as estimate parameter values, then the first and second steps are conducted iteratively.

Knowledge Elicitation, itself, may be performed in five steps:

- Motivate the experts (explain the reason for conducting the session)
- Structure the discussion (tell the expert exactly what is expected and in what format)
- Precondition the experts (to reveal biases and encourage truthful judgments)
- Encode the information (record what the expert says)
- Playback information to get expert confirmation

After the elicitation session, the risk analyst evaluates the answers to make sure that the responses truly reflected what was required of the model. The second and third steps may require iteration.

Scoring refers to the assignment of a numerical value to an expert's probability. Scoring is used as a way of rewarding and conditioning experts and the scores also may evolve into weights for combining probability assessments of experts. Development of a scoring method involves two questions (Cooke, 1991):

- Does the score reward those features that are desired in subjective probability assessments?
- Does a score introduce a reward structure that distorts or biases the assessment of probabilities?

Combining Judgments. Much effort in RA has been devoted to combining the judgment of multiple experts who are rendering an opinion on the same problem. For example, seismic risk analyses of nuclear power units relies heavily on the use of multiple experts to estimate the seismicity of a region and the strength of equipment and structures. Similarly, multiple experts are involved in the consequence assessment of nuclear power units with respect to the estimation of source terms and doses. Assignment of human error probabilities to unique scenarios obviously depends upon opinion and expertise. According to Cooke (Cooke, 1991), the range of models may be divided into three categories:

- Classical. This model constructs a weighted combination of expert probability assessments (IEEE–STD–500); Bernreuter et al., 1984; Cooke et al., 1988).

- Bayesian. These methods take the perspective of a decision maker and modify a prior distribution in accordance with expert distributions under various attitudes toward experts (Mosleh and Apostolakis, 1982, 1986; Winkler, 1968; Morris, 1974, 1977).

- Psychological Scaling. These models for estimating probability distributions originally derive from the estimation of relative intensities of psychological stimuli based on pair-wise comparison. They do not produce numerical estimates. Rather, they provide relative scales of the experts opinions with one or more degrees of freedom used for independent calibration (Embrey and Kirwan, 1983).

Only the first two methods have been applied in RA. These methods are still plagued by less than satisfactory techniques to assign weights to experts. Furthermore, the elicitation process itself has a number of pitfalls that influence the verisimilitude of the responses of experts (Kahneman et al., 1982; Mosleh et al., 1987).

2.3.5 Analytical Methods

These methods are used when events in a scenario reflect physical/chemical processes rather than statistical failure of components. They are extensively used for RA of launch vehicles, spacecraft, and radioisotope thermoelectric generators (Interagency Nuclear Safety Review Panel, 1997). Another common application is the calculation of equipment failure probability owing to seismic hazards.

The methods are largely ad-hoc, reflecting the basic physics of a situation. One common approach however, is to calculate failure probability using a double integral such in Eq. (2-2).

$$\mathbf{p(failure)} = \int_0^{\infty} \mathbf{P}_{\mathbf{stress}}(\varphi_1) \int_0^{\varphi 1} \mathbf{P}_{\mathbf{strength}}(\varphi : \varphi_1) \partial\varphi \partial\varphi_1 \tag{2-2}$$

This approach is useful for situations in which failure occurs owing to a generalized stress overcoming a generalized strength, when both stress and strength are uncertain quantities expressed as probability distributions. For example, this could be applied to calculations of overpressure failure probability of tanks, pipes, and vitrification systems. In the previous equation

p(failure) — probability of failure (a scalar quantity)

$P_{stress}(\varphi_1)$ — probability distribution over a generalized stress, φ_1

$P_{strength}(\varphi:\varphi_1|\_\varphi)\_$ — probability over generalized strength, φ, such that generalized stress is greater than or equal to generalized strength.

The input distribution in this equation and in other analytical approaches often involve, in part, expert judgment.

2.4 CONSEQUENCE ANALYSIS

Consequences, herein, are concerned with source terms and dose equivalents of chemical and radioactive material. The determination of health effects from intake or dose involves the complex areas of biology, physiology, toxicology, and biochemistry to name a few. These areas are beyond the scope of this report. In plain language,

- *Source term* is a released quantity of hazardous substance (radioactive or chemical or both), its location (or site), and its characteristics.

- *Dose (from chemical hazards)* is the mass of a substance given to an organism and in contact with the exchange boundary (e.g., skin, lungs, gastrointestinal tract) per unit weight of the organism per unit time of exposure (e.g., mg/kg-day). Synonymous terms used in RA are intake and administered dose.

- *Dose (from radioactive hazards)* is the absorbed energy in a given mass of tissue (Joules/kg or rads) multiplied by the appropriate weighting factors (International Commission on Radiological Protection, 1977a) (resulting in rem).

Other sections of this report have not been organized according to the nature of the hazard (i.e., chemical or radiological) because RA methods were essentially in consonance. However, a formal distinction is made in this section because of the disparate nature of RA objectives and methods used to evaluate chemical and radiological hazards.

2.4.1 Chemical Hazards

Consequences of chemical hazards focus on dose and health effects. Rather than development of sophisticated mathematical and physical/chemical process methods in RA, the emphasis has been on relatively simple methods that assist the making of conservative decisions with respect to remediation of toxic substances and corrective actions for accidental as well as operational releases. The primary motivation, guidance, and methods derive from the EPA Superfund efforts, the Clean Air Act Amendment of 1990 (Clean Air Act Amendment, 1990), the OSHA risk management code (Occupational Safety and Health Administration, 1991), and state risk management programs such as California's Risk Management and Prevention Program (California State, 1988). All of these programs use methods of calculating dose consistent with EPA practices and guidelines (U.S. Environmental Protection Agency, 1989a).

2.4.1.1 Definition of Risk

Risk is defined in terms of carcinogenic and noncarcinogenic effects. For carcinogens, the linear low-dose model is assumed to be valid for Risk < .01, such that

$$\textbf{Risk} = \textbf{CDI} \times \textbf{SF} \tag{2-3}$$

where, Risk is a probability of an individual developing cancer, is a chronic daily intake (CDI) averaged over 70 yr (mg/kg-day); and SF is a slope factor of the cancer-to-dose relationship for that chemical in units of inverse intake. For higher levels of risk, an exponential equation, analogous to the exponential reliability model, is used:

$$\textbf{Risk} = \textbf{1} - \textbf{exp}(-\textbf{CDI} \times \textbf{SF}) \tag{2-4}$$

The basic equation for total cancer risk associated with all substances exposing an organism is the simple sum of the individual substance risk as given above for all pathways that can affect the same individual.

For noncarcinogens, a numerical measure called a Hazard Quotient (HQ), which is not a probability, is used:

$$\textbf{HQ} = \frac{\textbf{Intake}}{\boldsymbol{RfD}} \tag{2-5}$$

19/36

where, Intake is estimated dose and *RfD* is a reference dose of the substance below which no adverse health effects are expected to occur. The basic equation for total noncarcinogenic risk associated with all substances exposing an organism is the simple sum of the individual substance HQ quantities for all pathways that can affect the same individual. Acceptability of the chemical hazard occurs for total HQ <1.

Cancer risk is not mixed with HQ. The conditional probability of the occurrence of a pathway or the occurrence of release of a substance is not included in either summation.

The method for calculation of CDI and Intake are discussed below and *RfD* is provided by an EPA database (U.S. Environmental Protection Agency, 1993b). The specific numerical values for these equations depend on things like the chemical, pathway, length of exposure (e.g., chronic, subchronic, short-term), medium of exposure[5] (e.g., food, soil, water, air), and composition of the chemical (e.g., particulate, vapor).

An intermediate quantity, such as airborne concentration (in mg/liter) is often used in lieu of risk (Occupational Safety and Health Administration, 1991; National Institute of Occupational Safety and Health of the Center for Disease Control, 1997). Permissible levels of air concentrations are derived from an acceptable level of risk (10^{-6}). This allows a convenient method of control by a regulatory agency.

Thus, assessment of risk for chemicals, as defined above, is quantitative in so far as risk is expressed as a number. However, chemical risk assessment is not a consistent mathematical approach because the non-carcinogenic risk is simply a relative index, not a physical or probabilistic quantity. Therefore, full quantification of uncertainties is not done. Furthermore, the definition of risk does not include the frequency of an accident-initiating event or the frequency of a scenario. It is acceptable, however, to reduce the cancer risk number by multiplying by the occurrence frequency of a source term.

Indeed, source terms are usually measured or inferred from measurement. It is rare that they are calculated without measurement. If source terms are to be calculated in an RA, a bounding estimate is usually performed. More sophisticated techniques such as used in the nuclear industry are generally not used for chemical risk assessments. Methods of dose or intake calculations may be grouped into two categories, neither of which are mutually exclusive because both are consistent with EPA practices and guidelines: EPA Risk Assessment Guidance (U.S. Environmental Protection Agency, 1989a) and Risk-Based Corrective Action (American Society for Testing Materials, 1995).

2.4.1.2 Risk Assessment Guidance

This is the basic EPA guidance for dose calculations that is currently used for essentially all hazardous waste sites or sites containing hazardous chemicals (petrochemical facilities). This general procedure includes three steps as summarized below (U.S. Environmental Protection Agency, 1986, 1988a,b, 1989a).

[5] Exposure is defined as contact of an organism with chemicals of concern at the exchange boundary (e.g., skin, lungs) and available for absorption.

Step 1. Characterization of Exposure Setting. By means of site survey and other area resources, this step characterizes the physical characteristics of the site and the surrounding population. General physical characteristics include climate, meteorology, vegetation, soil type, and hydrology. Population characteristics include location relative to site sources, land use (i.e., residential, agricultural, commercial, or recreational), special sensitivities, and activity patterns. Both current and future characterizations are necessary.

Step 2. Identification of Exposure Pathways. This step is a qualitative identification of exposure pathways starting with the source of hazardous material and ending with the population identified in Step 1. Each exposure pathway describes a unique mechanism for exposing the population. Exposure is determined for each chemical and each pathway from source site to population. Characteristics included in an exposure pathway are, for example, source term, release mechanism, environmental fate, routes of exposure (e.g., inhalation, ingestion), and specific points of contact of the chemical with the population. With respect to tank leakage and remediation operations, a particular concern is that the exposure point is the same as the source point.

Step 3. Quantify Exposure. The guiding principle behind quantification of exposure to obtain dose is to calculate a "reasonable maximum exposure." A minimum of quantitative analysis is performed to achieve the proper balance of cost-effective remediation guided by this principle. Simple, conservative equations have been developed that are to be used with a great deal of expert judgment. In this method, the term exposure is essentially synonymous with intake and dose. A generic equation for calculation of chemical intake has been developed (U.S. Environmental Protection Agency, 1989a) and is as follows:

$$\mathbf{I = C\ \frac{CR * EFD}{BW * AT}} \tag{2-6}$$

where

I — intake; the amount of chemical at the exchange boundary (mg/kg of body weight/day)

C — chemical concentration at the exchange boundary; the 95-percent confidence limit of the average concentration over the exposure period (mg/liter)

CR — contact rate; the amount of contaminated medium that is exposed to the body per unit time or per event (liters/day of water or liters/accident)

EFD — exposure frequency and duration which is the product of exposure frequency (days/yr), and exposure duration (yr)

BW — body weight; the average body weight of the population over the exposure period

AT — average time; period over which the exposure is averaged (days).

These quantities are called "exposure factors" that are pathway and site specific. However, guidance is provided for the calculation of all factors, and many factors are prescribed by convention depending on the population category and pathway (U.S. Environmental Protection Agency, 1989b; Fields, 1991). When a quantity such as airborne concentration is used in lieu of Intake, then essentially I = C in the above equation.

As a first screening estimate, the quantity C is taken as the source term without any fate modifications. Typically, the source term is a measured quantity. The determination of exposure at the exchange boundary is estimated, whenever possible, from environmental monitoring of data. Chemical transport and environmental fate models are used if this is not possible, and a more accurate characterization is needed. However, no such models are acceptable for remediation or corrective action unless calibrated against specifically applicable data for the site and chemicals. A wide variety of models are available (U.S. Environmental Protection Agency, 1988b, 1989c; Whelan et al., 1992).

Of particular interest for RA of privatized vitrification operations at Hanford would be Whelan et al. (1992) who refers to a computational computer code called Multimedia Environmental Pollutant Assessment System (MEPAS). This code was developed at Pacific Northwest Laboratory, has been calibrated against Hanford site data, and is used for DOE Hanford site remediation efforts. Risk values, in accordance with EPA guidance and models, are computed for chemical and radioactive carcinogens, and HQs are computed for non-carcinogens. The model is physics-based and uses standard transport (e.g., straight-line, Gaussian model using wind speed and atmospheric stability category) and exposure computations, given a source term. The model includes submodels for groundwater, surface water, and overland and atmospheric pathways. It includes exposure models for inhalation, ingestion, external dose, and dermal contact of an organism. As an example, the atmospheric pathway model includes dilution and transport, washout, and deposition. Resuspension and probabilistic assessment of wind direction do not appear to be included.

Uncertainties in the entire three-step process are recognized as being very large and qualitatively characterized. A procedure for the detailed qualitative characterization of uncertainties is provided (U.S. Environmental Protection Agency, 1989a). Uncertainty information is considered an important input to the remediation or corrective action decision making process. Quantitative methods of parameter uncertainties in the above intake formula, and sometimes for the carcinogenic risk formulation, are sometimes used. These methods would include moment methods, and sampling methods (Monte Carlo) will be described in section 2.5 of this report. There are no uncertainty analysis methods unique to the chemical industry.

2.4.1.3 Risk-Based Corrective Action

The recently updated Standard Guide for Risk-Based Corrective Action (RBCA) Applied at Petroleum Release Sites (American Society for Testing Materials, 1995) provides a three-tier approach for assessment and corrective action. The first tier assesses dose to populations by assuming that the population is at the source and by using generic site exposure factors. The second tier provides simple formulas that take credit for separation between source and target populations and includes site specific exposure factors. The third tier may include sophisticated physical, chemical, dispersion, transport, and fate modeling. All equations are geared toward leading to a level of individual lifetime cancer risk (usually about 10^{-6}) among a standard population characterized by standard exposure factors (Smucker, 1996). For example, if a residential population is currently, or is expected to be, near the site, a certain fraction of adults, children, and sensitive people with specific breathing and ingestion rates is used to calculate dose. All equations in Tier 1 and 2 are consistent with EPA guidelines and practices, as described in section 2.4.1.2, including the use of specific EPA recommended exposure factors as inputs to the equations.

The Tier 1 and Tier 2 calculations in the RBCA approach produce screening levels of acceptable source concentrations. The Tier 1 assumptions clearly produce the lowest acceptable on-site concentrations because of the assumption that receptors are at the source, and the risk must remain at the 10^{-6} level over a lifetime. The measured on-site concentrations are compared against the acceptable screening levels. Remediation is not necessary if measured values are lower than the screening levels. If this is not the case, then either the next tier of calculations are attempted, the site is permanently remediated, or interim remediation steps are taken.

Tier 3 provides for application of the more sophisticated environmental transport and fate models to demonstrate that concentrations at the site are acceptably low. Again, remediation efforts must be taken for any chemical, path, and population that exceeds the implied risk level.

2.4.2 Radiological Hazards

Consequences of radiological hazards focus on source terms, dose, and health effects of radioactivity exposure to a population. With the combined efforts of the nuclear industry, the NRC, the DOE, and the national laboratories, an enormous amount of literature has accumulated about the physical/chemical/biological processes associated with consequences of terrestrial and space-bound nuclear power sources.

2.4.2.1 Definition of Risk

Methods to calculate source terms are generally deterministic in nuclear RA, with a significant exception in space nuclear power RA. Some methods probabilistically account for weather variability when computing doses. By combining the frequency of a scenario with the consequence associated with that scenario, a *de facto* probabilistic definition of risk is used: frequency of dose. Two kinds of dose are typically of interest: population or collective dose (e.g., measured in person-rad for dose and person-rem for dose equivalent) and maximum individual dose in either rad or rem. Sometimes airborne concentration (e.g., measured in curies or grams per cubic meter) is used as the metric of interest instead of rem or rad.

2.4.2.2 Source Terms

Both the space and terrestrial nuclear RA practitioners have developed and relied on highly complex physical/chemical process models for the prediction of source terms (Nuclear Regulatory Commission, 1983; Baybutt, 1986; Lockheed-Martin Corporation, 1997a,b; Interagency Nuclear Safety Review Panel, 1997). Small-scale experiments or partially applicable tests have allowed a moderate measure of calibration or validation of these models. Large uncertainties remain.

For space nuclear power applications, estimation of source terms includes (i) accident scenarios involving launch vehicles and the space vehicles that carry the power source; (ii) the progression of accident-induced insults upon the power source (explosion, thermal, impact, shrapnel); (iii) the resistance of the power source to these insults; (iv) the amount of radioactive material released as a result of the insults and the location of release; (v) a characterization of the state, physical/chemical properties, and isotopic composition of the released material; and (vi) the modification or fate of released material owing to severe environmental effects such as explosion fireballs or very hot thermal environments. The general concept behind determining the sources terms in space nuclear power applications (Lockheed-Martin Corporation, 1997b; Interagency Nuclear Safety Review Panel, 1997) is to obtain statistics on the occurrence of key events during an accident by simulating the accident a large number of times (or trials). Detailed physical and chemical modeling of all relevant accident phenomena is done while input parameters are allowed to have uncertainty. Both Monte Carlo and Latin Hypercube sampling techniques are used. If a simulation trial results in a source term (and many do not), it is characterized by its relevant parameters such as amount, energy, state, particle sizes, and location. The output of a simulation results in probability distributions over the source term characteristics such as mass, particle size, and location. Isotopic composition of fuel is determined by measurement to obtain initial conditions during production. ORIGEN2 (Bell, 1973; Croff, 1980) is then used to predict isotopic composition at the launch date (Lockheed-Martin Corporation, 1997b).

For terrestrial nuclear units, source term estimation has attempted to calculate the progression of radioactive material originally in the nuclear reactor core through meltdown, release from the reactor vessel, and subsequent release from containment boundaries or containment bypass (Nuclear Regulatory Commission, 1975; Fauske and Associates, Inc., 1983; Tanabe et al., 1982; Sandia National Laboratory, 1985; American Nuclear Society, 1985, 1986; Madni, 1991). These deterministic models often rely on the solution of coupled energy and mass transfer equations. Source terms are characterized in a manner similar to those described for space nuclear applications but are deterministic. Isotope composition of fuel is generally calculated using codes such as ORIGEN, ORIGEN2 and HARMONY (Breen et al., 1965); which have been in use for decades. Calculational methods are embodied in large computer codes that are quite specifically oriented to the terrestrial or space power units.

2.4.2.3 Transport/Dispersion and Dose

The pathways of interest to health effects of people are atmospheric (i.e., inhalation, cloud shine, and ground shine) and ground (i.e., ingestion from foods that have been directly contaminated and resuspension). Uptake of radionuclides from soil to vegetables is significant for land contamination and cleanup considerations. Uptake by fish has not been shown to be significant in comparison to the others for most applications (Interagency Nuclear Safety Review Panel, 1990). Methods for transport of released radioactive material from both terrestrial and space nuclear units have emphasized atmospheric transport because the highest probability and most severe release mechanisms produce atmospheric releases. The methods include transport, dispersion, and the associated dose to local populations within the same computer codes. Three types of transport/dispersion and dose methodologies will be described herein by examples: (i) simple pathway models with straight line, Gaussian air transport without weather variability; (ii) air transport models with weather variability; and (iii) sophisticated air transport and deposition models using regional wind trajectory data.

Essentially all the codes estimate the air concentrations (e.g., curies/liter or mg/liter). Dose may be calculated using standard dose conversion factors (International Commission on Radiological Protection, 1977a,b, 1979, 1991, 1993, 1995; U.S. Department of Energy, 1988).

Examples of Simple Pathway Models

Some of the simple models track air pathways only with subsequent deposition on the ground and uptake into food. Others track multiple release pathways such as air, water, and ground radiological contamination. All such models use a straight line, Gaussian air transport and dispersion model with doses calculated at a single radial distance from the source or multiple distances from the source to an input population distribution. A drawback of any Gaussian model is that its accuracy greatly diminishes with distance away from the original plume. Results are presented in terms of point estimate air concentrations. Intake (or dose) is obtained using International Commission on Radiological Protection (ICRP) or NRC recommended conversion factors. Two examples, CAP88-PC and GENII, are described herein.

CAP88-PC (U.S. Environmental Protection Agency, 1992) is used for dose assessments surrounding facilities that release airborne radionuclides. CAP88-PC uses a modified Gaussian plume equation to estimate the average dispersion of radionuclides released from an elevated point or area plume source to the air. Plume rise can be either buoyancy or momentum driven. Population doses are estimated using a circular grid and population density input around the facility. The program computes radionuclide concentrations in air, rates of deposition on ground surfaces, concentrations in food, and intake rates to people from ingestion of food produced in the assessment area. Estimates of the radionuclide concentrations in human uptake of produce, leafy vegetables, milk, and meat are made by coupling the output of the atmospheric transport model with the NRC Regulatory Guide 1.109 (Nuclear Regulatory Commission, 1977) terrestrial food chain models. Dose and risk are estimated by an Intake equation similar to that presented in section 2.4.1. The effective dose equivalent is calculated using the Publication 26 factors (International Commission on Radiological Protection, 1977b).

GENII (Napier et al., 1988) may be used for a wide range of radionuclide release mechanisms. The code can calculate doses from acute and chronic releases into the atmosphere, surface water, groundwater, and soil contamination. Air transport and dispersion is modeled with a straight-line Gaussian formulation to estimate air and ground deposition concentrations on a grid for 16 directions and up to 10 distances. Radiation doses to either individuals or populations from a wide variety of potential exposure scenarios are calculated using ICRP Publication 26 and 30 (International Commission on Radiological Protection, 1979).

Examples of Air Transport Models with Weather Variability

The Air Transport model with the weather variability method was developed for nuclear reactor radiological consequence assessment and implemented in the CRAC series of codes. A significant difference between the CRAC series of codes and other consequence methods is that output is in terms of complementary cumulative distribution functions (CCDFs)[6] for dose and health effects. In these codes, the CCDFs reflect the variation of weather and/or wind conditions as a function of time and distance from the source term point of release. The most popular of such codes in terrestrial nuclear power plant RA applications are CRAC, CRAC2 and CRACIT. A synopsis of the three CRAC codes, which were developed in the 1970s, is provided below.

CRAC (Nuclear Regulatory Commission, 1975) was the first integrated consequence code for nuclear reactor risk analysis. It used a Gaussian atmospheric dispersion model. The Gaussian model requires dispersion coefficients. CRAC chose a simplified approach for this based on Pasquill-Gifford atmospheric stability categories (Martin and Tikvaart, 1968). CRAC included models for rise of a plume containing a concentration of radioactive material, dry and wet deposition of the material, and radioactive decay. It tracked the passage of the plume as it transported and dispersed downwind according to local weather data.

A significant achievement of the code was that it accounts for changes in weather (but not wind direction or wind speed) as a function of time and distance by allowing hourly changes in stability category. The principle effect of these changes is to change how the plume grows as a function of time. CRAC is probabilistic in that it selects (by a random number generator) source term release times throughout a year and tracks the specific dispersion, plume rise, and transport according to the appropriate weather data. CRAC calculated dose and health effects by overlaying a population grid on the air concentration (e.g., curies/m3) and deposited ground concentration (e.g., curies/m^2). Doses owing to direct inhalation, resuspension inhalation, ingestion, and external radiation from cloudshine and groundshine were included.

CRAC2 (Ritchie et al., 1981) was a revision of CRAC, the most significant of which is a different weather sampling model. Both CRAC and CRAC2 use an entire year of data in one-hour increments from a single weather station. CRAC2 groups the 8,760 samples into 29 bins. All data in each bin has similar weather characteristics. The code then samples from each bin. The probability of each bin is determined from the number of data samples within it. The code samples from all 29 bins. This process somewhat alleviates the problem of inadequate sampling that plagued CRAC but introduces another uncertainty with respect to the verisimilitude of the binning criteria.

CRACIT (Woodard and Potter, 1979) was the most ambitious revision of the original CRAC code. The code employs a method that requires input of digitized terrain data, which allows calculation of the space- and time-dependent wind field in three dimensions. Therefore, it is capable of accounting for changes in weather, wind speed, and wind direction over time and space using multiple sampling stations of weather data. This revision is a significant improvement over previous CRAC versions. It solves the set of transport and diffusion equations without the Gaussian plume model approximation up to a distance of 14.5 km from the source after which the segmented Gaussian plume model is used.

[6] This is the probability (or frequency) denoted on the y-axis of equaling or exceeding the number of health effects or the dose value on the x-axis. Therefore, it is sometimes called a Probability of Exceedance curve. See section 2.5 for further discussion.

An Example of a Sophisticated Air Transport and Deposition Model

An example of the evolution of the modeling of transport and dispersion since the 1970s and 1980s is HYsplit4. This is the latest version of the HY-split series, which has been developed at National Oceanic Atmospheric Administration (NOAA) Air Resources Laboratory over the last 15 yr. The development has been both a means toward understanding the global spread of pollutants from point sources and a way of predicting the trajectories of abnormal pollutant releases (both chemical and nuclear).

HYsplit4 (Draxler and Hess, 1997) is a hybrid single-particle Lagrangian integrated trajectory model that computes simple air parcel trajectories and complex dispersion and deposition simulations. It uses multiple nested meteorological data for accurate altitude variation of meteorology. This code allows transport and dispersion of a plume of particles or a group of particles influenced by temporal and spatial (three-dimensional) varying wind trajectories from multiple-station data.

This Lagrangian model can compute air concentrations through either of two assumptions. In a puff model, the source is simulated by releasing pollutant puffs at regular intervals over the duration of the release. Each puff contains the appropriate fraction of the pollutant mass. The puff is advected according to the trajectory of its center position, while the size of the puff (both horizontally and vertically) expands in time to account for the dispersive nature of a turbulent atmosphere. In a Lagrangian particle model, the source can be simulated by releasing many particles over the duration of the release.

In addition to the advective motion of each particle, a random component to the motion is added at each step according to the atmospheric turbulence at that time. In this way, a cluster of particles released at the same point will expand in space and time simulating the dispersive nature of the atmosphere. A hybrid approach is incorporated into this code in which the calculation uses particle dispersion in the vertical direction and puff dispersion in the horizontal. The dispersion rate is calculated from the vertical diffusivity profile, wind shear, and horizontal deformation of the wind field. Both the puff and particle dispersion equations are formulated in terms of the turbulent velocity components. These velocity components are a function of the turbulent diffusivities. Stability and mixing coefficients (vertical and horizontal) are computed from the meteorological data using first principles and vertical heat fluxes and momentum. There is no need to define stability categories. The dispersion of a pollutant is calculated by assuming either a normal or uniform horizontal distribution within a puff or from the dispersal of a fixed number of particles.

Using the latest data and models, Hysplit4 includes wet and dry deposition (Hicks, 1986), radioactive decay, resuspension (Interagency Nuclear Safety Review Panel, 1993), and multiple pollutant species.

In contrast with simple Gaussian codes, this code is capable of accurate tracking of released particles over an entire region (hundreds to thousands of miles). The code has been extensively tested and validated using tracer experiments and more complex pollutants such as nitrates, sulfates and radionuclides. However, it is not capable of probabilistic sampling of alternative times of source term release, i.e., each release must be treated by another run of the code. Hysplit4 does not provide CCDFs and its output is a grid in space and time of air concentrations and ground deposition.

2.5 UNCERTAINTY ANALYSIS

This section is not a discussion of uncertainties in chemical, nuclear, and aerospace RA. Some of these have been alluded to in previous sections. The establishment of uncertainty or confidence limits using statistical and Bayesian methods has been described in section 2.3. This section surveys the three most used categories of methods for mathematical propagation of uncertainties throughout an RA. These areas are moment methods, sampling methods, and discrete probability methods. Among sampling methods, only Monte Carlo and Latin Hypercube will be discussed because these are the most widely used techniques. This is preceded by a discussion of the two major types of uncertainties and the illustrative presentation of uncertain results in the form of CCDFs. The National Council on Radiation Protection and Measurement recently published a monograph that provides overview guidance for both chemical and radiological contamination on (i) when and when not to perform an uncertainty analysis, (ii) methods for uncertainty analysis, and (iii) elicitation of expert judgment during an uncertainty analysis (National Council on Radiation Protection and Measurement, 1996).

2.5.1 Aleatory and Epistemic Uncertainties

Two broad categories of uncertainties may be defined as aleatory uncertainty (having to do with chance) and epistemic uncertainty (having to do with knowledge) (Apostolakis, 1993). A recent issue of Reliability Engineering and System Safety was devoted to this topic (Helton and Burmaster, 1996). A simple example will illustrate the distinction between these types of uncertainties. Consider a fair coin (one that has equal probabilities of heads and tails) and a fair flipping experiment where the number of heads and tails are recorded. Given the number of fair flips, the probability of the occurrence of any number of heads can be calculated. Aleatory uncertainty arises because it has only to do with chance. The aleatory uncertainty cannot be reduced by increasing the number of coin flips. That is, the outcome of the next flip cannot be predicted with better than 50-percent accuracy over a large number of flips. Other examples of aleatory uncertainty would include which card will be drawn from a random deck, or the amount of time between decays from a sample of radioactive atoms.

Now consider the possibility that the coin is biased in that one face may be more probable than the other. The outcome of many coin flips is recorded again. This case contains both aleatory and epistemic uncertainties. The epistemic uncertainty arises because it is not known *a priori* whether or not the coin is biased. After a limited number of flips, a result that is not 50-percent heads and 50-percent tails may be because of an insufficient number of flips or due to the bias. Continuing to flip the coin will reduce the epistemic (knowledge) uncertainty because if the outcome continues to be different from 50-percent heads and 50-percent tails after a very great number of trials, there is a very strong inference that the coin is biased. Other examples of epistemic uncertainty would include the half-life of an unknown radioactive sample or the probability of an earthquake of a given magnitude occurring at a site.

In general, aleatory uncertainty refers to the inherent variation of a physical process over many similar trials or occurrences. An example variable that exhibits such uncertainty is meteorological conditions. In general, epistemic uncertainty refers to both the state-of-knowledge about the physical processes and the ability to measure and model them. Obtaining additional information, by performing additional experiments and analysis, can reduce this uncertainty. For example, the failure rate of a particular component on a launch vehicle could be accurately known if a sufficient number of trials is performed which demands the operation of the component. Since we do not have these experiments, do not exist uncertainty in the failure rate must be expressed by using a probability distribution. Taking this concept a step further, modeling of meteorological conditions is subject to epistemic uncertainty because the knowledge and technology is not sufficient to precisely model its aleatory uncertainty.

Both forms of uncertainty are described using probability distributions in RA. Uncertainties in the individual events and phenomena modeled in an RA are propagated through the model (by methods discussed below) to obtain resultant distributions. In other words, generally, an output probability distribution may be thought of as a function of its input distributions. A common form of presentation of the resultant distributions (as well as some of the input distributions) is a family of CCDFs. Figure 2-3 shows an example CCDF family (Interagency Nuclear Safety Review Panel, 1990).

The CCDFs display the number of times per mission (a frequency) along the y-axis of equaling or exceeding a number of fatal cancers (a consequence) along the x-axis. They represent the sum of the CCDFs of individual scenarios that contribute to the total risk.

Each curve in the family of CCDFs conveys a level of confidence that the true frequency/consequence relationship is on or below that curve. The curve marked “95-percent Confidence Risk Curve” shows that those who have constructed the curve are 95-percent confident that the true frequency/consequence relationship falls on or below the curve. Similarly, the curve labeled “5-percent Confidence Risk Curve” indicates only a 5-percent confidence that the true risk curve can fall on or below it and a 95-percent confidence that the true risk curve must be above it. The 5-percentile and 95-percentile curves are standard ways to represent a lower bound and an upper bound in a risk analysis. The “Median” curve represents that the true answer is as likely above as below it. Thus, this family of risk curves represents epistemic uncertainty (e.g., representing lack of knowledge about the relevant phenomena) about aleatory uncertainty.

From an orthogonal perspective, the probability of occurrence of each x-axis value (grams or cancer fatalities) is uncertain. This uncertainty is represented by a probability distribution on the frequency (or conditional probability) of occurrence of that particular x-axis value. This distribution has, of course, a mean value that is the first moment of the distribution. Therefore, the risk curve labeled “Mean” is the locus of mean values of the distributions all x-axis values. It shows that the mean frequency of equaling or exceeding four fatal cancers is about one in a million per mission. A simplified, but not always accurate, way to distinguish between aleatory and epistemic uncertainties while viewing a family of CCDFs resulting from an RA, is that aleatory uncertainty is primarily responsible for the variation of results along the x-axis, and epistemic uncertainty is primarily responsible for the variation of results along the y-axis.

2.5.2 Moment Methods

The first and second moments of a probability density function (i.e., probability distribution) are the mean and variance. In many cases, all that is needed about the uncertainties are these two quantities. In fact, it has been shown that, for RA performed, to make a decision about safety of the very next mission, facility, or event (i.e., the next future occasion), the mean value of the underlying uncertainty is all that is needed

24/36

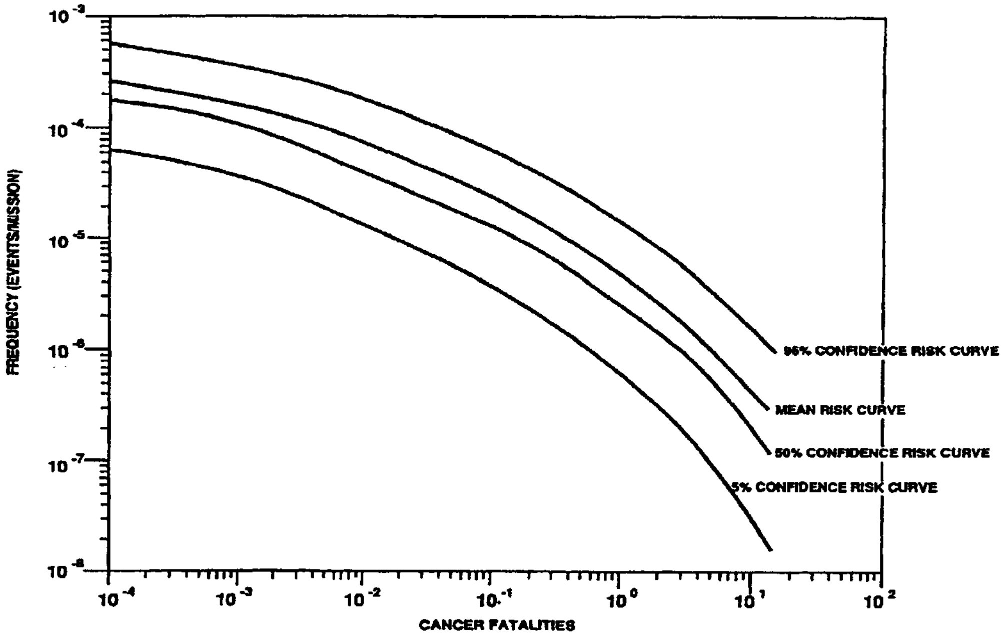


Figure 2-3. Example family of complementary cumulative distribution functions

(Howard, 1988). Howard also showed that assessing the probability of occurrence on n future occasions requires assessing, in general, the first n moments of the underlying distribution.

Moment methods calculate the resultant moments of a distribution from the corresponding moments of the input event distributions. For simple cases of probabilistic addition and multiplication, the "Method of Moments" (Murchland and Weber, 1972) may be used. This method is based on the mathematical properties of the mean and variance of a function whose operation is addition or multiplication of its variables. The variables need not be independent. For more complex functions, the "Taylor Series Expansion Method" (Shooman, 1990) provides an approximate solution for a resultant mean and variance as well as an estimate of the approximation error. This method is based on approximating the resultant distribution as a Taylor series of the input variables.

2.5.3 Discrete Probability Methods

This method is useful for distributions that are not defined over a set of continuous points (a histogram or binomial). A discrete probability distribution is a set of ordered pairs of numbers such that one number in the pair is a variable value, and the other number in the pair is the probability of that value. The sum of the probabilities of the values in a distribution equals one (Nuclear Regulatory Commission, 1983). Any two such discrete distributions may be combined using essentially any arithmetic operation by setting up a matrix. This method becomes very difficult to execute if values of the input variables are correlated or depend on each other.

2.5.4 Sampling Methods

Sampling methods are the most widely used in risk and uncertainty analysis because of their ability to be used with essentially any set of probability distributions combined with essentially any function. They also have the ability to handle correlated variables. In the last decade, inexpensive commercial and government software that allows relatively fast running times for complex risk problems has become available.

Generally, an output probability distribution may be thought of as a function of its input distributions. Sampling is a process by which values are randomly drawn from probability distributions, and the sampled values are operated upon in accordance with the function. Many random draws occur, and each pass through all of the input distributions is called a trial. (Sometimes a trial is also called a realization or observation.) The result of a set of trials is called a simulation. The term simulation arises because the process is the mathematical equivalent to or simulation of actual experiments or trials of the events that are represented by the input probability distributions. For example, intake of a chemical is represented by a formula shown in section 2.4.1.2. If each of the variables on the right-hand side of the equation is uncertain then the left-hand side of the equation (*I*) is also uncertain. In theory, a series of many experiments or accidents could be run. In each of the accidents, a different source term is generated with different concentrations, exposure frequencies, and contact rates. The release would be tracked and intake measured for each experiment. At the end of the series of experiments, the *I* would be well represented by a probability distribution. In practice, because running such experiments could be expensive (or even dangerous), simulation can be attractive. If the probability distributions for the quantities on the right-hand side of the equation can be estimated, then the resultant intake can be simulated by a sampling method.

The key to a successful sampling method is the greatest accuracy of the resultant distribution using the fewest number of trials. By far, the Monte Carlo and the Latin Hypercube techniques have received the most developmental attention and have the widest applicability. Both methods have been applied in nuclear waste applications.

2.5.4.1 Monte Carlo

Monte Carlo simulation (Orvis and Frank, 1981; Rubinstein, 1981) relies on the generation of pseudorandom numbers by a computer. The entire range of the distribution is open to sampling at each trial. Thus, Monte Carlo samples tend to cluster at the part of the distribution with the highest probabilities. For enough trials, the entire input distribution can be well represented. In many cases, however, limiting the number of trials because of time, money, or computer memory constraints can lead to unacceptable error in the output quantities of interest (mean, variance, 95-percentile). Fishman (1996) discusses two forms of error reduction techniques to compensate for this problem. The first form alters the method for generating the samples and leads to adjustments in the estimation of the output quantities of interest. Some of these techniques are called importance sampling, stratified sampling, and correlated sampling. The second form, such as control variate methods, collects data during the simulation that can be used to obtain a better estimate of the quantity of interest. None of these alternative methods are commonly used in RA.

2.5.4.2 Latin Hypercube

Latin Hypercube simulation, a form of stratified sampling, limits the sampling technique such that the clustering of trials cannot occur (Iman and Shortencarrier, 1984; Iman and Helton, 1985). The input probability distributions are stratified or divided into equal probability segments. During each trial (or observation, as it is called for this method), a random sample is taken from each segment. This technique gives better representation of the low probability end or "tails" of probability distributions with fewer trials than the normal (unaltered) Monte Carlo technique.

2.6 OTHER TOPICS

2.6.1 External Events

Both the NRC risk assessments (Nuclear Regulatory Commission, 1991a,b) and California chemical facility risk management programs (Los Angeles County Fire Department, 1991) request a review of the hazards associated with external events that are commonly considered earthquakes, floods, fires, and high winds. However, the national mandated chemical risk programs (Occupational Safety and Health Administration, 1991) do not mention external events, and the chemical risk assessment guidance documents (American Institute of Chemical Engineers, 1992) do not provide explicit guidance on their assessment.[7]

The methodology used is quantitative, which was achievable because the last two and a half decades has seen a substantial methods development effort aimed at the prediction of damage in nuclear power units caused by fires, floods, earthquakes, and winds. In fact, extreme instances of such events, called Design Basis Events, must be considered in the design of nuclear power plants, adding considerable robustness over and above what is required by the Uniform Building Code.

In general, the assessment of risk owing to external events is divided into three major steps. First, the frequency of the occurrence of an external event, at the site of interest, is estimated with uncertainties as a function of the severity of the event. For example, the exceedance frequency of winds as a function of velocity would be estimated. This step called "hazard analysis" in the language used in nuclear external event analysis. Second, the conditional probability of equipment or structural damage, at each level of severity, is estimated. For example, the probability of an earthquake causing the tear or rupture of a pipe is estimated as a function of ground acceleration. This probability is often called "fragility analysis" or "capacity analysis" in the language used in nuclear external event analysis. Because of containment structures, structural redundancy, equipment redundancy, and specially designed safety systems, a third step is needed for nuclear power plant RAs. In this step, the effect on the plant's ability to compensate for damage caused by the external event is assessed. This step may include the assessment of the frequency of damage to the nuclear core and release of radioactivity as a result of the spectrum of severity of the external event. This step is called "systems analysis" in the language of nuclear external event analysis.

[7] An exception to this is in California (California State, 1988) where external events are somehow to be added into a HAZOP study.

Thus, methods derived from the nuclear industry are inherently probabilistic because they are focused on obtaining the frequency of severe damage to the plant and the subsequent possibility of releasing radioactive material. Methods regarding hazard analysis are general so they could be used at any site. Development of accident scenarios and assessment of consequences (i.e., systems analysis) would include methods that are applicable to privatization operations risk analysis. These would use the techniques outlined in sections 2.1 through 2.5 of this report. Applicability of methods and data used in nuclear plant fragility analysis to TWRS risk analysis is not as clear because of the many assumptions and nuclear equipment specific *ad hoc* techniques used for this.

There is not a standard method of analysis for RA of external events. Therefore, the following discussion will be limited to presentation of the literature that describes methods. Reasonable overviews of methods of external events for nuclear units are found in the PRA Procedures Guides (Nuclear Regulatory Commission, 1983) and other documents (Nuclear Regulatory Commission, 1989a; Budnitz et al., 1985). In addition, the PRA Procedures Guide provides a checklist and procedure to determine which external events (if any) should be included in an RA.

2.6.1.1 Earthquakes

Several studies have described methods used and have characterized the frequency versus severity of earthquakes at nuclear power plant sites in the United States (Nuclear Regulatory Commission, 1988, 1989b, 1994b; Electric Power Research Institute, 1989). The principle damaging effects of an earthquake is to accelerate the ground. Methods to estimate ground motion and the structural response to ground motion have been developed (Newmark and Hall, 1978; Kennedy et al., 1984a; Electric Power Research Institute, 1991a). Liquifaction may be a concern associated with ground motion in certain types of soils (Seed, 1983, 1984). There are several schools of methods used to determine the seismic fragility or capacity of equipment and structures at nuclear units (Merz, 1991b; Kennedy and Ravinda, 1984; Kennedy, 1985; Nuclear Regulatory Commission, 1986, 1987, 1990). Special methods have been developed to analyze the seismic fragility of relays (Merz, 1991a).

2.6.1.2 Fires

Fire risk analyses of nuclear and chemical facilities are similar because both attempt to determine the likelihood of fires, the severity of fire, the equipment damage owing to a fire, and the ultimate consequences of a fire (Electric Power Research Institute, 1993; Technica, Ltd., 1985; Kazarians et al., 1985; Society of Fire Protection Engineers, 1995). Both account for the possibility of suppression systems working or malfunctioning (Hall, 1990). Fire incidence data has been collected for nuclear units, and generic rates of occurrences of fire have been derived that are specific to nuclear units (Wheelis, 1986). Fire incidence data for non-nuclear units has been collected in the National Fire Incident Reporting System of the National Fire Protection Association. Fire growth and damage propagation models for fires in compartments have been developed specifically for nuclear units (Frank and Moieni, 1986; Siu et al., 1988). More generally applicable models have been developed at the National Institute of Standards and Technology (NIST) (Rockett, 1990; Mitler and Rockett, 1987). Some research has been done on the fragility or robustness of equipment against fires, particularly for electrical cables and structural materials (Nowlen, 1989; Society of Fire Protection Engineers, 1995). Conservative assumptions about the effects of fire on equipment, particularly electrical equipment, are usually made in a fire RA.

2.6.1.3 Floods and Winds

Typically, an RA of floods and winds is not performed with the same level of analytical sophistication and has not been the subject of as much methods development activity as fire and earthquake RA. This lack of activity is because nuclear power units are designed to withstand, without significant damage, flood levels and wind velocities far in excess of historically observed or inferred levels (i.e., Design Basis Events). Thus, the emphasis has been on either determining the frequency of exceeding a very conservative design basis or showing that no damage will be done to the unit even if the design basis is exceeded. The focus in the chemical industry risk management programs is to verify that the facility complies with the Uniform Building Code.

The frequency of winds as a function of direction and velocity on a regional, and sometimes local, basis is available from NOAA, and some data also has been collected by NIST. The U.S. Army Core of Engineers and the National Weather Service keep track of river water levels. One area of concern regarding floods has been the failure of dams, particularly earthen dams. Such data is also collected by the U.S. Army Core of Engineers. Data regarding storm surges caused by ocean-derived storms, such as hurricanes, are collected by NOAA.

2.6.2 Human Reliability Analysis

The genesis of the technology in this area lies in the defense and nuclear industry (Swain and Guttman, 1983). Nuclear accidents to date as well as the risk assessment predictions strongly suggest the importance of human actions and errors in either improving or exacerbating a nuclear accident scenario. Therefore, an enormous amount of research and methods development has occurred worldwide to understand the ability of operators to respond to and recover from nuclear accident scenarios. Several survey books that summarize the field up to the time of their publication are available (Dougherty and Fragola, 1988; Gertman and Blackman, 1994; Hollnagel, 1993). Each book characterizes and categorizes methods differently. One can distinguish, however, a first generation of methods (Swain and Guttman, 1983; Hannaman and Spurgin, 1984; Embrey et al., 1984; Hall et al., 1982) from a second generation of methods (Hollnagel, 1998; Spurgin and Moieni, 1991). The first generation of methods took into account phenotype only. That is, only the outcome or observed manifestation of human endeavor was modeled. The second generation attempts to account for both phenotype and genotype. The latter is the cause, involving human cognitive function, underlying the specific action. The first generation of methods were geared to filling in the blank in a fault tree or event tree that had a box for a human error probability in a manner analagous to hardware failures. The second generation of methods take a more sophisticated approach to modeling human actions. These methods attempt to account for people's cognitive functions during nuclear accident situations. All methods are plagued by sparse data and the use of a good deal of judgment.

2.6.3 Software Risk

Although software reliability methods are reasonably well established (Shooman, 1983; Musa et al., 1990), software risk is an emerging area of RA. Software reliability attempts to predict when a software development program has reached an acceptable level of residual errors so that it can be released for open use. The impetus for software RA, however, is the recognition of the increasing use and number of accidents associated with software-driven digital control systems in every aspect of technology (Dunn and Frank, 1994). Methods range from attempts at modeling software using a fault tree to attempts at mathematically proving that software does what it is supposed to do (Parnas et al., 1990; Bowman et al., 1991; Leveson, 1994). The thrust of software risk assessment, however, is to look at the software within the context of the operating system and environment. The objective is to attempt to include software errors and their likelihood within the overall set of accident scenarios. There is as yet no satisfactory methodology in this area (Butler and Finelli, 1991).

3 SUMMARY, OBSERVATIONS, AND COMMENTARY

3.1 SUMMARY

This document is a survey of safety RA methods, derived from RA theory and practice in the chemical, nuclear, and aerospace industries, that might be of use for regulatory decision making and promulgation of regulations for the privatized vitrification project at Hanford. It is not a method handbook, guidance document, tutorial, or manual. Methods discussed herein include the following:

- Identification of hazards, failure modes, and initiating events
- Development, structuring, and presentation of scenarios
- Calculation of the frequency and probability of events
- Uncertainty analysis
- Calculation of source terms and dose for radiological and chemical hazards
- Other topics such as fire, flood and earthquake RA, software RA, and human reliability

Because of the enormous body of literature about risk methods and techniques, it is not feasible to present a complete description of individual RA methods. An extensive Bibliography of work referenced herein is provided in Section 4 for those who wish to learn more about individual techniques.

3.2 SIGNIFICANCE OF RISK ASSESSMENT FOR THE REGULATOR

Remediation facilities and systems are being designed and constructed because the current situation has been deemed an unacceptable long-term risk. The objective of a licensing and regulatory process, therefore, is to ensure that the "cure is better than the disease." That is, regulatory efforts should emphasize guidance and safety systems such that the long-term risk, when remediation is included, is less than the risk associated with the current situation. In addition, regulations should ensure safety through the short term during operation of the active remediation systems (the vitrification systems).

The uses of RA depend on the decisions to be made. Decision making is essentially a prediction and selection activity. Based on best available information, the decision maker tries to predict the outcome of each prospective strategy and select the "best" with respect to criteria. Assuring the safety of an operating system involves, for example, decisions regarding inherent safety features, engineered safety systems, administrative controls, and operation and maintenance philosophy. A comprehensive RA discovers scenarios that might lead to release of hazardous materials despite the safety systems. Because of the predictive ability of RA, how to best prepare for a hazardous material release becomes a crucial decision.

Although a regulatory agency does not engage in design, it does have the responsibility of review and approval of aspects of design, operation, maintenance, and emergency preparedness that are essential for safety. RA gives a regulatory agency a tool for anticipating accidents and preparing regulatory strategies that will mitigate risk.

Example objectives of an RA for regulatory purposes might be

- Identify hazards
- Rank risk significance of systems
- Review and approve safety systems to meet safety criteria
- Review and approve limiting conditions of operation and allowed system outage times
- Review and approve the array of parameters to be monitored during operation
- Review and approve emergency operating procedures
- Review and approve emergency plans
- Evaluate residual risk after design is complete

3.3 OBSERVATIONS AND COMMENTARY ABOUT RISK ASSESSMENT METHODS

To the best knowledge of the author, this is the only survey that has combined RA methods derived from the chemical industry with those used in the nuclear and aerospace industries in the United States. This statement is, of course, based on the experience of the author. The following sections provide some observations and commentary derived from comparing RA approaches in these three industries.

3.3.1 Typical Risk Assessment Practice

Although the NRC, the EPRI, and the nuclear industry have funded a great deal of research into advanced methods of RA, practical applications within the industry are far more modest. For example, since 1989, each commercial nuclear power plant licensee has been requested to perform RAs called Individual Plant Evaluations that include hardware failures and human errors within the plant as well as external events. Guidance documents (Nuclear Regulatory Commission, 1989c, 1991b) have recommended acceptable methods for these. Neither document included requests for calculation of dose to the local population nor quantitative uncertainty analyses even though the NRC had developed such methods. Thus, in practice, methods used tend to closely conform with those requested by the NRC and deemed acceptable to the NRC.

A similar situation exists with respect to chemical risk methods deemed acceptable to the EPA. Even though industry groups have provided RA guidance documents for risk methods, in practice, methods are concentrated in evaluating intake, dose, and health effects in a prescribed manner (see section 2.4.1 of this report). Although uncertainties are recognized to be important, the EPA guidance documents do not emphasize quantification of uncertainties. Furthermore, these documents provide little guidance about methods for scenario development and calculation of scenario frequencies. This lack of guidance closely follows the EPA philosophy of reasonable maximum exposure estimates.

By contrast, the aerospace industry, particularly in space-nuclear applications, is relatively new to applying modern RA techniques. RA techniques used in practice are among the most sophisticated available. Scenarios are developed with frequencies and uncertainties from initiating event through health effects. An attempt is made to use and develop risk models that depict events and phenomena as accurately as feasible taking advantage of the available literature.

3.3.2 Commonality of Scenario Structuring Methods

Scenario structuring methods are nearly identical among the three surveyed industries. Aerospace and chemical industries rely somewhat more on initiating event identification methods than terrestrial nuclear applications. This is largely because these industries must analyze a wider variety of designs with new designs continuously emerging. By contrast, the basic initiating events of nuclear power units were identified decades ago with little change over the year.

In some cases, nearly identical methods have been developed in parallel and given different names. A good example of this is the combined use of event trees and fault trees for scenario development that originally emerged from the Reactor Safety Study (Nuclear Regulatory Commission, 1975). This method is very similar to Cause-Consequence analysis (American Institute of Chemical Engineers, 1992) which also uses event trees and fault trees. The primary difference appears to be the way in which event trees are drawn (System Safety Society, 1993). In other cases, the same methods (e.g., Failure Mode and Effects Analysis, experience-based methods) have been used in all three industries.

3.3.3 Importance of Uncertainty and Typical Uncertainty Analysis Practice

Clearly, RA involves uncertainty as does essentially any analysis that involves assumptions, data, and the use of judgment. A prospective analysis about safety is no exception. In essence, promulgation of regulations for safety involves data, assumptions, and judgment. Therefore, it is important to include quantitative uncertainty analysis as part of RA to ensure that regulations are conservatively established.

Chemical RA emphasizes qualitative treatment of uncertainties with respect to parameters, assumptions, and modeling. An occasional need for a quantitative treatment of uncertainty of the exposure factors for intake and health effects is also recognized. A simple Monte Carlo method is most often used for this qualitative treatment. Accident frequencies and their uncertainties are not included. Uncertainties in source terms, owing to possible alternative future accidents, are not treated.

An extensive array of methods for quantitative uncertainty analysis was developed in research funded by EPRI, NRC, and DOE. The most frequent use of uncertainty analysis is for the uncertainty in the frequencies of scenarios leading to damage of the nuclear core. Uncertainties in the phenomenology of accident progression beyond core damage to source terms are generally not analyzed. When dose and health effects are calculated (e.g., by a code such as CRACIT), the uncertainty in weather is included. Exposure factor uncertainties are not included. Modeling uncertainties, which probably are as significant as weather uncertainties in the source term and dose computations, are generally not included. However, some uncertainty analysis is performed to obtain the probability of either breaching or bypassing the reactor containment structures. Research into a more complete modeling of uncertainties, which would also include modeling uncertainties, has been performed.

Space nuclear power RA applications have taken advantage of the funded research for terrestrial nuclear power. These RAs exhibit sophisticated simulation as well as event tree structured methods. They treat both epistemic and aleatory uncertainties in accident scenario probabilities, source terms, and consequences (e.g., dose and health effects). Modeling, parameter, and phenomenological uncertainties have been included to varying degrees. Uncertainties are developed for accident frequencies and source terms (e.g., uncertainties in the amount of release as well as the characteristics of the release). Consequences are calculated with treatment of uncertainties in weather, wind direction, wind speed, and exposure factors.

3.3.4 Basis for Preference Among Methods

The literature indicates that a wide variety of RA techniques have been developed and are in use. Because RA is simply a logical, structured thought process to identify and quantify scenarios and their consequences, it lends itself to methodological flexibility. After all, each analyst has a somewhat different ways of visualizing scenarios. Any structured, logical method that helps an analyst do that can be useful.

From time to time, one or another segment of the RA community will proclaim the superiority of one scenario structuring approach over another. For example, a completely specious controversy that has involved the RA community for decades involves the controversy between using large event trees and small fault trees or vice versa. (Other controversies have been over whether one or the other should be used exclusively.) These arguments are not born from a reasoned appraisal of alternative methods. This survey shows them all to be of a category called belief nets, conceptually derived from information theory. As such, there is no essential difference between them because the fidelity of scenario representation using any belief net is independent of the particular diagrammatic form (or forms) it takes.

Realistically, the set of methods to select for an RA largely depends on the objective of the analysis and the preference of the analysts. Of course, there is also a dependence on the types of hazards to be analyzed and the complexity of the systems. It is, therefore, premature to suggest or require one set of methods over another for the Hanford privatized vitrification project.

29/36

4 REFERENCES

Abernathy, A. 1983. *Weibull Analysis Handbook.* AFWAL-TR-83-2079. Aero Propulsion Laboratory. Dayton, OH: Wright-Patterson AFB.

Acosta, C., and N. Sui. 1993. Dynamic event trees in accident sequence analysis: Application to steam generator tube rupture. *Reliability Engineering and System Safety*. January, 1993.

American Institute for Chemical Engineers. 1985. *Guidelines for Hazard Evaluation Procedures*. New York, NY: American Institute for Chemical Engineers, Center for Chemical Process Safety.

American Institute of Chemical Engineers. 1989a. *Guidelines for Chemical Process Quantitative Risk* Analysis. New York, NY: American Institute of Chemical Engineers, Center for Chemical Process Safety.

American Institute of Chemical Engineers. 1989b. *Guidelines for Process Equipment Reliability Data with Data Tables.* New York, NY: American Institute of Chemical Engineers, Center for Chemical Process Safety.

American Institute for Chemical Engineers. 1992. *Guidelines for Hazard Evaluation Procedures* 2^{nd} *Edition with Worked Examples.* New York, NY: American Institute for Chemical Engineers, Center for Chemical Process Safety.

American Nuclear Society. 1985. *Proceedings of the ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, February 24–March 1, 1985.* La Grange Park, IL: American Nuclear Society.

American Nuclear Society. 1986. *Proceedings of the International ANS/ENS Topical Meeting on Thermal Reactor Safety, San Diego, California, February 1986.* La Grange Park, IL: American Nuclear Society.

American Society for Testing Materials. 1995. *Standard Guide for Risk-Based Corrective Action Applied at Petroleum Release Sites.* ASTM E 1739-95 (updated 1996). Philadelphia, PA: American Society for Testing Materials.

Apostolakis, G. 1978. Probability and Risk Assessment: The subjectivistic Viewpoint and some suggestions. *Nuclear Safety*: 19(3).

Apostolakis, G. 1981. *Bayesian Methods in Risk Assessment, Advances in Nuclear Science and Technology, Vol. 13.* New York, NY: Plenum Publishing Company.

Apostolakis, G. 1986. On the use of judgment in probabilistic risk analysis. *Nuclear Engineering and Design* 93.

Apostolakis, G. 1988. Expert judgment in probabilistic safety assessment. *Accelerated Life Testing and Expert's Opinions in Reliability.* C.A. Clarotti and D.V. Lindley, eds. Corso, Italy: Society Italiana di Fisica.

Apostolakis, G. 1993. A commentary of model uncertainty. Model Uncertainty: Its Characterization and Quantification. *Proceedings of Workshop I in Advanced Topics in Risk and Reliability Analysis.* NUREG/CP–0138. Washington, DC: Nuclear Regulatory Commission.

Baybutt, P. 1986. Uncertainties in modeling physical and chemical phenomena in reactor accidents. *Nuclear Engineering and Design* 93.

Beiser J., and S. Rigdon. 1997. Bayes prediction for the number of failures of a repairable system. *IEEE Transactions on Reliability* 46(2).

Bell, M.J. 1973. *ORIGEN: The ORNL Isotope Generation and Depletion Code.* ORNL–4628. Oak Ridge, TN: Oak Ridge National Laboratory.

Berger, J.O. 1993. *Statistical Decision Theory and Bayesian Analysis.* Second Edition. New York, NY: Springer-Verlay.

Bernreuter et al. 1984. *Seismic Hazard Characterization of the Eastern United States: Methodology and Interim Results for Ten Sites.* NUREG/CR–3756. Washington, DC: Nuclear Regulatory Commission.

Bhattacharya, S.K. 1967. Bayesian approach to life testing and reliability estimation. *Journal of American Statistical Association* 62.

Blanton, et al. 1993. *Savannah River Site Generic Data Base Development.* WSRC–TR–93–62. Aiken, SC: Savannah River Site.

Bowman, W.C., et al. 1991. An application of Fault tree analysis to safety critical software at Ontario Hydro. G. Apostalakis, ed. *Probabilistic Safety Assessment and Management.* London, England: Elsevier Science Ltd.

Breen, R.J., et al. 1965. *HARMONY: System for Nuclear Reactor Depletion Computation.* WAPD–TM–478. Westinghouse Electric Corporation.

Budnitz, R., et al. 1985. *An Approach to the Quantification of Seismic Margins in Nuclear Power Plants.* NUREG/CR–4334. Livermore, CA: Lawrence Livermore National Laboratory.

Butler, R., and G.B. Finelli. 1991. The infeasability of experimental quantification of life-critical software reliability. *ACU SIGSOFT.*

Cacciabue, P.C., and A. Amendola. 1986. Dynamic logical analytical methodology versus fault tree: The case study for the auxiliary feedwater system of a nuclear power plant. *Nuclear Technology* 74: 195–208.

California State. 1988. *California Health and Safety Code.* Chapter 6.95, Article 2.

Clean Air Act Amendments of 1990. PL 101–549. 1990.

Cooke, R.M. 1991. *Experts in Uncertainty: Opinion and Subjective Probability in Science.* Oxford, England: Oxford University Press.

Cooke, R.M., et al. 1988. Calibration and information in expert resolution: A classical approach. *Automatica* 24.

Croff, A.G. 1980. *ORIGEN2: A Revised and Updated Version of the Oak Ridge Isotope Generation and Depletion Code.* ORNL–5621. Oak Ridge, TN: Oak Ridge National Laboratory.

Devooght, J., and C. Smidts. 1993. *Probabilistic Dynamics: The Mathematical and Computing Problems Ahead.* T. Aldemir, N. Sui, A. Mosleh, P.C. Cacciabue, and G. Goktepe, eds. New York, NY: Springer-Verlag.

Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications.* Washington, DC: American Institute of Aeronautics and Astronautics.

Dougherty Jr., E., and J. Fragola. 1988. *Human Reliability Analysis.* New York, NY: John Wiley and Sons.

Draxler, R.R., and G.D. Hess. 1997. *Description of the Hysplit-4 Modeling System.* Technical Memorandum ERL ARL–224. Washington, DC: National Oceanographic and Atmospheric Administration.

Dunn, W., and M. Frank. 1994. Risk assessment and management of safety-critical, digital industrial controls–present practices and future challenges. *Proceedings of PSAM-II, March 1994.* PSAM Corporation.

Electric Power Research Institute. 1989. *Probabilistic Seismic Hazard Evaluations at Nuclear Plant Sites in the Central and Eastern United States: Resolution of the Charleston Earthquake Issue.* EPRI NP–6395–6041. Palo Alto, CA: Electric Power Research Institute.

Electric Power Research Institute. 1991a. *A Methodology for Assessment of Nuclear Power Plant Seismic Margin, Revision 1.* EPRI NP–6041. Palo Alto, CA: Electric Power Research Institute.

Electric Power Research Institute. 1993. *Fire Induced Vulnerability Evaluation (FIVE) Methodology*. Palo Alto, CA: Electric Power Research Institute.

Embrey, D., and B. Kirwan. 1983. A comparative evaluation of three subjective human reliability quantification techniques. K. Coombes, ed. *Proceedings of the Ergonomics Society's Conference.* London, England: Taylor and Francis.

Embrey, D., et al. 1984. *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment.* NUREG/CR–3518. Washington, DC: Nuclear Regulatory Commission.

European Space Agency. 1992. *Hazard Analysis Requirement and Methods.* ESA PSS–01–403. Paris, France: European Space Agency.

Event Analysis, Inc. 1985. *MORT Guide, Guidance to the Management Oversight and Risk Tee Chart, for Use with the STEP Investigation System.* Event Analysis, Inc.

Fauske & Associates, Inc. 1983. *MAAP User's Manual.* IDCOR Technical Report 16.1. Chicago, IL: Fauske & Associates, Inc.

Fields, Jr., T. 1991. Memo (March 25) to distribution. Human Health Evaluation Manual, Supplemental Guidance: Standard Default Exposure Factors. OSWER Directive 9285.6-03. Washington, DC: U.S. Environmental Protection Agency, Office of Emergency and Remedial Response.

Fishman, G. 1996. *Monte Carlo Concepts Algorithms, and Applications.* New York, NY: Springer-Verlag.

Fleming, K., et al. 1983. On the analysis of dependent failures in risk assessment and reliability evaluation. *Nuclear Safety* 24: 5.

Frank, M.V., and S.A. Epstein. 1986. Application of artificial intelligence to improve plant availability. *Intelligent Simulation Environments.* P. Luker and H. Adelsberger, eds. Society for Computer Simulation Series 17(1).

Frank, M.V., and P. Moieni. 1986. A probabilistic model for flammable pool fire damage in nuclear power plants. *Reliability Engineering and System Safety* 16.

Frank, M.V. 1995. Choosing among safety improvement strategies: A discussion with example of risk assessment and multi-criteria decision approaches for NASA. *Reliability Engineering & System Safety* 49(3).

Gertman, D.I., et al. 1989. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR).* NUREG/CR–4639. Washington, DC: Nuclear Regulatory Commission.

Gertman, D., and H. Blackman. 1994. *Human Reliability and Safety Analysis Data Handbook.* New York, NY: John Wiley and Sons.

Green, A.E., and A.J. Bourne. 1972. *Reliability Technology.* New York, NY: John Wiley and Sons.

Haasl, D. 1965. Advanced concepts in fault tree analysis. *Proceedings of the System Safety Symposium.* Seattle, WA: Boeing Co.

Hall, J. 1990. *U.S. Experience with Sprinklers.* Fire analysis and Research Division Publication. Quincy, MA: National Fire Protection Association.

Hall, R., et al. 1982. *Post-event Human Decision Errors: Operator Action Trees/Time Reliability Correlations.* NUREG/CR–3010. Washington, DC: Nuclear Regulatory Commission.

Hannaman, G., and A. Spurgin. 1984. *Systematic Human Action Reliability Procedure (SHARP).* EPRI NP–3583. Palo Alto, CA: Electric Power Research Institute.

Helton, J., and D. Burmaster, eds. 1996. *Reliability Engineering and System Safety* 54.

Hicks, B.B. 1986. Differences in wet and dry particle deposition parameters between North America and Europe. *Aerosols: Research, Risk Assessment, and Control Strategies.* Chelsea, MI: Lewis Publishers 973–982.

Hollnagel, E. 1993. *Human Reliability Analysis: Context and Control.* London, England: Academic Press.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method: CREAM.* London, England: Elsevier Science Ltd.

Howard, R.A. 1988. Uncertainty about probability: A decision analysis perspective. *Risk Analysis* 8(1).

Howard, R.A., and J.E. Matheson. 1984. Influence diagrams. *The Principles and Applications of Decision Analysis.* Menlo Park, CA: Strategic Decisions Group.

Iman, R., and J. Helton. 1985. *A Comparison of Uncertainty and Sensitivity Analysis Techniques for Computer Models.* NUREG/CR–3904. Albuquerque, NM: Sandia National Laboratory.

Iman, R., and M. Shortencarrier. 1984. *A Fortran 77 Program and User's Guide for the Generation of Latin Hypercube and Random Samples for Use with Computer Models.* NUREG/CR–3624. Albuquerque, NM: Sandia National Laboratory.

Institute of Electrical and Electronic Engineers, Inc. 1984. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.* IEEE–STD–500. Washington, DC: Institute of Electrical and Electronic Engineers, Inc.

Interagency Nuclear Safety Review Panel. 1990. *Safety Evaluation Report for Ulysses.* Washington, DC: Interagency Nuclear Safety Review Panel.

Interagency Nuclear Safety Review Panel. 1993. The role of resuspension of radioactive particles in nuclear assessments. *Proceedings of the Interagency Nuclear Safety Review Panel (INSRP), Technical Interchange Meeting, Cocoa Beach, Florida, September 21–23.* Washington, DC: Interagency Nuclear Safety Review Panel.

Interagency Nuclear Safety Review Panel. 1997. *Safety Evaluation Report for the National Aeronautics and Space Administration Cassini Mission.* Washington, DC: Interagency Nuclear Safety Review Panel.

International Commission on Radiological Protection. 1977a. *Recommendations of the International Commission on Radiological Protection.* Publication 25. New York, NY: International Commission on Radiological Protection.

International Commission on Radiological Protection. 1977b. *Recommendations of the International Commission on Radiological Protection.* Publication 26. New York, NY: International Commission on Radiological Protection.

International Commission on Radiological Protection. 1979. *Recommendations of the International Commission on Radiological Protection.* Publication 30. New York, NY: International Commission on Radiological Protection.

International Commission on Radiological Protection. 1991. *1990 Recommendations of the International Commission on Radiological Protection.* Publication 60. New York, NY: International Commission on Radiological Protection.

International Commission on Radiological Protection. 1993. *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 2, Ingestion Dose Coefficients.* Publication 67, Ann ICRP 23(3/4). New York, NY: International Commission on Radiological Protection.

International Commission on Radiological Protection. 1995. *Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 4, Inhalation Dose Coefficients.* Publication 71, Ann ICRP 25(3/4). New York, NY: International Commission on Radiological Protection.

Kahneman, P. Slovic, and A. Tversky, eds. 1982. *Judgment Under Uncertainty: Heuristics and Biases.* Cambridge, MA: Cambridge University Press.

Kaplan, S. 1986. On the use of data and judgment in probabilistic risk and safety analysis. *Nuclear Engineering and Design* 93.

Kazarians, M., et al. 1985. Fire risk analysis for nuclear power plants: Methodological developments and applications. *Risk Analysis* 5.

Kennedy, R. 1985. Various types of reported seismic margins and their use. *Proceedings of EPRI/NRC Workshop on Nuclear Power Plant Re-evaluation to Quantify Seismic Margins, August 1985.* EPR NP–4101.Palo Alto, CA: Electric Power Research Institute.

Kennedy, R., and M. Ravindra. 1984. Seismic fragilities for nuclear power plant risk studies. *Nuclear Engineering and Design* 79(1).

Kennedy, R., et al. 1984a. *Engineering Characterizations of Ground Motion - Task 1, Effects of Characteristics of Free-Field Motion on Structural Response.* NUREG/CR–3805. Washington, DC: Nuclear Regulatory Commission.

Knowlton, R.E. 1992. *A Manual of Hazard & Operability Studies: The Creative Identification of Deviations and Disturbances.* Vancouver, British Columbia: Chemetics International, Ltd.

Lercari, F.A. 1988. *Risk Management and Prevention Program Guidance.* Sacramento, CA: California Governor's Office of Emergency Services.

Leveson, N. 1994. Software safety analysis. *Proceedings of the High Consequence Operations Safety Symposium.* SAND94–2364. Albuquerque, NM: Sandia National Laboratory.

Lockheed Martin Corporation. 1997a. *Cassini Titan IV/Centaur RTG Safety Databook.* Revision B. NAS3–00031. Valley Forge, PA: Lockheed Martin Corporation.

Lockheed Martin Corporation. 1997b. *General Purpose Heat Source-Radioisotope Thermoelectric Generators in Support of the Cassini Mission Final Safety Analysis Report (FSAR).* CDRL C.3. Valley Forge, PA: Lockheed Martin Corporation, Missiles and Space, Valley Forge Operations.

Los Angeles County Fire Department. 1991. *Risk Management & Prevention Program Guidelines.* Los Angeles, CA: Los Angeles County Fire Department.

Madni, I. 1991. MELCOR modeling of the PBF severe fuel damage test 1-4. *Probabilistic Safety Assessment and Management.* New York, NY: Elsevier Science Publishing Co.: 1,327–1,332

Martin, D.O., and J.A. Tikvaart. 1968. A general atmospheric diffusion model for estimating the effects on air quality of one or more sources. *61st Annual Meeting of the Air Pollution Control Association.*

Martz, H.F., and M.C. Bryson. 1993. On combining data for estimating the frequency of low-probability events with applications to sodium valve failure rates. *Nuclear Science and Engineering* 13: 267–280.

Martz, H., and R. Waller. 1991. *Bayesian Reliability Analysis.* Malabar, FL: Krieger Publishing Company.

Merz, K. 1991a. *Seismic Ruggedness of Relays.* PRI NP–7147. Palo Alto, CA: Electric Power Research Institute.

Merz, K. 1991b. *Generic Seismic Ruggedness of Power Plant Equipment.* Revision 1. EPRI NP–5223. Palo Alto, CA: Electric Power Research Institute.

Milici, A., et al. 1996. The use of the dynamic flowgraph methodology in modeling human performance and team effects. *Probabilistic Safety Assessment and Management.* Volume I. New York, New York: Spring-Verlag Publishers.

Mitler, H., and J. Rockett. 1987. *User's Guide to FIRST, a Comprehensive Single-Room Fire Model.* CIB W14/88/22. Gaithersburg, MD: National Institute of Standards and Technology.

Morris, P. 1974. Decision analysis expert use. *Management Science* 20.

Morris, P. 1977. Combining expert judgments: A Bayesian approach. *Management Science* 23.

Mosleh, A., and G. Apostolakis. 1982. Models for the use of expert opinions. *Workshop on Low-Probability/High Consequence Risk Analysis.* Arlington, VA.

Mosleh, A., and G. Apostolakis. 1986. The assessment of probability distributions from expert opinions with an application to seismic fragility curves. *Risk Analysis* 6(4).

Mosleh, A., et al. 1987. *Methods for the Elicitation and Use of Expert Opinion in Risk Assessment.* NUREG/CR–4962. Washington, DC: Nuclear Regulatory Commission.

Mosleh, A., et al. 1988. *Procedures for Testing Common Cause Failures in Safety and Reliability Studies.* NUREG/CR–4780. Washington, DC: Nuclear Regulatory Commission.

Murchland, J., and G. Weber. 1972. A moments method for the calculation of a confidence interval for the failure probability of a system. *Proceedings of the 1972 Annual Reliability and Maintainability Symposium.* Institute of Electrical and Electronic Engineers.

Musa, J., et al. 1990. *Software Reliability.* New York, NY: McGraw Hill Book Company.

Napier, B., R. Peloquin, D. Strenge, and J. Ramsdell. 1988. *GENII - The Hanford Environmental Radiation Dosimetry Software System, Vol. 1: Conceptual Representation.* PNL–6584. Richland, WA: Pacific Northwest Laboratory.

National Aeronautics and Space Administration. 1987a. *Methodology for Conduct of NSTS Hazard Analyses.* NSTS 22254. National Aeronautics and Space Administration.

National Aeronautics and Space Administration. 1987b. *Instructions for Preparation of Failure Mode and Effects Analysis (FMEA) and Critical Items Lists (CIL).* NASA/JSC, NSTS 22206. Washington, DC: National Aeronautics and Space Administration.

National Council on Radiation Protection and Measurement. 1996. *A Guide for Uncertainty Analysis in Dose and Risk Assessments Related to Environmental Contamination.* NCRP Commentary No. 14. Washington, DC: National Council on Radiation Protection and Measurement.

National Institute of Occupational Safety and Health of the Center for Disease Control. 1997. *NIOSH Pocket Guide to Chemical Hazards.* Washington, DC: Government Printing Office Document 97–140.

Newmark, N., and W. Hall. 1978. *Development of Criteria for Seismic Review of Selected Nuclear Power Plants.* NUREG/CR–0098. Washington, DC: Nuclear Regulatory Commission.

Nowlen, S. 1989. *A Summary of Nuclear Power Plant Fire Safety Research at Sandia National Laboratories, 1975–1987.* NUREG/CR–5384. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1975. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* WASH–1400 (NUREG–75/014). Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1977. Calculation of Annual Doses to Man from Routine Releases of Reactor Effluents for the Purpose of Evaluating Compliance with 10 CFR Part 50, Appendix I, Revision 1. *Regulatory Guide 1.109.* Washington, DC: Nuclear Regulatory Commission, Office of Standards Development.

Nuclear Regulatory Commission. 1983. *PRA Procedures Guide.* NUREG/CR–2300. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1986. *Seismic Fragility of Nuclear Power Plant Components, Phase I.* Vol. 1. NUREG/CR–4659. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1987. *Seismic Fragility of Nuclear Power Plant Components, Phase II, Motor Control Center, Switchboard, Panelboard and Power Supply.* Vol. 2. NUREG/CR-4659. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1988. *Evaluation of External Hazards to Nuclear Power Plants in the United States—Seismic Hazard.* Supplement 1. NUREG/CR–5042. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1989a. *Recommended Procedures for the Simplified External Event Risk Analysis for NUREG–1150.* DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1989b. *Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains.* NUREG/CR–5250. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1989c. *Individual Plant Examination: Submittal Guidance.* NUREG–1335. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1990. *Seismic Fragility of Nuclear Power Plant Components, Phase II, Switchgear, I&C Panels (NSSS) and Relays,* Vol. 3. NUREG/CR–4659. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1991a. *Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities—10 CFR 50.54(f).* General letter 88-20, Supplement No. 4. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1991b. *Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities.* Final Report. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1993. Model uncertainty: Its characterization and quantification. *Proceedings of Workshop I in Advanced Topics in Risk and Reliability Analysis.* NUREG/CP–0138. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1994a. *Definition of Risk.* NUREG-1489, C.4.4.4. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1994b. *Revised Livermore Seismic Hazard Estimates for 69 Nuclear Power Plant Sites East of the Rocky Mountains.* NUREG–1488. Washington, DC: Nuclear Regulatory Commission.

Nuclear Regulatory Commission. 1997a. *Standards for Protection Against Radiation.* Code of Federal Regulations, Title 10—Energy, Chapter 1—Nuclear Regulatory Commission, Part 20. Washington, DC: U.S. Government Printing Office.

Nuclear Regulatory Commission. 1997b. *Domestic Licensing of Production and Utilization Facilities.* Code of Federal Regulations, Title 10—Energy, Chapter 1—Nuclear Regulatory Commission, Part 50. Washington, DC: U.S. Government Printing Office.

Nuclear Regulatory Commission. 1997c. *Disposal of High-Level Wastes in Geologic Repositories*. Code of Federal Regulations, Title 10—Energy, Chapter 1—Nuclear Regulatory Commission, Part 60. Washington, DC: U.S. Government Printing Office.

Nuclear Regulatory Commission. 1997d. *Domestic Licensing of Special Nuclear Material.* Code of Federal Regulations, Title 10—Energy, Chapter 1—Nuclear Regulatory Commission, Part 70. Washington, DC: U.S. Government Printing Office.

Nuclear Regulatory Commission. 1997e. *Licensing Requirements for the Independent Storage of Spent Nuclear Fuel and High-Level Radioactive Waste.* Code of Federal Regulations, Title 10—Energy, Chapter 1—Nuclear Regulatory Commission, Part 72. Washington, DC: U.S. Government Printing Office.

Occupational Safety and Health Administration. 1991. *Process Safety Management Regulations, 20 CFR 1910.* Washington, DC: Occupational Safety and Health Administration.

Orvis, D., et al. 1981. *Guidebook for the Reliability, Availability and Maintainability Analysis of NWTS Repository Equipment.* ONWI–334. Washington, DC: Nuclear Regulatory Commission, Office of Nuclear Waste Isolation.

Parnas, D.L., et al. 1990. Evaluation of safety critical software. *CACU* 33(6).

Raouf, A., and B.S. Dhillon. 1994. *Safety Assessment: A Quantitative Approach.* Ann Arbor, MI: Lewis Publishers.

Ritchie, L.T., et al. 1981. *Calculation of Reactor Accident Consequences.* Version 2. Prepared by Sandia National Laboratory. NUREG/CR–2324. Washington, DC: Nuclear Regulatory Commission.

Rockett, J. 1990. *Using the Harvard/NIST Mark VI Fire Simulation.* NISTIR 4464. Gaithersburg, MD: National Institute of Standards and Technology.

Rubinstein, R.Y. 1981. *Simulation and the Monte Carlo Method.* New York, NY: John Wiley and Sons.

Sandia National Laboratory. 1985. *MELPROG-PWR/MODO: A Mechanistic Code for Analysis of Reactor Core Melt Progression and Vessel Attack Under Severe Accident Conditions.* SAND85–0237. Albuquerque, NM: Sandia National Laboratory.

Seed, H., et al. 1983. Evaluation of liquefaction potential using field performance data. *ASCE Journal of Geotechnical Engineering* 109(3).

Seed, H., et al. 1984. *The Influence of SPT Procedures in Soil Liquefaction Resistance* Evaluations. Report No. EERC 84/15. Berkeley, CA: University of California, Earthquake Engineering Research Center.

Shachter, R.D., and M.A. Peot. 1992. Decision making using probabilistic inference methods. *Proceedings of the Eighth Conference on Uncertainty in Artificial Intelligence, February 1992.* Stanford, CA.

Shisko, R. 1995. *NASA Systems Engineering Handbook.* SP–6105. Washington, DC: NASA.

Shooman, M. 1983. *Software Engineering.* New York, NY: McGraw Hill Book Company.

Shooman, M.L. 1990. *Probabilistic Reliability: An Engineering Approach.* 2nd Edition. Malabar, FL: Robert E. Krieger Publishing Company.

Siu, N. 1994. Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety* 43: 43–73.

Siu, N., et al. 1988. COMPBRN III—A fire hazard model for risk analysis. *Fire Safety Journal* 13.

Smucker, S.J. 1996. Memo (August 1) to PRG Table Mailing List. Preliminary remediation goals 1996. San Francisco, CA: U.S. Environmental Protection Agency, Region 9.

Society of Fire Protection Engineers. 1995. *The SFPE Handbook of Fire Protection Engineering.* 2nd Edition. Quincy, MA: National Fire Protection Association.

Spurgin, A., and P. Moieni. 1991. Interpretation of simulator data in the context of human reliability modeling. G. Apostolakis, ed. *Probabilistic Safety Assessment and Management.* Elsevier, NY: Elsevier.

Swain, A., and H. Guttman. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* NUREG/CR–1278. Washington, DC: Nuclear Regulatory Commission.

System Safety Society. 1993. *System Safety Analysis Handbook.* Albuquerque, NM: System Safety Society.

Tanabe, F., et al. 1982. Post-facto analysis of the TMI accident (1): Analysis of thermal hydraulic behavior by use of RELAP4/MOD6/U4/J2. *Nuclear Engineering and Design:* 69.

Technica, Ltd. 1985. *Manual of Industrial Hazard Assessment Techniques.* London: England: World Bank.

U.S. Department of Defense. 1984a. *Military Standard System Safety Program Requirements.* MIL–STD–882a. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense. 1984b. *Military Standard System Safety Program Requirements.* MIL–STD–882b. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense. 1991. *Reliability Prediction of Electronic Equipment.* MIL–HDBK–217F. Washington, DC: Department of Defense.

U.S. Department of Defense. *Failure Mode and Effects Analysis.* MIL–STD–1629. Washington, DC: Department of Defense.

U.S. Department of Defense. 1993. *Failure Rate Sampling Plans and Procedures.* MIL–STD–690. Washington, DC: Department of Defense.

U.S. Department of Energy. 1988. *External Dose-Rate Conversion Factors for Calculation of Dose to the Public.* DOE/EH–0070. Washington, DC: U.S. Department of Energy.

U.S. Department of Energy, and Washington State Department of Ecology. 1996. *Tank Waste Remediation System, Hanford Site, Richland, Washington, Final Environmental Impact Statement.* DOE/EIS–0189. Washington, DC: U.S. Department of Energy.

U.S. Environmental Protection Agency. 1986. *Guidelines for Exposure Related Measurements.* Federal Register (51): 34042. Washington, DC: U.S. Environmental Protection Agency.

U.S. Environmental Protection Agency. 1988a. *Proposed Guidelines for Exposure Related Measurements.* Federal Register (53) 48830. Washington, DC: Government Printing Office..

U.S. Environmental Protection Agency. 1988b. *Superfund Exposure Assessment Manual.* EPA/540/1-88/001. Washington, DC: U.S. Environmental Protection Agency, Office of Emergency and Remedial Response.

U.S. Environmental Protection Agency. 1989a. *Risk Assessment Guidance for Superfund, Volume 1 Human Health Evaluation Manual (Part A).* EPA/540/1-89/002. Washington, DC: U.S. Environmental Protection Agency, Office of Emergency and Remedial Response.

U.S. Environmental Protection Agency. 1989b. *Exposure Factors Handbook.* EPA/600/8-89/002. Washington, DC: U.S. Environmental Protection Agency, Office of Health and Environmental Assessment.

U.S. Environmental Protection Agency. 1989c. *Exposure Assessment Methods Handbook (draft).* Washington, DC: U.S. Environmental Protection Agency, Office of Health and Environmental Assessment.

U.S. Environmental Protection Agency. 1992. *User's Guide for CAP88-PC, Version 1.0.* 402–B–92–001. Las Vegas, NV: U.S. Environmental Protection Agency.

U.S. Environmental Protection Agency. 1993a. *Risk Management Program for Chemical Accidental Release Prevention.* Washington, DC: U.S. Environmental Protection Agency.

U.S. Environmental Protection Agency. 1993b. *Integrated Risk Information System (IRIS).* Washington, DC: U.S. Environmental Protection Agency.

Vaurio, J. 1994. Estimation of common cause failure rates based on uncertain event data. *Risk Analysis* 14: 4.

Vesely, W., F. Goldberg, N. Roberts, and D. Haasl. 1981. *Fault Tree Handbook.* Washington, DC: Nuclear Regulatory Commission , Office of Nuclear Regulatory Research.

Wheelis, W. 1986. *User's Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base.* NUREG/CR–4586. Albuquerque, NM: Sandia National Laboratory.

Whelan, G., et al. 1992. Overview of the multimedia environmental pollutant assessment system (MEPAS). *Hazardous Waste & Hazardous Materials* 9(7).

Winkler, R.L. 1968. The consensus of subjective probability distributions. *Management Science* 15.

Winkler, R.L., and W.L. Hays. 1975. *Statistics: Probability, Inference, and Decision.* 2nd Edition. New York, NY: Holt, Rinehart & Winston.

Woodard, K., and T. Potter. 1979. *Modification of the Reactor Safety Study Consequence Computer Code (CRAC) to Incorporate Plume Trajectories.* Transactions of the American Nuclear Society, Vol. 33. La Grange Park, IL: American Nuclear Society.