NUREG-1050

Probabilistic Risk Assessment (PRA) Reference Document

Final Report

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

NOTICE

Availability or Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555

2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances.*

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

GPO Printed copy price: $6.50

NUREG-1050

Probabilistic Risk Assessment (PRA) Reference Document

Final Report

Manuscript Completed: August 1984
Date Published: September 1984

Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ABSTRACT

This document describes the current status of probabilistic risk assessment (PRA) as practiced in the nuclear reactor regulatory process. The PRA studies that have been completed or are under way are reviewed. The levels of maturity of the methodologies used in a PRA are discussed. Insights derived from PRAs are listed. The potential uses of PRA results for regulatory purposes are discussed. This document was issued for comment in February 1984 entitled "Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application." The comments received on the draft have been considered for this final version of the report.

CONTENTS

CONTENTS (Continued)

ILLUSTRATIONS

TABLES

PREFACE

The Nuclear Regulatory Commission (NRC) is faced with many types of decisions in discharging its legal responsibilities for the regulation of nuclear power plants. These may be summarized as follows:

1. How safe should plants be?

2. How safe are they?

3. Does the safety of plants need to be improved?

4. How should the desired level of safety be ensured during the lifetime of the plant?

5. Can the regulatory process be better focused to improve the regulation of plants?

6. What issues require research to improve the state of knowledge and enhance effective regulation?

The first question involves sociopolitical considerations. In the past, the determination of appropriate levels of safety has been largely qualitative, based on judgment. Quantitative safety levels would also be inherent in any safety goals that might be implemented by the NRC in the future. This document does not address the first question, except for the role that probabilistic risk assessment (PRA) would play in the implementation of any quantitative safety goals.

The central aim of this document is to evaluate the level of PRA development to determine how this analytical tool should be used in regulation as an aid to answering questions two through six, as well as to assess the likelihood that more research will improve the usefulness of PRA.

The probabilistic methods used in PRA cover a wide range of technical disciplines, from statistics to human-behavior sciences. Deciding how PRA should be applied by the NRC to regulatory issues requires an understanding of the existing information base and a knowledge of the methods used in performing a PRA. Therefore, this document provides an overview of the level of development attained by the various elements of PRA, the uncertainties in PRA that confront the regulatory decisionmaker, and the research under way to improve the methods, reduce the uncertainties, and allow more effective decisionmaking in the face of remaining uncertainties.

Historically, answers to safety questions have been based on conservative deterministic techniques, and the regulation of safety has relied on defense in depth. Much of the regulatory conservatism arises from a healthy caution generated by the uncertainty associated with the current knowledge of phenomenology and of plant response to accidents and transients. PRAs generate many insights to aid the decisionmaker, which derive from a realistic integral view of plant design and operation. Although PRAs suffer from the same substantial uncertainties as do deterministic analyses, they attempt to address them more explicitly, add discipline to the evaluation of the operation of a plant, and result in a more complete understanding of risk-important systems and functions, interactions among systems, and the importance of human actions.

Uncertainties must be considered carefully before a decision is reached. The fact that PRAs provide a mechanism for displaying areas of uncertainty (more so than do conventional deterministic analyses) is actually a strength of PRA rather than evidence of a weakness in PRA methods. The weakness that must be guarded against is the tendency to take the PRA best estimates of risk, core-melt frequency, or system unavailability as givens without considering the uncertainties associated with these estimates. One of the principal advantages of PRA is the potential for providing additional qualitative and quantitative perspectives on the overall importance of uncertainties. Proper consideration of these uncertainties can enhance engineering judgment.

Insights into plant design and operation are among the most important results of PRAs. Important insights were gained from the first large-scale PRA performed in the United States -- the Reactor Safety Study (RSS) revealed, for example, that small-break loss-of-coolant accidents (LOCAs) and transients, rather than the large LOCA, are the principal contributors to risk. Since the RSS, PRA has become a widely used discipline, practiced by both the NRC and the nuclear industry. It touches a wide range of issues and decisions.

The growing library of PRAs provides a rich information base of risk and reliability insights that are relevant to the NRC mission, but these insights have not been published in a comprehensive way. This document distills this information and provides an overall perspective of the insights that PRAs have provided.

This document is timely. It marks the end of a decade since the RSS was published and comes at a time when the use of PRA to illuminate engineering judgment is becoming widespread. There is increasing use of PRAs in regulation in such applications as the resolution of most unresolved safety issues, the assignment of priorities to generic safety issues, and the consideration of the broad issue of severe core damage. Thus, now is the proper time to pause and delineate carefully the role that the assessment of risk and reliability should play in the evaluation of reactor safety and in regulatory decisions.

ACKNOWLEDGMENTS

Preparing this reference document on probabilistic risk assessment (PRA) has been a challenge. The state of the art of PRA, insights gained from the results of PRAs to date, and the appropriate uses of PRA in the regulation of nuclear power are complex and controversial subjects. It is to the credit of all who participated in writing this document that substantive consensus was achieved.

Principal credit goes to Joseph A. Murphy, whose technical guidance and long hours of dedicated labor made this document possible. However, essentially equal credit must go to the other contributing writers, as follows:

David C. Aldrich, Sandia National Laboratories
Allan S. Benjamin, Sandia National Laboratories
Robert J. Budnitz, Future Resources Associates, Inc.
Jack W. Hickman, Sandia National Laboratories
Vojin Joksimovich, NUS Corporation
William E. Vesely, Battelle Columbus Laboratories
Jonathan Young, Energy, Inc.

Please note that the word "authors" is not used. The effort was truly cooperative, with substantial criticisms and revisions of each individual's contributions resulting in an amalgamation of knowledge and viewpoints and a higher quality document than would have otherwise been possible.

Credit is also due to Richard Denning, Battelle's Columbus Laboratories, and Daniel Alpert, Sandia National Laboratories, for their valuable input in the area of accident phenomena and consequence analysis, to Roger Breeding, Energy, Inc., for his contribution to the discussion of the level of development of PRA; and to the many people in the NRC who read and commented upon various drafts of this document.

Last, but certainly not least, credit must be given to Pamela S. Bloomfield, Pamela L. Foust, and Sheri Hichar for their untiring effort in preparing drafts on a very short time schedule; and to Ausra M. Richards for her competent performance as technical editor. Without their work, the effort would have gone for naught.

A draft of this document was issued for comment and was the subject of a peer review NRC workshop held on February 22-23, 1984. Chairmen of the two panels of the workshop were Dr. Herbert J. C. Kouts, Brookhaven National Laboratory, and Dr. Norman C. Rasmussen, Massachusetts Institute of Technology. Panelists were knowledgeable persons in government, the nuclear industry, public interest organizations, and academia, as well as consultants and contractors expert in

the performance of PRAs. This final version of this report reflects the comments received at the workshop and from the public. The final step in the peer-review process will be an independent review of the final document by the National Science Foundation, to start in the summer of 1984.

Malcolm L. Ernst, Deputy Director
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research

EXECUTIVE SUMMARY

This is an executive summary of the important conclusions of the report. This summary is in the form of listings of the more important findings. Since there are important exceptions and nuances difficult to portray in such a summary, the reader is strongly urged to read both the individual chapters for more detailed findings and supporting rationale, and the appendixes for a fuller understanding of the technical bases.

What Is PRA?

PRA is an analysis that: (1) identifies and delineates the combinations of events that, if they occur, will lead to a severe accident (i.e., severe core damage or core melt) or any other undesired event; (2) estimates the frequency of occurrence for each combination; and (3) estimates the consequences. As practiced in the field of nuclear power, PRAs focus on core-melt accidents, since they pose the greatest potential risk to the public. The PRA integrates into a uniform methodology the relevant information about plant design, operating practices, operating history, component reliability, human actions, the physical progression of core-melt accidents, and potential environmental and health effects, usually in as realistic a manner as possible.

What Is The State of Development of PRA?

- Qualitative systems analysis (logic modeling) for internal accident initiators has reached a relatively high level of development, where development is defined as the degree of confidence that changes in the state of knowledge will not result in substantial changes in the major insights drawn from PRAs. Therefore, a relatively high degree of confidence can be placed in the qualitative insights drawn with regard to dominant accident sequences from internal events and their more important contributors. One area where improvement is needed is the modeling of common-cause failures.

- Qualitative systems analysis for external accident initiators (seismic, fire, flood) has reached a medium level of development, which means that a fair degree of confidence can be placed in the qualitative insights drawn with regard to dominant accident sequences from external events and their more important contributors. Again, the modeling of common-cause failures needs to be improved for all initiators.

- Advances have been made in the modeling of human performance, and the likelhood of operator errors generally can be quantified to order-of-magnitude precision, particularly those errors which arise from failure to follow written procedures. However, the quantification of errors of misdiagnosis and potential recovery actions to terminate an accident sequence has substantial uncertainty and needs improvement.

- The data base is fairly good for events of high frequency,* but poor for events of low frequency, such as failures of very reliable systems (e.g., the reactor protection system), the occurrence of high-magnitude seismic events, or the occurrence of common-cause failures. This means that internally initiated accidents normally can be quantified with a fair degree of confidence, but normally one has only poor confidence in the quantification of externally initiated accidents because the results tend to be dominated by low-frequency initiators. It is not likely that the data base for low-frequency events will improve appreciably in the near future.

- Estimates of source terms are currently made with poor confidence, principally because of lack of knowledge regarding the phenomena of core-melt progression, radionuclide transport inside the reactor coolant system and the containment, and containment performance. Extensive research is under way which should result in substantially improving the state of knowledge of the phenomenology of core melt, radionuclide transport, and the resultant containment loadings and response. However, uncertainties will likely remain quite large.

- The calculation of consequences, given a source term and the meteorology, can be performed with reasonably high confidence. However, there is still a stochastic uncertainty associated with the actual meteorology at the time of a major radiological release, which means that the actual consequences as a function of location away from the site cannot be predicted with much precision prior to an accident. Also, the actual behavior of the affected population during emergency actions (sheltering, evacuation) is not well understood.

---

*As used herein, high-frequency events are those which are often observed in plant operation. Low-frequency events are those rarely observed, having a return frequency less than once in 1000 reactor-years.

What Are The Principal Conclusions Regarding Uncertainties?

- Uncertainties in estimating core-melt frequency due to internal initiators are generally reported to be an order of magnitude or less above and below the best estimate. However, these estimates may not include the effects of modeling assumptions.
- Uncertainties in estimating core-melt frequency due to external initiators currently are generally about a factor of 10 to 30 above and below the best estimate.
- Uncertainties in estimates of the source term presently are very large but have not been well analyzed in PRAs.
- Uncertainties in mean early fatalities, given a large source term, could range from about a factor of 5 above the best estimate to nearly zero, in large part due to assumptions made about emergency actions taken, including evacuation.
- Uncertainties in mean population dose, given a source term, would lie within a factor of 3 or 4 of the best estimate, while uncertainties in estimates of latent cancer deaths could be approximately a factor of 10 above and below the best estimate.
- There is some question whether the statistical techniques employed in PRAs have been implemented properly, particularly in assigning probability distributions to parameters based on limited data.
- Completeness does not seem to be the principal limitation when examining the general insights gained from a PRA on dominant sequences, since the data base is large enough so that a rare and unusual type of failure likely would not affect the conclusions regarding dominant sequences. However, from time to time some issues (e.g., pressurized thermal shock) will warrant regulatory attention even though they had not previously been considered important from either a probabilistic or a deterministic perspective.
- Design and construction errors should already be part of the data base for higher-frequency events and thus would be inherently included in a PRA. However, such errors for low-frequency events probably would not be in the data base. It is unclear what uncertainties this would imply for the PRA estimates.

- PRAs could be made more reproducible from one analyst to the next by specifying the data, modeling, success/failure assumptions, and phenomenology to be used. However, even under such circumstances, differences of a factor of 3 or more between analysts in estimates of core-melt frequency would not be surprising.

- One method for propagating data uncertainties (the Bayesian approach) is reasonably well developed. Approaches based on classical statistics need to be explored. More work needs to be done on propagating knowledge uncertainties (e.g., phenomena), and uncertainty and sensitivity analyses need to be more widely used and better organized and displayed to assure that users of PRA information are better informed as to the important uncertainties.

<u>To What Extent Have PRA Results Been Validated?</u>

- The frequency estimated for severe core-damage accidents is usually low (on the order of once in 10,000 reactor-years). It is not possible to validate the results directly because sufficient data does not exist. Therefore, it is necessary to attempt to validate as many of the constituent parts of the PRA as possible.

- Plant-specific design or operational features can have an important influence on dominant accident sequences; therefore, a generic validation of results is difficult.

- Estimates of accident-initiator frequency are reasonably well validated by plant data for those events which occur relatively often.

- To some extent, failure-rate estimates have been validated, particularly for active components.

- Some validation of computer codes has occurred, mainly through benchmark comparisons. Much remains to be accomplished in this area.

- The validation level of a PRA is not thorough or detailed; however, this level of validation is usually not much worse than the degree of validation achieved by alternative analytical tools.

<u>Does Operating Experience Reasonably Conform To The Results of PRAs?</u>

- Transient information and failure data are used as input to the PRAs. Transient information is reasonably reliable; however, the data base for equipment and human failures needs improvement.

- The initial results of the accident precursor program being conducted by the Office of Nuclear Regulatory Research, NRC, indicate a fair degree of agreement (order of magnitude) with PRA results relative to the estimated likelihood of core melt as well as to the major accident contributors.

Can Generic Insights Be Drawn From PRAs?

- Generic insights can be drawn from PRA with regard to aspects of design and operations important to the dominant accident sequences. However, plant-specific features could be of significant importance to the estimation of core-melt frequency or risk.

- The degree to which generic insights can be relied upon in regulation depends on the regulatory use and the specific safety issue under consideration.

What Are The Major Insights That Have Been Drawn From Present PRAs?

Note: Only global insights are provided below. The reader is referred to Chapter 3 and Appendix B for more detailed insights.

- The process of performing PRA studies yields extremely valuable engineering and operational insights regarding the integrated safety performance of nuclear power plants.

- The estimated frequency of core melt is higher than had been thought prior to performing the Reactor Safety Study; however, most core melts are not expected to result in large offsite radiological consequences.

- The range of core-melt frequency point estimates in U.S. PRAs published to date covers about two orders of magnitude (about 10^{-5} to 10^{-3} per reactor-year). It is extremely difficult to pinpoint generic reasons for the difference.

- The specific features of dominant accident sequences and the estimates of risk vary significantly from plant to plant, even though plants meet all applicable NRC regulatory requirements.

- Estimates of early fatalities and injuries are very sensitive to source-term magnitudes, and a major factor in the estimate of source-term magnitude is the timing of containment failure (early or late compared to core melt). With large source terms, they are sensitive to emergency response assumptions, but this dependence decreases in importance if source terms are reduced.

- Estimates of latent cancer fatalities are sensitive to source-term magnitudes, but site-to-site differences are relatively small for a given source term.

- Estimated onsite economic losses resulting from a core-melt accident are generally much larger than estimated offsite economic losses.

- Generally, airborne radiological pathways are much more important to risk than liquid pathways.

- Accidents beyond the design basis (such as those caused by earthquakes more severe than the safe-shutdown earthquake) are the principal contributors to public risk.

- Small LOCAs and transients are usually dominant contributors to estimated core-melt frequency and risk, while large LOCAs usually are not.

- Dominant contributors to risk are not necessarily the same accident sequences as the dominant contributors to core-melt frequency.

- Human interactions, including test and maintenance considerations, are extremely important contributors to the safety of plants.

- Common-cause (dependent) failures are important contributors to estimates of core-melt frequency and plant risk.

- Earthquakes, internal fires, and floods seem to play an important role in estimates of core-melt frequency and plant risk, although this tentative conclusion appears to be highly plant specific.

- The failure of long-term decay heat removal is a major functional contributor to estimated core-melt frequency.

- The reliability of systems, components, and human actions important to safety must be maintained during operation. Degradation in their reliability can sharply increase risk or the likelihood of core melt.

<u>What Is The Usefulness of PRA In The Regulation of Nuclear Power Plants?</u>

- PRA results are useful, provided that more weight is given to the qualitative and relative insights regarding design and operations, rather than the precise absolute magnitude of the numbers generated.

- It must be remembered that most of the uncertainties associated with an issue are inherent to the issue itself rather than artifacts of the PRA analysis. The PRA does tend to identify and highlight these uncertainties, however.

- PRA results have useful application in the prioritization of regulatory activities, development of generic regulatory positions on potential safety issues, and the assessment of plant-specific issues. The degree of usefulness depends on the regulatory application as well as the nature of the specific issue, and the reader is referred to Chapter 2 for more detail and specific examples.

- PRAs are not very useful from a quantitative standpoint for some issues. However, PRAs can still provide useful regulatory insights even for these issues. For example, the risk from sabotage is difficult to quantify due to uncertainty in the frequency of attempted acts and the nature of and likelihood of success for sabotage attempts; however, PRA methods can still provide good qualitative insights with regard to important (vital) plant areas and weaknesses.

- The need for plant-specific PRAs depends on the intended application. Most regulatory uses would not be dependent on the availability of a plant-specific PRA.

- The basic attributes of a PRA are not highly compatible with a safety-goal structure that would require strict numerical compliance on the basis of the quantitative best estimates of a PRA. However, there could be useful application if the structure were less strict or the goals were set so conservatively that there would be little regulatory concern if the actual value substantially exceeded those goals.

- The results of a PRA should only be one consideration in regulatory decisions, i.e., they should not replace other conventional considerations. When assessing the weight to be given to PRAs in a decision, one should consider:

  - The scope and depth of the PRA (i.e., does the nature of the PRA reasonably match the needs of the decision);

  - The degree of realism embodied in the PRA;

  - The results of peer reviews, which could add to or subtract from the credibility of the PRA results;

  - The credibility of qualitative insights obtained from the study;

- The quantitative results of the PRA compared to desired safety levels, and the uncertainty bounds surrounding the PRA analyses;

- The uncertainties associated with the issue, considering both the regulatory benefits of uncertainty reduction and the desired degree of regulatory conservatism;

- The results of sensitivity studies that show the risk or core-melt-frequency importance of the major uncertainties; and

- The values and impacts of alternative regulatory actions.

PROBABILISTIC RISK ASSESSMENT (PRA) REFERENCE DOCUMENT

1. INTRODUCTION

In the plan to evaluate the NRC's Safety Goal Policy Statement (issued for comment NUREG-0880, Revision 1, dated May 1983), the Office of Nuclear Regulatory Research was directed "to collect available information on PRA studies concerning the risks of plants licensed in the U.S. It is essential that a reference document be prepared and receive peer review so that the staff, licensees, and public have a common base of information on the dominant contributors to the probability of core melt and to the public risk due to radiation from serious nuclear accidents, the strengths and weaknesses of current plant designs and operations, and the usefulness of PRA and the safety goals in assessing such strengths and weaknesses." This report, presenting the current state of the art of PRA and guidance for its potential uses in the regulatory process, has been prepared in response to that directive.

This document discusses the purpose and content of a PRA and the level of development of, and the uncertainties associated with, the various elements of PRA methodology (Chapter 1). With this information as a base, the report next discusses (Chapter 2) potential uses of PRA in regulation, whether or not used in conjunction with safety goals, and presents important considerations in using the results of PRAs in decisionmaking. Chapter 3 identifies the studies and discusses the results obtained from the PRAs performed to date, as well as several other special studies of limited issues. Generic insights can be derived from the studies of limited issues and from the studies of dominant accident sequences and the systems, functions, and human actions found to be important from the perspective of core damage or risk; and insights can also be gained relative to areas amenable to improvement and to means for preventing the degradation of plant safety with time.

The three appendixes provide extended coverage of the material contained in Chapters 1 and 3 and a description of probabilistic studies of limited scope that have been performed on a number of technical issues. These appendixes are written in jargon familiar to the PRA practitioner and are designed to provide technical credibility to the document. To improve the readability, most of the detailed references were omitted from the chapters, but they are provided in the appendixes.

The state of knowledge necessary for performing certain steps of a PRA is rapidly evolving. For example, progress has been made in the understanding of (1) the phenomenology associated with severe core-damage accidents, including accident progression; (2) radionuclide behavior in the fuel, the reactor-coolant system, and the containment; and (3) the performance of the containment under the varied temperature and pressure conditions that can occur in severe core-damage accidents. Research in these areas is being conducted by both government and industry, and it is reasonable to expect better understanding of the phenomena in the future. As some of the uncertainties are narrowed and estimates are improved, the insights and recommendations provided herein may also change. Thus, updates of the information presented here may be desirable from time to time as the state of the art progresses.

1.1 Description of PRA

Probabilistic risk assessment (PRA) is an analysis process that quantifies the likelihood and consequences of the potential outcomes of postulated events. As practiced in the nuclear power field, PRA has focused on events that have the potential to result in reactor core damage and subsequent impact on public health and safety. The combination of likelihood and consequences is referred to as a measure of risk.

The methods used in PRAs have also been applied to selected issues such as system reliability for single systems, station blackout, or containment response. In most of these cases, the "consequences" of interest are defined, and the measure used is the likelihood of the various events leading to the consequence of concern.

The objective of PRA is to identify and delineate the combinations of events that, if they occurred, could lead to undesirable public consequences and to estimate the magnitude of those consequences and their respective probabilities. Relevant information about plant design, operating practices, operating history, component reliability, human reliability, accident processes, and potential environmental and health effects is processed through various analytical models to obtain an estimate of plant safety. A PRA uses both logic models depicting combinations of events that could result in core damage or core melt and physical models depicting the progression of accidents and the transport of radionuclides from the reactor core to the environment. The models are evaluated probabilistically to provide both qualitative and quantitative insights about the level of risk and to identify the design, site, or operational characteristics that are the most important to risk.

1.1.1 PRA Study Process

A PRA is a multidisciplinary study involving a team of individuals with differing expertise. The major steps in the analysis are shown in Figure 1. The analysis involves

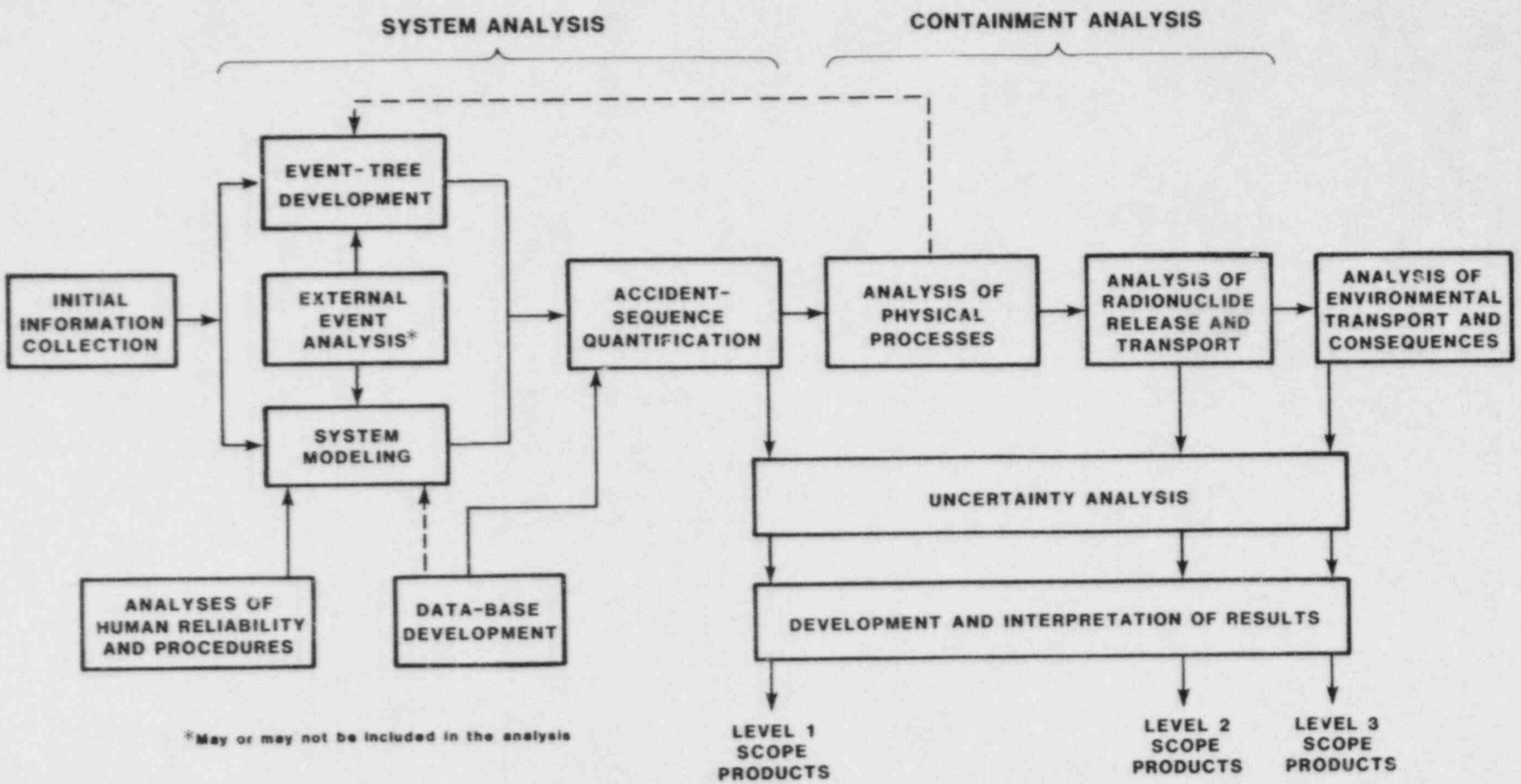


Figure 1. Risk Assessment Procedure

developing a set of possible accident sequences and estimating their outcomes. To this end, various models are used, and a great deal of data is analyzed. Depending on the scope and the objectives of the study, the models may treat plant systems, the response of the containment, radionuclide transport, and offsite consequences.

Plant-system models generally consist of event trees and fault trees. Event trees delineate initiating events and combinations of system successes and failures, while fault trees depict ways in which the system failures represented in the event trees can occur. These models are analyzed to estimate the frequency of each accident sequence.

Several different models are required to represent the events that occur during the accident but before the release of radioactive material from the containment. They cover the physical processes induced by each accident sequence in the core, the reactor-coolant system, and the containment as well as the transport and deposition of radionuclides inside the containment. The analysis examines the response of the containment to these processes, including possible failure modes, and evaluates the potential for the releases of radionuclides to the environment.

The offsite consequences of the accident, in terms of public-health effects and economic losses, are estimated by means of environmental transport and consequence models. These models use meteorological data (and sometimes topographic data as well) to assess the transport of radionuclides from the site. Local demographic data and health-effects models are then used to calculate the consequences to the surrounding population.

An integral part of the PRA process is an uncertainty analysis. Uncertainties in the data and uncertainties arising from modeling assumptions are propagated through the analysis to estimate the uncertainties in the PRA results. The uncertainty ranges that were estimated for core-melt frequencies and risks in past PRAs included, with very few exceptions, those due to uncertainties in the data (i.e., those due to imprecisions in statistical estimation), uncertainties in data extrapolation, and unit-to-unit variations. In earlier studies, uncertainties attributable to modeling and assumptions were usually not included in the PRA uncertainty analyses; sometimes, however, their impacts were considered separately in sensitivity analyses, to some extent. Many of the later studies include subjective estimates of the uncertainty contribution due to modeling assumptions.

The results of the risk assessment are analyzed and interpreted to identify the plant features and operational practices that are the most significant contributors to the frequency of core melt and to risk. They can also be used to generate a variety of qualitative information on the events and failures associated with various consequences. Throughout the analysis, realistic assumptions and criteria should be used. When information is lacking or controversy exists, it may be necessary to introduce conservatisms or to evaluate bounds, but the goal of a PRA study is to perform an analysis that is as realistic as possible.

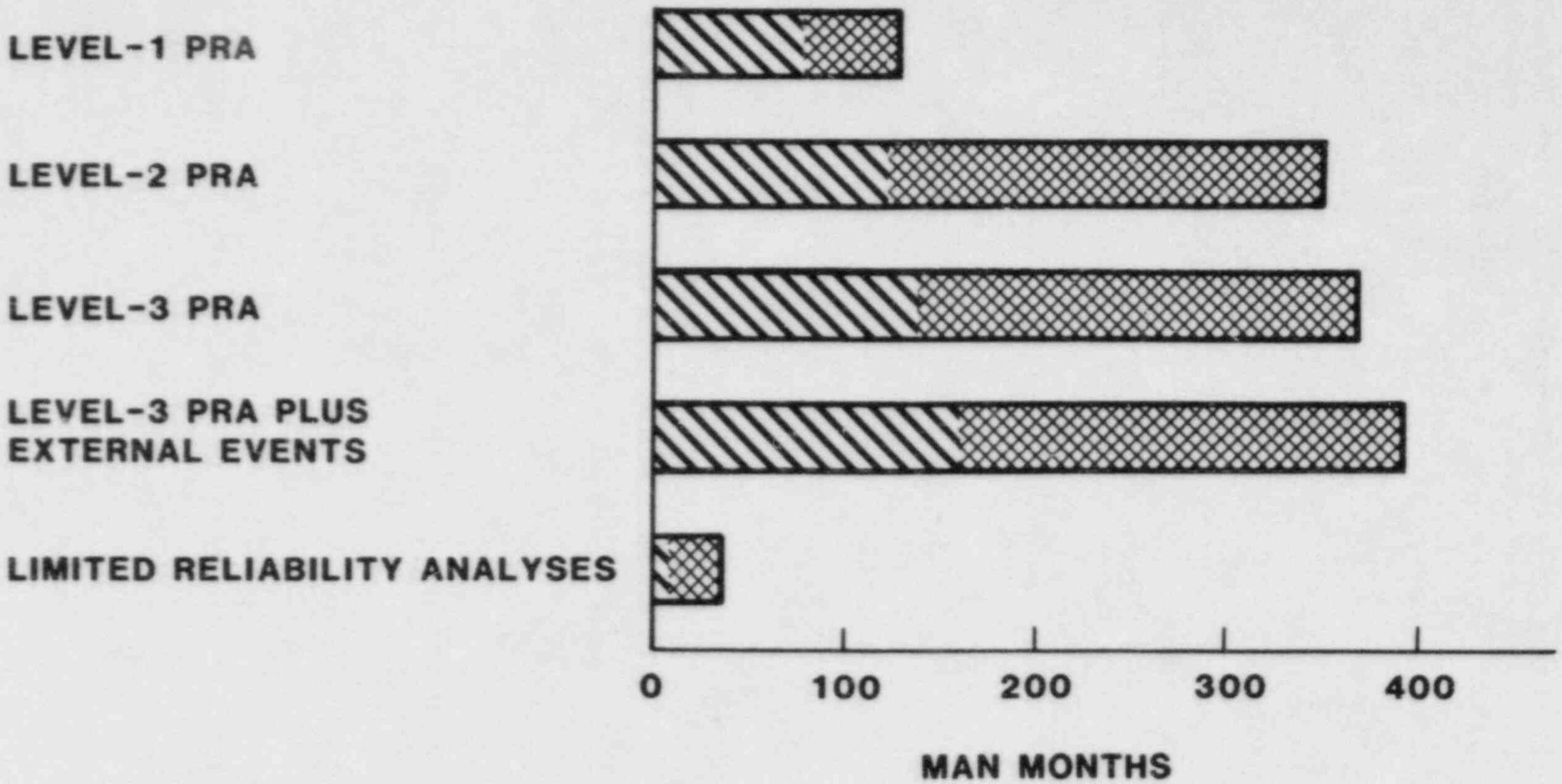
1.1.2 Levels of Scope in PRA Studies

The scope of PRA studies varies considerably, depending on the objective. The most common objective is the estimation of core-melt frequency. The PRA Procedures Guide (NUREG/CR-2300) termed this a level 1 PRA, which consists of an assessment of plant design and operation, emphasizing sequences that could lead to a core melt. External events, such as floods or earthquakes, may or may not be included. The result is a list of the most probable core-melt sequences, their frequencies, and insights into their causes. Such a scope provides an assessment of plant safety and of the adequacy of plant design and operating procedures from the perspective of preventing core melt, but it does not permit an assessment of containment response or the public risk associated with the plant.

In addition to the analyses performed in a level 1 PRA, a level 2 PRA analyzes the physical and chemical phenomena of the accident, the response of the containment, and the transport and release of radionuclides from the core to the environment. This type of study does not provide an assessment of public risk, because offsite consequences are not assessed. It does, however, provide insights into this risk by generating the frequencies and magnitudes of the release categories. (Release categories are defined in order to group together accident sequences that result in similar releases of radionuclides from the containment.)

A level 3 PRA analyzes the transport of radionuclides in the environment and assesses the public-health and economic consequences of accidents in addition to performing the analyses of levels 1 and 2. Thus, a level 3 study provides an assessment of public risks.

The level of effort varies with the scope and the depth of the analysis. As can be seen from past experience in Figure 2, the largest variability in effort lies in a level 2 analysis. It seems reasonable to expect that the efforts expended in this area will diminish significantly in the future as ongoing research on accident phenomena and source terms is completed.



NOTE: DATA TAKEN FROM PRA PROCEDURES GUIDE (NUREG/CR-2300): LEVELS 1, 2 AND 3 ARE DEFINED IN THE PRA PROCEDURES GUIDE. CROSS-HATCHING INDICATES RANGE OF ESTIMATE.

Figure 2. Level of Effort Required

1.1.3 Utility of PRA Information for Decisionmaking

Decisions regarding the safety of nuclear plants have been based on a general acceptance of a set of generic engineering practices, regulatory requirements, and specific design and operational features for each plant. These decisions have included a de facto expression of an acceptable level of safety for each plant; the issuance of a license to operate a plant is predicated on a finding that there is no undue risk to the health and safety of the public. This implies that if the design and operation comply with all the applicable regulations and design criteria, the plant is safe enough.

This approach to safety results in a large set of design criteria and operational requirements without any distinction as to their relative importance. However, in practice some decisions are made regarding which criteria or issues receive more emphasis than others. The basis for these judgments is a mixture of plant experience, engineering judgment, and present policy.

Within the context of current design and regulatory practice, both the PRA process and the specific results provide additional information that can aid in making decisions regarding

- Compliance of plant design and operation with the intent of criteria
- Allocation of resources to specific safety issues
- Acceptable levels of safety

Probabilistic risk assessment treats the entire nuclear plant and its constituent systems in an integrated fashion that cuts across traditional lines separating the various design and operational disciplines. Therefore, PRA shows how systems interact during failure conditions and whether the overall intent of the design is still met. For example, PRA can show whether the single-failure criterion is satisfied when all the subsystems and supporting systems of the emergency core-cooling system (ECCS) are considered, such as emergency power, service water, heating, ventilating, air conditioning, and instrument air.

Because it "propagates" faults across design interfaces or boundaries, PRA introduces quantitative safety indices to the consideration of plant safety. These indices include quantitative statements of the likelihood and consequences of postulated accidents. Furthermore, PRA develops quantitative likelihood measures for the various contributors to an accident (e.g., initiating events, component failures, and human errors). These quantitative indices can provide useful information in the decision process.

When resources are to be allocated among issues, the PRA results can provide measures of importance, such as the relative expected frequencies of system failure or the relative estimated frequency and offsite consequences of the sequences involving the failure of a particular safety function. Furthermore, the quantitative measures developed in PRA studies for plants already accepted as safe enough by standard regulatory practice can provide an indication of an acceptable level of safety.

Although PRA provides very useful qualitative and quantitative information, the accuracy and the robustness of that information are in fact limited by our overall state of knowledge. PRA is only a method for collecting and treating the body of knowledge we have amassed. This knowledge is expressed in accumulations of data and in models of system behavior and of physical and chemical processes. Any set of PRA results, therefore, will reflect the incompleteness and inherent variability of the data base, as well as the limitations and simplifications of the modeling procedure that result from our state of knowledge.

However, a very important attribute of the PRA method is that it can measure the effects of the limitations in knowledge on the results. This measurement is done by uncertainty analysis for the lack of experience that is inherent in the data base, and by sensitivity analyses for shortcomings in the models. PRA techniques can also bound the quantitative measures estimated by considering the statistical uncertainties in the input data. These bounds indicate to the decision-maker whether different numerical results represent significant differences in the perceived level of safety.

Sensitivity analyses provide the means by which to examine the impact of changes in understanding or assumptions. The impact of changes in a particular model is determined by comparing the PRA results with and without the changes. In this way, the PRA can illustrate the significance of a difference of opinion regarding the degree of realism inherent in a model or the correctness of a certain mathematical representation of a physical process. Sensitivity analyses also provide information that is useful in judging the credibility of the PRA results in a particular context.

It is important to recognize that uncertainties and needs for improvements in the state of knowledge are not unique to PRA; they reflect a lack of data or experience or a lack of knowledge about system response, human behavior, or accident phenomena. These uncertainties are present in estimates made by means of PRA techniques, deterministic modeling, or so-called engineering judgment. They reflect current experience and knowledge, and the state of the overall technology. PRA analyses, however, usually display uncertainties more explicitly than do other analytical approaches, even though the extent of the uncertainty is the same in all cases.

Displaying the uncertainties provides important information to the decisionmaker. A proper uncertainty analysis can provide an estimate of how this lack of experience and/or knowledge affects engineering insights drawn from PRA. This is done by propagating uncertainties through the analysis or by performing sensitivity analyses. Thus, the treatment of uncertainties should logically be considered a strength of PRA rather than a limitation.

The PRA results already available have expanded the body of information available to the decisionmaker.

Before discussing the regulatory uses of PRA in detail (in Chapter 2), it is useful to review briefly the historical development of PRA and its use in regulation and to discuss the current state of the art in PRA methods and applications, compared to regulatory needs.

1.2 Past and Present Practices

1.2.1 The Reactor Safety Study

The first comprehensive application of PRA techniques was the NRC-sponsored Reactor Safety Study (RSS), which is widely regarded as a piece of work that broke new ground in many areas. The RSS was the first broad-scale application of event- and fault-tree methods to a system as complex as a nuclear power plant. Its principal objective was to reach some meaningful conclusions about the risks of U.S. commercial nuclear power plants.

For various reasons, the RSS report became one of the more controversial documents in the history of reactor safety. The impact of the controversy was demonstrated by the NRC's reaction to the Lewis report (NUREG/CR-0400). The Commissioners asked the NRC staff to document where, if anywhere, they had relied on RSS results or insights in the years since its publication in 1975. The staff responded by producing a rather voluminous report outlining essentially every regulatory action in which the RSS had been cited, including letters to licensee representatives, hearing testimony, and more formal safety reports and decisions. The staff document, produced in early 1979 just before the accident at Three Mile Island (TMI), exemplifies what the Lewis Committee called the "siege mentality." The staff concluded that, with only one or two exceptions, no RSS insights or results had been used as a substantive part of any staff decisions or actions. However, RSS results or methods were applied on a few occasions shortly after its publication, and these applications were important.

One was the technical basis for the revised emergency planning guidelines of the "Emergency Planning Task Force" report, in which RSS results provided the basis for the 10- and 50-mile emergency planning zones for plume and ingestion exposures. Another was the assignment of risk-based priorities to the "unresolved generic safety issues." A third important application was the analysis of the anticipated transient without scram (ATWS) issue.

1.2.2 Developments after TMI

The TMI accident revealed that perhaps reactors were not "safe enough," that the regulatory system had some significant problems (as cited in both the Kemeny and Rogovin investigations), that the probability of serious accidents was not vanishingly small, and that new approaches were needed. Suddenly, the potential value of PRA as a regulatory tool--and of the insights of the RSS itself--became apparent to the reactor-safety community.

People observed that the RSS had found transients, small loss-of-coolant accidents (LOCAs), and human factors to be dominant contributors to the overall risk and that the TMI accident sequence contained all three of these. It became apparent that PRA methods could be used to allocate the limited resources available for the improvement of safety, provided this allocation was done with care (the Lewis Committee had recommended this only a year earlier). Most important, the reactor community understood that the concept of accident-sequence analysis, as an intellectual discipline separate from other (equally valid) approaches to reactor-safety analysis, provided insights that could not be obtained in any other way.

The initial applications of PRA methods in the aftermath of TMI were specifically directed at issues of high immediate concern. For example, PRA methods were used to study the reliability of auxiliary feedwater systems in pressurized-water reactors (PWRs). The studies revealed that the availability on demand of systems that fully met regulatory requirements ranged over two orders of magnitude, and some auxiliary feedwater systems, in which at least one train was thought to be fully independent of ac power, were discovered to lack that feature. As another example, PRA methods were used in the Rogovin Special Inquiry to study the phenomena involved in the TMI partial core degradation and the a priori likelihood of the TMI accident.

The methods and data bases of the RSS were used in the RSS Methods Applications Program (RSSMAP), which investigated four plants of newer design than those considered in the RSS. The analyses used a survey type of approach that was much less extensive than those in the original RSS, and they were only abbreviated level 2 studies. The RSSMAP began before TMI, but the results were not published until after TMI.

Soon thereafter, the NRC staff initiated the Interim Reliability Evaluation Program (IREP), a series of plant-reliability studies (level 1) that did not include external events but were intended to cover first one, then four other operating-reactor designs to develop methods for the efficient use of PRA to analyze other designs of operating reactors. These IREP studies were followed by full-scale utility-sponsored PRAs for four plants judged by the NRC to pose potentially large risks because of the high population densities near their sites (Limerick, Indian Point, Zion and Millstone 3), and for a fifth plant (Big Rock Point) to provide risk-related insights to assist in evaluating proposed regulatory requirements. These privately sponsored studies represented an important breakthrough because they were the first to be sponsored, managed, and directed by utilities. Since the initiation of these studies in 1979-1980, utilities have undertaken several other studies. In all, about 10 full-scope (level 3) PRAs have been completed under utility sponsorship. Sometimes the motivation was to prepare for possible new regulatory requirements, but sometimes the utility managements wanted to obtain PRA insights on their own merits.

1.2.3 Current Use of PRA in Regulation

The NRC is currently making extensive use of reactor risk assessment in the regulation of nuclear power plants. Risk assessment perspectives are being used in the prioritization of generic safety issues and reactor safety research subjects. They also provide important information in the development of technical solutions to unresolved safety issues, generic safety issues, and severe accident policy issues, and in the increasingly important value/impact analysis of proposed new requirements. These perspectives also are important for use in standard plant licensing, in environmental impact analyses of license applicants as required by the National Environmental Policy Act (NEPA), and in the safety evaluation of a wide variety of requests by licensees for exemptions from particular requirements. They will play a key role in the Integrated Safety Assessment Program, which is an outgrowth of the Systematic Evaluation Program (SEP). Examples of current applications are presented below.

Newly proposed generic safety issues are screened by their importance to the plant risk. This provides a technical basis with which to allocate staff resources to the technical resolution of safety issues, and also coordinates issue resolution. Estimates of the risk attached to the proposed issues, developed using PRA-based methods and insights, play a key role in priority evaluation and resource allocation.

PRA provides the central theme of the development of NRC policy concerning requirements to limit the risk posed by severe reactor accidents. The policy for the generic approval, by rulemaking, of new standard plant designs requires the applicant to employ risk-assessment techniques as a design tool, and to include a PRA in his license application. Near-term Construction Permit applicants must supply a PRA within two years of the granting of a construction permit, which includes consideration of alternative designs for core and containment heat-removal systems to enhance the safety of the plant in a cost-effective manner.

Many of the unresolved safety issues and generic safety issues under study or recently resolved by the staff have been analyzed with risk assessment techniques. The station blackout issue and the dc power issue were analyzed principally using PRA techniques. Risk perspectives were also employed in the analysis of ATWS and the reactor vessel thermal shock problem. Many other issues, among them systems interactions and decay-heat removal, are employing PRA methods or results.

The NRC employs PRA methods to assess the environmental impact of the severe-accident spectrum in environmental statements required under NEPA. Until recently, it was the practice of the NRC to employ accident likelihood estimates and release magnitudes drawn from a rebaselined version of the WASH-1400 results. These were then inserted into the CRAC code, a consequence analysis and risk evaluation code, together with site-specific parameters to develop the environmental analysis of severe accident risk. This is formally equivalent to studying a generic reactor at the particular site of interest. However, as more plant-specific PRA's are submitted, the staff practice may evolve toward the use of fully plant-specific PRA's for environmental statements.

Concern that reactors located in regions of particularly high population density might pose a disproportionate share of the societal risk has led the NRC to consider special provisions to mitigate severe reactor accidents at such plants. In each case where the PRA review has been completed, the PRA has identified a few alterations in plant design or operation that would be very effective in reducing the vulnerability of the plants to severe reactor accidents, and shown that expensive alterations to containment systems were not necessary.

Licensees are also requesting exemptions from specific requirements using PRA-based information. The leading example of this approach has been the PRA of Big Rock Point submitted by Consumers Power Company. Initially, the utility took this approach to avert the premature shutdown of the plant. They had calculated that full compliance with all the new requirements spawned by the accident at TMI would cost more than the plant could earn in its remaining years of power generation. Also, it was felt that many of the TMI action-plan items were poorly suited to a plant of the unique design of Big Rock Point. Consumers Power Company offered to perform a risk assessment of the plant, and to fix any prominent accident vulnerabilities revealed by the study, to the extent that their economic analysis indicated to be feasible. Such a risk-management program is looking increasingly attractive.

In summary, the NRC is using PRA methods and results in varying degrees in many generic regulatory applications and some plant-specific ones as well. The applications cover almost the whole technical spectrum of regulation, and many times the studies are of less scope than a level 1, 2, or 3 PRA. For information, Appendix C provides a more complete listing and discussion of the application of limited-scope probabilistic studies in the regulation of nuclear power plants.

1.3 The State of the Art in PRA Methods

It is important to recognize that the level of experience and understanding varies among the different parts of the PRA. Thus, the reliance placed on PRA insights should depend upon the strength of those areas of PRA used to obtain the insights. The different areas have each reached a different level of development, or state of the art. This section summarizes the state of the art for all the areas that make up a complete PRA; a more extensive discussion is contained in Appendix A.

1.3.1 Level of Development

A PRA study is multidisciplinary. Depending on its scope, a PRA may require analyses of plant systems, human behavior, the progression of core-melt accidents, radionuclide behavior, health effects, and seismic hazards. However, not all the areas of analysis involved have reached the same level of development. For example, the methods of reliability analysis have been used in some form since World War II, whereas the methods used for analyzing core-melt progression are new and unique to reactor technology.

The use of PRA in the regulatory process should consider what parts of the PRA exhibit the greatest strengths and what parts may be weaker. A particular area of analysis can be characterized by its degree of validity or realism, stability, and need for improvement.

The fact that improvement is needed in an area raises the related question of the feasibility of achieving significant progress in that area in the next few years.

The degree of validity or realism of a method refers to the extent that approximations or conservatisms may have been knowingly or unknowingly introduced. This may have been done because of insufficient knowledge or because of the need to simplify the model. Validity is a measure of how closely the model represents actual reality. In some cases, there is so little experience with the phenomena of interest that it is difficult to reach a definite conclusion on the validity of a model. The uncertainty associated with a result may reflect inherent variation in the data base, questions about the validity of the model, or both.

Stability is a measure of the rate of change of the analysis methods in an area. If no significant changes in the methods have appeared recently, and if the methods in use are generally accepted by most of the experts in the area, the analysis area may be termed stable. This implies a certain degree of reproducibility. That is, for a stable area, different analysts working separately on a given problem will produce comparable results by similar or equivalent methods. Note that stability does not necessarily imply validity. A method may be recognized as using quite imperfect models in certain areas, yet because of the complexity of the problem there has been little progress, so the method has remained stable. The recognized need for improvement in an area is an indication that there is not overall satisfaction with the methods, and this depends on our perceptions of the state of technology in that area. These perceptions are subject to change. For example, for several years after the RSS there was little dissatisfaction with, or interest in, the area of radionuclide release, transport, and deposition after severe core damage or melting. As a result of measurements made at TMI after the accident and ongoing research, it was recognized that some of the conservative assumptions might not be appropriate, and the need for improvement in this area changed accordingly.

1.3.2 System Analysis

System modeling in PRA studies is usually considered to have reached a high level of development. The degree of validity is fairly high, and recent improvements have mostly been in the areas of further automation and increased ability to treat large and complex systems. The areas needing the most improvement are human interactions and dependent failures. The data base is also weak in certain places. The techniques of fault trees and event trees have advanced considerably since their initial application in the RSS, and a variety of approaches to their use are available. The insights drawn from system modeling are generally quite solid, even though issues about the completeness of the analysis persist.

The treatment of the underlying assumptions in system analysis (e.g., success criteria, time dependences, thermal-hydraulics phenomena) is an unresolved issue. The transient-initiator data base has improved substantially, but improvements are still desirable in the failure-rate data base, since the ranges (and error factors) are quite broad for some important areas. Progress has been made recently in the collection and analysis of component data, but more is needed. Few analyses of LOCA initiators are available, and causal data are sparse. Thus, the overall understanding of the root causes of failure has not improved substantially. This also affects the ability to model dependent failures, and quantitative efforts in this area remain largely subjective. The improvements in data have not changed the insights gained from analyses very much. It is believed that the conservatisms and the simplifications in the modeling do not have a strong influence on these insights, either.

The modeling of human interactions introduces substantial uncertainty. This is particularly true of operator errors of commission and errors originating in misdiagnosis of accident conditions. However, even in the area of errors caused by failure to follow existing procedures, the uncertainties are of the same order of magnitude as those associated with component failure data. Progress has been made recently in this difficult area, and much more work is now under way. Within a few years, this aspect of system modeling is expected to become more systematic and the results more reproducible.

In summary, the whole area of PRA system modeling has advanced somewhat since the RSS, particularly in the area of initiating event-mitigating system interactions. The conclusions and insights it affords are usually reasonably sound, if appropriate consideration is given to the uncertainties and if great numerical accuracy is not required for the particular application. Most important, system modeling has provided insights about the relationships among systems, failures, and phenomena that could not have been obtained in any other way.

There continue to be rather large uncertainties in the <u>numerical</u> bottom-line results of PRAs (core-melt frequency, offsite risk) for a variety of reasons. One key reason is that, for some accident-sequence initiators, the likelihood of the initiator is so low that such events have rarely, if ever, happened. In such cases (examples of which include very large pipe breaks, large earthquakes, and failures of the reactor protection system function), the PRA analysis must rely on synthesized estimates that are difficult to perform and uncertain because of the lack of data associated with them. For other initiators (including the more common transients, the smaller earthquakes, and most fires), there is a valid data base that can be relied on in the analysis, and the uncertainties are smaller. It turns out that the numerical results of PRA are more reliable when the accident sequence quantification relies on combining several reasonably well-known rates and failure likelihoods; on the other hand, the results are somewhat less reliable when the key numerical inputs are synthesized from various analyses and extrapolations rather than taken from direct observed experience.

1.3.3 Accident Progression, Containment Response, and Radionuclide Transport

This area includes analyses of the thermal-hydraulic response of the plant to an accident, the progression of severe accidents, containment performance under severe accident loadings, and the characteristics of radionuclide releases to the environment (source terms) for accident sequences or groups of sequences. The analyses include a wide range of phenomena, some of which are not well understood.

In general, the validity of the analyses in these areas is low. In large part this is due to the lack of experimental results against which to compare the models. Some of the areas, especially radionuclide behavior in postmelt environments, are sufficiently complex that it would be very difficult to construct models based on first principles even if results from realistic core-melt experiments were available. Thus, the entire area is currently in a state of flux resulting from the widely perceived need for improvements and the results of current research.

Different models are required to model different phases in the progression of an accident: core degradation and melting within the vessel, steam and water circulation before vessel failure, the dispersal of the molten portion of the core upon vessel failure, core-concrete interactions, and the coolability of the debris bed on the containment floor. Structural analysis is needed to determine the response of the containment to thermal and pressure stresses. Hydrogen generation and mixing in the containment are of special concern. It is also necessary to estimate the amount of energy that can be released in steam explosions after the fall of the molten core into water in the bottom of the vessel or in the reactor cavity.

The characteristics of radionuclide releases to the environment are described in terms of various timing and location parameters, the thermal energy release rate, and the quantities of radionuclides released. The quantities of radionuclides of the various elements available for release from the plant depend on the processes by which radionuclides are released from the fuel and transported through the reactor-coolant system, the containment, and possibly buildings external to the containment before reaching the environment.

Analyses have shown that both natural and engineered retention mechanisms can significantly reduce the inventory of radionuclides available for release if enough time is available for those mechanisms to act. Therefore, source terms are strongly affected by whether or not the containment fails and, if it fails, by the time and the mode of failure.

The capabilities in all these areas of analysis have improved substantially since the RSS and are currently rapidly changing. Since the TMI accident, severe-accident research has expanded broadly, the aim being not so much to improve PRA but to acquire information about severe-accident behavior for possible use in plant regulation. Large experimental and mechanistic code-development efforts have been initiated or redirected to explore important severe-accident phenomena. Advances have also been made in the PRA analysis capabilities, including improved codes and methods for developing and quantifying containment event trees.

Shortly after the TMI accident, questions were raised about the appropriateness of the methods used to analyze source terms in the RSS and subsequent PRAs. In the face of complex problems and large gaps in the existing body of knowledge, the RSS chose to make conservative assumptions for source-term predictions in some areas; that is for some of the radionuclides in certain accident sequences, the RSS methods estimate higher release fractions than we now believe would be observed in an actual accident. These overpredictions may be significant in many cases. As a result of suspected deficiencies, a number of research programs have been undertaken to improve the ability to realistically model radionuclide release and transport in severe accidents.

Many uncertainties are associated with the predictions of severe-accident progression, containment response, and radionuclide transport. Presently, few sensitivity studies exist, the validation of models and codes for the broad range of severe-accident phenomena is extremely limited, and quantitative uncertainty estimates are not available. As a minimum, current research can be expected to provide a better characterization of source-term uncertainties and in some important areas reduce the conservatisms in PRA analyses.

Since the analysis of in-plant consequences is rapidly changing, the method is unstable. Indeed, developments are occurring so rapidly that, for a PRA being undertaken today, it is difficult to recommend a set of computer codes. Major advances are currently being made in the understanding of processes controlling radionuclide release and transport. However, processes that are closely coupled to the progress of extensive fuel damage, such as the release of the less volatile radionuclides from fuel or the generation of hydrogen during core slumping, will likely always have large uncertainties because of the difficulties associated with experimental validation. Likewise, it is difficult to establish an experimental basis for the models of pressure-vessel failure, core dispersal from the vessel, and debris-bed reactions.

1.3.4 Health and Economic Consequence Analysis

The health and economic consequence analysis portion of a PRA provides estimates of the frequency distribution of possible offsite consequences for core-melt accidents. Models have been developed which describe the transport, dispersion, and deposition of radioactive materials and predict their resulting interactions with the environment and the effect on the human population. Consequences can include early fatalities and injuries, latent cancer fatalities, genetic effects, land contamination, and economic costs.

The validity in this area is relatively high. The analysis methods have been fairly stable for some years overall, but the need for certain specific improvements is recognized. Improvements in some recent PRAs have included more detailed treatment of certain meteorological and topographical effects, and enhanced models for the mitigation of radiation exposure (e.g., evacuation and sheltering).

The first comprehensive assessment of consequences was performed in the RSS. Since that study, modeling capabilities have been improved, model and parameter evaluation studies have been performed, and existing models have been applied to provide guidance in such areas as emergency planning and reactor siting. In addition, the importance of potential consequences resulting from releases of radioactive materials to liquid pathways has been examined.

Uncertainties in offsite-consequence predictions have not yet been assessed comprehensively, although their magnitude can be inferred from the large body of existing parametric (or sensitivity) analyses in which consequences are calculated for a range of plausible values of a key parameter or model. The PRA Procedures Guide (NUREG/CR-2300) made a tentative listing of the relative contribution to total uncertainty of the major parameters and models in an offsite-consequence analysis. Important contributors to uncertainty were the magnitude of the source term, the form and effectiveness of emergency response, the rate of dry deposition (fallout during rainless periods) of particulate matter from the plume, the modeling of wet deposition (washout by rainfall), and the dose-response relationships for somatic and genetic effects.

It also appears that the condensation of moisture in the released plume could have a significant impact on reducing consequences. This potential effect is currently being evaluated.

All the consequences depend directly on the radionuclide source term, and the health effects depend upon the population density in the area surrounding the site as well. The uncertainties in the calculated risk stemming from uncertainties in the source term do not generally reflect upon the models in the offsite consequence analysis, but relate to the radionuclide behavior analysis as discussed in the preceding section. For estimates of the consequences resulting from very large source terms at a highly populated site, and given that the source term is known (i.e., source-term uncertainty is not included), the following crude estimates of uncertainties can be made:

- Mean early fatalities could range from approximately a factor of 5 above present "best" estimates to nearly zero. This broad range is in large part due to uncertainty in the effectiveness of short-term emergency response near the plant.

- The uncertainty in the mean predicted population dose (person-rem) is estimated to be a factor of 3 or 4, while the uncertainty in the predicted mean number of latent cancer deaths (which depends on the population dose) is approximately a factor of 10.

- In general, the uncertainties are larger in the extremely low-probability, high-consequence portion ("tails") of predicted consequence-frequency curves.

Ongoing research is focused on quantifying and, where possible, reducing uncertainties. Although uncertainties are likely to remain quite large, a thorough examination of their origin and magnitude will provide both a firmer basis for the application of consequence analyses and a better understanding of their limitations.

1.3.5 External Initiators

External initiators are discussed separately, principally because the method for treating them is, in some respects, different from the method for treating so-called internal initiators. The external initiators differ from the internal initiators in that they are likely to cause important concurrent events that complicate the response of the plant to the initiator and may degrade offsite mitigation efforts. For example, a severe external flood is almost certain to affect the possible evacuation of the nearby population, and a tornado or hurricane severe enough to damage the plant is also likely to cause a loss of offsite power. External events include

1. Earthquakes
2. Internally initiated fires
3. Floods (both external and internal)
4. High winds (tornadoes and hurricanes)
5. Aircraft, barge, and ship collisions
6. Truck, train, and pipeline accidents
7. External fires
8. Volcanoes
9. Turbine missiles
10. Lightning

The basic approach consists of quantifying the expected frequencies of the various initiating events, determining their effects on various pieces of equipment, and determining the resulting effect of any degradation or failures on plant performance.

The validity of the analyses for many external initiators remains questionable because of the lack of appropriate experience against which to judge models or because the problems are inherently complex and difficult to treat. The methods of analysis for most of the external initiators are now in a state of flux, and the need for improvement in the current treatment of most of the important initiators is recognized. These are discussed below.

The analysis of external initiators has seen major advances in the last decade. Much active developmental work is in progress, and abilities in this area should continue to improve. However, the uncertainties associated with such analyses are still significantly larger than those associated with most internal initiating events, principally because of uncertainties associated with the development of the hazards curves (i.e., the frequency of occurrence of an event exceeding a given magnitude). Nuclear power plants are carefully designed and engineered to be resistant to external initiators at the levels expected to occur. Taking normal design safety margins into account, the external initiators that are found to pose a significant threat to the plant are extremely severe and thus exceedingly rare. As might be expected, predicting the frequency of these unusual occurrences is very difficult, and the resulting expected frequencies have very large uncertainties.

For seismic events, a consensus prevails that the uncertainties in the core-melt frequency remain quite large for seismic PRA analyses. For these results, error factors of 10 to 30 (implying ranges of about 100 to 1000 for the 5 to 95% confidence interval) might be reasonable at present. A major contributor to this uncertainty is the likelihood of the very large earthquakes that dominate the analysis. These large numerical ranges for quantitative results do not negate the significant engineering insights obtained. Many of these insights are new and could not be acquired with traditional methods. In particular, the system vulnerabilities and common-cause dependences revealed have indicated areas where further investigation is warranted and where regulatory consideration may be required.

It is still too early to judge the achievable accuracy of the fire analysis methods. The uncertainties are probably larger than those for internal initiators. The engineering insights obtained from the few fire analyses performed to date have already been very useful and are in no way invalidated by the large uncertainties in the quantitative results. These uncertainties will probably be reduced somewhat by the results of current research.

While engineering insights are available concerning vulnerabilities from high winds, the estimates of core-melt frequency or risk from high winds are highly uncertain due to the difficulties in determining the frequency with which wind speeds high enough to significantly damage a reactor may be expected.

Flooding analysis is complicated by several factors. The fragility of safety equipment (especially electrical equipment) exposed to the spray from an internal pipe or tank break is very difficult to analyze quantitatively. Flood-induced corrosion can compromise the ability of safety equipment to remain operable during the recovery period after a particular flood has been nominally "controlled." Another flaw in the analysis is the limited ability to quantify partial blockages of drains or sumps that are relied on to carry away floodwaters. Finally, flooding (especially from an external source) can randomly deposit solid matter like sludge, silt, or even sizable objects in or on reactor plant equipment. These effects are difficult to analyze. The data base and analytical methods for coping with these issues are not well developed. The possibility also exists that unusual dependences among equipment (e.g., spatial colocation of electrical or support equipment) will cause additional vulnerabilities. Difficulties in modeling human intervention can also complicate the analysis.

External initiators such as aircraft impacts, pipeline accidents, external fires, volcanoes, and turbine missiles are typically analyzed probabilistically by performing a bounding analysis on their frequency of occurrence. An estimate is then made of whether the initiating event is serious enough to merit "concern." The main insight gained from the analyses performed on these "other" initiators (numbers 5 through 10 in the list above) are that, generally, they have minor risk significance. Few of them have required further study. This insight is quite important, because it indicates the effectiveness of the deterministic design and operational requirements in ensuring plant adequacy in these areas. The design and regulatory approaches seem to be adequately conservative.

1.3.6 Uncertainty Analysis

The preceding sections have discussed the sources of uncertainty in PRA results (parameter variation, modeling, completeness). Uncertainty analysis provides a framework for properly combining and describing the uncertainties associated with various elements of the analysis to determine the overall uncertainties associated with the results (e.g., risk) or intermediate quantities (e.g., sequence frequency).

Risk analysts are only at the threshold of performing comprehensive uncertainty analyses. A variety of techniques have been used or proposed. However, many are still being developed and, in general, the methods have not been applied in all their combinations for all parts of the PRA. The uncertainties which are generally quantified in PRAs are those which are due to parameter or data uncertainties. Uncertainties which are due to alternative models or alternative assumptions need to be separately considered by sensitivity analyses. In specific cases, the effects of different modeling assumptions can be as large, or larger than, the uncertainties stemming from the data or parameter estimation.

Because of the different probability distributions which are used in PRAs to quantify parameter uncertainties, the propagated output-probability distributions describing uncertainties in the results are themselves uncertain. Stated confidences or probabilities associated with given ranges (or error factors for the risk results) are consequently also uncertain. PRA uncertainties should be considered "fuzzy" values that account principally for the input-parameter uncertainties which have been explicitly quantified.

The significance of many of the modeling simplifications and assumptions which exist in a PRA can be revealed by performing sensitivity studies to evaluate the impacts of model alternatives and different assumptions. They can also be treated by assigning uncertainties to parameters subjectively and propagating these uncertainties.

Well-developed methods are available for estimating uncertainties in the parameters derived from the basic data and propagating them through the analysis. While the two principal approaches used differ, they may produce similar results, particularly when the data base is large. They can also differ substantially, reflecting the assumptions on which they are based.

Uncertainty and sensitivity analyses need to be better organized and displayed. The sensitivity and uncertainty analyses that are performed in a PRA have not always been well organized and discussed together in one place in the report. If this is done, it will provide a better understanding of the dominant uncertainty contributors, aid in identifying robust utilizations of the results, and better identify areas where additional research is needed.

1.3.7 Sabotage

Sabotage as an initiating event has not been traditionally included in PRAs, but the threat of sabotage has long been recognized and treated outside the PRA arena. PRA techniques have occasionally been used to do various vital-area and penetration analyses related to sabotage, but the risk of sabotage itself has never been estimated, principally because of difficulties in quantifying the threat frequency.

1.3.8 Conclusions

Because a complete PRA includes so many diverse areas of analysis and because the issues are so complex, it is impossible to condense the current state of the art to a single table or figure. The preceding summary is as concise a presentation as it is prudent to present at this time. There are wide differences among the various areas in the degrees of validity, stability, and need for improvement. A more complete discussion of these topics is contained in Appendix A.

However, it is possible to summarize the progress that has been made in the last decade, since the publication of the RSS. This is done in Table 1. It is clear that while significant progress has been made in some areas, much remains to be done if PRA is to reach its full potential.

Table 1

PRA Progress in the Past Decade

System modeling

- Methodology basically unchanged since RSS
- Improved computer codes now allow efficient handling of more complex models
- Improved treatment of dependent failures

Human interactions

- Improved techniques for handling procedural errors
- Cognition and comprehension errors are often considered but modeling is still relatively crude
- Analysis now includes recovery actions, but further improvement is needed

Data base

- Significant improvement for transient initiators
- Only modest improvement in other areas

Accident progression, containment response, and radionuclide transport

- Significant improvement in analytical abilities
- Area currently undergoing rapid change
- Generally only subjective uncertainty estimates currently available
- No experiments to provide validity in some areas

Consequence analysis

- Some improvement in modeling capabilities
- Sensitivity analyses available for many modeling assumptions
- Comprehensive uncertainty analysis not yet available

External initiators

- Major advances in recent years
- Great confidence cannot be placed in quantitative results of low-frequency events
- Significant improvements for seismic events but data base for very large earthquakes is limited
- Methodological improvements in fire and flood analyses

Uncertainty analyses

- Some improvements in methods
- Comprehensive treatment not yet available

2. REGULATORY USES OF PROBABILISTIC RISK ASSESSMENT

2.1 Introduction

The evolution of PRA methods for the study of reactor safety has been rapid in the past few years. Today, the number of full-scope PRAs completed or under way is large, the number of skilled practitioners has grown rapidly to many dozens, and the applications of PRA have spread to include many (perhaps most) of the important areas of concern in reactor safety. This is a remarkably rapid growth, especially considering the short history of PRA.

Chapters 1 and 3 clearly show that PRA techniques generate useful information about, and insights into, the design and operation of a nuclear power plant by providing not only an improved understanding of the full range of accident sequences but also a means for assessing their importance. The regulator can use this information to supplement the decision process. Just as clearly, many limitations in our knowledge lead to uncertainties in conventional technical analyses as well as in the quantification of the risk. These uncertainties must be reflected in the use of the results of any analysis, including PRA. Proper use of the PRA results in the regulatory process should emphasize the applications that rely heavily on well-developed methods and minimize the uses that rely heavily on the methods that are weak.

In the perfect regulatory system, there would be complete understanding of the phenomena that characterize the technology, the nature of the risks being regulated, the way that these potential risks might be actualized through undesired events (either rare unexpected events or more common, though stochastic, events), and the consequences of the undesired events. If such a full understanding existed, the problem of regulating would become to decide how safe is safe enough, and the potential for consequences or risks exceeding the safety limit would be eliminated or mitigated by various design, construction, and operational safety practices. The resulting level of risk, known as the residual risk, would be acceptable as a matter of public policy.

In this ideal framework, regulation would still confront many difficult decisions, such as how to weigh the costs against the benefits of regulatory actions or how to balance the time value of decisions that take long times to implement. However, such decisions would be made with a full, accurate understanding of the technical issues.

This ideal state is one to strive for, but the regulatory structure now in place recognizes that we have imperfect knowledge in many areas, and decisions still must be made.

However, we are reasonably confident that we can conservatively define regulatory requirements despite the difficulty in precisely stating the goals or measuring the absolute level of risk in quantitative terms. Over the years, the regulatory system has evolved using traditional engineering practices supplemented by additional safety measures and analyses in an attempt to ensure that sufficient conservatism exists even with our incomplete state of knowledge. Concepts such as the single-failure criterion and the family of design-basis accidents were introduced to require designers and operators to protect against the more likely accidents. This regulatory approach has been generally successful, in that operating experience combined with the results from the PRAs performed to date indicate that accidents outside the design basis contribute the major portion of the risk. Furthermore, this risk is generally reasonably low in comparison with other societal risks.

Despite its success, the current regulatory structure is not without its problems. The general process of adding conservatism as specific issues arise and the tendency to analyze the plant system by system have led to regulatory practices that are not always well integrated. This can result in uneven coverage of the safety issues, difficulty in assigning priority to new safety issues, and difficulty in determining if an acceptable level of safety has been attained. In addition, conservatisms properly introduced because of a lack of knowledge can become institutionalized, thus making it difficult to relax requirements after further knowledge of plant behavior is acquired.

In recent years, it has been recognized that PRA can offer the regulator a realistic description, probabilistic in character when necessary, that is applicable to many safety issues in varying degrees. The integral nature of the analysis and the explicit consideration of the interactions between systems can shed additional light on an issue. PRA is, of course, only one of many regulatory tools, and its applicability is not universal: for some issues it cannot shed much light at all. Like other analytical methods, its uncertainties can sometimes be so large as to make its insights of little use. In other cases, the PRA insights are robust in spite of the inherent uncertainties. At times, the ability of PRA to focus attention on the uncertainties resulting from a lack of knowledge provides vital information to the regulator, even if the level of risk is not well defined. Like any analytical method, PRA cannot, and should not, dictate a decision. It can only lay out technical facts, relationships, conclusions, and their uncertainties, so that the decisionmaker can better comprehend the issues.

As discussed in Chapter 1, PRA methods have attractive features that allow the decisionmaker to give PRA insights considerable weight in the proper circumstances. Chief among these features are that PRA's approach to a technical (safety) issue is intended to be quantitative, that the general approach strives for a "best estimate" description, and that PRA permits an analysis of the importance of uncertainties. Another strong feature of PRA is that, for the more complex analytical problems such as overall system behavior or intersystem interactions, the PRA methodology is intrinsically integrated and comprehensive (although this may not be successfully accomplished in practice by every PRA analyst).

Naturally, PRA has limitations that must be understood before it is used. Chapter 1 and Appendix A present a rather comprehensive assessment of the current state of the art of PRA methods.

The regulatory decisionmaker must evaluate each analysis, whether deterministic or probabilistic, and judge whether the assumptions and boundary conditions employed by the analyst are sufficiently valid and the results sufficiently robust to justify using the analysis in making regulatory decisions. No technical analyses, whether deterministic or probabilistic, are ever formally complete or completely certain. In most instances, the uncertainties identified in PRAs are also inherent in deterministic analyses.

The qualitative insights presented in Chapter 3 and Appendix B derive primarily from examining the quantitative results of several studies in light of their uncertainties and sensitivities. These insights are reasonably robust, and, while many of them are qualitative, in most cases they could not have been generated if the analyses did not quantify.

In some cases, PRA methods are the only available way to give a quantitative character to an issue. For example, the regulator may wish to ensure that emergency onsite power will be adequate. In practice, such assurance is implemented by requiring certain maintenance and test practices, certain resilience against undesired external conditions (earthquakes, flood, power surge, etc.), certain protection against system interactions, and the like. What PRA techniques can provide is the context for the requirements: the accident sequences during which the onsite power system is needed. PRA can illuminate whether the existing regulatory requirements are adequate and, if not, why not. The PRA analysis is not only descriptive of the interrelationships among the various systems but also quantitative, which permits attention to be focused on the important interrelationships.

Another strength of PRA lies in its ability to link various plant failures with their consequences in a comprehensive way. This strength is especially valuable where diverse elements of a safety design come into play, such as a sequence involving support-system failures aggravated by human error or a sequence initiated by an earthquake but compounded by the unavailability of equipment from another cause.

When making comparisons with another risk-based analysis or with a criterion or goal, the estimated uncertainty bounds must be carefully examined. Neither the uncertainty range nor the probability distribution of values through the range is likely to be known as precisely as the PRA results might indicate, because of the arbitrariness in some details of the statistical techniques or the omission of important considerations, such as modeling assumptions. An uncertainty range can thus be viewed as a range within which the true value can be expected to be with some high but fuzzy confidence, such as roughly 90%, with some unknown distribution, provided no bias is introduced by the selection of statistical parameters. If the uncertainty bounds (modified to incorporate the effects of uncertainties attributable to modeling and assumptions) do not overlap, the decisionmaker can assign high confidence to the results, provided they have been subjected to an adequate peer review.

Obviously, the decisionmaker does not require perfect information, and it would be inappropriate to dismiss PRA information simply because overlap occurs. In any decision process, all available information should be considered, and credibility should be based not only on the estimated accuracy but also on the judgments of technical experts and the degree of conservatism appropriate for the decision. The current state of knowledge indicates that, when various options are being evaluated or compared, generally a difference in point estimates (single values, medians, or means) of core-melt frequency of a factor of 3 or more is likely to be significant. Differences of less than a factor of 3 may well have uncertainty bounds that will overlap significantly (i.e., the upper bound of the smaller estimate will be greater than the lower bound of the larger estimate) so that there may not be any true difference in the items being estimated. Of course, where uncertainties are very large, the above general guidance would have to be used with caution.

Even if a significant degree of overlap appears in the uncertainty bounds, the decisionmaker still may have useful information because he or she can evaluate the source and nature of the uncertainties associated with each alternative, recognizing the possibility that comparisons of point estimates may be in error, with this potential for error depending on the degree of overlap. Nevertheless, even if quantitative results are for practical purposes indistinguishable, a plausible and previously unidentified failure path can sometimes be identified, in which case the decisionmaker has acquired useful information.

Uncertainty reduction should also be given serious consideration when a regulatory action is assessed. A safety feature that has little effect upon a point estimate of reactor risk but substantially reduces the upper limit of the estimate would have a positive value because of the enhanced confidence that the health and safety of the public are protected.

Clearly, as the discussions that follow reveal, PRA results and insights supplement the information that would be available to the decisionmaker from deterministic evaluations alone. Of course, many types of regulatory decisions exist, and the weight given to the qualitative and quantitative PRA results depends on the application.

One should recognize that a properly characterized increment of information gleaned from the application of PRA methods, even if highly uncertain, is better than no information at all.

2.2 The Regulatory Process

Before discussing how PRA might be used in regulation, one should understand how regulatory decisions are made. Several elements constitute the regulatory decision process. The first is to determine the information needed and the analytical methods appropriate for the decision. This could include qualitative and quantitative analyses, deterministic and probabilistic analyses, assessments of operating experience, and value-impact assessments. After the appropriate methods have been identified, analyses are performed and assessed as to technical credibility, employing technical peer review as appropriate. The next step in the decision process is the synthesis of all the applicable information to gain insights into the safety significance of the issue, conceptualize alternative resolutions of the issue (including the "no action" alternative), and evaluate the impacts of the various alternatives.

The final step is to develop recommendations for regulatory action. This step must consider the information base with its inherent uncertainties. It may also include further peer and public review with appropriate feedback loops for additional analysis and synthesis.

The analysis should display all of the important values and impacts (and their uncertainties) associated with a proposed regulatory change in an organized and understandable form for the decisionmaker and other interested parties. Information should be displayed so that the decisionmaker can understand the sensitivity of any conclusion to variations in the important inputs. All major assumptions underlying each conclusion and the information from which it is drawn should be explicitly presented. In some cases, the constraints of time may not permit detailed uncertainty and sensitivity analyses to be performed. If this occurs, the analyst should at least qualitatively discuss those factors believed to be dominating the results, and the decisionmaker should recognize that the understanding of the uncertainties associated with the analysis may be weak.

A key question facing the decisionmaker, assuming he or she has all of the important information from PRAs in a scrutable form, is what weight to give to the qualitative and quantitative PRA insights versus all of the other available and pertinent information. There is no "cookbook" answer to this question, because it will depend heavily on the nature of the issue, the results of the PRA, the nature of other information, and other factors that could affect the overall judgment. However, some characteristics of the PRA results and study process that would be considered are:

- The scope and depth of the PRA (i.e., does the nature of the PRA study reasonably match the needs of the decision).

- The results of peer reviews, which could add to or subtract from the credibility of the PRA results.

- The qualitative insignts obtained from the study. For example, do the qualitative insights into the dominant accident sequences appear reasonable from an operational or engineering perspective? This includes an assessment of the degree of realism associated with the study.

The impact of alternative regulatory actions on the estimated risk, together with the ease and costs of their implementation, should be evaluated.

It is clear from the above discussion that PRA can be very useful in regulation. In fact, there is no longer any question about <u>whether</u> PRA will be used, but only <u>how</u> it will be used in reactor regulation.

2.3 Applications of PRA Methods in Regulation

Three different types of regulatory applications will be discussed: applications for prioritizing resources (Section 2.3.1); generic applications (Section 2.3.2); and plant-specific applications (Section 2.3.3). For each type, some specific examples will illustrate how PRA methods and results can affect regulatory decisionmaking.

2.3.1 Prioritization of Resources

Because of its integrated nature and reliance on realistic information, PRA presents some of the best available information concerning the specific ways in which the critical safety functions at nuclear power plants can fail. This information can be used to guide and focus a wide spectrum of activities designed to improve the state of knowledge regarding the safety of individual nuclear power plants as well as that of the nuclear industry as a whole. The resources of both the NRC and the industry are limited, and the application of PRA techniques or insights provides one more useful tool to permit the decisionmaker to allocate these resources effectively.

Chapter 3 and Appendix B discuss those items that have importance with respect to either plant risk or the frequency of core melt as determined in published PRA results. While the completeness of such a listing cannot be assured for plants that have not been analyzed, these items have been found to affect significantly either the predicted frequency of core melt or the risk associated with a given plant. Such items could be examined to see whether they are generic and are likely to affect other plants of similar or even dissimilar design.

The nature of the decisions necessary to allocate regulatory resources does not require great precision in PRA results. In assigning research or prioritizing efforts to resolve generic safety issues, it is sufficient to use broad categories of risk impact (e.g., high, medium, and low). The reasoning is that a potential safety issue would not be dismissed unless it were clearly of low risk. Thus, one or more completed PRA studies can often be selected as surrogates for the purpose of assigning priorities, even though they clearly do not fully represent the characteristics of some plants, provided the nature of these differences is reasonably understood and can be qualitatively evaluated. A given issue can then be evaluated in terms of the number of plants affected, the risk impacts on each plant, the effect of modifications in reducing the risk, and the effect of additional knowledge on improving the prediction of plant risk or core-melt frequency or in reducing or defining more clearly the associated uncertainties. These generic measures of significance, combined appropriately with other information (e.g., cost of resolving the issue) can be used to evaluate the issue under consideration. Obviously, a principal source of uncertainty may lie in the use of a representative plant model (a "surrogate") to represent a broad class of reactors.

The uncertainties involved in the measure used for assigning priorities are generally such that only large (order of magnitude or greater) variations should be considered important.

Thus, if core-melt frequency were the measure, it would generally be inappropriate, based on the estimated frequency alone, to conclude that an issue associated with an estimated core-melt frequency of 3 x 10^{-5} per reactor-year is significantly more important than one associated with a core-melt frequency of 1 x 10^{-5} per reactor-year. However, it would normally be appropriate to assign a high priority on the basis of a core-melt-frequency estimate of 10^{-4} per reactor-year, compared to an estimate of 10^{-6} per reactor-year.

As with any priority-assignment method, the final results must be tempered with an engineering evaluation of the reasonableness of the assignment, and the PRA-based analysis can serve as only one ingredient of the overall decision. One of the most important benefits of using PRA as an aid to assigning priorities is the documentation of a comprehensive and disciplined analysis of the issue, which enhances debate on the merits of specific aspects of the issue and reduces reliance on more subjective judgments. Clearly, some issues would be very difficult to quantify with reasonable accuracy, and the assignment of priorities to these issues would have to be based largely on subjective judgment.

One example where PRA has been usefully applied is the prioritization of generic safety issues and TMI action items, recently accomplished by the Office of Nuclear Reactor Regulation and the continuing effort to evaluate new issues. In this effort, each issue is assessed as to its nature, its probable core-melt frequency and public risk, and the cost of one or more conceptual fixes that could resolve the issue. A matrix is developed whereby each issue is characterized as a high, medium, or low priority, or whether the issue should be summarily dropped from further regulatory consideration. This matrix considers both the absolute magnitude of the core-melt frequency or risk and the value-impact ratio of conceptual fixes, using $1,000 per person-rem as the monetary value of risk reduction. Risk-reduction estimates are normally made using surrogate PWRs and boiling-water reactors (BWRs), based on existing PRAs.

One principal benefit of this prioritization, compared to other methods for allocating resources to safety issues, is that important assumptions made in quantifying the risk are displayed and uncertainties in the analyses are estimated. One limitation is that some of the issues, such as those dealing with human factors, are only very subjectively quantified. Thus, the uncertainties can be large. Also, uncertainties resulting from the surrogate approach could be large, but these uncertainties are not addressed extensively.

The net result of this prioritization is felt to be beneficial, nevertheless. It is believed that, although the uncertainties may be large, the process forces attention on these uncertainties to a much higher degree than if the quantification were not attempted. Also, the uncertainties are normally part of the issues themselves and not just an artifact of the PRA analysis. Since the matrix used would not result in dropping an issue unless the issue is orders of magnitude away from being cost-effective <u>and</u> orders of magnitude away from reasonable safety criteria such as the proposed safety goals, it would be very unlikely that an issue would be dropped which, upon closer examination, would actually be a significant threat to public health and safety. Conversely, it is expected that some of the safety issues ranked high or medium, after closer examination and resolution, might turn out not to warrant further regulatory attention.

Information from PRAs can also be used to guide the allocation of resources in inspection and enforcement programs. A catalog of information derived from PRAs indicates that certain surveillance tests and maintenance activities are significant contributors to the estimated frequency of plant damage or to risk. If a class-generic risk profile were available, it could be used to determine appropriate importance measures regarding critical surveillance testing and maintenance activities that can, if not done properly, significantly alter the predicted core-melt frequency or risk. Importance measures of various types could be used in assigning priorities for inspection auditing, the training of operators and maintenance personnel, and the implementation of quality-assurance and reliability-assurance requirements. The generation of such information for each class of operating plant would provide a rough ordering of important operating activities that should assist a reactor inspector in efficiently directing the inspection effort at a given facility. Similarly, generic insights (available by reactor class) would assist both the licensee and the regulator in identifying and preventing or mitigating potentially significant operational occurrences at a plant, even if a plant-specific PRA is not available.

2.3.2 Generic Regulatory Applications

Perhaps the greatest potential utility of PRA techniques to the regulators lies in providing technical support for generic decisionmaking. NRC's decisionmaking ranges from the broadest scope (such as the general design criteria) to the narrowest (such as branch technical positions on testing and maintenance intervals). PRAs can be aimed at strengthening or relaxing regulatory requirements, or providing greater support for positions already existing.

There is a strong consensus that applications for examining the broad fabric of regulation are probably PRA's greatest potential contribution to regulatory decisionmaking, because PRA has proven to be the most widely applied analytical method that significantly integrates across diverse safety areas. Such a reexamination is thought to be timely, because our technical understanding has grown since the time when many of the regulations were established. A piecemeal reexamination would be neither integrated nor comprehensive.

PRA can have wide applicability in generic rulemaking or other regulatory changes. Indeed, this has already occurred in the past year or two. Whenever NRC's Committee for the Review of Generic Requirements (CRGR) has considered a new regulatory requirement that is amenable to PRA analysis, a limited analysis has generally been performed, and useful insights have been obtained.

Generic lessons learned from plant-specific PRAs have provided the impetus for several regulatory actions. Virtually every PRA performed to date has identified some previously unrecognized deficiency in plant design or operations that has an important impact on safety. These deficiencies have usually been associated with dependences among systems or with human-machine interfaces and have often resulted in voluntary changes in design or operational practices by the utility. It has usually been possible to examine whether any gaps in the generic regulatory fabric are revealed by these deficiencies, or whether the problem is entirely specific to one plant. If a generic problem is revealed, regulatory action has resulted through modifications to branch positions, regulatory guides, or the regulations, as appropriate.

The problem areas so identified do not have to be present at all nuclear plants. Rather, PRA is of sufficient use if the insights gained have identified potential safety issues at only one or a few plants that could occur in a way that had not previously been considered. Of course, once an issue is identified and analyzed, the ultimate action taken by the regulator would typically require great care in balancing the perceived benefits against various costs and impacts, in both a financial and an engineering sense. Experience suggests that many of the issues would involve only relatively simple and inexpensive procedural remedies.

PRAs have also identified areas where regulatory effort has been or potentially might be overemphasized, in the sense that the actual safety significance of some issues has been shown to be negligible. In such situations, the PRA results can be used to direct regulatory and industry resources away from areas that have little safety return. However, this requires a very careful evaluation of the stated and unstated uncertainties and the underlying assumptions.

Much information has been gained from limited generic studies of specific issues, using the PRA methodology to examine either reliability or intersystem relationships. While these limited studies have usually not been sufficient to analyze well the absolute level of risk involved, they have often indicated the relative importance of problems. This was certainly the case in one of the most important early applications, which was a thorough study of the reliability of auxiliary feedwater systems (AFWS) in PWRs. This study will be discussed in detail below.

Often, the insights of PRA emerge more from the qualitative relationships, rather than the numerical aspects of the calculations. Again, this was true of the AFWS study, where both the qualitative and quantitative results played a role in decisionmaking.

There are a few problems with generic applications, of which the most important is ensuring that the insights gained from the study of one or a few plants are broadly applicable. In fairness, this "surrogate" problem is present for any analytical method that provides the technical foundation for a generic decision. However, PRA studies sometimes appear to present more difficulties than do some other types of analyses, because their greater level of detail can reveal plant-to-plant differences that other approaches may not contemplate.

The catalog of plant systems, components, and operational practices that have had a significant impact on core-melt frequency or risk in various PRA studies can lead to generic insights for each of a variety of classes of plants. The number of plant classes (or surrogates) could be large, however, because many of the risk-significant features of the plant occur in the balance of the plant, where the design is less standardized.

However, the degree of detail necessary in establishing the classes as surrogates depends on the nature of the decision being made. In general, the decisionmaker will not rely on small differences in numerical results and will temper the PRA insights gained from PRAs with engineering judgment. Sorting the reactor population into a large number of classes of plants just to improve the numerical accuracy often will not be necessary.

As an extension of surrogate or plant-class type of analyses, insights can be obtained for a given type of accident sequence that may apply broadly to a large group of reactors (e.g., ATWS in BWRs) or may apply in a somewhat different manner to several different classes of plants (e.g., station blackout). The plant classes do not necessarily have to have the same basic risk profile; rather, they need only to react similarly to a given accident sequence for the generic insights to be valuable.

The use of surrogates to represent classes of plants for generic regulatory activities does entail modeling uncertainty, because subtle system and human interactions may have a pronounced effect on the actual risk of a specific plant. Therefore, the possible existence of risk outliers precludes the confident use of the surrogate approach to estimate "bottom-line" risk or core-melt frequency for plants that have not been subjected to a detailed PRA. The presence of an unidentified plant-specific risk outlier does not necessarily invalidate the analysis of the regulatory issue under review, although the relative importance of the issue may be affected.

Thus, there are two different groups of generic applications of PRA: those relying on a large number of plant-specific PRA studies from which general conclusions are drawn, and those relying on a generic PRA analysis or on only a few plant-specific studies chosen to represent the broader plant population. One example of each such type of application will be discussed next.

An example of a generic regulatory application is the study of AFWS. Shortly after the accident at TMI, the NRC conducted a series of studies to review the adequacy of the design of AFWS at operating PWRs. The emphasis of the studies was to identify any variability in the designs that might lead to variations in AFWS reliability, particularly when examined in the context of those accident sequences that involved the AFWS and had been found dominant in previous PRAs. To better ensure that the results represented true plant variabilities, close interaction between all analysts involved was essential. Analyses of the various plants were done using common procedures, a standardized data set, and uniform sets of analytical assumptions. Thus, a significant effort was made to reduce to a minimum the variability in results arising from the analyst.

The AFWS analyzed were viewed in the context of three different accident sequences, and quantitative results were generated for AFWS unavailability given the pertinent conditionalities of each sequence. No formal uncertainty analyses were performed. One key result of the study was that the system failure probabilities for existing plants licensed to the same regulatory requirements varied by a factor of about 100. Because experience with analyzing multitrain mechanical systems using prescribed data, methods, and assumptions tells us that an uncertainty in the central estimate should be (plus or minus) a factor of 3 or less, this variability of results indicated that the actual AFWS reliability was significantly different from plant to plant. The major cause in the variability was identified to be the dependence of the AFWS on support systems (e.g., service water, ac power) or suction-side valving and means of initiation. As a result of this key insight, the regulators were able to prepare deterministic regulatory requirements to preclude the types of interactions and failures that could significantly degrade the AFWS. A numerical reliability range for AFWS was also adopted as a goal in the Standard Review Plan.

It should be noted that the regulatory action primarily relied on the integral engineering logic regarding system design and operation under accident conditions that was developed as the models were constructed. Thus, what was important were the insights gained from viewing AFWS in an integrated manner in the light of those accident sequences for which its response is essential. The numerical results served only to assist in screening the important features from others. Quantitative unavailability results were calculated but were not used as absolute criteria. Their use in screening these systems was done in a relative manner. Since the basic design elements and functions were not vastly different from plant to plant, the relative comparisons were more robust than the absolute values calculated. Even here, however, the uncertainty in the selective comparisons was recognized, even though intentionally not calculated, and small differences in relative comparisons were not considered significant.

The AFWS study was of the type in which a specific system is studied for all plants to derive system performance information. Studies of this type largely avoid the "surrogate" problem referenced above.

There are many other situations where a generic issue must be handled broadly because of the time and effort that would be needed to study a given accident sequence or the performance of important systems in detail at all plants. Here, generalized insights gained from existing studies of similar plants are required. An example of such an application is the rulemaking on anticipated transients without scram (ATWS). This issue was first addressed deterministically, but in the middle to late 1970s probabilistic techniques were used both to identify dominant accident sequences involving no scram and to assess the risk associated with such events.

The uncertainties of the analyses were large for several reasons: the ATWS event involves the failure of a highly reliable safety system (the trip system) for which there is little failure data, the likelihood of core melt given a large pressure transient (in a PWR) or high BWR suppression-pool temperatures is open to question, the physics and thermal hydraulics of the accident sequences are design-specific and complex, and the source terms from such events are very controversial and sensitive to specific containment design. In the analyses, the staff considered only three design variations (W, CE/B&W, GE), assumed that core melt was synonymous with exceeding Service Level C pressures for PWRs or 200°F suppression pool temperature for BWRs, and assumed that all core melts would result in a source term equivalent to a BWR Category 2 release as defined in the RSS.

With all of the uncertainties and simplifying assumptions, one might ask how the PRA results could be used to help make the ATWS decision, particularly since the value-impact analyses of the proposed fixes were not determinative for the decision. (The value-impact of the recommendations ranged from about 0.4 to 3, based on $1,000 per person-rem.) While many of the staff assumptions in the estimation of benefits in these value-impact analyses were acknowledged to be conservative, some were not. Also, industry-generated costs of fixes were generally used, even though the staff thought that these might be overstated.

The basic rationale for the decision was a mixture of deterministic and probabilistic viewpoints. The usefulness of PRA in developing the rationale for the decision was primarily in better defining the problem and suggesting where corrective action might be most effective. Considerations included the following:

- The probabilistic techniques gave good insights as to the possible accident sequences and contributed to a focused discussion of the most important aspects of the issue, including uncertainties.

- The data base for reactor trip-system component failures and the reliability analyses indicate that common-cause failures, though very infrequent, represent the principal contributor to trip-system unavailability.

- While the trip breakers appear to be the components most susceptible to common-cause failure, based on the limited number of common-cause failures observed in the operating experience, other components of the trip system have also been affected by common-cause failures.

- Diversity as a philosophy makes most sense for systems that require high reliability, since it gives greater assurance that common-cause failures will not contribute to unacceptably high unavailabilities.

- Conservatism is warranted in areas where there are substantial questions as to system performance, thermal hydraulics, and the physical phenomena associated with core degradation.

- One of the principal considerations in the ATWS recommendations was improved reliability assurance. This was evident in the statement of considerations and in the emphasis on diversity. Such an emphasis would provide additional assurance that systems important to safety would not be degraded, which means that some of the uncertainties in the risk assessments would be narrowed.

Two conclusions can be drawn with regard to the use of PRA in generic regulatory applications. The first is that such applications are strongest when they rely on PRA insights at the system, component, function, or accident-sequence level and are less strong when they rely on insights at the level of core-melt frequency or offsite risk. Also, PRA should be used not only to consider areas where additional regulatory actions are needed but also to reexamine the fabric of regulation to determine whether a relaxation of certain requirements is warranted.

2.3.3 Plant-Specific Applications

Almost every plant-specific PRA has identified design or operational deficiencies. In many cases, these deficiencies have been rectified not primarily because of the calculated frequency values, but simply because the plant owner and operator recognized that a specific portion of the plant (or of the operating practices) did not function in the way it was intended. Thus, the qualitative knowledge from PRA can be used to improve operational performance without a high degree of reliance on the numerical estimates of core-melt frequency and risk.

A plant-specific PRA, performed early in the design process, can yield a tremendous number of insights about the integrated performance of the plant. Because of the lack of specific design details in some areas, as well as the lack of plant-specific data, the results of such an analysis cannot be considered a true prediction of plant risk or of the frequency of core melt. Rather, such a design-stage analysis generates useful information on potential weaknesses in the design, and it allows an evaluation of the efficacy of design modifications. PRA studies of the British PWR design (Sizewell B) and of standardized designs under development by U.S. vendors are examples of how PRA is being used as a tool to improve the safety and reliability of new designs. A plant-specific analysis during the design phase could be used to focus quality-assurance activities on the areas with the highest potential for reducing risk. Again, the real significance of such an analysis lies not in the precise numerical estimates, but rather in the insights into important design features and critical human-machine interfaces, which can be carefully considered in the detailed design process.

Another use for a plant-specific PRA is in the evaluation of proposed generic solutions to unresolved safety issues and other generic items. Because of plant-specific differences, particularly in the balance of the plant, a plant-specific PRA may be able to identify a regulatory action for that plant that is more efficient than the generic solution. The regulatory decisionmaker can consider this as an alternative when generic requirements are set.

An example of using a plant-specific PRA in this manner is the study performed for Big Rock Point. Here, the licensee (Consumers Power Company) performed a probabilistic assessment of the Big Rock Point plant in order to address the relative safety concerns of the TMI action items. As a result of the study, the licensee initiated several plant modifications to reduce the frequency of core melt as indicated by his study. These voluntary actions that addressed the dominant sequences included:

- Replacement of a manual valve (located inside containment) with an automatic dc-powered valve to provide alternate makeup to the emergency condenser, which would reduce the potential for overpressure events and a stuck-open safety valve

- Revised procedures to utilize the high-pressure feedwater system with recirculation from the containment, to reduce dependence on the reactor depressurization system

- Installation of position locks on seven valves in the post-LOCA recirculation system, to reduce the potential for misalignment of the system after test or maintenance

- Elimination of the 15-minute delay for the containment spray actuation, to reduce the potential failure at high temperatures of essential systems inside containment

Subsequently, the NRC staff concurred that the licensee could be relieved of making additional modifications to improve control-room habitability and adding an additional senior reactor operator. Both of these items were from the TMI Action Plan. Additional relief from TMI Action Plan items is under consideration by the staff.

The availability of plant-specific PRA insights allows the regulator to assign priorities, on a plant-specific basis, to the various licensing issues and inspection activities associated with a given plant. An important factor in this process is that the regulator not rely on the quantitative results, but consider the qualitative insights and the associated uncertainties, stated and unstated. Of particular importance is the detailed knowledge of system performance and the variety of interactions between systems and components and between the operators and the various plant systems and subsystems.

A plant-specific PRA can be used to evaluate the importance of operating events and to assess the safety of the plant when equipment is not operable. Also, a catalog of accident sequences and the estimates of their frequencies can be used to train emergency-response personnel in what to expect. This could lead, for example, to improving the set of symptoms to be used as trigger points for the declaration of site or general emergencies and to developing guides on the diagnosis and prognosis of accidents as they progress. The models generated could also provide the tools with which to optimize allowable outage times and surveillance intervals and can be used in evaluating the advisability of plant shutdown when equipment is out of service beyond the outage times allowed in current technical specifications.

Given that a plant-specific PRA has been performed, steps should be taken to track the performance of the plant to ensure that the level of safety identified in the study has not been degraded with time. Thus, the PRA should be, in effect, a living document that is used and appropriately updated. The PRA should be used in the context of a safety or reliability assurance program to evaluate operational occurrences and to check the significance of experience data as they are acquired.

Plant-specific analyses have also been used in studies such as the SEP. The SEP is an integrated reevaluation of the eight oldest operating plants to ascertain whether variances from current regulatory positions are important to safety and, if so, what actions should be taken. In SEP, PRA techniques have been used as a tool in the integrated assessment of many issues. The studies utilized plant-specific studies when available but also performed some limited-scope exercises and relied on surrogate analyses when appropriate. These studies have been very useful in providing risk-based information for decisions as to whether these older plants require modifications to conform to current regulatory positions.

Some studies have been initiated in response to a concern expressed by the NRC relative to the risk associated with a facility. The Indian Point PRA study is an example of this.

The licensees for the two Indian Point plants submitted probabilistic assessments to the staff to provide additional perspective on the safety of their plants. After a review of the PRAs, the staff had several interactions with the licensees regarding dominant contributors to core-melt frequency and severe offsite consequences. Several design and operational modifications that addressed the dominant contributors were implemented before the plants were restarted. For Indian Point 2, these modifications included:

- The installation of a bumper between the control-room building and an adjacent structure and connecting the ceiling tiles to the grid structure, to reduce the potential for an earthquake disabling the control room

- The installation of alternative power lines for a charging pump, component cooling water pump, and two service water pumps, to reduce the potential of a fire resulting in a reactor-coolant-pump-seal failure and loss of ECCS, leading to core melt

- Modification of the technical specifications to require a plant shutdown in the event of a severe hurricane off the New Jersey coast, to reduce the potential for a loss of all ac power, through the loss of high-wind-sensitive structures.

Subsequent analyses indicated that these modifications had a high value-impact ratio. For Indian Point 3, the modifications included connecting the ceiling tiles to the grid structure and providing alternative sources of power to charging, component cooling water, and service water pumps, in a manner similar to Unit 2.

The Indian Point study was also used as the basis for testimony at an adjudicatory Atomic Safety Licensing Board (ASLB) hearing to evaluate the safety of the plant. The hearing has been completed, and the hearing board has published its findings. However, the NRC had not acted upon that decision at the time this document was prepared. In this hearing, as in a few other recent cases, PRA results and insights have been successfully used as a part of the technical information evaluated by the ASLB panels. This success indicates that PRA information can be of use in adjudicatory hearings, just like any other technical information.

2.4 PRA and Safety Goals

The previous discussions have pointed out that, although PRA results are uncertain, useful reliability and risk insights can still be gained from such studies. Considering these conclusions, the question arises whether quantitative safety goals can find useful application in the regulation of nuclear power plants. The answer is probably "yes," but careful attention must be paid to the structure of such goals, and their implementation also must be carefully considered.

There are many ways that quantitative safety goals could be constructed. For example, they could be expressed as unacceptability or acceptability limits*; as aspirational goals that should be striven for; or as a broad range of acceptable safety that one anticipates, with some plants expected to fall above the stated values and some below. The description of the qualitative goals in the NRC's policy statement indicates that the intent is to establish a broad range of acceptable risk (as opposed to criteria) that is below any serious concern for public health and safety. However, one can interpret the quantitative goals as acceptance criteria. For example, if a plant met the quantitative goals, then no improvements in the plant or operations would be necessary; but, if the goals were not met, then proposed improvements would be subject to a cost-benefit test.

The setting of any safety goal is somewhat arbitrary and depends on the perception of the risk that the public is willing to accept from that particular activity. Acceptable risk in practice would have a wide range of values based on the difficulty of measurement, desired conservatisms, the difficulty in getting consensus on appropriate levels, and the fact that society's definition of "acceptable risk" depends on many factors associated with the activity itself (i.e., there is no universal level for all human activities). Thus, any public risk safety goal is basically a very fuzzy limit and difficult to define as a clear line between acceptable and unacceptable risk.

Similarly, PRAs have equally fuzzy characteristics. One characteristic of a PRA is that the numerical risk estimates generated by the PRAs are uncertain and are generally less useful than the qualitative insights on the dominant accident sequences and the dominant contributors to these sequences. A second characteristic is that, generally speaking, more faith can be placed in the assessment of component or system reliability than in estimates of core-melt frequency, and estimates of public risk are even more uncertain than estimates of core-melt frequency. A third characteristic is that, even if the authors of a PRA were severely constrained by having the regulator prescribe for them the data base, methods, success/failure assumptions, uncertainty distributions, and phenomena to be used in PRAs, one might expect

*An unacceptability limit would be a relatively high value that, if exceeded, would clearly not be acceptable; i.e., the risk must be reduced regardless of any other considerations. An acceptability limit would be a relatively low value that, if achieved, would clearly be acceptable; i.e., no further regulatory action would be required regardless of any other considerations.

substantial variations in estimates of core-melt frequency performed by different analysts on the same plant; variations of a factor of 3 or more would not be surprising at all, with a greater variation expected for the assessments of risk. However, such a prescription would be difficult to achieve in practice, and in fact could be unwise in that it could constrain both the identification of new general safety insights and the development of PRA methods. This could, in turn, lead to ignoring potentially dominant contributors to core-melt frequency or risk, or being overly conservative in the regulatory approach to an issue that has little safety significance.

To exemplify the above, for estimates of core-melt frequency the upper and lower bounds of uncertainty typically might be about a factor of 10 above and below the central estimate. This means that, if the central estimate of the core-melt frequency is 1×10^{-5} per reactor-year, one normally can be reasonably certain that the actual value does not exceed 1×10^{-4} per reactor-year. Likewise, if the central estimate is 1×10^{-4} per reactor-year, it is perhaps about equally likely that the actual value is either substantially above or substantially below 1×10^{-4}. Therefore, if one were to establish 1×10^{-4} per reactor-year as an acceptance level for the estimates of core-melt frequency, the following questions would have to be considered:

- In generic applications of PRA, how should this 1×10^{-4} value be allocated to individual accident sequences such as station blackout, ATWS, pressurized thermal shock, etc?

- To what degree should the PRA analysts be constrained by prescriptive requirements on the conduct of the PRA in order to limit the variability in the results due to the assumptions of the analyst?

- What degree of confidence would the regulator require that a specific estimate of core-melt frequency actually is less than the safety goal; i.e., is the safety goal sufficiently conservative that a median* estimate (roughly 50-50 likelihood) provides reasonable protection to public health and safety?

- What degree should considerations other than numerical compliance play in the implementation of the safety goal; i.e., what role or weight should be given to the qualitative insights gleaned from the PRA?

---

*The word "median" is used loosely, since one really does not know the estimated distributions well enough to calculate medians with accuracy.

Similarly, if quantitative safety goals are established either as acceptability or as unacceptability limits, then it is necessary to ensure that

- The risks are indeed acceptable or unacceptable. In this regard a value of 0.1% of total risk for the affected population around a plant may be too stringent as an unacceptability limit, but might be appropriate as an acceptability limit. In contrast, a value of 1×10^{-4} per reactor-year for core-melt frequency might be viewed by some as being too high as an acceptability limit, considering the financial impact on society and the perceived public unacceptability of a core-melt accident.

- A sufficient degree of uniformity in the conduct of a PRA, in the performance of uncertainty and sensitivity analyses, and in the documentation of results is provided to limit controversy and litigation as much as possible to areas of plant design and operation, instead of assumptions in the analysis.

- Provision is made for the consideration of dominant accident sequences and their principal contributors--not just the total core-melt frequency or risk.

- The goal formulation carefully considers the degree of confidence required as to whether the limits are achieved or exceeded. For example, if a "50-50" confidence level is sufficient for regulatory purposes, a core-melt frequency acceptance value set somewhere in the range of 10^{-5} to 10^{-4} per reactor-year might be appropriate as a part of the goal formulation. However, if greater confidence is needed, then the number probably should be substantially larger.

If, however, the goals are treated as aspirational goals or expected broad ranges, rather than acceptability or unacceptability limits, then the regulators would have more flexibility in applying the goals, and some of the above considerations would become less important. However, the drawback of using the goals as general benchmarks against which to measure plant safety is that it becomes less clear to the regulatory staff, the industry, and the public, how the goals are really being used and whether they are actually being met.

All things considered, it appears that the strengths of PRA are more compatible with the philosophy of establishing quantitative safety goals as expressions of the range or general level of safety that is anticipated from the nuclear industry. In formulating a safety goal as a general level of expected safety, one could still establish upper and lower extremes. If these extremes were approached or exceeded, the regulator would be strongly advised either to take action at the upper extreme or to desist from further regulation at the other extreme. In the "gray" area between these extremes, regulatory action would likely be governed principally by considerations other than the absolute value of the core-melt or risk estimates, including costs and benefits.

The above discussion is not intended to make a final judgment on the usefulness, structure, or implementation of numerical safety goals. Such a judgment should only be made at the end of the two-year period for the evaluation of the safety goal. The only purpose is to provide some perspective as to the general structure of a safety goal that would be most compatible with the strengths and weaknesses of PRA.

2.5 Conclusion

PRA has proved valuable in providing insights into plant design and operation, the relative importance to safety of specific plant characteristics, regulatory issues, and alternative regulatory actions even though its quantitative results are imprecise. Thus, it is recommended that the use of PRA in regulation focus on applications where issues or alternatives are placed in fairly broad categories reflecting their relative importance. These applications can include plant-specific as well as generic actions. The categories should be broad enough to be appropriate even after considering the range of uncertainties. Plant-specific applications of PRA results are not recommended where the results are to be used for a strict compliance type of comparison against some numerical standard of acceptability.

The various ways regulators might use PRA techniques, results, and insights to supplement and augment the information derived from traditional analytical techniques have been discussed in detail in this chapter. The more important conclusions are presented below.

- Assignment of priorities to regulatory issues. The issues should be assigned to broad categories, and this assignment should not require much precision from the PRA input. These assignments can aid significantly in allocating limited resources to risk-significant issues. Regulatory areas amenable to this use include generic safety issues, inspection procedures, enforcement actions, and regulatory research. Value-impact analyses would be useful in reaching a decision. However, some issues would not be amenable to reasonable quantification and thus would still require a more subjective assignment of priorities.

- Generic regulatory applications. Such uses focus on areas where additions to existing regulatory requirements appear necessary, as well as on regulated areas that appear to be unimportant to risk. The scope and depth of the PRAs, the degree to which differences between plant classes need to be considered, and the role that uncertainty and sensitivity analyses would play would depend on the particular issue under review.

- Plant-specific applications. Many plant-specific uses of PRA have evolved besides the comparison of "bottom-line" numbers with numerical criteria as a licensing or compliance exercise, and such usage is recommended. For example, PRA results are used to provide information for plant-specific decisions on exemptions from existing requirements or the imposition of additional requirements, for the development of

  - Plant-specific limiting conditions for operation and surveillance testing requirements
  - Plant-specific operating, testing, and maintenance procedures
  - Requirements for training and quality-assurance programs
  - Emergency response and operating procedures
  - Plant-specific inspection programs
  - Reliability-based design requirements for any new plants that are not well into the design phase

  and for the assessment of operating experience to gain plant-specific insights.

  For such plant-specific applications, the PRAs would either have to be plant specific or would have to draw on information that was sufficiently design specific to be a reasonable surrogate for that plant class.

  One question that must be resolved is whether the usefulness of plant-specific applications is sufficient to warrant a regulatory requirement for the performance of such analyses by the industry. Such PRAs could be useful in integrating and assigning priorities to all identified safety issues applicable to that plant, in addition to searching out any risk outliers that would not be identified from the risk insights gleaned from PRAs of similar plants. They could also be useful as a basis for a comprehensive reliability program aimed at preventing the degradation of plant safety over the lifetime of the plant.

Many of the generic and plant-specific applications listed above can draw from the relative insights provided by PRAs. In many situations, these qualitative insights would be more important than the quantitative results. However, where the quantitative results are given significant weight, an analyst must be careful to consider whether the results of sensitivity analyses conducted over reasonable uncertainty bounds (including alternative modeling assumptions) would affect the decision significantly, compared to the use of point estimates.

3. PRA STUDIES AND INSIGHTS

Although the application of PRA techniques to nuclear power safety in the United States started essentially with the NRC-sponsored RSS in 1975, PRA was not widely used until after the accident at TMI.

In the five years since the accident at TMI, numerous plant-specific PRAs and generic PRA studies have been undertaken both in the United States and abroad. These studies, taken individually or collectively, have provided many significant insights into items important to risk and safety. This chapter discusses the major PRA studies that have been performed or are under way, briefly reviews special-issue PRA studies, and discusses the principal insights obtained from these studies. More detailed discussions of the insights and studies are provided in Appendixes B and C, respectively.

3.1 Major Studies

As of late 1983, 13 full-scope (level 3) PRA studies and at least 9 PRAs of level 1 or 2 had been completed for U.S. light-water reactors. This section provides an overview of the PRAs that have been performed and of the types of reviews that have been conducted.

3.1.1 Plant-Specific PRA Studies

3.1.1.1 Completed Level 3 Studies

Table 2 lists the plants for which full-scope PRAs have been completed. Two of the plants listed, Surry Unit 1 and Peach Bottom Unit 2, were those analyzed in the RSS. The motivation for the RSS, which was sponsored by the NRC, was to make a realistic quantitative estimate of the risks from commercial U.S. nuclear power plants and compare it with estimates for other, non-nuclear risks accepted by society.

The motivation varied for the other level 3 studies, which were sponsored by the utilities or their research organization (the Electric Power Research Institute, or EPRI), although several were performed in response to NRC actions or requests. For example, the Commonwealth Edison Company commissioned the full-scope PRA for the Zion plant after the NRC staff concluded from a study of the demography composed to other reactor sites that the plant might represent a large fraction of the total risk from all U.S. nuclear power plants. The Consolidated Edison Company and the Power Authority of the State of New York (PASNY) initiated the studies for Indian Point Units 2 and 3, respectively, for similar reasons. The Limerick and Millstone PRAs were requested directly by the NRC because their sites are also close to metropolitan areas. The Big Rock Point study was

Table 2

Completed Full-Scope (Level 3) PRAs

Plant	Issuance	Operating License	Rating (MWe)	NSSS/AE*	Containment	Sponsor	Report
Surry 1	1975	1972	788	W/S&W	Dry cylinder	NRC	NUREG-75/014 (WASH-1400)
Peach Bottom 2	1975	1973	1065	GE/Bechtel	Mark I	NRC	NUREG-75/014 (WASH-1400)
Big Rock Point	1981	1962	71	GE/Bechtel	Dry sphere	Utility	USNRC Docket 50-155
Zion 1 & 2	1981	1973	1040	W/S&L	Dry cylinder	Utility	USNRC Dockets 50-295 and 50-304
Indian Point 2 & 3	1982	1973	873	W/UE&C	Dry cylinder	Utility	USNRC Dockets 50-247 and 50-286
Yankee Rowe	1982	1960	175	W/S&W	Dry sphere	Utility	USNRC Docket 50-29
Limerick 1 & 2	1983	----	1055	GE/Bechtel	Mark II	Utility	USNRC Dockets 50-352 and 50-353
Shoreham	1983	----	819	GE/S&W	Mark II	Utility	USNRC Docket 50-322
Millstone 3	1983	(1986)	1150	W/S&W	Dry cylinder	Utility	Controlled document
Susquehanna 1†	1983	1982	1050	GE/Bechtel	Mark II	Utility	Draft
Oconee 3†	1983	1974	860	B&W/Duke	Dry cylinder	EPRI/NSAC	Draft
Seabrook	1984	----	1150	W/UE&C	Dry cylinder	Utility	Draft

*NSSS--nuclear steam system supplier; AE--architect-engineer.

†Completed but not yet publicly available.

initiated by the Consumers Power Company as a way to evaluate the cost versus risk-reduction benefit of implementing plant modifications proposed by the NRC under the SEP and post-TMI requirements.

The remaining level 3 PRAs were initiated in general because the sponsors wanted to estimate the risk of the plant and to identify the plant characteristics most important to risk. In addition, they wanted to have a plant-risk model that could be later used in making decisions about possible modifications to plant design, operations, maintenance procedures, and emergency plans. In most cases, these activities were perceived to be a part of future risk-management programs.

Four major comprehensive studies have been omitted from the table because they have received less attention since they are foreign or are for different reactor types. These are the German Risk Study (Deutsche Risikostudie) sponsored by the West German Federal Ministry for Research and Technology and conducted on the Biblis "B" 1200-MWe reactor; the DOE-sponsored high-temperature gas-cooled reactor (HTGR) study named AIPA (Accident Initiation and Progression Analysis) on a General Atomic large HTGR; the DOE-sponsored study for the Clinch River Breeder Reactor; and the Sizewell B study sponsored by the U.K. Central Electricity Generating Board.

3.1.1.2 Completed Level 1 and 2 PRAs

All of the level 1 and 2 PRAs completed to date in the United States have been performed under one of the NRC-sponsored programs, the RSSMAP or the IREP. Under RSSMAP, RSS methods were applied in a survey fashion to four plants with reactor and containment designs different from Surry 1 and Peach Bottom 2 in order to determine the sensitivity of dominant accident sequences to plant design. The four RSSMAP studies, which did not include external events or risk estimates, can be viewed as limited-budget level 2 studies. The IREP studies involve rather detailed system analyses of five plants, which were carried forward only to the point of estimating core-melt frequencies. They can be viewed as expanded level 1 studies. The Ringhals 2 study, sponsored by the Swedish State Power Board, was a level 1 study.

3.1.1.3 PRA Studies Under Way

Several PRAs of varying scope are being, (or are to be) completed, all sponsored by utilities or EPRI. In addition, a number of PRA studies are under way or are being initiated in other countries (e.g., Taiwan, Japan, Switzerland, Italy, Spain).

3.1.2 Reviews of PRA Studies

3.1.2.1 Reviews of Specific Studies

PRA studies are generally subjected to a self-initiated (internal) review that typically includes a multidisciplinary review team within the study organization and then a review by a separate peer review group. In addition, many PRA studies have been subjected to an independent review by the NRC, supported by the national laboratories and various consultants. Appendix B lists several reviews of this type. Such reviews generally assess the validity of the results and interpretations of a single study. In some instance, these NRC reviews have led to revisions of the original PRA analyses, including the addition of new accident sequences and revisions to modeling assumptions.

By contrast, the review performed by the Risk Assessment Review Group (also known as the "Lewis Committee") was directed toward a generic assessment of PRA techniques and data. The group conducted a comprehensive review of the RSS, supplemented by presentations from a wide spectrum of technical consultants. The Lewis panel criticized some of the analytical techniques and regarded the uncertainty ranges on results to be greatly understated. However, it concluded that the RSS was "a substantial advance over previous attempts to estimate the risks of the nuclear option."

The two-phase review of the Indian Point PRA, sponsored by the General Accounting Office (GAO), also has the objective of providing broader insights on methodology and results as well as assessing the technical quality of the risk assessment. For example, one finding of the phase I GAO review was that "the Indian Point PRA ... suffers from the same fundamental problem of all PRAs: uncertainty and incomparability of results." Phase II has not been completed.

3.1.2.2 Reviews of Multiple Studies

A knowledge of the results, insights, applications, and efficiency of the variety of approaches to PRA can be of significant value to nuclear utilities and to regulators. Since PRA studies generally produce multivolume reports that are difficult to comprehend and assess without extensive and dedicated scrutiny, several reviews of multiple PRAs have been conducted with the objective of providing broad insights into what the collection of studies is telling us. The multiple-study reviews reveal similarities and contrasts between the methods and results from the different studies. From such correlations and contrasts, generic bases can be derived for decisionmaking on regulations that affect plant design and operations.

To date, there have been three noteworthy multistudy reviews:

1. EPRI-Review of Five PRA Studies. In 1982, EPRI initiated a review of the PRA reports for Big Rock Point, Zion, Limerick, Grand Gulf, and Arkansas Nuclear One. This review, completed in 1983, provides a summary and interpretation of the results of the five studies to serve the needs of management as well as technical specialists.

2. Accident Sequence Evaluation Program (ASEP). This program is sponsored by the NRC as part of the Severe Accident Research Plan (SARP). ASEP uses existing NRC- and utility-sponsored PRAs as well as a number of the generic "special studies" described in Section 3.2. The objective is to identify the accident sequences that have the greatest potential for dominating core-melt frequency or risk in LWR plants and to determine plant characteristics and uncertainties that affect these frequencies as a function of specific classes of plants.

3. Industry Degraded Core Rulemaking Program (IDCOR). Fourteen PRA studies were reviewed to assist the utility industry in developing a technical position on issues related to severe-accident rulemaking. This review provided information on risks associated with severe accidents, the basis for an investigation of accident phenomena, and the potential impact on risk of proposed changes in plant design or operation.

3.2 Special-Issue Studies

Many studies on so-called special issues relating to reactor safety, licensing, and siting have used PRA techniques as their principal analytical tool. These studies have been conducted by both the NRC and the industry. A rather complete listing and discussion of these special-issue studies is provided in Appendix C. A more limited discussion follows.

NRC-sponsored studies were performed primarily to support regulatory actions that affect all plants or large classes of plants. These studies in many cases have drawn from the large information base created by the NRC- and industry-sponsored PRAs with respect to models, accident sequences, risk profiles, and insights about important contributors to risk. In some cases, substantial original effort was expended. Historically, these studies play an important role in the use of PRA in the regulatory process, at least equal to and perhaps surpassing the role associated with full-scale PRAs.

Industry-sponsored studies have been performed primarily to assist decisionmakers in selecting design options, to address NRC-raised licensing issues, and to support licensing and environmental requirements with regard to Class 9 accidents.

These studies have also drawn from the large information base or have involved a substantial original effort.

Many of the special studies have addressed unresolved safety issues and "task action" plans. Perhaps the first well-known use of PRA insights in the regulatory process occurred in 1978, when the NRC staff performed a study to categorize the existing technical and generic issues facing the Commission. One hundred thirty-three task action items were reviewed and assigned to four broad categories ranging from those having high risk significance to those not directly relevant to risk. Of the 133 items, 16 fell in the high-risk category. The ranking aided the selection of the generic issues that would be designated "unresolved safety issues." This effort was recently redone to include all TMI action plan issues and issues identified since the TMI accident.

Unresolved safety issues and the task-action plan items that have been addressed by PRA methods include ATWS, the design and procedural requirements for dc power systems, the reliability of ac emergency power systems in station blackouts, the significance of water hammer in dominant accident sequences, the significance of fracture toughness of supports for steam generators and reactor coolant pumps in response to earthquakes, and the impact of recirculation blockage after a LOCA from debris in a containment sump.

After the TMI accident, the NRC sponsored a series of studies to review the design of auxiliary feedwater systems in U.S. PWRs. This effort led to a recognition of the value of applying PRA techniques at the system level. A quantitative requirement on auxiliary-feedwater availability was added to the standard review plan. Probabilistic models have been used by the NRC staff to provide a basis for modifying technical specifications for testing intervals and allowed outage times for redundant systems.

Selected topics in the SEP have been assessed for the incremental risk associated with adopting proposed modifications, e.g., loose-parts monitoring, fire protection, etc.

One special study, which is quite different from the others mentioned above, reviewed licensee event reports (LERs) to identify potential accident "precursors"--events that could have developed into severe core-damage sequences if combined with certain other postulated failures. The results were used to estimate core-melt frequencies for operating plants.

A few of the special studies have dealt with matters of alternative containment design, reactor siting, and emergency planning. These include both LWR and HTGR studies. In addition, a number of HTGR studies dealt with the subject of design options; some of them were reported back in 1977. Another example of an early application by the industry would be the seismic risk analysis of Diablo Canyon.

One of the most comprehensive efforts the industry has sponsored related to the ATWS issue. A series of reports was issued by EPRI on systems and transient-event studies that were performed to help improve understanding of the issue. In addition, an evaluation of proposed ATWS-related modifications was sponsored by a consortium of U.S. utilities.

3.3 Insights

The insights gained from the PRA studies briefly discussed above have been subdivided into global, plant risk, dominant accident sequences, and plant safety enhancements.

3.3.1 Global Insights

In addition to plant-specific and generic insights, the PRAs performed to date have yielded certain global insights that it is believed apply not only to the plants analyzed but to all or most current nuclear power plants, based on our knowledge of their general design and operating characteristics.

- The process of performing PRA studies yields extremely valuable engineering and safety insights. Conceptual insights are the most important benefits of PRAs, and the most general of these is the entirely new way of thinking about reactor safety in a logic structure that transcends normal design practices and regulatory processes. PRA methods introduce much-needed realism into safety evaluations, in contrast with more traditional licensing analyses that generally use a conservative, qualitative approach that can mask important matters.

- The estimated frequency of core melt is generally higher than had been thought before the RSS and subsequent U.S. studies. However, most core melts are not expected to result in large offsite consequences. The small fraction of accidents that might lead to large offsite consequences generally involve either an early failure of the containment in relation to the time of core melt, or a containment bypass. For other containment failure modes, the retention properties of the containment are substantial.

- The range of core-damage-frequency point estimates in the current library of PRAs covers about two orders of magnitude (about 10^{-5} to 10^{-3} per year). An examination of variability in the results indicates that quantitatively pinpointing reasons for the differences is extremely difficult. It is possible, however, to uncover general reasons for the variability that are attributable to plant design, operation, site characteristics, scope of the studies, PRA methods employed, and analytical assumptions postulated. At this time, caution must be exercised in comparing the quantitative results of various PRAs.

- The specifics of dominant accident sequences and the estimates of risk vary significantly from plant to plant, even though each plant meets all applicable NRC regulatory requirements.

- The following insights about offsite consequences have been identified:

  - Estimated risks of early fatalities and injuries are very sensitive to source-term magnitudes and the timing of releases and emergency response.

  - For core-melt accidents, the estimated offsite economic losses are generally much smaller than the estimated onsite losses.

  - Estimates of early health effects and offsite property losses differ greatly from one site to another, but site-to-site differences are substantially less for latent cancers and onsite property damage.

  - Airborne pathways are much more important than liquid pathways.

- Accidents beyond the design basis (including those initiated by earthquakes beyond the safe-shutdown earthquake) are the principal contributors to public risk. This indicates that the designers, operators, and regulators have been generally effective in reducing the risks from expected operational occurrences and designbasis accidents.

- PRA studies have provided a diverse assessment, compared to traditional safety analysis, of the ways in which various elements of reactor safety contribute to risk. Among the principal insights are the following:

  - Human interactions* are extremely important contributors to safety and reliability of the plants.

  - Test and maintenance considerations are important contributors to safety and reliability of the plants.

  - Dependent failures are important contributors to plant risk.

---

*Including all types of interactions that humans can have, either with a system or with other humans, that can impact the frequency or consequences of an accident sequence.

- The failure of long-term decay heat removal is a major functional contributor to core-melt frequency.

- Small LOCAs and transients are dominant contributors to core-melt frequency in most PRAs, while large LOCAs are usually not.

- Earthquakes, internal fires, and floods seem to play an important role in plant risk, although this tentative conclusion appears to be highly plant-specific.

While much attention has been placed on dominant accident sequences and ways to reduce risk even further, one of the most important insights gained from PRAs is the need to identify and maintain the reliability of risk-important systems and components at or near the levels now present. Degradation of such systems or components can sharply increase risk or the likelihood of core melt. A safety or reliability assurance program appears to be the desirable way to proceed. This may or may not require safety goals.

3.3.2 Plant Risk

The results of a number of studies, including the RSS, indicate important distinctions between contributors to different types of outcomes of potential accidents. The risk cannot be measured in terms of any single indicator, and changes in plant configuration that significantly affect one indicator may or may not affect the others. For example, a modification that reduces the frequency of core melt may not significantly affect public risk, and vice versa. Hence, a risk-management strategy that focuses on core-melt frequency is not likely to result in the same set of actions as a strategy that focuses on public risk.

The results of PRA studies are expressed in terms of core-melt frequencies, frequencies of radionuclide releases of various magnitudes, or curves presenting the frequencies of occurrence of different consequences (e.g., early and latent fatalities), depending on the level of the PRA.

3.3.2.1 Core-Melt Frequencies

One of the results of a PRA study is the identification of the accident sequences that are the dominant contributors to core-melt frequency. An analysis of several published PRAs has shown the relative contribution to core-melt frequency of several salient features of the dominant accident sequences as summarized below:

- The split between LOCA and transient contributors to core-melt frequency is about equal for PWRs and about 10:90 for BWRs. However, some recently completed studies for newer PWRs indicate ratios similar to those for BWRs.

The split is attributable to the emphasis placed on independence and separation of safety equipment trains. Such designs reduce contributions from rare events like pipe ruptures, but make it more difficult to protect the plant from frequent events.

- The failure of long-term decay-heat removal is a major functional contributor to core-melt frequency for both PWRs and BWRs. It is associated with LOCAs in PWRs and with transients in BWRs.

- In general, anticipated transients without scram are small contributors to core-melt frequency in PWRs but significant contributors in BWRs.

3.3.2.2 Radionuclide Releases and Offsite Consequences

- The results of many of the studies done shortly after the RSS indicated that the dominant core-melt and dominant radionuclide-release sequences largely coincided. This resulted from the conclusion that each core-melt sequence leads to a containment failure with a fairly high likelihood of a large radionuclide release to the atmosphere. Hence, the core-melt sequences with the higher frequencies generally yielded higher frequencies of significant releases. A departure from this trend is seen in more recent PWR studies, which have not found that all core-melt sequences lead to containment failure.

- The accident sequences that appear to emerge as dominant contributors to release are those in which either radioactive material bypasses the containment or the containment fails concurrently with (or shortly after) core melt. This early containment failure may be caused by major common-cause initiating events, such as earthquakes. Such sequences are not necessarily the dominant contributors to core-melt frequency (e.g., interfacing-system LOCA).

- Some of the insights about source terms gained since publication of the RSS are:

  - Early source-term predictions generally ignored some potential processes and phenomena that would reduce atmospheric releases and are therefore likely to be overestimates.

  - For those core melts that do not cause containment failure, the retention properties of the containment are substantial.

  - If the containment fails a long time after core melt, only small to moderate release fractions result. The range between the predictions of various studies is extremely wide for these cases, and further resolution from current analytical and experimental programs is expected.

- Only containment bypass, early overpressurization sequences, or sequences involving common-cause containment and core-cooling failures lead to large releases. Because of the existence of dose thresholds, the occurrence of early health effects is generally limited to these containment-failure modes.

- All offsite consequences are sensitive to the amount of radioactive material released during an accident (the source term). However, early fatalities and injuries are particularly sensitive because of the existence of dose thresholds for these effects. If potential source terms for the most severe accidents are substantially smaller than previously assessed (by at least one order of magnitude), then the risk of early fatalities generally would no longer be a principal concern.

- In addition to the source-term magnitude, the estimated number of early health effects is very sensitive to assumptions about the nature and effectiveness of potential emergency protective measures. For large releases of radioactive material, prompt evacuation and sheltering are potentially effective means of reducing the numbers of early health effects. Latent cancer fatalities are not as sensitive to emergency response assumptions because larger areas and longer exposure times are involved.

- The weather (wind speed, rain, or dry weather) at the time of the accident can have a very large effect on offsite consequences. However, the variation in weather from site to site does not appear to affect the total risk appreciably because the probabilities of weather types that contribute the most to variation in consequences are not significantly different in different climates. However, total risk depends strongly on site characteristics such as population density and land use, and these considerations are important for reactor siting.

3.3.2.3 Externally Initiated Accidents

- PRA studies have provided a new understanding of the importance of externally initiated accidents to public risk. In addition, specific insights into system response and methodology application have been derived. The impact of external initiators appears to be highly plant-specific.

- Those external initiators involving the plant site, such as seismic, external flooding, and high winds, are generally accompanied by loss of offsite power, which contributes to associated systems unavailabilities.

- For seismic events:

  - Earthquakes significantly larger than the SSE are the significant seismic contributors to public risk.

  - Local ground and subsoil conditions have been an important issue in all PRAs addressing seismic risks.

- Most of the fires found to be important to core-melt frequency or risk are those whose likelihood and/or severity are substantially reduced by the new NRC regulatory approach now being implemented (Appendix R, 10 CFR 50, and associated regulatory guides and standards).

- For high winds, metal-sided structures are more fragile than other structures and most equipment and are more likely to compromise the overall plant safety.

3.3.3 Dominant Accident Sequences

The RSS showed that the risk posed by the two plants studied stemmed primarily from a few accident sequences. Thus, the understanding of risk, and the ability to effectively reduce risk, hinges on an understanding of the accident sequences that dominate risk. The importance of the generic nature of the dominant accident sequences identified in the RSS was also recognized. If, for example, the dominant accident sequences were the same for all PWRs, then regulatory decisions or design alternatives that reduce the risk from the dominant accident sequences would be effective for all PWRs. Important insights include the following:

- Dominant accident sequences are <u>not</u> consistent across very broad classes of plants (e.g., all PWRs or all BWRs) because each plant is unique and may exhibit accident sequences that are peculiar to its individual design, operation, and siting.

- Dominant sequences can be categorized according to the sequence of plant functions that failed (as opposed to the sequence of specific events that occurred). Two accidents may have different sequences of specific events yet have the same sequence of functional failures. Functional accident sequences can be defined in terms of the initiating event (transient or LOCA) and then by the subsequent functional failures.

- Functional accident-sequence categories have been tentatively identified for PWRs and BWRs. Specific component failure modes or human interactions involved in these sequences can be expected to vary from plant to plant.

- Despite plant-to-plant variations, it appears that generic studies to support regulatory decisionmaking can be performed effectively by virtue of grouping the plants into a number of classes with similar dominant functional accident sequences.

3.3.4 Plant-Safety Enhancements

Next to an explicit quantification of public risk or core-melt frequency, the identification of specific safety concerns and the evaluation of possible solutions to implement risk management are probably the best recognized and most widely used applications of PRA. The performance of a PRA naturally leads to significant improvements in the understanding of the design and operation of the various systems, the response of the containment, and the role of plant operators under accident conditions. This understanding, in turn, often reveals design or procedural modifications and training programs that can enhance safety. There are numerous examples of changes that have been made or are under active consideration. Several are summarized below.

- The Big Rock Point study showed that several of the changes proposed under the post-TMI action plan and SEP did little to reduce the risk or were not cost effective, but the analysis did reveal several other areas where enhancements could be made. The study recommended seven changes (six design and one procedural).

- During the Shoreham study, two design changes were recommended and others were slated for further evaluation. One of the implemented changes was to modify the design of viewing windows on containment hatches so that their ultimate strength matched that of other structures in the containment. Even though these windows were previously rated for design-basis-accident pressures, they would have failed at lower pressures than other parts of the containment for dominant risk sequences. Another implemented change was the trip setpoint of the reactor-core-isolation cooling system, which permits the system to operate during a LOCA.

- The Zion study analyzed the relative risk-reduction benefits of both large- and small-scale proposed design modifications. These modifications included a refractory core ladle, a filtered-vented containment, and the addition of hydrogen recombiners, all of which had been selected for consideration the PRA. In the course of the PRA, it was readily identified that a fourth option, a diesel-driven containment spray pump modified to be independent of ac power, not only would cost considerably less but would also effect a greater reduction in an already very low risk level than the three costly alternatives that had been proposed prior to the PRA. More importantly, the results supported the decision option to leave the plant the way it is.

- In the aftermath of the TMI accident, the NRC mandated that a utility install an additional auxiliary feedwater pump at each unit of the two-unit plant. The detailed analysis of dependent failures involving support systems in this PRA determined that the number and type of pumps in the original (two-pump) design, which included one motor-driven and one turbine-driven pump, were not the keys to this system's contribution to risk reduction. The key was the fact that both pumps were dependent on an electrically powered chilled-water system. The third pump was installed in the turbine building so that it would be independent of the chilled-water system.

- The PRA for Indian Point 2 identified seismic events as an important contributor to core-melt frequency and latent health effects. The failure mode of greatest importance involved the loss of plant control as a result of disabling the control room. The sequence of events included a strong motion earthquake and the subsequent interaction of the control-room building roof line with an adjoining structure. The result was a possible collapse of the control-room roof and inaccessibility of plant controls. An analysis of this scenario identified an effective modification. It involved increasing the gap between the two buildings and installing rubber bumpers. This relatively inexpensive modification increased the seismic capacity substantially. As a result, the core-melt frequency due to seismic events was reduced by about a factor of 10. A similar reduction was achieved for the latent health effects.

- Several changes were recommended as a result of the RSSMAP and IREP studies. For example, the IREP study for Arkansas Nuclear One identified several procedural changes to reduce the probability of core melt. These included staggering the quarterly tests on the station batteries to reduce the probability of common-cause failures in the dc power supply; correcting the procedure for low-pressure pump tests to prevent leaving valves misaligned; and including sensors in the tests of the cooling system for the ac/dc switchgear room.

- Generic insights from conclusions on design and procedures that are replicated over a number of plants are evolving from such programs as Severe Accident Risk Reduction Program and IDCOR. Examples include reduction of the probability of interfacing-system LOCA by improving maintenance procedures for the interfacing check valves; changes to improve the reliability of auxiliary feedwater systems, ac power systems and the reactor protection system, etc. An example of how PRA techniques can be used in this manner is presented in Appendix B.

APPENDIX A

STATE OF THE ART OF

PROBABILISTIC RISK ASSESSMENT (PRA)

APPENDIX A

CONTENTS

CONTENTS (Continued)

ILLUSTRATIONS

APPENDIX A

STATE OF THE ART OF PROBABILISTIC RISK ASSESSMENT (PRA)

A.1 Introduction

PRA is a multidisciplinary process requiring data and analyses from system engineers, plant personnel, data analysts, human behavioral scientists, experts in accident phenomenology, geologists, and other specialists. Not all of the methods involved have reached the same level of development. Some, such as reliability analysis, have been practiced in some form since World War II. Others, such as the analysis of core-melt progression, are new and unique to reactor technology.

This section of this appendix consists of a brief discussion of the various tasks that comprise a PRA and presentation of the characteristics used to determine the state of the art. Following this general background material, the state of the art is discussed in Sections A.2 through A.6 for the six areas involved in a complete PRA. Accident processes, containment response, and fission-product behavior have been treated together in Section A.5 since they are closely connected. After a short consideration of sabotage, the appendix concludes with a summary.

A.1.1 Tasks Associated with PRAs of Various Scopes

The tasks associated with PRAs of various scopes are presented below. Each task is briefly described, and the relationships between tasks are discussed. The steps involved in the analysis are shown in Figure A-1.

Since PRAs require large amounts of information, the first step is information collection. The information that is required depends on the scope of the analysis and falls into three broad categories:

- Plant design, site, and operation information
- Generic and plant-specific data
- Documents on PRA methods

The next task is systems analysis, which involves the definition of accident sequences and analysis of the important plant systems. It also includes the development of a data base for initiating events, component failures, and human errors. It constitutes a major portion of the PRA and hence is divided into the several subtasks discussed below.

The event-tree-development subtask delineates the various accident sequences to be analyzed, combinations of initiating

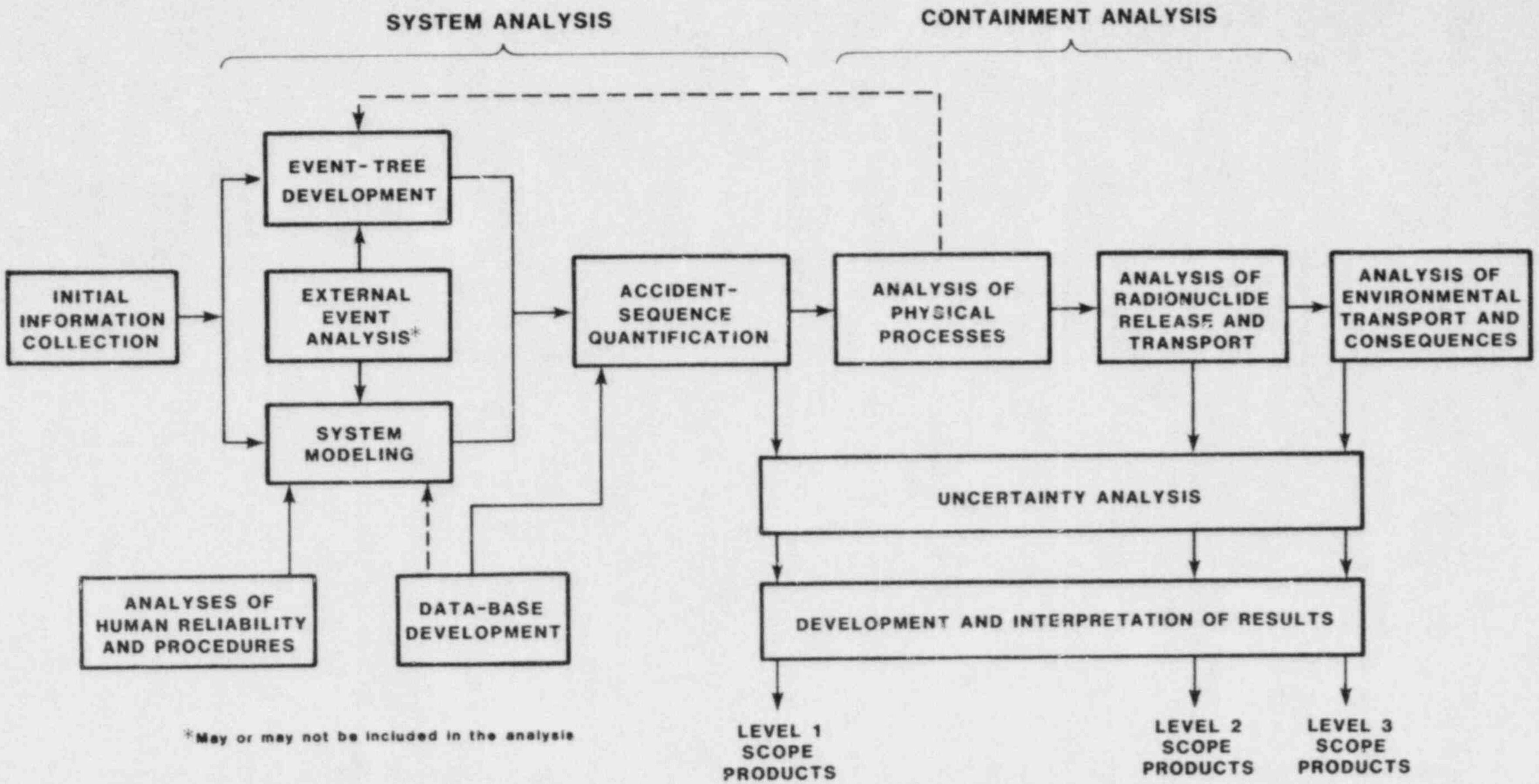


Figure A-1. Risk Assessment Procedure

events, and the successes or failures of systems. This activity includes an identification of initiating events and the systems that respond to each initiating event.

The system-modeling subtask involves the construction of models for the plant systems covered in the PRA. The systems to be analyzed and their success criteria are identified in conjunction with event-tree development in an iterative process. Assistance from thermal-hydraulic and containment analyses may be needed to derive realistic system-success criteria. The system models generally consist of fault trees developed to a level of detail consistent with available information and data.

Past PRAs have shown the importance of operator error. These human errors are included in the system models. The analysis performed in the human-reliability subtask involves a review of testing, maintenance, and operating procedures to identify the potential human errors to be included in the analysis. A review of the plant's administrative controls and procedures and the design of the control room is also performed to establish a foundation for the assignment of failure rates to the human errors found to be significant.

In the data-development subtask, a component data base is developed by compiling data, selecting appropriate reliability models, establishing the parameters for those models, and then estimating the probabilities of component failures. The data used may be generic industry data or plant-specific data, or a combination of both. Data on transient initiating events are also gathered and analyzed in this subtask.

The next major task involves the quantification of accident sequences. In order to quantify the frequencies of the accident sequences delineated in the event trees, failure rates are developed for each system, and frequencies are determined for each initiating event. Combining the appropriate system success and failure models with each class of initiating events yields a logical representation of each accident sequence that can then be treated mathematically, including uncertainties.

The containment analysis task is important for differentiating among the consequences of various core-melt accident sequences and consists of two subtasks: the identification of the containment-failure modes, and a prediction of the amount of radionuclides released to the environment for each accident sequence.

A core-melt accident would induce a variety of physical processes in the reactor core, the pressure vessel, the reactor coolant system, and the containment. Computer codes have been developed to assist in the analysis of these processes. The results provide insights into the phenomena associated with the accident sequence, a prediction of whether the containment fails, and the conditions and flows needed to determine the fission-product release and transport.

A containment-event tree is developed for each sequence of interest. If the containment is predicted to fail, the analysis predicts the time at which it will fail, where it will fail (i.e., whether radionuclides are released directly to the atmosphere through the containment building, or to the ground through the basemat), and the energy associated with the release.

For each core-melt accident that is postulated to breach the containment, it is necessary to estimate the quantity of fission products that would be available for release to the environment. In this subtask, the behavior of the radionuclides released from the reactor fuel during the accident is modeled. The model also considers fission-product transport and removal (e.g., deposition) inside the reactor coolant system and the containment before containment failure. The result of this analysis is a prediction of the amount and type of radioactive material released into the environment at the time of containment failure for each accident sequence.

The offsite consequence analysis assesses the risk to the general public associated with the plant by calculating the consequences associated with a given release, and combining this with the estimated frequency of that release. Consequences are generally expressed in terms of early fatalities, early injuries, latent cancer fatalities, genetic effects, and property damage. To perform this task, the analyst uses a computer model that begins with the quantities of various fission products released from the containment and analyzes their transport through the environment, using site-specific meteorological data and, in some cases, information on the local terrain as well. Data on exposure pathways, dosimetry, and population density are then used to calculate the radiation doses delivered to the population, and a health-effects model is used to estimate mortalities and morbidities. The economic consequences usually computed are those resulting from relocation of the population and interdiction or decontamination of the land. The results of the analysis are usually consequence distributions (e.g., plots of the predicted frequency for consequences of varying magnitudes) for each accident-release category.

External initiators, frequently excluded from earlier PRAs, include winds, fires, earthquakes, and floods. This task uses the models developed in the system analysis, which are either analyzed independently from the perspective of external events or modified to reflect external events explicitly. Additional event trees are sometimes developed to delineate the external event sequences to be analyzed. The results of the external initiator analysis may be incorporated into the accident-sequence analysis or may be developed separately all the way through the consequence analysis.

The final step in performing PRAs of various scopes is to integrate the results of the various tasks, determine the overall uncertainty, and interpret the results. This integration includes, among other things, the tabulation of frequencies for accident sequences important to risk, the development of complementary cumulative distribution functions for the plant, and the development of distributions reflecting the uncertainties associated with accident-sequence frequencies.

To provide focus for the assessment, the results are analyzed to determine which plant features are the most important contributors to risk. These engineering insights constitute a major product of the analysis. Insight into the relative importance of various components and the relative importance of various assumptions to the results may be developed from the uncertainty and sensitivity analyses. A discussion of these insights provides additional perspective to the analysis.

A.1.2 Level of Development

When using PRA in regulation, one must consider the strengths and weaknesses of each part, in addition to the strengths and weaknesses of the whole process. In other words, the level of development of the different methods used in PRA must be taken into account. The level of development of an analysis method depends upon several characteristics: stability of the method, degree of validity or realism, reproducibility, degree of uncertainty, desirability of major progress to improve the method, and feasibility of achieving that progress, especially in the near future.

The stability of a method is a measure of the rate at which the methodology is improving. A methodology undergoing rapid development is unstable, and its results must be utilized with caution because our level of knowledge may expand rapidly in the near future. This does not imply that stable methodologies are necessarily more satisfactory or that their results can be used without caution.

The degree of validity or realism is the extent to which approximations or conservatisms may have been knowingly or unknowingly introduced into some parts of the PRA because of unknowns, attempts to simplify the models, or error. Whether the ultimate "result" is valid within its stated uncertainties, and whether it is conservative or nonconservative, will depend on the degree of realism. The degree of validity is ultimately measured by comparison with experiments that demonstrate how the real world behaves. In some areas, a lack of relevant experiments can make complete validation difficult or impossible.

Reproducibility refers to how standardized and accepted certain methods, assumptions, and data are. In an area with high reproducibility, different analysts confronted with the same system would proceed in similar manners and produce analyses that were comparable. For an area with low reproducibility, different analysts would use different methods and produce results which differed significantly.

Most of the uncertainties associated with PRA reflect a lack of data, experience, and knowledge about system response, human behavior, accident phenomenology, and the other areas involved. These uncertainties also exist in deterministic modeling and in engineering judgment. PRA usually should display the uncertainties associated with an analysis explicitly, and this has focused attention on them. This explicit treatment of uncertainties by PRA is a strength rather than a limitation; it provides important information to the decision-maker. A proper uncertainty analysis permits the user to evaluate the impact of the lack of experience and knowledge on the engineering insights drawn from PRA. The remaining sections of this appendix address the current level of development of the various elements of PRA methodology and practice.

A.2 System Modeling

A.2.1 Background

System models delineate the behavior of plant systems in response to potential initiating events, the outcome being either a successful termination of the accident sequence without significant core damage or else progression to core damage or core melt. System modeling identifies the important accident sequences and determines their frequencies of occurrence. Each sequence is a unique combination of system failures and successes.

The two aspects of plant and system modeling are developing the models, and evaluating and quantifying them. Although each of these aspects has its own unique characteristics, the activities in each depend strongly on the state of the art in the other. For example, the ability to evaluate and quantify the models depends on their complexity.

The development of the system models consists of applying techniques for postulating potential events associated with plant equipment and operation and displaying these events graphically. In general, this is done by inductively constructing models that examine the effects of various functional (or system) successes or failures following a given initiating event (typically, event trees). This is, in turn, followed by models that deductively trace the undesired system failures identified by the event tree back to their potential root causes (typically, fault trees). These models can be used to estimate the frequency of each accident sequence and to identify the dependences and interrelationships that can affect plant performance. The dependences considered include functional relationships, human error, shared hardware, and shared support systems. The treatment of dependences is partially determined by the level of resolution of the modeling activity, which, in turn, usually depends on the objective of a specific study.

One objective of system modeling is to evaluate the significance of faults in the context of an accident. However, the level of resolution of system models is partly determined by the data available to quantify the models. The modeling effort is often terminated at the level where reasonable quantities of data exist. Thus, for example, if data exist for diesel generators, the analyst may not model the constituent parts of the engine explicitly. Where adequate data do not exist for certain characteristics, assumptions may be made. Thus, for example, the analyst may assume that a comprehensive preoperational testing program identified significant design, construction, and fabrication errors, and therefore he or she will not include such errors in the plant models. However, since failures of these types contribute to the overall hardware-failure rates used in quantification, they are implicitly considered to some extent.

Model development is currently somewhat constrained because the discrete, binary modeling techniques* usually used may not apply directly to continuous processes. This usually does not introduce significant difficulties because accident timing is replicated by arrangement of event-tree headings in a temporal fashion, i.e., listing first those events expected to occur first, and different time domains can be modeled explicitly when necessary.

Quantitative evaluation of the models yields the predicted probability of system failures and the expected frequency of occurrence for the accident sequences. The quantification process requires that system success states be considered as well as failure states, when those successes are important to the postulated outcome. Accident sequences are often combined in categories based on similar outcomes.

---

*Fault trees usually model a component as either operable or failed. They usually do not consider faults such as a valve 50% closed or a pump delivering 60% of rated flow.

Computer codes are usually employed to identify minimum cut sets (the smallest sets of faults that can result in the accident sequence, including the initiating event and all specified system successes and failures). These codes also compute the probability of system failure and the frequency of the accident sequence based on the logic contained in the models and the input data.

Although many of the computational techniques have been developed to accommodate large models, PRAs generally produce system models so large that they require reduction in size before and during the evaluation process. Some of this reduction is manual, and some employs computational techniques. The objective of model reduction is to retain only the important and numerically significant information. The two major techniques associated with reduction are: (1) coalescing events independent from other models into a single event, and (2) truncating models and/or cut-set results based on numerical criteria. These reduction efforts are aided by computational techniques that can identify independent submodels or can keep track of the number of minimum cut sets which are not numerically included in the quantitative result. Thus, while the truncation process introduces some compromises, the effect of these compromises can usually be determined in at least a bounding manner and the truncation criteria altered if they appear to have a deleterious impact.

System modeling is partially a process of coalescing large amounts of information and grouping that information into a small number of classes, within each of which all the information shares similar characteristics. Therefore, the results represent the manipulation of classes of information sharing similar qualities. However, since these classes contain information that, while similar, is not identical, this agglomeration process can reduce the precision of the results. For this reason, the system modeling effort should be an iterative process in which the sensitivities of the models to the various assumptions made are explored.

System-modeling accuracy can be affected by the accuracy of the thermal-hydraulic modeling. On one hand, the accident sequence provides data on plant system states for input to the accident-process analysis. On the other hand, the thermal-hydraulic analysis of conditions before the onset of core damage provides information needed to determine system operability and classify accident sequences. The ability to postulate accident sequences accurately depends upon the ability to understand the early accident progression and the impact on system operation and functional performance. Uncertainties in the knowledge of the progression of the accident, particularly in its early phases, contribute to the difficulties of accurate system modeling. This can lead to conservative assumptions regarding system operability requirements because in many cases only conservative analyses used for licensing determinations are available.

Because of the limited ability to treat them quantitatively, certain issues are considered only at a functional level involving little detailed modeling. These include such issues as pressurized thermal shock, reactor vessel rupture, and certain containment failures (e.g., failure at less than burst pressure). Technical resolution of the likelihood of these events will allow them to be included in greater detail in future PRAs. Other considerations may be outside the boundary conditions of the study, because of the specific objectives for the study. These boundary conditions should be identified explicitly in the documentation of the analysis. In addition to these known omissions, there may be omissions of which the analysis team is unaware: for example, an unknown failure mode for a particular component, an interaction between two systems that was not considered, or an initiating event that was overlooked.

Thus, there is always the possibility that the PRA models themselves are incomplete. While the potential for omissions remains a concern, it is believed that omissions that could significantly alter or negate insights gained from PRAs are unlikely, due to the number of PRAs that have been performed to date. Although completeness cannot be demonstrated, except within the very rough bounds of operating experience, the consensus of the PRA community is that most of the major insights obtained from PRA are valid and will remain valid, even if new accident sequences and sequence dependences are identified and added to the model. Obviously, however, unrecognized sequences or dependences could change the quantitative total core melt or risk results significantly.

Identifying initiating events is a particularly difficult area in which to establish completeness. Techniques for identifying these events include reviewing general nuclear plant operating experience, developing master logic diagrams, and analyzing initiating-event/mitigating-system interactions. Initiating events are classified by potential mitigating actions. While these classes provide only representative cases and not the particulars of each event, they do represent the functional requirements of the class. The analyst must consider the context in which the various events in a class of initiators might occur and construct the models accordingly.

The greatest strength of plant modeling lies in the process itself. Following the patterns of investigation dictated by application of the modeling techniques results in a rigorous look at plant design and operation. This provides the analyst with insights, in addition to those gained in the traditional design-review process, which result in improved ability to identify potential design problems or operational weaknesses and provide a means for suggesting optimum solutions.

Another advantage of PRA system modeling is that it constructs an integrated framework for examining the importance of individual items associated with plant design and operation. This means that the results represent the synthesis of knowledge about such diverse items as human-error rates and thermal-hydraulic conditions. Not only are these diverse items treated in a combined model, but their importance to the results can be compared, individually or in groups. Also, the resulting model provides the context in which to address the importance of various issues as they arise.

The utilization of the system models to perform sensitivity studies is of significant value. A sensitivity study consists of changing some aspect of the modeling input (such as probability data, basic assumptions, plant design, system-success criteria, or physical-process understanding), followed by changing the model development and/or its evaluation and comparing the results to the previous output. The differences provide a measure of the impact of a proposed change. Sensitivity studies also yield results that can assist in indicating the numerical magnitude of selected modeling uncertainties and assumptions and suggesting areas where more detailed analysis is desirable.

A.2.2 State of the Art

The basic approach to system modeling is much the same as it was for the Reactor Safety Study (RSS) (NUREG-75/014) a decade ago. The RSS identified the accident sequences using an inductive event-tree analysis technique and the system failures using a deductive fault-tree analysis approach. These models were evaluated and quantified with a combination of computer and manual techniques. While the basic approach to plant modeling activities has continued to include models for both accident sequences and system failures, many refinements in technique, especially in evaluating and quantifying models, have occurred since the RSS was published. Many of these changes have broadened the scope of the modeling activity, and other changes have resulted from attempts to make the modeling activity more comprehensive.

Since the RSS, the application of event-tree and fault-tree analysis techniques to PRAs of nuclear power plants has resulted in the development of various descriptions and procedures for using these methods. Among the most prominent are the PRA Procedures Guide (NUREG/CR-2300) and the Interim Reliability Evaluation Program Procedures Guide (NUREG/CR-2728). These provide some consistency in the development of plant models. The level of resolution of the final models can vary with the method selected and is dictated by the objective of the study once the method is selected. Some variability may enter, based on the experience and interest of the individual analyst.

Some techniques have been developed to allow the analyst to spend less time in actual model construction, so that more effort can be spent on the investigative aspects of system modeling. These techniques, developed for system failure modeling, consist of either abbreviating the model graphics or using preconstructed fault-logic modules, as appropriate, for fault-tree construction. While these refinements remove some of the drudgery from the modeling effort, they do not necessarily reduce the likelihood that the inexperienced analyst will build a model that may not accurately represent the system being analyzed and, if not used properly, could increase the likelihood of modeling error.

The investigation of common-cause failures has also been refined. Indeed, Section A.7 addresses an entire class of potential common-cause failures (external events). Dependencies associated with support systems are explicitly modeled. Some other types of common-cause failures, such as manufacturing defects and installation errors, are not usually treated explicitly in the models. An estimate of their importance can be gained by considering dependent failure data and modifying the quantitative results, if necessary. Information on the root cause of the dependent failures may not be available, but the quantitative results can include the effect of the dependences, to some extent.

Improvements have occurred in the treatment of initiating events. Developments in the analysis of the initiating event/mitigating system dependence now accommodate a more explicit treatment of the dependences. Modeling techniques, primarily the failure-mode-and-effects analysis, are being used to identify plant faults that can be accident initiators and can also degrade mitigating systems or cause their failure. Additional techniques, such as constructing a master logic diagram, assist in identifying a more complete set of initiators. Finally, external events are now considered as special initiators. This has led to their improved treatment and recognition of the importance and potential influence of these events.

The identification of accident sequences has undergone some refinements primarily because of two items. The first is the changing state of knowledge of accident phenomena, which affects the structure of the event trees and the outcome of certain sequences. Examples of this effect are changes in the understanding of the ability of certain centrifugal pumps to pump saturated fluid and the ability to cool the core after some melting occurs. Second, previous PRAs have raised questions about realistic success criteria for various plant systems under accident conditions. Changes in definition here can affect not only system failure models but also accident-sequence delineation activities by identifying new event-tree headings or changes in the outcome of previously identified sequences. Some PRAs now include best-estimate thermal-hydraulic calculations to support the plant modeling effort in this regard.

Since the RSS, considerable activity has been devoted to developing computerized techniques to evaluate and quantify plant models. The PRA Procedures Guide (NUREG/CR-2300) identifies the plethora of codes now available for this purpose. The primary motivations behind this activity are to handle larger models and to accommodate the interest in both the qualitative and quantitative aspects of the modeling activity. In addition, analysis activity shows a trend toward the evaluation of plant models on the accident-sequence level, resulting in the need to manipulate the system models in groups to support such diverse interests as accident phenomenology, system-success criteria, and identification of recovery actions. This analysis provides qualitative information for evaluating accident sequences or system failure or both, depending upon the focus of the analysis.

Validation of PRA results through experience is not now readily available because, by its very nature, PRA deals with events which are predicted to be very rare. This raises questions about the correctness of the results and is especially important when considering the utilization of results in an absolute sense. However, certain portions of the analysis can be verified to some extent by comparison to operating data. If PRA results are to be used to make decisions about regulation, the validity issue in relation to plant design and operation is also important. Currently, resolution of the validity issue involves examination of the proper application of the methods, improvements in the completeness and accuracy of the PRA plant-modeling techniques, and comparison of plant experience with predictions to assist in methodological development.

A.2.3 Limitations and Uncertainties

The primary uncertainties and limitations associated with system modeling fall into the two broad categories of completeness and representativeness. The degree to which these uncertainties and limitations affect the results of system modeling depends on the use intended for the results. Therefore, the inherent uncertainties and limitations associated with system modeling must be recognized in light of the nature of the results that are required.

The completeness issue was discussed in section A.2.1. It is not possible to identify all possible occurrences which may affect the initiation and ultimate course of accident sequences. However, because the analysis involves a detailed search for such interrelationships, there is a general feeling in the PRA community that most of the insights gained are valid, but that the quantitative results may be more uncertain than usually identified.

A model by its nature is an abstraction, a compromised representation of physical reality, so inevitably representativeness becomes a concern. Many assumptions must be made during plant modeling. In addition, the constraints imposed by the modeling techniques themselves require a number of compromises. Coupled with a limited understanding of some physical processes, these facts constitute the issue of validity or representativeness of plant modeling. The degree to which this is a problem is difficult to measure because few references are available. The effect of compromises can often be assessed, and conservatism may be introduced intentionally when knowledge of plant response is lacking.

The issues of validity and completeness influence the subsequent use of the results to support judgments about the level of safety of nuclear plants. PRAs are very useful as tools to use in understanding the general level of safety of a plant or the importance of an issue, but high reliance on numerical results is not prudent until many of these issues identified above are better resolved. This lack of perfect validity and absolute completeness is only a relative problem; however, judgments based upon the results can be made, even though the results have some limitations. Understanding these limitations can assist the user in drawing appropriate conclusions from the results.

A.2.4 Potential Improvements

The single greatest source of improvement to plant modeling techniques is likely to be increased experience in both actual nuclear-power generation and model usage. For example, over a period of time, the question of completeness will continue to be addressed. If previously unidentified events should occur, the completeness of the models can be enhanced by considering these new kinds of occurrences. If no new events should occur, even greater levels of confidence in the completeness of the existing models will be warranted. Likewise, increased operating experience and continuing data collection will provide empirically derived values for initiating-event frequencies and component-unavailability data that can be used to improve parameter estimation.

Scaled thermal-hydraulic experiments and improved analytical techniques may provide a better understanding of some accident processes, which may, in turn, provide an enhanced ability to model the systems involved and determine more realistic success criteria. With increased experience, some of the modeling techniques themselves may be modified to improve and extend their capabilities.

Although improvements will undoubtedly result, some limitations seem to be inherent in the modeling techniques and will probably continue to exist. The need for formulating assumptions and constraints with respect to plant models is a direct outgrowth of the inability to consider everything or know everything. Assumptions and constraints, by definition, introduce uncertainty and exclude information from the analysis.

A.3 Human Interactions

Experience in many industries has shown the importance of human interactions in the operation and safety of various types of plants. PRA methodology has emerged as a promising tool for prospectively assessing the effect of humans on the plant risk and for understanding the man-machine interface.

Human actions are important in the operation, control, maintenance, and testing of equipment in virtually all industrial activities. These beneficial interactions, including repair and recovery operations, often enable various systems to achieve high availability. However, a dichotomy exists: although such human interactions are largely responsible for maintaining high availability, the human contribution to accidents that do occur has been estimated as high as 90% in the cases of the airline (NUREG/CR-2744) and chemical industries (Joschek, 1982).

Published PRAs for nuclear power plants have yielded similar findings (Joksimovich et al). Past PRAs have indicated that both beneficial and detrimental contributions of the human influence affect the order of dominant sequences and, hence, the risk profile of the plant. They have pointed out the importance of human actions that can cause initiating events or result in the unavailability of plant systems before an initiating event. Surveys of licensee event reports indicate that a significant number of equipment failures are human-related. Beneficial human interactions include the diagnosis of accident sequences and recovery of safety functions. PRA techniques provide a framework for assessing the importance of human interactions in a spectrum of accident sequences.

The definition of specific accident sequences in PRA studies provides the analysts with a tool for determining where the human might affect the risk estimates. For example, the uncertainties in the quantitative impact can be assessed, the ways in which humans influence the course of an accident can be described, and the importance of humans in a particular sequence can be quantified.

A.3.1 Background

The basic methodology for considering human interactions stems from the techniques first developed in the RSS (NUREG-75/014). The RSS, in addition to representing the first full-scale application of PRA techniques to LWRs, also used a human reliability technique called THERP (Technique for Human Reliability Error rate Prediction). THERP, initially developed in 1961, has undergone a number of improvements since. The limitations in the early methodology were recognized and have stimulated numerous discussions with human behavioral experts outside the PRA field to gain suggestions for improvements. As a result, a revised version of the Human Reliability Analysis Handbook was recently prepared (NUREG/CR-1278). The revised version attempts to improve the consistency of trained analysts and to expand upon models for the diagnosis function in accident response. The application of the THERP methodology was documented by examples in NUREG/CR-2254.

The proposed THERP diagnosis model is generic for all events; therefore, considerable judgment is required in applying it because data collection has not been directed toward diagnosis. A need remains for diagnostic models to consider the different thought processes associated with specific accident conditions. Human decisions have been key factors in several actual events, and in some cases poor judgment or lack of comprehension has increased the severity of the event.

The techniques used in the PRA studies to model human errors vary considerably. For example, some current PRAs try to account for cognitive human behaviors with techniques such as the operator action tree (NUREG/CR-3010), time-reliability correlations (NUREG/CR-3010), confusion matrices (Potash et al), and specific recovery models (NUREG/CR-2787). A review of five recent PRA studies (Joksimovich et al) showed that the modeled human interactions have a major influence on the core-melt frequency and the ordering of the dominant sequences in many instances. Furthermore, some of the human-error analysis methods appear to be specific to a particular study and have been integrated differently with the other tasks, making reviews and comparisons difficult. Thus, while the development of techniques was expanding rapidly, approaches for integrating the techniques into PRAs lagged behind.

A.3.2 State of the Art

The most recently published PRAs benefited from the groundwork established in the RSS. In general, they have recognized the importance of human interactions, although this is not always stated quantitatively. The types of human interactions identified in the recent PRA studies included the following:

- Type 1. Prior to an initiating event, plant personnel can compromise equipment and availability by inadvertently disabling it during normal operation or when the plant is down for repair or testing.

- Type 2. By committing an error, plant personnel can initiate an accident.

- Type 3. By following procedures during the course of an accident, plant personnel can operate standby equipment that would terminate an accident.

- Type 4. Plant personnel, attempting to follow procedures, can make a mistake that aggravates the situation or fails to terminate an accident.

- Type 5. By improvising, plant personnel can restore and operate initially unavailable equipment to terminate an accident.

For each type of human interaction, the three important questions are: (a) how are the human interactions incorporated, (b) which techniques for modeling human interactions are used, and (c) what type of data are available? These are addressed below.

Type 1 interactions are modeled by selections of system unavailability data or by modeling explicitly, using the THERP technique, the procedures for performing tests or maintenance. Type 1 interactions are generally included in all PRA studies and are easily incorporated into the standard fault trees. The data in NUREG/CR-1278 are generally applicable, but the human-error probabilities may not include all aspects of decision making.

Type 2 interactions are generally implicit in the selection of initiating events. They usually include human effects already in the outage-frequency data base which, because of agglomeration, may not identify specific human interaction causes. A few studies have identified specific human-caused initiating events through failure-modes-and-effects search methods.

Type 3 interactions involve the success and failure in following preestablished procedures and the ability to select the correct procedures given the information available to the operator. The THERP technique has been used to develop the framework for quantifying the reliability of following a procedure. More recent developments such as OATS (NUREG/CR-3010) and the improved THERP diagnosis model (NUREG/CR-1278) account for correctly selecting the appropriate procedure. Such interactions may be incorporated into the logic of the fault trees and event trees by the system analysts or factored into the analysis during accident-sequence quantification. The data used generally are derived from NUREG/CR-1278 or expert opinion techniques such as paired comparisons or psychological scaling (NUREG/CR-2255).

Type 4 interactions are the most difficult to identify and model. Modeling requires iterations between the human-reliability analysis and the system analysis to help identify the important human interactions which could aggravate the situation. A technique has been developed to help identify these human actions (Potash et al). A confusion matrix is constructed to help the analysts identify cases where the operator's mental image of the plant differs from its actual state, and thus the operator's actions become "the right actions for the wrong event." Quantification is carried out by the use of expert opinion. Only a few PRAs have attempted to include this type of interaction, and those only to a limited degree. Once the actions are identified, they can be incorporated into the logic structure of an event tree or fault tree or factored into the quantification process. Very few data are available for predicting these types of human interactions. However, retrospective analysis can usually identify these kinds of causes.

Type 5 recovery actions are generally included in the evaluation of accident sequences that dominate the risk profile. These actions may include the recovery of previously unavailable equipment or the use of nonstandard procedures to ameliorate the accident conditions. They can be incorporated into the PRAs as recovery factors on the frequency of the accident sequences. Quantification has often been based on estimates of the probability indicated by curves of recovery versus time without considering the many additional parameters which may be important. In most cases these estimates have been developed by expert opinion.

The incorporation of human interactions into PRAs has often been left to the judgment of the systems analysts. The need for detailed interactions between the systems analysts and human factors specialists was identified in the <u>PRA Procedures Guide</u> (NUREG/CR-2300), and further guidance appears in a draft report which has been issued for review and comment (Hannaman et al).

A.3.3 Limitations and Uncertainties

The usefulness of human-interaction analysis in PRA can be enhanced significantly by addressing the issues that currently contribute to limitations:

- Human behavior has been recognized as a complex subject for centuries and does not lend itself to simple models such as those for component reliability. Thus, the analysis of human interactions is the area of systems analysis most dependent on the judgment of experienced analysts.

For example, the assessment of recoveries may be bounded by a single parameter, such as a failure probability of 0.2 (NUREG/CR-1659), whereas in another study the recoveries may be given more realistic assessments on a judgmental basis (NUREG/CR-2787).

- The description of the human influence has not been fully developed since human effects have often been classified as either success or failure to match equipment failure logic. In most PRAs, the use of techniques such as THERP or OATS results in the assignment of successes and failures to each branch of the tree. The possibility of other operator conditions, which might affect the system in other ways, has not always been considered. A framework for helping analysts make such considerations is available (Hannaman et al), and further improvements are anticipated in this area.

- Generic human-failure data have been applied on a judgmental basis, because a simplified mode of the various parameters that affect human performance has not yet been fully developed. The current techniques for selecting data from NUREG/CR-1278 and applying them to a human reliability analysis (HRA) tree requires considerable judgment and may not be completely reproducible by other analysts (Brune et al). A simple model of human behavior, such as the OAR model, or a model based on recovery time alone improves the reproducibility but does not provide information on how the likelihood of recovery varies with other parameters. Structured use of expert judgment is one way to assess this quantitative impact (NUREG/CR-2986).

- Human dependences have been assessed primarily among the humans rather than as part of human-plant interactions. The modeling of human dependences from the HRA viewpoint is described in NUREG/CR-1278. Although the technique provides for quantitatively assessing these dependences between humans, the human-system dependences may need to be addressed in greater detail. This is an area where the diagnostic models need to address multiple options. The multiple-option concept can be addressed in the confusion matrix (Potash et al) and in the structuring of expert judgment (NUREG/CR-2255).

- Techniques for considering sensitivities and uncertainties currently address the quantification uncertainty in the data as opposed to alternate logic for incorporating the human. One of the weaknesses in the quantification of human-interaction uncertainties is that the modeling techniques introduce a structure for incorporating a single human link to the system-reliability model. The current techniques for assessing the uncertainty of the quantitative impact of the error rates are based on changing the parameter of interest (e.g., the human-failure probability) and comparing this changed condition to the unperturbed condition (NUREG/CR-2906). An improvement would be to examine changes in the logic structure also. This requires an improved ability to state the assumptions involved in incorporating the human interaction.

While the impact of these current limitations on the risk profiles assessed in published PRAs is difficult to state, many analysts feel that they are within the stated uncertainty bounds. The major impact on risk is felt to be on the probability of accidents as opposed to the consequences.

A.3.4 Potential Improvements

The analysis of human interactions in a PRA is clearly a developing art. Improved areas for the analysis of human-system interactions in future PRAs are likely to include:

- Development of interim methods for considering the importance of operator decisionmaking under accident conditions (NUREG/CR-1278)

- Development of certain representations of the time dependent impact of human interactions on the success or failure of a system or safety function, e.g., OATS (NUREG/CR-3010)

- Use of a more structured technique for developing data from expert opinion (NUREG/CR-2986)

- Development of more systematic approaches for incorporating human interactions into the PRA framework (Hannaman et al) and better integration of the systems and human reliability analyses

- Collection of training simulator data to verify some of the judgmental data and support the development of simple models of human behavior (Kozinsky and Pack)

Improved consideration of these factors in PRA should lead to substantially greater understanding of possible human behavior under accident conditions.

However, limitations to the detailed description of human interactions will still exist, and they should be recognized. Both the qualitative description of the human-plant interaction logic and the quantitative assessment of those actions relies upon virtually untested judgments of experts. One area needing additional work is the development of simple mathematical human-effect models that are adequate for PRAs. Such correlations as OATS are simple to apply, but give little improved information about the behavior characteristics of the operation. Factors which lead to variations in the results should be identified from the information in the simulator studies. More detailed models, currently under development, are needed so that the collection of data is directed toward identifying parameters that are likely to influence the probabilities of human interactions in an accident situation.

The critical review of PRAs by experts in the area of human interactions has generated advances. However, the depth of the techniques must be expanded so that the impact of changes in design, procedures, operations, and training, etc., can be measured in terms of a change in a risk parameter such as the core-melt frequency. Then tradeoffs or options for changing the risk profile can be identified. To do this, the methods for identifying the key human interactions, for developing logic structures to integrate human interactions with the system-failure logic, and for collecting data suitable for their quantification must be strengthened. These items remain to be accomplished before the associated uncertainties can be substantially narrowed.

A.4 System Model Data Requirements

A.4.1 Background

The data that are used in a PRA can be divided into those required for the analyses of system models, accident processes, containment response, fission-product release and transport, and offsite consequences. Each of these sets of data is needed as input to the models, usually implemented in the form of computer programs. Only the data required for system-model evaluation is considered here; the data required for the other portions of a PRA are considered in later sections where the specific models are discussed.

The different types of system model data generally used in a PRA consist of:

- Initiating-event data, e.g., transient frequencies, pipe-rupture frequencies
- Component-failure data, e.g., valve-failure rates, pump-failure rates
- Test data, e.g., surveillance-test intervals
- Maintenance data, e.g., unscheduled and scheduled maintenance intervals and durations for pumps
- Common-cause data, e.g., fractions of failure causes which result in multiple valve failures
- Human-error data, e.g., human-error rates, recovery probabilities

* Uncertainties associated with the above data, e.g., error factors representing approximate 95% bounds on the data

Chapter 5 of the PRA Procedures Guide (NUREG/CR-2300) discusses these different types of data in more detail.

The data which are used in a PRA can be either generic or plant-specific in nature. Generic data represent a class of reactors or class of components. The class can have any nature, encompassing individuals with similar specifications or with dissimilar specifications. Examples of generic data are failure rates for emergency core-coolant pumps for PWRs and transient-occurrence frequencies for BWRs. At a minimum, the generic data values consist of a central data value for the class (e.g., a median value) and a characterization of the spread of individual data values in the class (e.g., the difference between the maximum value and minimum value). A probability distribution describing the variation of individual data values in the class is sometimes provided. Various generic data sources are available for PRAs and are described in the PRA Procedures Guide. Generic data sources include RSS data, licensee event evaluations, and compilations of plant-maintenance logs.

Plant-specific failure data are obtained from the reactor being analyzed by the PRA. They are obtained from the plant's records and reflect the peculiarities of that particular plant. Even for plant-specific data, failure histories of similar type components are usually aggregated. The statistical treatments used to analyze plant-specific data are described in the PRA Procedures Guide. Obtaining plant-specific data can be a significant effort in a PRA.

Generic data are used in most PRAs to supplement the available plant-specific data. The approaches which are used to integrate generic data with plant-specific data vary. Whenever generic data are used to characterize the performance of a component, a value representing an average member of the generic class is used. This may not be very near the actual value for that specific component. For example, an average failure rate for a motor-operated valve in the industry may be assigned to a particular valve in the plant; however, that specific valve's failure rate may differ from the average. Therefore an important consideration is whether possible variations from the average can affect the risk results. Uncertainty analyses or sensitivity analyses accommodate this; the PRA Procedures Guide describes some methods used for these analyses.

In areas where insufficient generic or plant-specific data are available, subjective opinions are used. These are not explicitly based only on analyses of past history, but also represent the opinions of the analyst, other individuals involved in the PRA, or outside experts about appropriate values for the parameters, based on their feelings, experience, and knowledge. Subjective opinions are often used for human-error rates and common-cause failure probabilities. Sensitivity studies or uncertainty analyses are important for evaluating subjective judgment because of the range of variability.

A.4.2 State of the Art

The RSS based its estimates on approximately 17 reactor-years of experience. At the present time, over 400 reactor-years have been accumulated in the United States. The analysis of this experience to obtain required PRA data has been spotty. A brief review of the different data areas is given below.

Initiating-event data for transients have significantly improved since the RSS. Data have been tabulated for a wide spectrum of transients for both PWRs and BWRs, and both generic and plant-specific values have been tabulated (EPRI NP-2230). LOCA initiating-event data have improved only marginally since the RSS. Many current PRAs still use RSS values for LOCA initiators or modify them to include valve or pump rupture and leakage contributions.

A significant amount of plant-specific component-failure data has been generated for those plants which have been subjected to PRAs. In general, these sources of data have not been combined into an industry-wide data base or used to upgrade an existing generic data base. The generic component-failure data used in current PRAs have generally not improved much over those used in the RSS, and many current risk analyses use the RSS data base or some variant as their generic data base. The improvements that have occurred have not exerted a major influence on either the numerical results of the PRAs or on the insights obtained. Current data bases, including plant-specific data bases, generally do not relate component-failure rates to root causes of failure; therefore, the corrective actions required if the failure rates imply high risks are seldom clear.

Test and maintenance data, including limiting conditions for operations, are generally obtained from plant technical specifications. Plant-maintenance logs also sometimes provide more precise values. Corrective maintenance intervals and durations are among the more difficult data to obtain and are occasionally subjectively estimated after discussions with plant personnel.

Dependent failure data, which describe the likelihood of multiple failures from common causes, have improved only marginally since RSS. Common-cause probabilities remain largely subjectively estimated and generally are not tailored to specific plant environments, maintenance, and operation.

Since the RSS, human-error analyses for routine procedural errors have become more codified; however, human-error data are still largely subjective with little validation from experience. Human-error data for cognitive (decision) errors and for comprehension errors under accident conditions are still generally unavailable. Also, a significant amount of data indicating the likelihood of the operator correcting or mitigating accident situations does not exist.

A.4.3 Limitations and Uncertainties

Uncertainties in data are generally expressed as error factors where the error factor is the ratio of the upper bound estimate to the median value or best-estimate value. The upper bound estimate is usually an approximate 95th percentile value (i.e., there is a 95% probability, or confidence, that the true value is less than this upper bound). If the upper and lower bounds are multiplicatively symmetrical about the median, the lower bound is usually an approximate 5th percentile value, and the range (the ratio of the upper bound estimate to the lower bound estimate) is the square of the error factor. The range thus represents approximately a 90% confidence range or probability for the value. This assumes that the median estimate is unbiased. If a significant bias exists, the confidence or probability of the true value being between the estimated bounds could be significantly less.

For present transient-initiating-event data, the error factors are considered to be small, only about 2 to 3. For loss-of-coolant initiating-event data, the error factors are thought to be 3 to 10.

Component-failure-rate data have error factors of approximately 3 for active components (pumps, valves, etc.). For passive components (pipes, wires, etc.), the error factors are generally in the range 10 to 20; passive-component-failure rates are generally substantially lower than active-component-failure rates, even considering the uncertainties.

Data on test and maintenance intervals and durations generally have associated error factors on the order of 2 or less when derived from plant records. Corrective-maintenance intervals and maintenance durations have larger errors.

Error factors for common-cause probabilities involving two or more coupled failures usually increase as the probability values decrease. For common-cause probabilities in the vicinity of 10^{-5}, the error factor generally is of the order of 3 to 10. These error factors apply to the probability of multiple failures occurring (i.e., unavailabilities).

The above error-factor values represent gross averages over PRAs which have been performed and can vary from PRA to PRA. PRAs which use plant-specific data generally have smaller uncertainties (error factors) than those that use only generic data. Uncertainties arising from data uncertainties are generally the only ones that are explicitly quantified in a PRA. Uncertainties in dependent-failure data and human-error data often dominate the data uncertainties associated with calculated system unavailabilities and accident frequencies. The specific effect of data uncertainties, however, depends on application. When a single contributor dominates the risk, then the uncertainties in data for that contributor will have significant impacts on the results. When many unrelated contributors contribute equally to the risk, then the data uncertainties for any one contributor will not have a large impact.

A.4.4 Potential Improvements

A significant amount of plant-specific data has been generated by the PRAs already performed. However, these data have not been assembled together for plant comparisons and for developing a generic data base. A data system like NPRDS could be the vehicle for assembling, comparing, and summarizing this plant experience. Such a data system could be particularly valuable for identifying trends with time, for showing outlier component and system behavior, and for providing information on the causes of component failures.

Because of their importance and their present large uncertainties, additional plant experience on dependent failures and human error are the areas where data collection can effect the greatest improvement. The realism of models and data for test and maintenance can also benefit from improvements. These improvements would allow more realistic analysis of plant technical specifications and would also allow evaluation of the reliability effects of testing and maintenance.

A.5 Accident Progression, Containment Response, and Fission-Product Release and Transport

A.5.1 Background

This section describes the status of capabilities for performing analyses of in-plant accident processes. These analyses determine the thermal-hydraulic response to the accident sequences, the progression of the accident, the response of the containment to severe-accident loadings, and the characteristics of any release of fission products to the environment (source terms). Some of the physical and chemical phenomena underlying these areas are not well understood at this time. Current research programs are rapidly increasing our knowledge and modeling capabilities in many of these fields. Because of the number of technical disciplines involved and the existing state of flux in analysis capabilities, only a summary of the issues can be presented here; the references provide more detailed information.

The potential public health hazard from an LWR accident derives from the release of radioactive fission products to the environment. Accident sequences that do not lead to significant fuel damage and containment failure contribute little to the offsite risk. The principal products of the in-plant consequence analyses performed for a PRA are called the environmental source terms. These source terms describe, for accident sequences or groups of accident sequences, the characteristics of the release of fission products in terms of:

- The conditional occurrence frequency for each accident sequence or sequence category
- The quantity of radionuclides released into the environment
- The time of release (with respect to reactor shutdown)
- The duration of release
- The warning time available for emergency actions
- The elevation (location) of release
- The thermal-energy-release rate into the environment.

Thermal-hydraulic codes are used to describe the progression of a severe accident from the time of the initiating event through core uncovering, fuel heatup, clad oxidation, fuel slumping, vessel failure, and fuel-concrete interactions. The distribution of core material as it exits the reactor vessel and the coolability of the core on the reactor building floor must also be considered.

The consequences of a core-meltdown accident are influenced strongly by whether the containment fails and, if it fails, by the timing and mode of failure. The principal threats to containment that must be evaluated in a PRA are overpressurization by rapid steam generation caused by a molten fuel-coolant interaction; shock loading from hydrogen detonation; rapid pressurization from hydrogen deflagration; thermal loading from hydrogen burning, hot gases, or thermal radiation from the core; missile production in a steam explosion; and basemat penetration. In addition, the possible effects of direct heating due to core material that forms aerosol particles upon vessel failure should be considered. Two other potentially important containment-failure modes involve the inability to isolate the containment at the time of an accident and the direct bypass of the containment, which could result if multiple failures occur.

The quantities of fission products available for release from the plant depend on the processes by which fission products are released from fuel, transported, and deposited in the reactor coolant system and containment (and in buildings outside the containment) before the fission products reach the environment. Natural and engineered removal processes will significantly decrease the fission products available for eventual release if conditions and timing allow their effective functioning. Transformations in physical and chemical form must also be considered. In the past few years, questions have been raised about the realism of the methods used in the RSS and subsequent PRAs to analyze these processes, which have resulted in a significant research effort in this area by both industry and government.

A.5.2 State of the Art

Methods for analyzing severe accident processes and fission-product release are described in some detail in Chapters 7 and 8 of the PRA Procedures Guide. Figures A-2 and A-3, taken from this guide, illustrate the steps taken in these analyses. Although these methods are changing rapidly, the guide provides a good introduction to the methodology developed in the RSS and to subsequent improvements in more recent PRAs.

A.5.2.1 Analysis of Severe Accident Processes

To perform analyses in the RSS (NUREG-75/014), the BOIL code<2> was developed to describe the boil-off and heatup of the fuel in the reactor vessel for accidents initiated by large breaks in primary system piping. Hand calculations were used to estimate the other accident phenomena. After the RSS, the MARCH computer code was written to enable a more consistent and efficient treatment of the physical processes in a severe accident (Wooten, R. O.). Some improvements were included in the modeling of processes, such as in the area of molten core concrete interactions, but, in general, the MARCH models remained very simple representations of complex processes. Most PRAs performed since the RSS have been performed with MARCH or at the same level of physical modeling as MARCH. Exceptions are the Zion and Indian Point Probabilistic Safety Studies, in which more detailed analyses were performed for important separate effects (Commonwealth Edison Co.; Consolidated Edison Co.).

In the period after TMI-2, severe-accident research expanded much more broadly, focusing on developing a better understanding of severe-accident behavior for possible use in plant

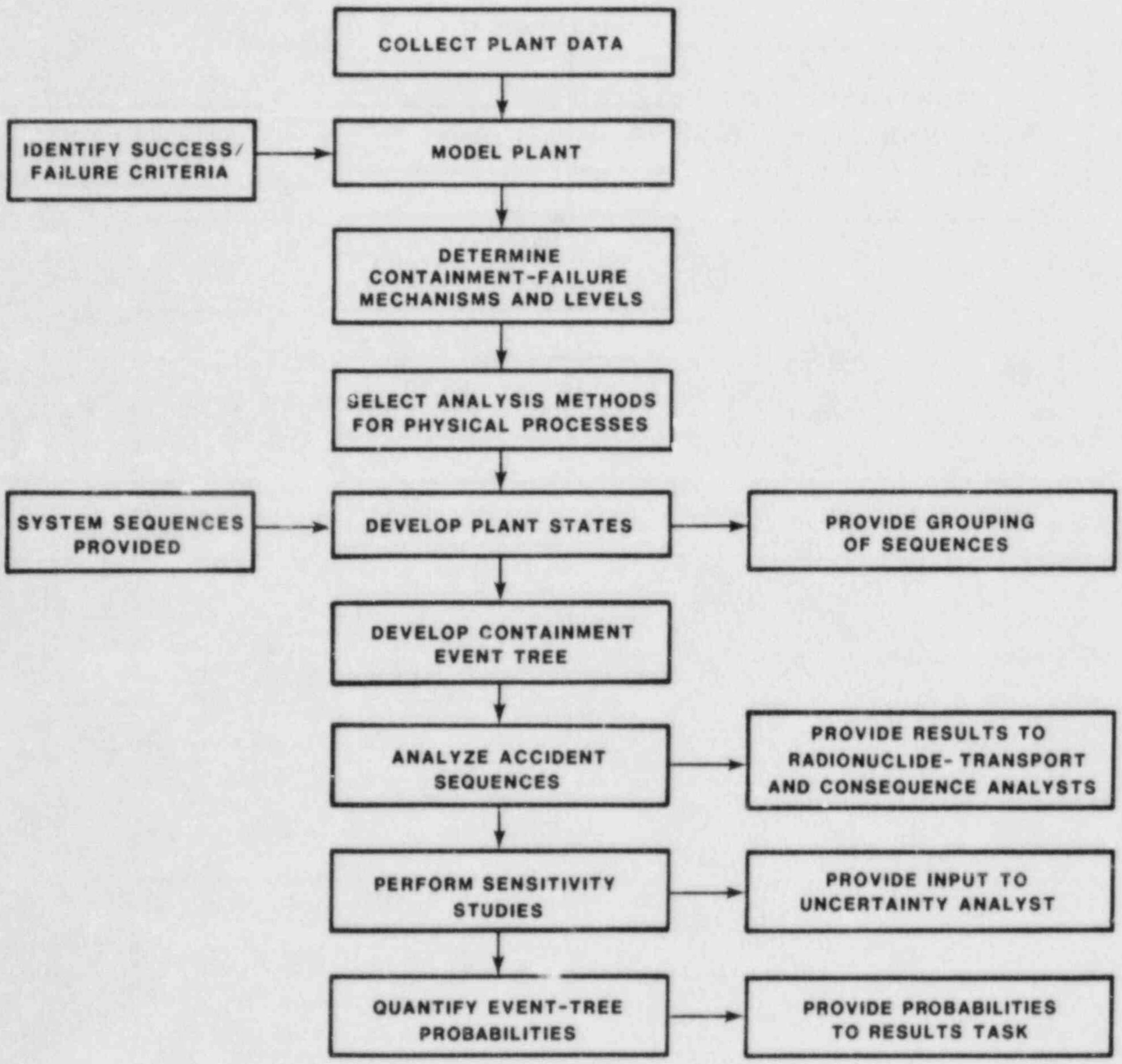


Figure A-2. Activities Diagram for Analysis of Physical Processes

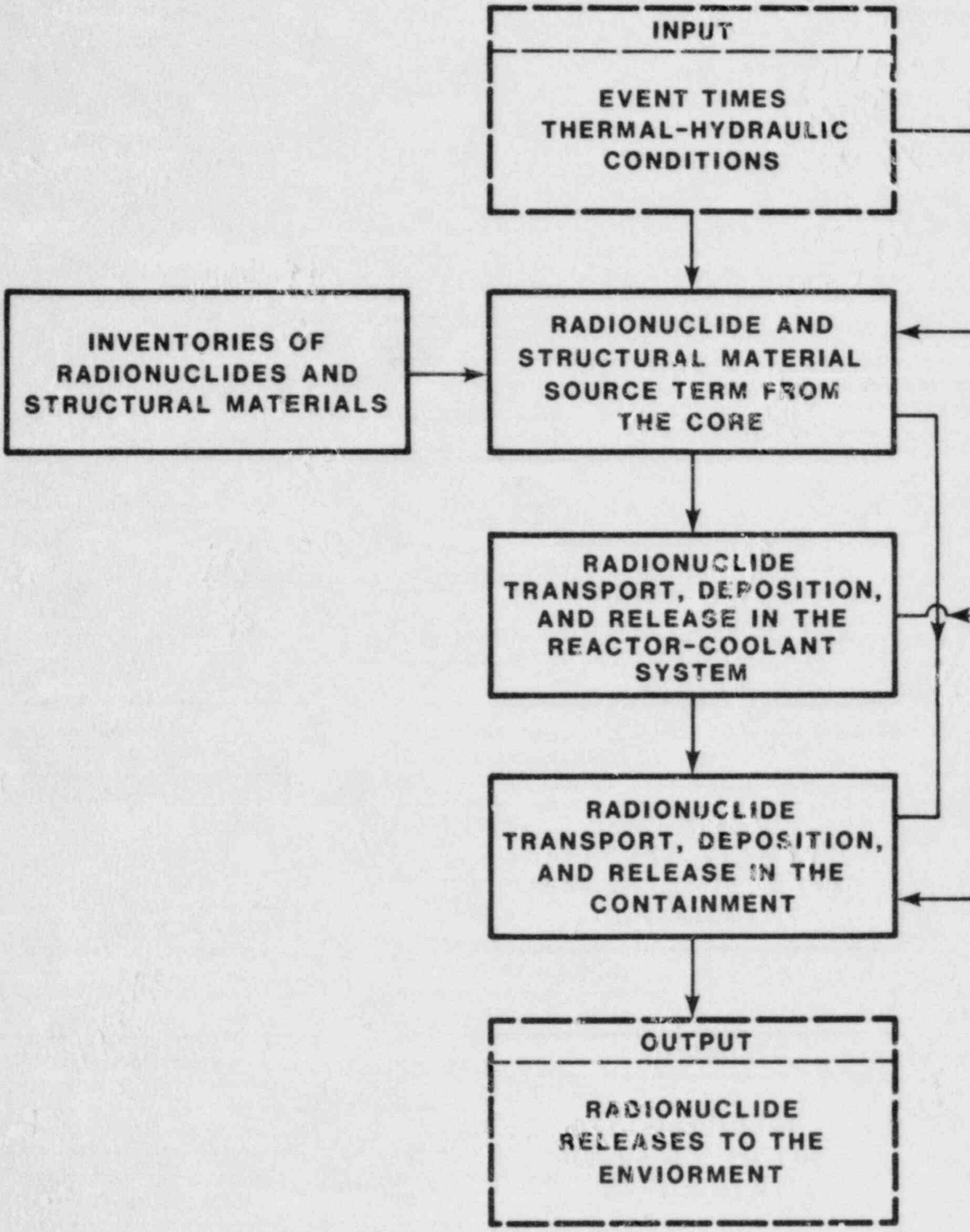


Figure A-3. Elements in Analysis of Radionuclide Behavior in the Reactor regulation. Experimental programs that had originally been developed to examine the performance of emergency core-cooling systems in loss-of-coolant accidents were redirected to examine the conditions of the reactor-coolant system preceding severe core damage in scenarios that would eventually lead to damage. These programs have provided a basis for validating codes such as TRAC (NUREG/CR-2054), and RELAP (NUREG/CR-1826) that can be used to predict if and when the core uncovers. Modeling efforts were also initiated to describe the progress of fuel degradation in more detail than in the simple models in MARCH. A more mechanistic description of the initial stages of core damage is provided by SCDAP (Allison, C. M.). SCDAP is intended for use in examining accidents in which the fuel is damaged but the progression of the accident is arrested before substantial melting occurs. The MELPROG (Young, M. F.) code is being developed to analyze the behavior of the degraded core for complete core-meltdown accidents through the time of vessel failure. Validation of the models is to be provided by experiments in the PBF, NRU, and ACRR facilities ("Upgraded"). The MEDICI (Bergeron, K. D.) and CORCON (NUREG/CR-2142) codes will describe the ex-vessel behavior of molten fuel. MEDICI will predict fuel coolant interactions in the reactor cavity. It will be validated against experiments at SNL and BNL. The CORCON code predicts the interaction between molten fuel debris and concrete. Validation experiments are being performed in the Large-Scale Melt Facility (NUREG-0900) at SNL and in the BETA facility (Rininsland, H.) in West Germany. These two codes will be integrated into the CONTAIN code, which analyzes the thermal-hydraulic response of the containment (NUREG/CR-2224).

A.5.2.2 Containment Response

Considerable research has also been undertaken to develop an improved understanding of steam explosions and hydrogen combustion. A broad range of small- and intermediate-scale experiments has been performed to investigate the mechanisms for the initiation and propagation of steam explosions in simulant mixtures of molten corium (mixtures of fuel and structural materials) and water. Although our knowledge of the conditions under which steam explosions will occur and of the energetics of the reactions has improved in recent years, significant uncertainties remain, particularly with regard to reactor-scale effects. However, the probability that an energetic steam explosion in a core-melt accident could lead to containment failure is now subjectively judged by many to be small (Corradini, M. L.).

Most of the hydrogen-behavior research program has been performed since the TMI-2 accident. This program has involved model development and extensive experimentation. Data have been collected to determine directional flammability limits as a function of composition, ignition requirements, and conditions leading to flame acceleration. The effects of engineered safety features on controlling hydrogen combustion have also been investigated. In cooperation with the Electric Power Research Institute (EPRI), large-scale tests are in progress at the Nevada Test Site (Rehm, T. A.). The HECTR code is being developed to predict the magnitude of loads generated in multi-compartment containments in hydrogen burning events (Camp, A. L.).

NRC and EPRI are currently sponsoring research programs to investigate a number of possible containment failure and leakage modes, including localized failures at penetration seals, valve failures, overheating of electrical penetrations, and gross structural failure under quasi-steady state pressurization. The largest of these programs involves scale-model tests of steel and reinforced-concrete containments (Von Riesemann, W. A.). These programs will support the development and validation of models for predicting the magnitude of leakage associated with the pressure and temperature conditions in the containment.

In a PRA, in-plant consequence analyses are performed for a discrete set of accident sequences or for conditions that are selected as characteristic of groups of accident sequences. In the same way that system-event trees are used to organize the systems-analysis aspects of a PRA, containment-event trees have been used to organize the consideration of the containment aspects of accident consequences. The containment-event trees employed in the RSS constituted a delineation of different containment-failure causes such as steam explosion or hydrogen burn. The probabilities assigned to these failure causes represented the best judgment available at that time.

In the more recent PRAs sponsored directly by utilities (e.g., Zion [Commonwealth Edison Co.], Indian Point [Consolidated Edison Co.], Limerick [Philadelphia Electric Co., 1981], Oconee, Big Rock Point [Consumers Power Co.], Midland, Seabrook, and the four IDCOR study plants) advances have been made in developing and quantifying containment event trees. Improved containment-event trees explicitly addressing the underlying phenomena contributing to containment failure have evolved, such that possible combined effects as well as mutually exclusive effects can be considered. For example, both hydrogen burning and a steam-pressure spike at vessel failure could, under certain circumstances, contribute to early containment failure because of overpressurization. In other cases the steam spike could render the containment atmosphere inert and prevent hydrogen burning. Such advances allow the judging of branching probabilities on the containment-event tree at a level where individual phenomena are addressed and where dependences are explicitly considered. Radionuclide transport and release phenomena are only beginning to be considered on containment-event trees.

A.5.2.3 Fission-Product Release and Transport

The codes that track the progression of fuel degradation provide input to the fission-product transport models that predict the airborne source term potentially available for release from the containment. For the RSS, the computer code CORRAL (Burian, R. J.) was developed to treat the transport, removal, and release of fission products. A significant effort was undertaken in the RSS to ensure that fission-product behavior was treated consistently with the data base and level of understanding existing at that time. The analysis was intended to be realistic, but the predicted releases of fission products in some circumstances appear to have been conservatively overestimated. This was due to limits in the existing ability to understand and model the underlying phenomena and to the method used to group the sequences in release categories by bounding the release fractions. In the RSS, fractional releases of fission products were developed for four release periods: gap, melt, core-concrete interaction (vaporization), and steam explosion (oxidation). Retention of fission products on surfaces of the reactor-coolant system was not analyzed in the RSS. At the time, iodine was generally believed to be transported as I_2, which was not expected to be significantly retained in the reactor-coolant system.

The modeling of iodine behavior in CORRAL is largely empirical, based on the behavior of elemental iodine (I_2) in the Containment Systems Experiments (CSE) (Postma, A. K.). A simple aerosol model in CORRAL, which was used to predict the behavior of the less volatile fission products, was also based on the CSE tests. This model is quite primitive in comparison with existing aerosol transport codes. Recently, the CORRAL models have been shown to underpredict the removal of aerosols from the containment atmosphere in accident sequences in which the containment safety features are inoperable. Credit for fission-product retention in buildings outside of the containment was provided in the RSS only for the containment bypass sequence (for the PWR) and for some containment-isolation-failure sequences (for the BWR).

Following the RSS, the NRC undertook several research programs to improve the ability to model fission-product release and transport in severe accidents. Fuel heatup and release experiments were performed on actual irradiated fuel segments (Osborne, M. F.). These experiments complemented experiments performed with simulant materials in the SASCHA facility in West Germany (Albrecht, H.). The initial version of the TRAP code (NUREG/CR-0632) was also written in this time period to predict the retention of vapors and aerosols in the reactor-coolant system.

Shortly after the TMI-2 accident, questions arose about the magnitude of the possible conservatism in the RSS fission-product source terms and the lack of realism in the source terms prescribed in 10 CFR 100 (DiNunno, J. J.) as a basis for regulation. In 1981, the NRC published an evaluation of the "Technical Bases for Estimating Fission Product Behavior During LWR Accidents" (NUREG-0772). As a result of deficiencies identified in that review, several new research programs have been undertaken and existing programs augmented. The temperature range of the ORNL release tests has been extended, and new release tests with simulants have been initiated. Basic data have been collected by SNL on the high-temperature properties of fission-product species (e.g., CsI, CsOH, tellurium) and the reaction rates of these species with reactor-coolant-system surfaces (Elrick, R. M.). The chemistry of iodine/water systems has been extensively explored. Integral experiments for the validation of primary-system transport codes are also proceeding on an intermediate scale in the United States (NUREG-0900) and on a large scale the Marviken facility in Sweden. Similarly, validation experiments for containment transport models have been performed at the NSPP facility (Lotts, A. C.) and are being performed at Battelle Frankfurt Institute in West Germany.

Additional model development is also in progress. The FASTGRASS code is being extended to provide a mechanistic prediction of the release of both volatile fission products and noble gases from overheated fuel (NUREG-0900). The VICTORIA code, which will be integrated into MELPROG, will predict the release of fission products from liquified as well as from overheated fuel. The VANESA code has been developed to describe release during core-concrete attack (Gieseke, J. A.). TRAP-MELT has been upgraded in its ability to model aerosol agglomeration and reactions between vapor species and surfaces. The MATADOR computer code (Baybutt, P.) has been written as a replacement for the CORRAL-2 code for use in PRAs. The CONTAIN (with MAEROS routine), TRAP-CONT, and NAUA-4 codes (Bunz, H.) have been developed to perform more detailed analyses of fission-product transport in the containment building.

Thus, a whole new arsenal of analysis capability is under development. To examine the impact of the advanced methods of analysis on the predicted release of fission products to the environment in severe accidents, the NRC has undertaken the Source Term Reassessment Study, which includes analyses of sequences in five different plant designs.

A.5.3 Limitations and Uncertainties

Most of the uncertainties in the in-plant consequences of severe reactor accidents are not due to inherent deficiencies in the PRA techniques but stem from a lack of understanding and experience in accident processes and fission-product behavior associated with severe accidents. By using sensitivity studies and bounding analyses, the effect of these uncertainties on the results of a PRA can be examined explicitly, and they do not necessarily impede the use of the results in the decision process.

Uncertainties in the analysis of in-plant consequences in a PRA can be divided into four areas:

- Accuracy of the methods of analysis
- Data required by the analytical models
- Characterization of sequences
- Estimation of branching probabilities

The accuracy of methods for analyzing the source term (release of fission products to the environment), and the adequacy of their supporting data base, are questions receiving considerable attention at the NRC.

In considering the uncertainty in the release of fission products from the fuel, some differentiation should be made between the RSS models and current models. The fixed fractional releases during the gap and melt-release phases in the RSS approach do not account for differences in the timing of the release of different elements, which can have an important impact on their subsequent retention in the reactor-coolant system and containment. The timing of the release of material, and the quantities of inert materials released during the attack on concrete, differ substantially from those used in the RSS analyses.

Significant gaps in knowledge exist in the current level of understanding of release phenomena. Substantial advances have been made in the understanding of the chemical forms of fission products. There is general agreement that, in the reactor-coolant system, iodine is transported primarily in the form of CsI or HI rather than as I_2. Uncertainty still exists as to the chemical forms of many of the fission products in the fuel and the mechanisms by which they are released. Only limited aspects of the release of fission products from fuel are treated mechanistically. Currently, empirical correlations for the release rates of fission products as a function of temperature provide the best means for estimating the release from fuel. These correlations are based, however, on small-scale and simulant experiments. In general, changes in surface-to-volume ratios during melting, pressure effects upon release rates, and the chemical form of the released materials, are not taken into account. Evidence exists that enhanced release of fission products occurs as fuel liquefies during heatup or fractures during quenching (e.g., the TMI-2 accident and PBF test SFD 1-0). The START code models these conditions, but inadequate experimental data are available to support use of the code.

One of the greatest sources of uncertainty in predicting the release of fission products from fuel is the estimation of the temperature history of the fuel. Release of fission products is very sensitive to time at temperature. The MARCH code treats the melting of fuel, clad, and core internal structures very simplistically. Although more sophisticated models are under development, they have a very limited experimental basis.

The state of knowledge of fission-product transport in the reactor coolant system is changing very rapidly. The TRAP-MELT code models the transport and deposition of three important vapor species, CsI, CsOH, and tellurium, as well as aerosols. Basic data on the properties and deposition velocities of vapors are being provided, and validation experiments are underway. Integral information on reactor-coolant-system deposition will also be obtained in the PBF experiments. However, many potentially important phenomena are not modeled in TRAP-MELT or are modeled simplistically. For example, aerosol nucleation, chemical transformations, nuclear transformations, and chemical reactions with surfaces are not currently modeled. In addition, the prediction of fission-product behavior is sensitive to the thermal-hydraulic conditions in the reactor-coolant system, which are not well understood. Over the past year, the MERGE code (Freeman-Kelly, R.) has been developed as an extension of the MARCH code, providing an improved thermal-hydraulic model of the reactor coolant system specifically for use with TRAP-MELT. That is, MERGE performs multiple-volume thermal-hydraulic calculations for severe accident conditions, using compartments consistent with TRAP-MELT specifications. However, because few experimental data are now available on, for example, flow paths and conditions in the upper internals of the reactor vessel, significant uncertainties remain despite the improved modeling capability of MERGE. In summary, the development and application of methods for predicting retention in the reactor-coolant system are too formative to permit a good appreciation of their accuracy.

The status of modeling of fission-product transport in the containment is more advanced. As discussed earlier, the CORRAL code used in the RSS is not representative of the current state of the art. Although the airborne concentrations of aerosols predicted by CORRAL can differ by more than an order of magnitude from the results of the more mechanistic codes, estimates of the total quantities released to the environment have typically agreed within a factor of two.

Among the major sources of uncertainty that affect fission-product behavior in the containment are:

- The amount of steam condensation on aerosols
- The magnitude of diffusiophoresis
- Chemical changes during hydrogen combustion
- Partitioning of fission-product vapors between air and water
- Formation of organic iodides
- Nuclear transmutation
- Aerosol scrubbing in saturated water pools
- Aerosol scrubbing in ice beds
- The effects of multiple compartments in containment
- Resuspension of deposited aerosols

The most dramatic influence on the source term is determined by whether the containment fails or by the timing of containment failure. Loads on the containment can be produced by steam spikes resulting from molten-fuel/coolant interaction, hydrogen combustion, noncondensable gas generation, thermal radiation, missile generation, and steam explosions. Predicting each of these phenomena requires a detailed understanding of the progress of core-meltdown accidents that is not yet available. How the containment will respond to a given load is also quite uncertain. The ultimate strength of the shell of a containment structure can be estimated with finite-element structural codes. At some pressure less than this ultimate value, however, the containment may develop substantial leakage. If this leakage rate is sufficiently high, catastrophic failure will be precluded. Because of the uncertainties associated with the loading and response of containments, the NRC has established working groups in both of these areas to assist in evaluating the potential for containment failure.

The ongoing, NRC-sponsored activities addressing in-plant consequence uncertainties include the Severe Accident Uncertainty Analysis (SAUNA) working group (NUREG/CR-3440) and the Quantitative Uncertainty Estimation for the Source Term (QUEST) effort (Lipinski, R. J.). The SAUNA group is compiling a consolidated list of uncertainties that affect accident processes. The QUEST study is estimating the uncertainty associated with the fission-product source terms predicted by the Source Term Reassessment Study (Gieseke, J. A.).

The characterization of sequences is an additional source of uncertainties because only a few sequences are identified for detailed analysis. These sequences must be considered representative of a range of related sequences involving variations in ESF performance and operator response. When the sequence is analyzed, a single set of initial and boundary conditions is selected. Little investigation has been devoted to date to the variation in consequences that can occur in the analysis of a sequence by making different assumptions regarding the level of performance of the various systems that can alter the results and operator response.

The probabilistic quantification of in-plant consequences in the RSS relied on expert judgment to assess the probabilities of the different containment-failure mechanisms. A probabilistic method for analyzing in-plant consequences has not been developed because the associated phenomena are generally deterministic rather than random statistical processes. Recent studies have begun to quantify explicitly the uncertainties in these processes to improve the basis for determining containment-event tree branching probabilities. Considerable judgment must still be used in quantifying the branching probabilities, however, because they represent an evaluation of the state of knowledge rather than a measure of the frequency of a statistical process.

In summary, uncertainties in the accident processes, containment response, and fission product behavior analyses are large and largely unquantified. Because of the tendency to utilize conservative assumptions when understanding and experience are lacking, and due to the neglect of many retention and removal processes which could reduce the amount of radioactivity available for release, current analyses are likely to overpredict the source terms.

A considerable effort is being made to develop and validate methods of analysis for in-plant consequences. At the current time, however, these methods are still being developed, their sensitivities are largely unexplored, and the extent of validation is extremely limited. Note also that the cost of greatly narrowing some of the uncertainties in these methods may be prohibitive. As a minimum, the ongoing research can be expected to characterize accident source-term uncertainties better and, in some important areas, may result in reducing the conservatisms in the analyses employed in PRAs to date.

A.5.4 Potential for Improvements

The analysis of the phenomena associated with severe accidents is in a period of rapid transition. Indeed, developments are occurring so rapidly that, for a PRA being undertaken today, a set of computer codes is difficult to recommend. A key issue is the depth of analysis of fission-product behavior that will be required in PRAs. The decision will depend on the extent to which uncertainties are reduced through the use of complex models and on the degree of potential biases associated with the simpler models.

Future PRAs, therefore, are expected to employ a set of codes which have similar scope to the codes used in the Source Term Reassessment Study (i.e., MARCH2, MERGE, CORSOR, VANESA, TRAP-MELT, and NAUA) (Gieseke, J. A.). These capabilities would include a method for relating fission-product release from the fuel to the local condition of the fuel (as opposed to the RSS approach) and treatment of transport and deposition in the reactor coolant system. Use of the CORRAL2 code for containment analysis in a PRA cannot currently be justified. The MATADOR code was written to replace CORRAL2. This code has had limited use to date, however, and the relative merits/demerits of MATADOR versus CONTAIN (MAEROS) and NAUA are not clear. Some of the basic modeling simplifications in MARCH2 (e.g., a single fuel-melting temperature) limit its ability to support a detailed mechanistic treatment of fission-product behavior.

The NRC's MELCOR program (Sprung, J. L.) is developing a new, integrated package of in-plant and ex-plant consequence analyses codes to replace the existing MARCH2, MATADOR, and CRAC2 codes. MELCOR will contain improved and consistent treatments of the phenomena essential to the characterization of severe accidents, will be structured to permit the easy incorporation of new models, and will permit the quantification analysis of associated uncertainties. The first version of MELCOR is scheduled for completion in September 1984. It would, therefore, not be possible to use this code in a PRA prior to 1985.

The MAAP (BWR and PWR versions) (Kenton, M.A.; Gabor, J. R.) and RETAIN (Burns, R. D. III) codes have recently been developed by IDCOR for use in severe accident analysis. At the time of this writing, little information had been made publicly available on these codes. The availability of these codes will apparently also be restricted.

Ability to treat BWR plant features has lagged the ability to analyze PWRs. Recently, special consideration has been given to improving the ability to model the physical processes of severe accidents in BWRs in the NRC-sponsored Severe Accident Sequence Analysis program and in the IDCOR model-development effort. Model development for analyzing the effectiveness of suppression pools in fission-product scrubbing has been supported by the NRC (NUREG/CR-3317) and EPRI (Wassel, A. T.). Validation experiments are also in progress (Cunnare, J. C.).

It should be noted that some of the computer codes being developed by NRC contractors to model the progress of core-melt accidents are not intended for direct use in PRAs.

These codes are still in developmental stages, will have long running times, and will be difficult to utilize in a production mode involving many sequences and sensitivity studies. They will provide the means to explore important phenomena in detail and will provide a basis against which to judge the simplified production codes.

Advances can be anticipated in the analysis of containment performance in terms of failure pressure, failure location, and leakage rates upon failure. More realistic and plant-specific analyses will be required to evaluate the source terms for sequences involving late containment failures.

One of the most important advances to be fostered and anticipated over the next few years is the treatment of analysis uncertainties as an integral part of the accident source-term analysis and the probabilistic propagation of the uncertainties.

Additional research and model development will reduce some but not all of the current uncertainties. Major advances are currently being made in the understanding of processes controlling fission-product release and transport. Processes that are closely coupled to the progress of extensive fuel damage, such as the release of the less-volatile fission products from fuel, or the generation of hydrogen during core slumping, will always have a large uncertainty because of the difficulties associated with experimental validation.

A.6 Consequence Analysis

A.6.1 Background

Consequence analyses attempt to predict the frequency distribution of possible offsite consequences for potential accidents at nuclear power plants. Accident consequences can include early fatalities and injuries, latent cancer fatalities, genetic effects, land contamination, and economic impacts. Chapter 9 of the PRA Procedures Guide (NUREG/CR-2300) contains a recent discussion of the important elements of offsite consequence analysis.

The first comprehensive assessment of the consequences from potential accidents at nuclear power plants was performed in the RSS. The RSS, published in 1975, examined the aggregate risk posed by commercial nuclear power plants in the United States. As part of the study, a computer model (CRAC, for Calculation of Reactor Accident Consequences) was developed to predict the offsite consequences of releases of radioactive material to the atmosphere for typical (i.e., "generic") sites (NUREG-0340). CRAC models the atmospheric transport, dispersion, and deposition of released radioactive materials, and predicts the resulting interaction with and influence on the environment and man. The computational steps in the model are shown schematically in Figure A-4. Other computer models developed for offsite consequence analysis consist of these same basic steps. Given a description of the release of radioactive material (a source term) and files of meteorological, demographic, and land-use data as input, submodels for atmospheric transport and dispersion, radiation dosimetry, population location and behavior, offsite protective measures, radiological health effects, and property damage are used in turn to estimate the resulting frequency distribution of potential consequences. The distributions of results obtained are normally displayed in the form of complementary cumulative distribution functions (CCDFs) and expected (mean) values.

Since the completion of the RSS, several improvements have been made in the field of offsite consequence analysis (Aldrich, D. C.). Two improved versions of CRAC have been developed and are currently in use in the United States: CRAC2 (NUREG/CR-2552) and CRACIT. CRAC2, developed under an NRC-sponsored research program, incorporates significant improvements in the areas of weather-sequence sampling and emergency response. CRACIT (CRAC Including Trajectories), developed by Pickard, Lowe, and Garrick, Inc., includes modifications to the atmospheric dispersion and evacuation models that permit some of the unique features of a specific site (e.g., terrain, evacuation routes) to be considered. CRAC2 is widely used by utilities, National Laboratories, and NRC; CRACIT, which is proprietary, was used in the Zion and Indian Point PRAs. In addition to the U.S. models, offsite consequence models have been developed for use in risk evaluations in other countries; examples include the Sizewell PWR Inquiry in the United Kingdom and the German Reactor Safety Study.

To better understand the influence of different consequence modeling techniques, the International Comparison Study of Reactor Accident Consequence Models was organized in 1981 under the auspices of the Organization for Economic Cooperation and Development/Nuclear Energy Agency's Committee on the Safety of Nuclear Installations (CSNI) (OECD/NEA 1984). Approximately 30 organizations, representing 16 countries and the Commission of the European Communities, participated to some degree in the comparison study. As part of the study, a series of standard problems was specified to allow a step-by-step comparison of individual models as well as consequence and risk estimates. The study showed that a wide variety of modeling techniques and assumptions are being used to estimate the consequences of potential reactor accidents. The estimates of consequences made by the participants, however, were generally in fairly close agreement. In most cases where significant differences did occur, they could be explained readily by differences in modeling techniques or assumptions. A detailed comparison and evaluation of the

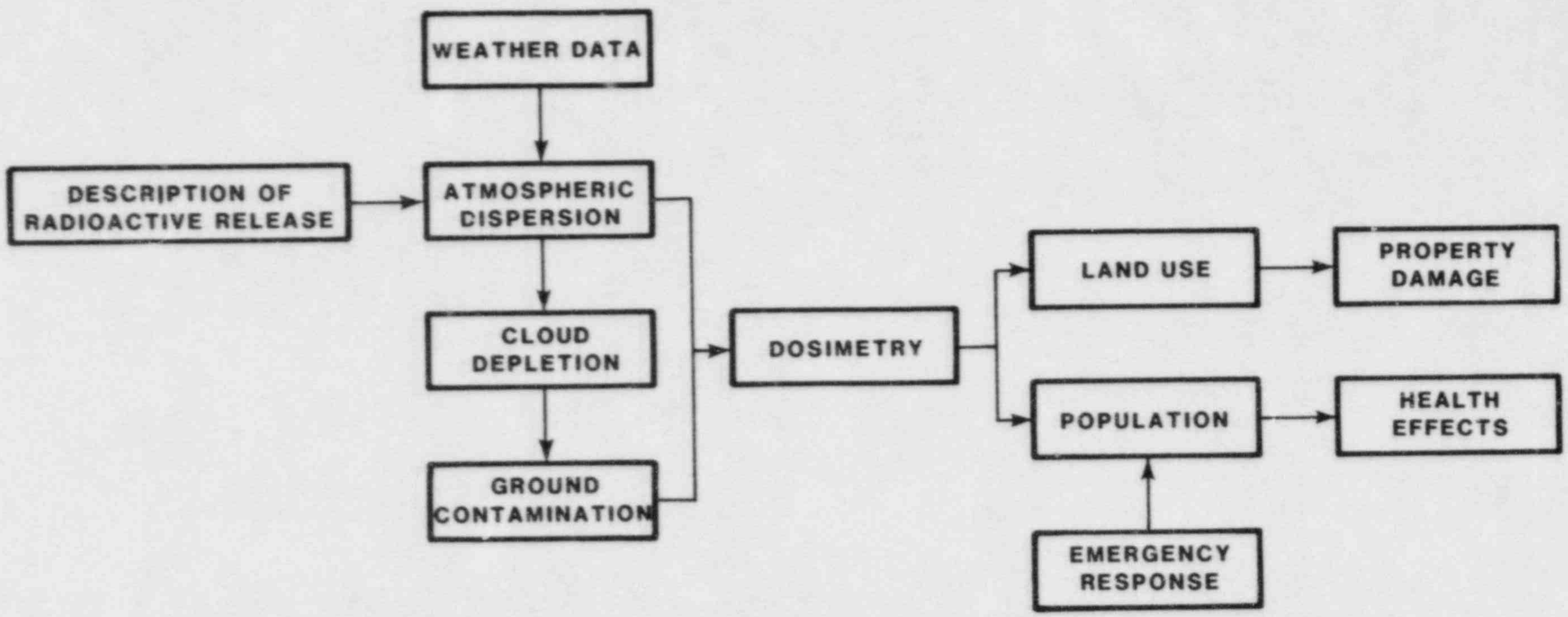


Figure A-4. Schematic Outline of Reactor Safety Study Offsite Consequence Model. CRAC results of the study, along with important observations and conclusions, are presented in the study's "Summary Report" (OECD/NEA 1984).

The potential consequences resulting from accidental releases of radioactive material to water pathways have not been examined with the same degree of detail as those resulting from releases to the atmosphere. Risks from the atmospheric pathway are generally considered to be dominant, because the time for the radioactive contaminants to initially reach the human population is usually significantly shorter for the atmospheric pathway. Therefore, hydrologic transport of contaminants allows for greater decay of radionuclides. In addition, the initial atmospheric exposure would usually be involuntary, whereas in most cases exposure to hydrospheric contamination could be largely avoided by the implementation of appropriate protective measures.

Several generic studies of the potential effects of radioactive releases to water pathways have been performed (NUREG-0440; NUREG/CR-1596). In general, these studies concluded that short-term radiation doses to individuals via liquid pathways would probably never be large enough to cause early health effects, and that for most sites the public risks posed by core-melt accidents will be dominated by releases to the atmosphere rather than by direct releases (e.g., basemat meltthrough) to liquid pathways. However, sites may exist with characteristics such that risks via the liquid pathways could be important relative to those from terrestrial pathways, and further analyses should be performed to identify those characteristics and to select appropriate models for evaluating risks at such sites. A review of previous liquid-pathway studies and a discussion of methods appropriate for performing site-specific liquid-pathway analyses are included in the PRA Procedures Guide (NUREG/CR-2300).

Potential economic consequences and risks from commercial nuclear power plants are receiving considerable attention because of their importance for cost/benefit analyses. Several recent studies have examined the economic consequences and risk from nuclear power plants (Starr, C.; NUREG/CR-2723; NUREG/CR-3673). These studies have pointed out the overriding importance of potential onsite costs (e.g., cleanup or repair and replacement power) to the overall consequences of reactor accidents. For example, the TMI-2 accident resulted in minimal offsite consequences but major damage to the plant. Moreover, relatively high-frequency "routine" forced-outage events have been shown to dominate the aggregate economic risks from reactor operation. Only for severe core-melt accidents will offsite costs (decontamination, land-use denial, health effects, etc.) equal or exceed the onsite costs, and then only for densely populated sites or extremely adverse weather conditions.

A.6.2 State of the Art

As already mentioned, the RSS was performed to assess the aggregate risk from commercial nuclear power plants in the U.S. Since the completion of the RSS, the capabilities of offsite-consequence analysis have been extended to provide assessments of the risk posed by reactors at specific sites and to provide guidance for planning and decisionmaking. Examples of site-specific applications of offsite-consequence analysis include the Limerick, Zion, and Indian Point PRAs and the recent environmental statements for Susquehanna and Fermi. In addition to use in risk evaluation, offsite-consequence analysis has been used to aid decisionmaking in several other areas. Examples include evaluation of alternative design features (NUREG/CR-0165), emergency planning and response (NUREG/CR-1131; NUREG/CR-1433), reactor siting recommendations (NUREG/CR-2239), and determinations of risk acceptability.

Even in the presence of large uncertainties, which are discussed below, offsite-consequence analysis can provide (and has provided) several useful insights and perspectives on severe reactor accidents. For example, analyses have shown that the extremely low-probability, high-consequence events ("tails") predicted to result from adverse weather conditions generally do not contribute significantly to the mean (or expected) consequences of reactor accidents. In addition, analyses clearly indicate that if releases of radioactive material as large as postulated in the RSS are possible, the potential effects could be extremely severe, and economic damage could exceed tens or even hundreds of billions of dollars. However, predicted consequences are substantially reduced for smaller accident source terms.

Currently, the capabilities for performing offsite-consequence analyses are more mature than those for the evaluation of accident progression, containment behavior, and source terms. In the development of offsite-consequence models, a large pool of supporting data is available from which to draw. Such data originate from studies on air pollution (atmospheric transport, dispersion, and deposition), nuclear weapons fallout (behavior of radionuclides in the environment), radiation therapy, and the Hiroshima and Nagasaki survivors (radiation health effects) and other areas. In general, relatively simple empirical relationships (i.e., "fits") can be derived from these data to model phenomena that are extremely complex in nature. In contrast, the phenomena associated with the progression of severe reactor accidents are much less well understood. Nevertheless, offsite-consequence analysis is not without significant uncertainties, as discussed below.

A.6.3 Limitations and Uncertainties

The limitations in offsite-consequence predictions stem principally from two sources: uncertainty in the models and uncertainty in the data required by the models. Modeling uncertainty arises from:

- An incomplete understanding of the phenomena and processes involved in the transport of released radionuclides to man and the health, environmental, and economic effects that result

- Simplifications made in the modeling process to reduce costs, complexity, and requirements for input data

Data uncertainties arise from problems associated with the quality, availability, and appropriateness of the data and from statistical variability. In addition to uncertainty in the models and data, the weather conditions during and following a release can have a very large impact on predicted consequences. The variability of meteorological conditions is usually addressed by treating weather as a stochastic parameter.

To date, a comprehensive assessment of the uncertainties in offsite-consequence predictions has not been performed. However, a large body of parametric (or sensitivity) analyses does exist in which consequences are calculated for ranges of plausible values of key parameters or models. The <u>PRA Procedures Guide</u> (NUREG/CR-2300) includes a tentative listing of the relative contribution to total uncertainty of the major parameters and models in an offsite-consequence analysis. The contributions of the factors to uncertainty were ranked as "major," moderate," or "low." This list, which was based on past parametric/sensitivity studies and the subjective judgment of the authors, contains 51 factors, 14 of which were deemed to be major contributors to uncertainty in at least one type of consequence. Among the "major" contributors are:

- The magnitude of the source term, which strongly influences all consequences

- The form and effectiveness of emergency response, which can make a large difference in predicted early health effects

- The dry deposition rate of particulate matter from the plume, which affects early health effects and the distances to which land-use restrictions or crop impoundment may be required

- The modeling of wet deposition caused by rainfall, which affects the low-probability, high-consequence end (tails) of the distributions of all consequences

- The dose-response relationships for somatic and genetic effects

In addition, questions have been raised over the importance of modeling atmospheric transport and dispersion with a "straightline" versus a trajectory model, particularly for sites located in areas of rough terrain or for sites located near the seacoast or the shore of a large lake. Though a complete evaluation of the importance of trajectory models on predicted risk has not been performed, the results of the CSNI International Comparison Study (OECD/NEA 1984) indicate that the influence of trajectory modeling is likely to be less than that of other major modeling assumptions for all sites except those with extremely complex terrain. Efforts to quantify better the uncertainties in the estimates of offsite consequences are currently underway and are described in the next section.

Even though a thorough examination of uncertainties in offsite-consequence analyses has not been performed, the magnitude of these uncertainties may be inferred from the results of the large number of existing sensitivity studies. For the consequences resulting from very large source terms at a highly populated site (NUREG/CR-2239), rough estimates of uncertainties can be made. Mean early fatalities could range from approximately a factor of five above present "best" estimates to nearly zero. This broad range is in large part due to uncertainty in the effectiveness of short-term emergency response near the plant. The uncertainty in mean predicted population dose (person-rem) is estimated to be a factor of 3 or 4, while the uncertainty in the predicted mean number of latent cancer deaths (which is a function of population dose) is approximately a factor of 10 above and below current best estimates. In general, the uncertainties are somewhat larger for the extremely low-probability, high-consequence portion ("tails") of predicted consequence frequency curves.

One effect which has not been considered to date in LWR offsite-consequence analyses is the possibility that condensation of moisture in the released plume could result in a significant fraction of the radioactive material being deposited in the immediate vicinity of the reactor. Were this to occur, the "rainout" of radioactive material could have a dramatic influence on risk, depending on the extent and location of the enhanced deposition. The likelihood of this occurring would depend on the nature of the containment breach and on the physical characteristics of the plume (e.g., temperature, momentum, moisture content). An NRC-sponsored program is currently examining this effect.

Clearly, all consequences are sensitive to the amount of radioactive material that could be released (the source term).

However, early fatalities and injuries are particularly sensitive because of the existence of dose-thresholds for these effects. If potential source terms for the most severe accidents are found to be substantially smaller than previously assumed (at least one order of magnitude), then the risk of early health effects would generally no longer be a principal concern. The consequences of such accidents, which could still be large, would primarily be latent health effects and land contamination, which is roughly proportional to the amount of long-lived radionuclides released (mainly cesium). In the limit, if aerosol releases are reduced to essentially zero, releases of just the inventory of noble gases (krypton and xenon) could still result in significant offsite radiation exposures.

In addition to dependence on the source-term magnitude, the numbers of estimated early health effects are very sensitive to assumptions about the nature and effectiveness of potential emergency protective measures. Studies have shown that for large releases of radioactive material, prompt evacuation and sheltering are potentially effective means of reducing the numbers of early health effects (NUREG/CR-1131). Latent cancer fatality predictions are not as sensitive to emergency response assumptions because of the larger areas and longer time frame involved.

As mentioned above, the weather at the time of the accident can have a very large influence on offsite consequences (e.g., low or high windspeed, rain or no rain). However, the variation in weather from site to site does not appear to affect total risk appreciably because the probabilities of weather types that contribute the most to variation in consequences are not significantly different in different climates. However, total risk is very dependent on the characteristics of a site, such as population density and land use, and these considerations are important for reactor siting.

A.6.4 Potential for Improvements

Five major sources of uncertainty in offsite consequence analysis were described above. The single largest contributor to the uncertainty in the offsite consequence estimates is uncertainty in the magnitude of the source term, which was discussed in the preceding section (A.5).

Efforts to improve consequence-analysis characteristics are under way in several areas as part of the NRC sponsored MELCOR program (Sprung, J. L.). Specifically, improvements are being made in the atmospheric dispersion and transport model; these include developing a multi-puff model which will permit the analysis of site-specific terrain and plume trajectories and provide an improved treatment of long-duration releases and precipitation modeling. Other improvements in modeling capabilities will include the incorporation of more detailed land-use characteristics, especially the differentiation of urban and rural areas, and a reevaluation of the available emergency-response data, which will provide improved estimates of the risk of early health effects. Improved models for radiological health effects and potential economic impacts are also being developed. In addition, a key objective of the MELCOR offsite-consequence modeling effort is to develop tools that can provide estimates of the uncertainties in the predicted consequences. Although uncertainties are likely to remain quite large, a thorough examination of their origin and magnitude will provide both a firmer basis for applying offsite-consequence analysis and a better understanding of its limitations. Finally, as mentioned above, an NRC-sponsored program is currently underway to assess the potential impact on offsite consequences of localized "rainout" from a moist plume.

These efforts, which will be completed in about one to two years, should provide improved estimates of offsite consequences, quantitative estimates of uncertainties, and increased confidence in the results, thus expanding the usefulness of offsite-consequence analysis.

A.7 External Initiators

PRA analysts have conveniently grouped accidents resulting from various "external events" into a separate category of analysis, principally because the method for treating them differs from the method for treating so-called internal initiators. The external initiators* are:

- Earthquakes
- Internal fires
- Floods
- High winds (tornadoes and hurricanes)
- Other
  - Aircraft impact
  - Barge and ship collisions
  - Truck, train, and pipeline accidents
  - External fires

*Both "internal initiators" and "external initiators" are misnomers, since the former category is usually taken to include accidents starting with loss of offsite electric power, while the latter usually includes internally initiated fires and floods.

- Volcanoes
- Turbine missiles
- Lightning

The unifying characteristic of all these initiators is the potential for the initiator not only to start an accident, but also to compromise simultaneously the efficacy of the safety systems needed to halt or mitigate the accident. In addition, some of these initiators (earthquakes and hurricanes, for example) are likely to cause a loss of offsite power and complicate evacuation of the surrounding area.

Each of the first four initiators listed above (earthquakes, internal fires, floods, and high winds) has been the subject of one or more comprehensive analyses that resulted in the estimation of values for core-damage frequency and offsite risk in a PRA. So far, none of the initiators listed in the fifth group ("other") has been subjected to such a comprehensive analysis in a PRA, typically because simpler analysis has shown the risk from these to be acceptably small.

A.7.1 Introduction to PRA Methodology for External Events

The basic approach to the probabilistic analysis of external initiating events is similar for all such types of events, and consists of four different types of analyses which are then combined. The sequence of these analysis steps is not necessarily in the following order, but all must be performed in a full analysis.

- The expected frequency of initiating events of various levels or magnitude must be determined. Considering floods, for example, the likelihood of floods of various sizes must be determined, recognizing that the very largest floods are much less likely than the somewhat smaller (though still quite large) floods. For the very largest and therefore very rare events, those that occur less frequently than once in a few hundred years, this task is very difficult, and the results possess large uncertainty.

- An analysis must determine the effects that various levels of the initiating event will have on the reactor building and specific pieces of equipment (components, systems, operator command and control functions, etc.). This includes determining the coupled likelihood of common-cause failures in which several systems or functions experience failure or degradation.

- The effect of degraded or inoperative systems, components, and safety functions is analyzed. The ability of the plant to reach a safe shutdown state is usually determined by event-tree and fault-tree methods.

- An analysis must be done on the phenomena and consequences associated with those rare accident sequences that lead to undesirable outcomes. This part of the analysis is nearly identical to that performed for internal initiating events.

The methodologies that have been developed for the various external initiating events differ in detail, of course. However, all external events are analyzed using the general approach just described, except in cases where the first part of the analysis shows that the expected probability of a sufficiently severe initiating event is so low that the overall contribution to risk would be very small. In such cases, the analysis can stop after the initiator frequencies have been determined.

The RSS (NUREG-75/014) used a relatively primitive approach to conclude that these initiators were probably unimportant. Most of the PRAs that followed the RSS in the first two or three years after its publication did not consider external events at all. Through methodological advances and some recent highly successful applications, the PRA methods for analyzing externally initiated accidents have matured enormously since the RSS. Major engineering insights are now available, even though large uncertainties persist in the numerical results of the analyses. The methodology for seismic analysis, for example, has reached a stage where the insights gained from recent PRA studies can be applied to specific components and structures.

The level of development among the various analysis areas for the different external initiators is uneven, and there are limitations to all of them. Thus for some external events, the likelihood of a major initiator (say, a very large earthquake or an extreme flood) is often neither known from the historical record nor reliably inferred from analysis based on extrapolations of that record. Also, the effect of some of these events on plant components, systems, and functions is in some cases not well understood. The "fragility" values used for equipment and structures are often based on incomplete data or approximate analysis. Finally, the ability to treat many of the common-cause and dependent failures is still limited.

For some of the categories of externally initiated accidents, the overall risk can be acceptably bounded by analysis limited to determining the frequency of the initiator in comparison with the calculated core-damage frequency of other accident sequences. This is typical of the initiators listed in the "other" category above, which have almost never been shown to be important contributors to overall plant risk. More importantly, the methods used for calculating the frequency of an initiator sufficiently large to compromise the plant (e.g., a large enough external fire, or a serious aircraft collision) are typically adequate to determine a very small upper bound with high confidence.

The categories where special discussion is needed are earthquakes, floods, internal fires, and high winds. In considering the uncertainties associated with PRA analysis of external initiators, it is important to understand that these are not qualitatively different from the uncertainties associated with the "internal" initiators. For both categories, the liklihood of some initiators is not known very well; examples include large pipe breaks, large earthquakes, failures of the reactor-protection system, and very high tornado winds. However, the likelihood of other initiators is known reasonably well in each category (examples include most transient initiators, most fires, smaller pipe breaks and valve failures, and internal floods). As it turns out, the circumstance that generally dictates whether the numerical uncertainty of a particular sequence will be modest or large is whether the numerical inputs to the quantification step are based mainly on real observed data or on information synthesized by analysis. As examples, we have considerably more confidence in our knowledge that a large airplane might strike a reactor about every million reactor years than we do that a large earthquake might occur near the site about every million years. While neither event has ever been observed, the former can be calculated from known data and reasonably firm models, whereas the latter can be calculated only from weak or non-existent data and poorly understood models.

A.7.2 Earthquakes

Section 11.2 of the PRA Procedures Guide (NUREG/CR-2300) describes the seismic hazard and fragility analyses. The reader is referred to that source if he wishes more detail than can be presented here.

A.7.2.1 State of the Art and Discussion of Uncertainties

Of all the various external initiators, earthquakes are the ones for which the PRA methodology is the best developed. Several comprehensive seismic PRAs have been completed,* and a significant amount of research has been completed (NUREG/CR-2105). These have developed the methods and explored their sensitivity to model and data uncertainties (USNRC; LLNL; OECD/NEA 1980). Recent seismic PRA results have been used to determine worthwhile plant modifications and in making regulatory decisions ("Special Proceedings"). Also, several specialized, limited studies of narrow issues have been performed using elements of the broader methodology.

---

*Commonwealth Edison Co.; Consolidated Edison Co.; Philadelphia Electric Co., 1983; Consumers Power Co.; NUREG/CR-3428.

Despite the relative stability of the methods, the results of the recent seismic PRAs are still highly uncertain. While the results are expressed in quantitative form, the key insights are widely accepted as qualitative.

Several different methods of seismic-hazard analysis are now available, and it is not currently clear which of them are preferable. The intrinsic problem with seismic-hazard analysis is that the dominant contributors to reactor risk come from ground motion significantly larger than the ground motion used as the design basis. Earthquakes with such large ground motion have return periods so long that their occurrence frequency cannot be accurately estimated from the historical record. This is especially true in the eastern U.S. but also applies to California. Thus, although the frequency of these very severe earthquakes is extremely small, the uncertainties in the frequency estimates are very large. These uncertainties propagate through to large uncertainties in the final results. The extrapolations used to determine the recurrence frequency of larger earthquakes are difficult because, for any given site or seismic province, a maximum earthquake motion is believed to exist that can be sustained by the specific geological features. Thus, the extrapolations are usually cut off in one fashion or another (NUREG/CR-2934). It turns out that the numerical results of some recent PRAs may be more sensitive to the nature of the cut-off procedure than to any other assumption.

There is also uncertainty in the characterization of the local ground motion due to these large earthquakes in terms of physical parameters such as frequency-dependent acceleration, velocity, and displacement; the shape of the motion in time; and the energy dispersion. Also, the data base on the attenuation from the earthquake to the reactor site is weak. Sometimes the historical record can be valuable in characterizing the expected motion of future earthquakes; but unfortunately many of the important historical earthquakes occurred before seismographs were in general use. The records for these earthquakes are limited to known structural damage, eyewitness reports, and the area over which the motion was felt. These can be less than reliable.

A model of the propagation of the earthquake motion from the fault through the rockbed and soil to the reactor building substructure and the interaction of the ground motion with that substructure is required to determine the motion felt by safety-related structures and equipment. Advances have been made in soil-structure interaction, under the auspices of the NRC's research program (NUREG-0961); and, although much remains to be accomplished, this area now contributes less to the overall uncertainties than some other elements of the analysis.

The fragility of structures and equipment is the other major element of seismic PRA. Here the progress has been significant in recent years, with studies of over a dozen reactors now completed. The fragility analysis relies partly on a data base that is neither strong nor extensive, and partly on analytical methods designed to overcome many of the weaknesses in the data base (Kennedy, R. P.). One obstacle to precise fragility analysis is the difficulty of characterizing the input motion adequately. Various surrogate accelerations have been proposed and used parametrically, each with limitations that offset some of its advantages. Furthermore, "failure" in the context of seismic PRA means failure to perform a safety function, not necessarily structural collapse or physical distortion. This distinction is often difficult to make in the course of the analysis.

Another issue is the statistical nature of the very problem addressed: obviously not all "identical" components (say, identical valves) will behave identically, even in a statistical sense. Yet the issue of most concern is that identical or similarly configured components might all fail together in an earthquake, defeating the redundancy of safety systems. This difficulty has not been resolved. Of course, the problem can be bounded by assuming complete independence and complete dependence as the extreme cases, and sometimes this approach is adequate (NUREG/CR-2105).

While the state of the art of fragility analysis is becoming more advanced as each new reactor is studied, there are still few practitioners in this area of PRA, and some of the estimates tend to be highly subjective. Many of the analyses are still underway at this time and have not been either published or reviewed.

The final element of seismic PRA analysis is linking the failures of structures and equipment into a systems analysis of the plant. Here the event trees developed in the other parts of a comprehensive PRA usually provide the basis for the analysis. Unfortunately, this part of the problem is not as easy to accomplish in practice as an analogous internal-events analysis, because a large earthquake can cause numerous failures that compromise redundant systems. The analyses completed to date, however, have found that the seismic risks are often dominated by accident sequences involving only a few important seismic-failure modes, often with degradation of the performance of certain structures or equipment.* This simplifies the analysis if it is valid to assume that the failure of these items leads to core melt. The inevitability of core melt has often been assumed with the full knowledge that it is conservative, sometimes highly so. The human factors aspects, such as recovery by the operators, have also not been treated in depth. Thus, despite some possible nonconservatisms, the seismic analyses tend to be conservative in character.

Overall, a consensus prevails that the uncertainties in the results (core-melt frequency, offsite risks) remain quite large for seismic PRAs: the error factors are estimated to be 30 or greater (implying spreads of factors of 1000 or greater in the 5 to 95% confidence interval). For the very largest earthquakes, the uncertainties can be even larger, up to factors of 10^5. In spite of these large uncertainties, significant engineering insights have been obtained using these PRA methods. The analyses have identified system vulnerabilities and dependent failures that indicate where further attention should be directed.

A.7.2.2 Major Insights

Several important insights have emerged from the completed PRAs that include seismic analysis:

- The significant seismic contributors to core damage or risk identified so far are significantly larger than the safe-shutdown earthquake (SSE). This indicates that regulatory attention is probably most beneficial to the extent that it focuses on assuring that significant margins exist for the SSEs now used.

- Because of its large fragility at very low acceleration values compared to other safety systems, loss of offsite power will almost always occur for any earthquake large enough to cause important damage to other parts of the reactor.

- With a few exceptions, the PRAs completed to date indicate that most major components behave very well, contributing rather little to overall risk. Examples include most piping, cable trays, compact valves, and most large pumps.

- The largest uncertainty in the quantification stems from the probability of the very large earthquakes that dominate the calculated risk. However, the engineering insights are not highly dependent on the actual numerical results.

- The problem areas that most seriously challenge the validity of the insights drawn from seismic PRAs are in the fragility analysis, especially dependences and correlations among failures, human factors issues, and in determining how equipment within or dependent on a structure will fail when the structure is degraded.

---

*Commonwealth Edison Co.; Consolidated Edison Co.; Philadelphia Electric Co., 1983.

- A few problem areas, such as building interactions, unreinforced masonry walls, piping runs between buildings, equipment anchorages, and battery racks, seem to recur in the seismic PRAs completed to date, and probably merit special attention at all plants.

- Uncertainties in the fragility data base are thought to be more important generally than uncertainties due to the fragility modeling.

- The methodology is not as reliable for earthquakes very much greater than the SSE as it is for earthquakes near the SSE level, in part because construction errors, which are not treated well, can be contributors at the very highest earthquake levels. PRA input to regulatory decisions involving sequences important only at these highest earthquake levels will be correspondingly less reliable.

A.7.2.3 Potential for Improvements

- More generally applicable insights should become available as more seismic PRA studies are completed. Up to now, the number of studies completed has been small, and the failures that have dominated the risk have been too plant-specific to allow much generalization.

- In contrast, major improvement in the quantification of seismic-sequence probabilities, from better understanding of the probabilities of the large earthquakes that seem to dominate seismic risk, will not progress very fast, because the intrinsic limitations (from the shortness of the historical record) are not likely to be dramatically overcome soon by analytical advances. However, progress may occur in understanding the "cut-off" issue, which is the issue of how to cut off the extrapolation of earthquake motion at high accelerations to account for the limitations in the ground's ability to sustain the largest motions.

- Integrated systems analyses that incorporate the seismic accident sequences with those due to "internal initiating events" are important and have been accomplished in the most recent applications. This will significantly improve insights.

- The role of operators in mitigating, or contributing to, the risks from seismic-initiated sequences is not well understood. Some progress is expected in this area, but this issue is likely to remain a difficulty for some time to come.

- Improvements will probably occur in the ability of analysts to choose and apply various surrogate means of characterizing the ground motion for the fragility analysis.

- Soil-structure interactions are already in reasonably good shape when considered in the context of the other larger uncertainties in seismic PRA. The ability to model and quantify these interactions will improve further in coming years as more studies examine sites with different physical conditions and configurations.

A.7.3 Internal Fires

A.7.3.1 State of the Art and Discussion of Uncertainties

Only recently has the probabilistic analysis of internal fires become an accepted part of a full-scale PRA. Only a very few PRAs have included fire analyses, and the methodology is currently undergoing rapid development. There have been significant improvements in the models recently, and important research is now underway (NUREG-0961).

The recent applications of the methodology in full-scale PRAs (e.g., Big Rock, Zion, Indian Point) have proven to be very useful. Primarily, they have demonstrated that the methodology can provide important engineering insights about plant vulnerability to fires. In addition, they have revealed the extent to which these insights can be relied on quantitatively, the problems with application to specific plants, and areas where the qualitative results may be generally applicable. Finally, these applications have been important in guiding future research and methodological development.

While several different approaches are evident in the literature, they share a common framework. Further details may be found in Section 11.3 of the PRA Procedures Guide (NUREG/CR-2300). Analysis begins with the identification of critical areas of vulnerability, then calculates the frequency with which fires might begin in each area, and follows with analysis of the extent to which critical safety functions and equipment are disabled by the fire. The spread of the fire to adjacent areas is considered as well as possible detection and suppression. Finally, the disabled equipment and functions are analyzed in a systems sense using event-tree/fault-tree methodology similar to that used elsewhere in PRA.

The initial phase of probabilistic fire analysis is the identification of critical areas. The criterion in this step is whether a fire could compromise important safety functions. In practice this criterion is narrowed to emphasize areas where multiple equipment could be compromised, in particular those areas where several trains of redundant equipment are colocated which perform the same safety function.

Identification often begins with the fire zones delineated in the more classical regulatory analysis, supplemented or modified by a walk-through with attention to questions such as potential for the cross-zone spread of fire and the likelihood that transient fuels might supplement fuels always present in a zone. While this part of the analysis remains more an art than a science, the general consensus is that uncertainties introduced by this aspect of the analysis are smaller than uncertainties from other aspects. Barrier identification feeds the fault-tree analysis by identifying candidate physical areas of concern for fire, or fire coupled with high-probability random failures.

The next phase of fire PRA is the determination of the frequency of fire initiation for each zone determined in the previous step to be important. The frequency can be specified by location within a large zone if fuel-loading conditions, cross-zone spreading potential, or other idiosyncracies require that level of detail. While a historical data base exists for fires initiated in various areas in the plant, it is not an adequate basis for determining initiation frequencies. The analyst must factor in location-specific information gained from his walk-through and other experience, which introduces important numerical uncertainties. Despite these numerical uncertainties, it is generally accepted that skilled analysts can consistently rank the important potential fire-initiating locations.

It is difficult to determine the likelihood of disabling equipment, given fire initiation. The fire analysis consists of four tasks:

- Analysis of fire growth and spread
- Analysis of the effectiveness of detection and suppression
- Assessment of component "fragility" to fire and combustion products
- Calculation of probability estimates (distributions) for fault-tree quantification. Overall systems analysis then proceeds through the containment-challenge and consequence-analysis steps, if appropriate.

Detection and suppression (manual and automatic) should be analyzed, in conjunction with fire spread and growth, as competing processes. Work to improve the methodology in this area is now underway in two areas: incorporating detection and suppression into the computer-based models used, and developing an analytical model for sprinkler effectiveness, which will provide the time of sprinkler actuation for a given fire.

This analysis problem is compounded by uncertainties concerning the modeling of detection and suppression, actual fuel availability (amount and character of transient fuels, etc.), the stochastic nature of fire growth over time, access for firefighting, and the size of the affected secondary zone where hot gases can cause equipment failures or induce secondary fires (or at least secondary equipment failures). Several important models have been developed to calculate fire-progression rates of the phenomena, but in even the best cases the uncertainties remain large (NUREG/CR-3239).

Whether the current analysis methods are complete, in the sense that they are capable of identifying all of the important vulnerabilities, is still an issue. Even the most advanced models available are only approximate in character. The analysis of failure modes for components exposed to the whole spectrum of combustion products needs more methodological development and more test data, as does the treatment of intercompartmental spread of fire and combustion products. Finally, the amount of uncertainty introduced by these assumptions and approximations is not known. Research on this question, along with studies of how well the analyst can be expected to perform in the detection-suppression arena, may contribute much to answering the question of the achievable accuracy from these probabilistic analyses (NUREG-0961).

The analysis of systems effects from fires involves the coupling of the fire studies with the event trees used in the analysis for the usual internal initiators. Simply adding the fire-induced failures to existing event trees is not adequate: the differences in timing, dependent failures, and human intervention (especially for fire suppression) can affect the development of the event trees. Event trees for the fire sequences must be drawn in an integrated way, taking into account the fire issues in parallel with the other initiators. In a proper analysis, the fire vulnerabilities would be integrated into the overall fault trees to allow a comprehensive treatment of dependent failures including secondarily induced failures. At the present level of development of fire PRA, this is only partly accomplished. Also, because human intervention cannot be analyzed as well for fires as is desirable, approximations or bounding calculations are required to determine the sensitivity of the final results.

The NRC has recently begun an integrated program of methodological development in this area, along with a program of applications intended to gain insights to guide the ongoing research (NUREG-0961). At the present time, the methods are fully capable of identifying and ranking important fire vulnerabilities and of providing useful insights. Research now underway will likely reduce the currently large uncertainties, but the achievable accuracy cannot be estimated at this time (Buchbinder, B.).

A.7.3.2 Major Insights

The PRAs performed to date that have incorporated fires have produced several insights:

- Most of the fires that have been found to be important to risk are those whose likelihood and/or severity are substantially reduced by the new NRC regulatory approach now being implemented.

- The nature of the fire phenomena is such that the conditional probability of containment failure, given a fire leading to core degradation, is likely to be significantly higher than the conditional containment-failure probability from other reactor accidents. This insight implies that great care must be taken to consider dependences in the containment analysis.

- The fire PRAs have generally revealed that the key vulnerabilities are in places where multiple safety systems are colocated, or where their controls, instrumentation, or support systems are collectively vulnerable. Whether this "finding" is the result of the PRA analyses, or simply the outcome of analyses based on this "finding" as a postulate, is not clear (probably some of each).

- The numerical results of these analyses are greatly influenced by the modeling of detection and suppression, human as well as automatic. These analyses are difficult, and research is now addressing this problem.

- The largest uncertainty in the quantification of fire-related risk seems to arise from the difficulty of determining the probability that a fire, once initiated, will disable critical equipment.

- The greatest issues concerning to the validity of the insights arise from the following questions: whether the analysis might have overlooked entirely some critical fire zones; how combustion products can induce failures; and and whether the human intervention in detection and suppression and in coping with the accident sequence has been modeled correctly.

- The dependence on the precise plant layout, including the amount of transient fuel loading, is so important that a fire PRA attempted before design details are available would probably not be very useful.

A.7.3.3 Potential for Improvements

- Major improvements in the usefulness of fire PRA results will occur simply from the continuing application of these techniques to more and more plants. This is probably one of the most important modes for progress in this field.

- Improvements in the ability to model secondary fire growth will occur soon as a result of the application of advanced models currently being developed by the NRC.

- Improvements in modeling of fire growth and spread, including comparison of different modeling approaches, will provide insights into the strengths and limitations of the various modeling schemes.

- The issue of the importance of intercompartment spreading, of both fires themselves and combustion products and hot gases, is an area where work now underway may yield important insights. However, these questions are highly configuration-dependent in actual application, and some limit probably exists as to how well this part of the overall analysis can be done. The areas of boundary penetration or failure, barrier-violating pathways such as ducts and drains, and isolation devices, require careful study.

- In the foreseeable future, the uncertainty in the PRA results will not be dominated by the ability to quantify fire initiation, but by the difficulty in determining the vulnerability of specific equipment given a type of fire, and the problem of quantifying the effects of human intervention in fire-suppression and accident-sequence mitigation. Particularly significant is the analytical difficulty in coupling suppression with fire growth (i.e., is statistical coupling adequate and can it be done, or is the much more difficult physical and mechanistic coupling required to achieve adequate results?).

A.7.4 High Winds

A.7.4.1 State of the Art and Discussion of Uncertainties

The "high winds" referred to here include both tornadoes and cyclones, which are meteorologically distinct phenomena. The cyclones include both hurricanes (tropical cyclones) and extratropical cyclones. In most PRAs, cyclones and tornadoes are treated separately.

The methodology for treating high winds in a PRA is similar to that used for earthquakes because each phenomenon can affect widely dispersed parts of a reactor plant simultaneously. This is in contrast to an internal fire or flood, whose effect is almost always confined to a particular part of the overall plant. High winds tend to directly affect the large structures rather than the specific pieces of equipment inside. Of course, the analysis is quite different in detail for high winds than for earthquakes. Offsite power is almost certain to be lost in any sizable wind storm.

The approach to analyzing high winds involves the same steps as for earthquakes. First, the likelihood of a hazard of a certain size must be worked out (i.e., an external wind field of a certain velocity and pressure). Next, the fragility of structures and equipment in the presence of the supposed hazard must be established. Finally, the probability that the overall reactor system can fail must be determined, given the failures of certain structures and equipment.

The level of development of this part of PRA is still only modest: Only a very few PRAs have included high winds in the overall analysis. Neither the methods for determining the wind-hazard potential nor the fragility analysis methods have been applied widely enough to gain an understanding of all of the problems with the analyses. However, some useful insights have already been obtained.

The phenomenological difference between hurricanes and tornadoes is due to the differing character of their winds. Hurricanes tend to produce mainly straight winds whose duration in a given location can range from tens of minutes to several hours. The speed of winds in hurricanes is limited to about 150 miles per hour (mph), with winds exceeding about 130 mph being rare. Tornadoes, on the other hand, can produce winds much higher than 200 mph, characterized by the familiar funnel form. Tornadoes typically last only a few minutes at any location. A further important distinction is that, while either type of wind can pick up objects and move them great distances, the likelihood of this is so much greater for tornadoes that analysis of "tornado missiles" is almost imperative, whereas missiles associated with hurricanes are seldom considered. An additional complicating factor is that hurricanes are usually associated with torrential rain and flooding; this association is also sometimes true for tornadoes.

Several methods are available to determine the likelihood of a tornado or cyclone producing a wind speed exceeding a particular value at a reactor site. These methods rely on historical records for the most part. Nearly everywhere in the U.S. there are enough data to provide a useful starting point. These historical records must be extended and modified to provide a useful foundation for the analysis for several reasons. First, because records may not exist for the reactor site, extrapolation from nearby sites may be needed. Second, the effect of local topographical features that will modify the wind profile must be included. Finally, because the data record is unlikely to contain any information for the very highest wind speeds of possible concern, extrapolation from the historical record will almost surely be needed. This last issue is a point of contention among the experts, since more than one method is available for doing the extrapolation, and the differences between the results of the different methods represent uncertainty in the initiator frequency.

Among the uncertainties in the hazard analysis, the calculated likelihood of a given wind speed at a site is currently significant. For example, at a given site, two different analytical methods might give annual probabilities of recurrence for a 150 mph wind that differ by more than an order of magnitude. While the spread can sometimes be smaller, the actual wind speed to which a particular building is exposed is also uncertain, because local buildings modify the open-field winds by as much as 10 or even 20 mph, sometimes corresponding to more than an order-of-magnitude difference in probability. Effects of building height must also be analyzed, although these are typically easier analytical problems. To obtain a much better analysis would require a mechanistic model to obtain the forces on structures from the free-field wind. No such model now exists, nor are there enough wind-tunnel data to support one, although a few selected experiments might vastly improve our analytical capabilities.

The problem of determining the likelihood of tornado missiles of various sizes is also quite difficult: The local availability and number of objects of various sizes for the wind to pick up (e.g., telephone poles, automobiles, trees, even heavier objects) must be determined. The likelihood with which a given missile type will attain a high enough speed to cause harm is also known only roughly. Thus, the effects of these missiles on the integrity of a reactor are not easy to analyze. Simulation studies could be of value in improving our analytical capabilities, but only if this issue turns out to be more important than it now seems.

The fragility analysis takes several forms. First and most important is the assumption, now considered a certainty, of the loss of offsite power and any exposed onsite power source. Second, structures must be analyzed. Here, the typical finding is that metal-sided buildings are much more vulnerable than concrete-sided ones, with failure modes including buckling, pressure collapse, and corners tearing away. For example, in the Indian Point PRA, the vulnerability of the reactor to winds was entirely due to metal structures. Strong concrete buildings with walls thicker than about 1 foot, by contrast, tend to be quite resistant. The tornado missiles are also assumed to be highly damaging for metal structures and exposed equipment such as tanks and pipes, while thick concrete structures are usually assumed to be rather immune to them; again, the Indian Point analysis assumed that any tornado missile striking any metal building causes its structural failure. The third and most difficult analysis is the fragility of equipment within a building. Here, the assumption is usually made that the failure of any building because of a high-speed windstorm will imply failure of all enclosed equipment.

Clearly, each of these assumptions is probably conservative in general, although not necessarily always so. For example, some concrete buildings could be more vulnerable at lower windspeeds than now thought because of design peculiarities. Also, the response of operators to extreme weather conditions is difficult to model. Finally, the complicating presence of torrential rain and flooding is not well analyzed for hurricanes in any of the analyses done to date.

The best way to summarize the present state of the art for high winds is that, while useful insights are available, the quantitative results for core-melt probability or offsite risk are highly uncertain.

A.7.4.2 Major Insights

- The threat from tornado missiles can only be modeled in the most approximate manner at present. They could pose an important threat, but their quantitative analysis is difficult because in general the spectrum of missiles of different types and sizes is not known, and the data base is weak. Despite these problems, results so far indicate that these missiles are probably significantly less important than the tornado winds themselves.

- In locations where hurricanes and/or tornadoes are a threat to other civil structures, they probably should be included as potential accident initiators in any comprehensive PRA.

A.7.4.3 Potential for Improvements

- A need exists for continuing analyses for high winds to supplement those very few now completed. These new analyses will indicate the extent to which lessons learned to date are generic or plant-specific.

- There is great potential for improving the way in which wind speed hazard frequencies are determined. Refinements, including improvements in calculating open-field wind speeds, better ways to account for local topographic features, and improved consideration of building shape factors and wake effects, could reduce the uncertainties in this part of the PRA analysis considerably.

- Analysis of the damage potential from tornado missiles will probably continue to be highly uncertain, mainly because of the difficulty in determining the number and nature of missiles as a function of tornado size.

- Especially for hurricanes, the present state of the art for hazards analysis is weak and introduces considerable uncertainty to the numerical conclusions.

- For high winds themselves (in contrast to tornado missiles), analysis of the fragility of buildings, especially metal-sided buildings, is in reasonably good shape at present, and contributes less to the overall uncertainty than does the windspeed hazard analysis. Moreover, progress in this aspect of the analysis will undoubtedly occur as more studies are done, including the application of the extensive existing data base from nonnuclear experience if it is deemed important to do so.

A.7.5 Flooding

A.7.5.1 State of the Art and Discussion of Uncertainties

The analysis of flooding as a cause of severe reactor accidents has not been included in most comprehensive PRAs to date, although flooding clearly poses a potentially serious challenge to overall safety. The methodology used to date has been limited to internal flooding and is similar to the approach used in studying internal fires: The analyst must first identify critical areas, then work out the probability that a flood might occur, then determine how long the source might continue and how long until the floodwaters are drained. Finally, the effect on critical safety functions must be determined, and the results integrated into the overall study using the event tree approach.

Flooding can result from either an external cause (river, lake, ocean, torrential rainstorm, etc.) or an internal cause (pipe break, tank rupture, etc.). In all PRAs to date that have considered externally initiated floods, the analysis has been limited to calculating the frequency of an external flood large enough to compromise important safety equipment or structures. In almost every case, this frequency, calculated conservatively or as a point estimate, has been shown to be small enough that further analysis has been unnecessary. This does not mean that external flooding is not a general problem because the analyses are highly site-specific. Thus, the remainder of this discussion will concentrate mainly on internal flooding, although much of the methodology is very similar.

In practice, internal flooding analysis is simpler than internal fire analysis for several reasons. First, the mechanisms for terminating the flooding are better understood, and their effectiveness can be accurately estimated. Second, the areal or volumetric effect of the flooding is much easier to determine, so the zone-designation problem can be handled better. Third, the rate of spread of the flood is usually known and limited. Finally, most of the fragility issues are thought to be understood, although by no means all of them.

Flooding analysis is complicated by several factors, however: Fragility of safety functions in the presence of a spray-type flood from a pipe break is very difficult to analyze quantitatively, for example. Also, the corrosion of equipment from the flooding can compromise the ability of a safety function to maintain its operation over the very long postaccident recovery period after a particular flood has been nominally "controlled." Another issue is the limited ability to quantify partial blockage of drains or sumps relied on to mitigate flooding. Finally, flooding (especially from an external source) can bring solid matter such as sludge, silt, or even sizable objects into areas where they could cause problems difficult to analyze.

Because time-sequence issues are different for most flooding scenarios than for accidents initiated from other sources, the analyst usually must think through these sequences separately and draw special event trees to handle their quantification.

The analysis of the probability of an internal flooding scenario of a given size and location starts by identifying all major piping or tanks that might be a source of water. The likelihood of a pipe break of a given size is not well known, the historical data base being sparse and not easily transferable to many important scenarios requiring study (indeed, this aspect dominates the ultimate uncertainty in these analyses at this time). Pipe leaks and breaks are not the only potential initiators of flooding, however: Another initiator is a possible failure of an isolation valve while a section of pipe is being maintained on-line during reactor operation. Since on-line maintenance (of, say, a valve or an instrument) occurs commonly during operation, a significant chance exists that the isolation valving might be opened either by the error of an operator or maintenance crew, or by hardware failure.

The analyst must determine the approximate flow rate of the break, as well as the ultimate capacity of the source of water (a tank, a large reservoir, or possibly just "city water"). With this information he can work out how much water will fill the available volume in how quick a time, taking into account drainage, sump capacity, and sump blockage. The analyst determines, for example, that a given compartment will fill up with water at, say, one inch per minute under certain conditions. Then the analyst must determine the likelihood, in a probabilistic sense, that operator intervention will terminate the flood at a given time, before it reaches whatever height will compromise critical equipment. While all of this seems straightforward, it poses for the analyst the need to make estimates (sometimes only postulates) about various probabilistic issues that are not well known.

Compounding the analytical problem is the issue of spray flooding from a pipe or tank leak, which could cause electrical failures at nearby locations. The data base and analytical methods for coping with this issue are weak. There is also the possibility that unusual dependences among equipment, for example because of spatial colocation of electrical or support equipment, will cause additional vulnerabilities. The difficulty in modeling human intervention can also complicate the analysis.

Despite the analytical difficulties, those few PRAs in which internal flooding has been analyzed have carried out this part of PRA quite successfully. The analytical problems, while by no means easily overcome, are fully tractable if uncertainties only in the order-of-magnitude range are sought.

A.7.5.2 Major Insights and Potential for Improvements

- Problems with analyzing the human-caused initiation of flooding (by inadvertent removal of isolation from an opened piping system) remain an important contributor to analytical uncertainty and will likely continue to be difficult for the analyst until either a better data base or better analytical methods are developed. Neither of these is now likely to happen soon.

- Development of experimental information on the fragility of equipment exposed to spray-flooding phenomena might strongly improve the analytical methodology and might not be very difficult to obtain if only modest data are sought.

- Until more attempts are made to carry out a full probabilistic analysis of internal flooding scenarios, the various methodological difficulties and potential achievements of flooding PRA analysis will not be fully known.

- Externally initiated flooding has not been found to be an important accident initiator. Analyses have typically placed acceptably small upper bounds on the core-melt probability from external floods by calculating that the frequency of sufficiently large external floods is small enough. There has been no comprehensive PRA of external flooding so far because it has not been necessary. However, this is very site-specific.

A.7.6 Other External Initiators

Besides the four major initiators discussed separately (earthquakes, high winds, internal fires, and floods), several other initiators which can threaten a nuclear reactor are usually considered within external events:

- Aircraft impacts
- Barge and ship collisions
- Truck, train, and pipeline accidents
- External fires
- Volcanoes
- Turbine missiles
- Lightning

The state of the art of analyzing all of these in the context of PRA is adequate at least conceptually, but they are all undeveloped in actual practice. Most of these have been examined at least to some extent in various PRAs, but never with a full-scale analysis.

Typically, these events are analyzed probabilistically by performing a bounding analysis on their likelihood. An initiating event serious enough to merit "concern" is usually semiquantitatively estimated. First, how large an external event must be to compromise important safety equipment is determined. Next, the likelihood that such a large initiator might occur is estimated. If the likelihood is small enough, or can be bounded well enough, the analysis ends with a statement to the effect that the event "does not contribute significantly."

This approach is fully adequate if carried out competently. Among the pitfalls in this approach are:

- The magnitude of the event needed to cause a significant accident may be seriously overestimated. That is, a much smaller (and more likely) event might lead to undesirable consequences.
- The analyst might overlook some coupled failure modes from the initiator.
- The analysis of the likelihood of occurrence might be badly flawed (for example, because no historical record exists and the extrapolation procedure used is erroneous, or because the historical data base is actually erroneous itself, or inapplicable).

The main insights gained to date from the analyses performed on these initiators is that they generally have small risk significance relative to earthquakes, winds, fires, and floods. This insight is quite important because it tells how good the deterministic design and operational requirements have been in assuring plant adequacy in these areas. The design and regulatory approaches seem to be adequately conservative.

The main limitation to the analysis is the possibility that some oversights, of the kinds mentioned above, could invalidate the conclusions. Given the conservatisms in the assumptions (specifically, even if the postulated external initiator is more probable than thought, the plant fragility analysis must still be performed with a high likelihood of plant survival), the general conclusion regarding the adequacy of plant design is likely to be correct.

A.8 Sabotage

Treatment of sabotage as an initiating event has not been traditionally included in PRAs. The threat of sabotage has been long recognized and treated outside the PRA arena. PRA techniques have on occasion been used to analyze various vital areas and penetrations related to sabotage, but the risk of sabotage itself has never been calculated, principally because of difficulty in quantifying the threat frequency.

The use of PRA techniques to address the sabotage issue dates back to 1975 when a fault-tree analysis was used to identify the combination of events which, if caused by a saboteur, could result in significant releases of radioactive material. Sabotage vulnerability studies have shown that sabotage cannot result in higher consequences than those considered in PRAs. A methodology was later developed which uses fault trees to aid identification of vital areas, that is, areas which warrant special attention when providing sabotage protection for the plant. The techniques used are not probabilistic.

Some probabilistic computer modeling has been used to identify weak links in physical protection systems. These codes, highly subjective in nature, model the detection and response capabilities of physical protection systems, given an external sabotage attempt. What has not been done is to develop models which allow meaningful predictions of the probability of a sabotage attack.

In some sense, a sabotage attempt can be regarded as another initiating event; the resulting accident sequences are not unlike those modeled in PRAs. The saboteur can be regarded as a common cause for the failure of several components or systems concurrently. The difficulty lies in being able to predict meaningfully the frequency of this initiating event. So-called random initiating events (component failures, human errors, earthquakes, etc.) can be estimated by considering past experience. The assumption inherent in looking at past experience and using that as a basis for future predictions is that the failure rates do not vary significantly from year to year. Uncertainties are placed on the estimate reflecting how much data one has on which to base the estimate.

Such an assumption cannot be made with confidence for acts of sabotage. The frequency of sabotage events is a function of social and political unrest, among other things, which may differ significantly with time. Therefore, existing statistical methods, which use past sabotage frequency experience to predict future sabotage frequencies, are not valid.

The development of PRA is not expected to improve this situation in the foreseeable future. Therefore, the evaluation of sabotage is expected to remain, appropriately, outside the scope PRAs, but the methods could provide assistance in evaluating the consequences of a given threat and in suggesting possibilities for mitigating such consequences.

A.9 Concluding Remarks

As this appendix has shown, PRA consists of a multitude of different disciplines, having different levels of development and different magnitudes and causes of uncertainty. The uncertainties must be recognized as being, for the most part, not unique to PRA, but reflecting a lack of data, experience, and knowledge about system response, human behavior, or accident phenomenology. Other uncertainties arise due to constraints inherent in the modeling process. These uncertainties exist whether the decisionmaker uses PRA, deterministic modeling, or so-called engineering judgment when making regulatory decisions.

Since its beginning, PRA has attempted to calculate and present the uncertainties in the results. This focuses more attention on the uncertainties than do other analysis methods. This information should be important to the decisionmaker, since it provides an estimate of how the lack of experience and knowledge impacts engineering insights drawn from the results. The treatment of uncertainties is thus a strength of the PRA method rather than a limitation.

The current level of development differs among the different portions of PRA. Thus, the reliance the decisionmaker places on the PRA insights should depend upon the different parts of the analysis involved. As the state of the art exists today, the following conclusions can be reached.

A.9.1 Systems Analysis

The methodology and information base for systems analysis is reasonably valid and stable. A relatively high level of confidence can be placed in insights about the relative importance of plant characteristics, dominant accident sequences, and core-damage frequencies from analyses done for internal initiators. The weakest part of the systems analysis is the human-reliability analysis, particularly in the areas of cognitive errors, misinterpretation or misunderstanding, and recovery actions. Thus, confidence is best placed on conclusions that are robust in the face of human-error uncertainties. The analysis techniques for common-cause and dependent failures are not as well developed as are the techniques for other areas.

A.9.2 Accident Progression, Containment Response, and Fission Product Transport

Currently, this represents the most uncertain and most unstable part of the PRA methodology, so much so that the best approach to the analysis is by no means clear in certain areas. In the area of accident-process analysis, the progression until severe core damage occurs is relatively well understood. Reactor vessel meltthrough, and the dispersal and possible fragmentation of the molten mass following this event, is perhaps the area where the least is known.

The ability to analyze the containment for catastrophic structural failure is quite good. Less attention has been paid to the failures of penetrations and seals, particularly at high temperatures, and the development of large leaks. Research is continuing on hydrogen generation, mixing, and ignition in the containment. Our knowledge in the area of fission-product release and transport is increasing rapidly at the current time. However, resolution of all the problems in this area may not come for several years. In summary, very limited confidence should be placed on insights derived from this part of the analysis at the present time.

A.9.3 Consequence Analysis

This type of analysis is relatively stable. Although it does not have as long a history of development as system analysis, a relatively high level of confidence can be placed on the resulting insights. However, the results are strongly dependent upon the input source term, i.e., upon the amount of radioactive fission products released to the environment.

A.9.4 External Events

The weaknesses in the analysis of accidents due to external initiators lie in large uncertainties in the initiators having a very low frequency of occurrence, the lack of data on component response to certain initiators, and the lack of uniformity in PRA methodologies for external initiators. It is especially difficult to establish reliable recurrence frequencies for the very severe natural phenomena (i.e., for the largest earthquakes, hurricanes, etc.) that happen much less often than once in a century. As a result, comparisons between internal and external event analyses or across different types of external events must be made advisedly. More confidence can be placed in insights which stem from comparisons within the analysis of a specific initiator type. That is, more confidence can be placed in an estimation of which seismic-initiated accident sequence dominates the frequency of core melt from seismic initiators than any conclusions about whether a seismic, fire, or small LOCA sequence dominates the overall core-melt frequency.

A.9.5 Uncertainties

The uncertainties generally quantified are those due to uncertainties in model parameters or data, i.e., those due to uncertainties in component failure rates, initiating event frequencies, etc. Uncertainties due to assumptions made about physical processes which are poorly understood, simplifications needed to construct the models, and events omitted because they are not within the scope of the study, often have not been explicitly considered and generally are considered separately by means of sensitivity analyses. In certain areas, the effects of different modeling assumptions can be larger than the uncertainties in the data. Because different and sometimes imprecise probability distributions are used for different parameters, the calculated uncertainties (error factors or confidence intervals) are not precise, well-defined quantities.

Relative PRA results often contain far less uncertainty than absolute PRA results, although this is not universally true. Insights and decisions should be based upon relative results whenever possible. This emphasizes the need for comprehensive sensitivity studies in the areas which possess the greatest uncertainties. At the present time, this seems to be a way to address some of the areas in which lack of data or knowledge requires crucial assumptions to be made.

REFERENCES

Albrecht, H., and H. Wild, "Investigation of Fission Product Release by Annealing and Melting of LWR Fuel Pins in Air and Steam," in Proceedings, ANS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Sun Valley, Idaho, August 2-6, 1981, American Nuclear Society, La Grange Park, IL, 1981.

Aldrich, D. C. et al, "Recent Developments in Reactor Accident Offsite Consequence Modeling," Nuclear Safety, Vol. 23, No. 6, November-December 1982.

Allison, C. M. et al, "Severe Core Damage Analysis Package (SCDAP), Code Conceptual Design Report," EG&G Idaho, Inc., EGG-CDAP-5937, 1981.

Baybutt, P. and S. Raghuram, "MATADOR--A Replacement for the CORRAL Computer Code for the Analysis of Radionuclide Behavior in LWR Containments," in NUREG/CP-0024, Proceedings of the Ninth Water Reactor Safety Research Information Meeting, October 26-30, 1981, Gaithersburg, MD, 1981.

Bergeron, K. D. and W. Trebilcock, "The MEDICI Reactor Cavity Model," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Brune, R. L., M. Weinstein, and M. E. Fitzwater, "Peer-Review Study of the Draft Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278," SAND82-7056, Sandia National Laboratories, Albuquerque, New Mexico, 1983.

Buchbinder, B., testimony before NRC Atomic Safety and Licensing Board, in "Special Proceedings, Indian Point Units 2 and 3," February 10, 1983.

Bunz, H., M. Koyro, and W. Schöck, "NAUA-Mod 4 - A Code for Calculating Aerosol Behavior in LWR Core Melt Accidents, Code Description and Users' Manual," KfK-3554 (Karlsruhe, Federal Republic of Germany: Kernforschungszentrum Karlsruhe, forthcoming).

Burian, R. J. and P. Cybulskis, CORRAL-2, Users Manual, Battelle Columbus Laboratories, January 1977.

Burns, R. D., III and W. A. Rodgers, "Fission Product Transport and Retention in Severe Degraded Core Accidents," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Camp, A. L., M. J. Wester, and S. E. Dingman, "HECTR: A Computer Program for Modelling the Response to Hydrogen Burns in Containments," presented at the Second International Workshop on the Impact of Hydrogen on Water Reactor Safety, Albuquerque, New Mexico, October 1982.

Commonwealth Edison Company, "Zion Probabilistic Safety Study," 1981.

Consolidated Edison Company and New York State Power Authority, "Indian Point Probabilistic Safety Study," 1982.

Consumers Power Company, "Big Rock Point Nuclear Power Plant Probabilistic Risk Assessment," 1981.

Corradini, M. L. and D. V. Swenson, "Probability of Containment Failure Due to Steam Explosions During a Postulated Core Meltdown Accident in a LWR," Sandia National Laboratories, SAND80-2132, 1981.

Cunnare, J. C., M. R. Kuhlmann, and R. Dehlberg, "The Scrubbing of FP Aerosols in LWR Water Pools Under Severe Accident Conditions-Experimental Results," ANS Topical Meeting in Snowbird, UT, July 1984, to be published.

DiNunno, J. J. et al, "Calculation of Distance Factors for Power and Test Reactor Sites," TID-14844, March 23, 1962.

Elrick, R. M. and R. A. Sallach, "Fission Product Chemistry in the Primary System," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Electric Power Research Institute, "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients," NP-2230, January 1982.

Fontana, M. H., "The Industry Degraded Core Rulemaking Program: IDCOR--An Overview," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Freeman-Kelly, R., "A User's Guide for MERGE," Battelle Columbus Laboratories, October 1982.

Gabor, J. R. and R. E. Henry, "The MAAP-BWR Severe Accident Analysis Code," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 -Sept. 1, 1983, Cambridge, MA, September 1983.

Gieseke, J. A. et al, "Radionuclide Release Under Specific LWR Accident Conditions," Draft, Battelle's Columbus Laboratories, July 1983.

Hannaman, G. W., A. J. Spurgin, and J. Wreathall, "Systematic Human Action Reliability Procedure," EPRI Project 2170-3, September 1983, Draft Report.

Joksimovich, V., M. Frank, G. W. Hannaman, and D. D. Orvis, "A Review of Some Early Large Scale Probabilistic Risk Assessments," EPRI NP-3265, Project 2171-1, Electric Power Research Institute, Palo Alto, CA, October 1983.

Joschek, H. I., "Risk Assessment in the Chemical Industry," in Proceedings, International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY, September 1982.

Kennedy, R. P., "Seismic Fragilities for Nuclear Power Plant Risk Studies," Second Specialist Meeting on Probabilistic Methods in Seismic Risk Assessment, Livermore, CA, 1983.

Kenton, M. A. and R. E. Henry, "The MAAP-PWR Severe Accident Analysis Code," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 -Sept. 1, 1983, Cambridge, MA, September 1983.

Kozinsky, E. J. and R. W. Pack, "Performance Measurement System for Training Simulators," EPRI NP-783, Electric Power Research Institute, Palo Alto, CA, 1982.

Lawrence Livermore National Laboratory, "Proceedings of Seismic Risk and Heavy Industrial Facilities Conference," 1983.

Lipinski, R. J. et al, "Uncertainty in Radionuclide Release Under Specific LWR Accident Conditions," Sandia National Laboratories, SAND84-0410/2, March 1984.

Lotts, A. L., "Monthly Highlights Report--ORNL Projects for the NRC Office of Nuclear Regulatory Research," Oak Ridge National Laboratory, June 1983.

NUREG-75/014, "Reactor Safety Study," WASH-1400, October 1975.

NUREG-0340, "Overview of the Reactor Safety Study Consequence Model," October 1977.

NUREG-0440, "Liquid Pathway Generic Study," February 1978.

NUREG-0772, "Technical Bases for Estimating Fission Product Behavior During LWR Accidents," June 1981.

NUREG-0900, "Nuclear Power Plant Severe Accident Research Plan," January 1983.

NUREG-0961, "Long Range Research Plan, FY1984 to FY1988," 1983.

NUREG/CR-0165, "A Value-Impact Assessment of Alternate Containment Concepts," Sandia National Laboratories, 1978.

NUREG/CR-0632, "TRAP-MELT User's Manual," Battelle's Columbus Laboratories, 1979.

NUREG/CR-1131, "Examination of Offsite Radiological Emergency Measurements for Nuclear Reactor Accidents Involving Core Melt," Sandia National Laboratories, October 1979.

NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Sandia National Laboratories, October 1983.

NUREG/CR-1433, "Examination of the Use of Potassium Iodide (KI) as an Emergency Protective Measure for Nuclear Reactor Accidents," Sandia National Laboratories, October 1980.

NUREG/CR-1596, "The Consequences from Liquid Pathways After a Reactor Meltdown Accident," Sandia National Laboratories, August 1981.

NUREG/CR-1659/3 of 4, "Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant," Sandia National Laboratories and Battelle's Columbus Laboratories, May 1982.

NUREG/CR-1826, "RELAP5/MOD1 Code Manual," EG&G, 1980.

NUREG/CR-2054, "TRAC-PD2-An Advanced Best-Estimate Computer Program for Pressurized Water Reactor Loss-of-Coolant Accident Analysis," Los Alamos National Laboratory, 1981.

NUREG/CR-2015, "Seismic Safety Margins Research Program," Vols. 1-10, Lawrence Livermore National Laboratory, 1981.

NUREG/CR-2142, "CORCON-MOD1: An Improved Model for Molten-Core/Concrete Interactions," Sandia National Laboratories, 1981.

NUREG/CR-2224, "CONTAIN - A Computer Code for the Analysis of Containment Response to Reactor Accidents - Version 1A," Sandia National Laboratories, to be published.

NUREG/CR-2239, "Technical Guidance for Siting Criteria Development," Sandia National Laboratories, 1982.

NUREG/CR-2254, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants," Sandia National Laboratories, July 1983.

NUREG/CR-2255, "Expert Estimation of Human Error Probabilities in Nuclear Power Plant Operations: Review of Probability Assessment and Scaling," Sandia National Laboratories, August 1982.

NUREG/CR-2300, "PRA Procedures Guide," American Nuclear Society and the Institute of Electrical and Electronics Engineers, January 1983.

NUREG/CR-2552, "CRAC2 Model Description," Sandia National Laboratories, March 1984.

NUREG/CR-2723, "Estimates of the Financial Consequences of Nuclear Power Reactor Accidents," Sandia National Laboratories, September 1982.

NUREG/CR-2728, "Interim Reliability Evaluation Program Procedures Guide," Sandia National Laboratories, March 1983.

NUREG/CR-2744, "Human Reliability Data Bank for Nuclear Power Plant Operations," Vol. 1, Sandia National Laboratories, March 1983.

NUREG/CR-2787, "Interim Reliability Evaluation Program, Analysis of the Arkansas Nuclear One-Unit 1 Nuclear Power Plant," Vols. 1 & 2, Sandia National Laboratories, August 1982.

NUREG/CR-2906, "Sensitivity of Risk Parameters Component Unavailability in Reactor Safety Study (PSAP/PSAB) Computer Codes," Brookhaven National Laboratory, May 1983.

NUREG/CR-2934, "Review and Evaluation of the Indian Point Probabilistic Safety Study," Sandia National Laboratories, 1982.

NUREG/CR-2986, "The Use of Performance Shaping Factors and Quantified Expert Judgement in the Evaluation of Human Reliability," Brookhaven National Laboratory, October 1983.

NUREG/CR-3010, "Post Event Human Decision Factors: Operator Action Tree/Time Reliability Correlation," Brookhaven National Laboratory, March 1983.

NUREG/CR-3239, "COMPBRN - A Computer Code for Modeling Compa' ent Fires," UCLA, 1983.

NUREG/CR-3317, "Technical Bases and Users' Manual for SPARC -- Suppression Pool Aerosol Removal Code," Battelle Northwest Laboratory, to be published.

NUREG/CR-3428, "Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant," Lawrence Livermore National Laboratory, 1983.

NUREG/CR-3440, "Identification of Severe Accident Uncertainties," Sandia National Laboratories, to be published.

NUREG/CR-3673, "Economic Risks of Nuclear Power Reactor Accidents," Sandia National Laboratories, April 1984.

Organization for Economic Cooperation and Development, Nuclear Energy Agency, "First Specialist Meeting on Probabilistic Methods in Seismic Risk Assessment," Lisbon, Portugal (October 1980); and "Second Specialist Meeting on Probabilistic Methods in Seismic Risk Assessment," Livermore, CA, May 1983.

Organization for Economic Cooperation and Development, Nuclear Energy Agency, International Comparison Study on Reactor Accident Consequence Modeling, Paris, 1984. Available from OECD Publications and Information Center, Suite 1207, 1750 Pennsylvania Ave. N.W., Washington, D.C. 20006-4582.

Osborne, M. F. et al, "Fission Product Release Under LWR Accident Conditions," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Philadelphia Electric Company, "Probabilistic Risk Assessment, Limerick Generating Station," Docket Nos. 50-352, 50-353, 1981.

Philadelphia Electric Company, "Limerick Severe Accident Risk Assessment," 1983.

Postma, A. K. and B. M. Johnson, "Containment Systems Experiment Final Program Summary," Battelle Northwest Laboratories, BNWL-1592, 1971.

Potash, L., M. Stewart, P. E. Dietz, C. M. Lewis, and E. M. Dougherty, Jr., "Experience in Integrating the Operator Contribution in the PRA of Actual Operating Plants," in Proceedings, ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY, Am. Nuclear Soc., LaGrange Park, Illinois, 1981.

Rehm, T. A., "Weekly Information Report," Memorandum to the Commissioners, March 30, 1984.

Rininsland, H., "BETA (Core-Concrete Interaction) & DEMONA (Demonstration of NAUA) -- Key Experimental Programs for Validation and Demonstration of Source Terms," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

"Special Proceedings, Indian Point Units 2 and 3," Dockets No. 50-247-SP and 50-286-SP (hearings held 1982-1983; Atomic Safety and Licensing Board Recommendations published October 24, 1983.

Sprung, J. L. et al, "Overview of the MELCOR Risk Code Development Program," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

Starr, C. and C. Whipple, "Coping with Nuclear Power Risks: The Electric Utility Incentives," Electric Power Research Institute, September 1981.

"Upgraded Severe Fuel Damage and Source Term Research Program," April 1984.

U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, "Colloquium on Seismic Risk Analysis," held in Bethesda, Maryland, September 27-29, 1982.

Von Riesemann, W. A. et al, "Structural Safety Margins of Containments," Ninth Water Reactor Research Information Meeting, Washington, D.C., October 1981.

Wassel, A. T. et al, "Removal of Radionuclides by Water Pools Under Severe Accident Conditions," Science Applications, Inc., July 1983.

Wooten, R. O. et al, "MARCH 2 Code Description and Users' Manual," Battelle's Columbus Laboratories, December 1982.

Young, M. F. and J. L. Tomkins, "MELPROG Code Development and Methods," in Proceedings, ANS International Meeting on Light Water Reactor Severe Accident Evaluation, Aug. 28 - Sept. 1, 1983, Cambridge, MA, September 1983.

APPENDIX B

INSIGHTS FROM PRAs

APPENDIX B

CONTENTS

ILLUSTRATIONS

ILLUSTRATIONS (continued)

TABLES

APPENDIX B

INSIGHTS FROM PRAs

In the course of performing PRA studies, those involved gain valuable engineering and safety insights. Conceptual insights are the most important benefits obtained from PRAs, and the most general of these is the entirely new way of thinking about reactor safety in a logic structure that transcends normal design practices and regulatory processes. PRA thought processes introduce much-needed realism into safety evaluations, in contrast with more traditional licensing analyses that generally use a conservative, qualitative approach, which can mask important matters.

This appendix provides information to supplement the discussion in Section 3.3. It discusses insights on plant risks in terms of core-melt frequencies, radionuclide releases, offsite consequences, and externally initiated events. In addition, it deals with the dominant accident sequences, important dependences, systems and human interactions, reliability or safety assurance programs, and, finally, briefly describes insights related to plant safety enhancements.

B.1 Plant-Risk Insights

Many studies, including WASH-1400 (RSS, 1975), indicate important distinctions among contributors to different types of outcomes of potential accidents. To illustrate this, Table B-1 presents some results from the Zion/Indian Point studies (Zion, 1981; Indian Point Units 2 and 3, 1982) comparing the accident initiators that are important contributors to core melt with those important to public risk. These results indicate that risk should not be measured solely in terms of any single indicator and that changes in plant configuration that significantly affect one indicator may or may not impact the other; thus, core-melt fixes may not impact public risk and vice versa. Hence, a risk-management strategy that focuses on core-melt frequency is not likely to result in the same set of actions as will a strategy with a focus on risk associated with the health effects.

The results of PRA studies are usually expressed in terms of core-melt frequencies, frequencies of radionuclide releases of various magnitudes, or curves presenting the frequencies of occurrence of different reactor-accident consequences (e.g., early and latent fatalities), depending on the level of the PRA.

Table B-1

Results from Zion and Indian Point PRA Studies

	Major Contributors		
	Core Melt	Public Risk	
Reactor Unit		Acute Fatalities	Latent Fatalities
Zion 1 and 2	Small LOCA	Seismic	Seismic
Indian Point 2	Fires, Seismic	Seismic, Interfacing LOCA	Seismic, Fires
Indian Point 3	Small LOCA, Fires	Interfacing LOCA	Fires

B.1.1 Core-Melt Frequencies

The estimated frequency of core melt is generally higher than had been thought before the RSS and subsequent U.S. studies. The range of core-damage frequency point estimates in the current library of PRAs covers about two orders of magnitude (about 10^{-5} per year to 10^{-3} per year). An examination of variability in the results indicates that quantitatively pinpointing reasons for the differences is extremely difficult. It is possible, however, to uncover general reasons for the variability that are attributable to plant design, operation, site characteristics, scope of the studies, PRA methods employed, and analytical assumptions postulated. At this time, extreme caution must be exercised in comparing the quantitative results of various PRAs.

One of the results of a PRA study is the identification of a relatively small number of accident sequences that represent the dominant contributors to core-melt. An analysis of the salient features of the dominant accident sequences from 11 PRAs yielded a characterization of accident-sequence categories as shown in Table B-2. The table shows the contribution (percentage) of each sequence category to the total core-melt frequency quoted in the study. In the cases of Zion, Big Rock Point, and Indian Point, the total core-melt frequency used in determining these percentages includes the contribution from external events. Externally initiated accident sequences were characterized by their effect on the plant, e.g., if an earthquake caused a loss of ac power, the sequence was categorized under loss of offsite power.

Table B-2

Core-Melt Sequence Contributions

Sequence Category	Percentage of Total Core-Melt Frequency										
	BRP[a]	Zion	Limerick	Grand Gulf	ANO-1[b]	Surry	Peach Bottom	Sequoyah	Oconee	IP-2[c]	IP-3[c]
Small LOCAs - Injection Failure	10	0	0	0	28	27	0	18	14	37	33
Small LOCAs - LTDHR[d] Failure	4	41	0	14	5	20	1	67	21	3	43
Large LOCAs - Injection Failure	0	3	0	0	0	4	1	0	0	0	1
Large LOCAs - LTDHR Failure	0	18	0	0	0	2	0	1	--	4	11
Transients - PCS[e] Not Available											
a. Loss of offsite power	14	18	48	27	20	7	0	0	12	26	3
b. Injection failure	36	0	34	0	23	14	2	5	15	28	2
c. LTDHR failure	5	0	0	38	0	0	0	0	21	0	0
Transients - PCS Available											
a. Injection failure	0	0	5	0	0	0	0	0	1	0	0
b. LTDHR failure	0	4	3	0	0	0	47	0	0	0	0
ATWS	0	15	2	14	4	9	47	0	11	0	1
Interfacing LOCA	9	0	0	0	0	9	0	9	5	0	0
TOTALS	78%	99%	92%	93%	80%	92%	98%	100%	100%	98%	94%

[a]Big Rock Point
[b]Arkansas Nuclear One - Unit 1
[c]IP-2 = Indian Point Unit No. 2, IP-3 - Indian Point Unit No. 3
[d]LTDHR is Long-term decay-heat removal (includes recirculation and RHR)
[e] Power conversion system

Figure B-1 represents a composite chart that combines the first five columns of Table B-2 (those studied in the EPRI NP-3265) for PWRs and BWRs respectively. The BWR chart does not include Big Rock Point because its design was considered atypical of other BWRs and its relatively high accident-sequence frequencies would have biased the results. The RSS BWR was substituted for it because it was deemed more representative of operating BWRs. The grouping was slightly modified in order to account for negligible contributions of large and interfacing LOCAs and small LOCAs to BWRs.

Figure B-1 provides a number of illuminating insights:

- The split between LOCA and transient contributors to core-melt frequency is about equal for PWRs and about 10:90 percent for BWRs. However, some recent work (Garrick, 1983) indicates ratios for newer PWRs similar to those for BWRs. This is attributable to the emphasis placed on independence and separation of safety equipment trains. Such designs reduce contributions from rare events such as pipe ruptures, but make it more difficult to protect the plant from frequently occurring events.

- The failure of long-term decay heat removal is a major functional contributor to core-melt frequency for both PWRs and BWRs. It is associated with LOCAs in PWRs and with transients in BWRs.

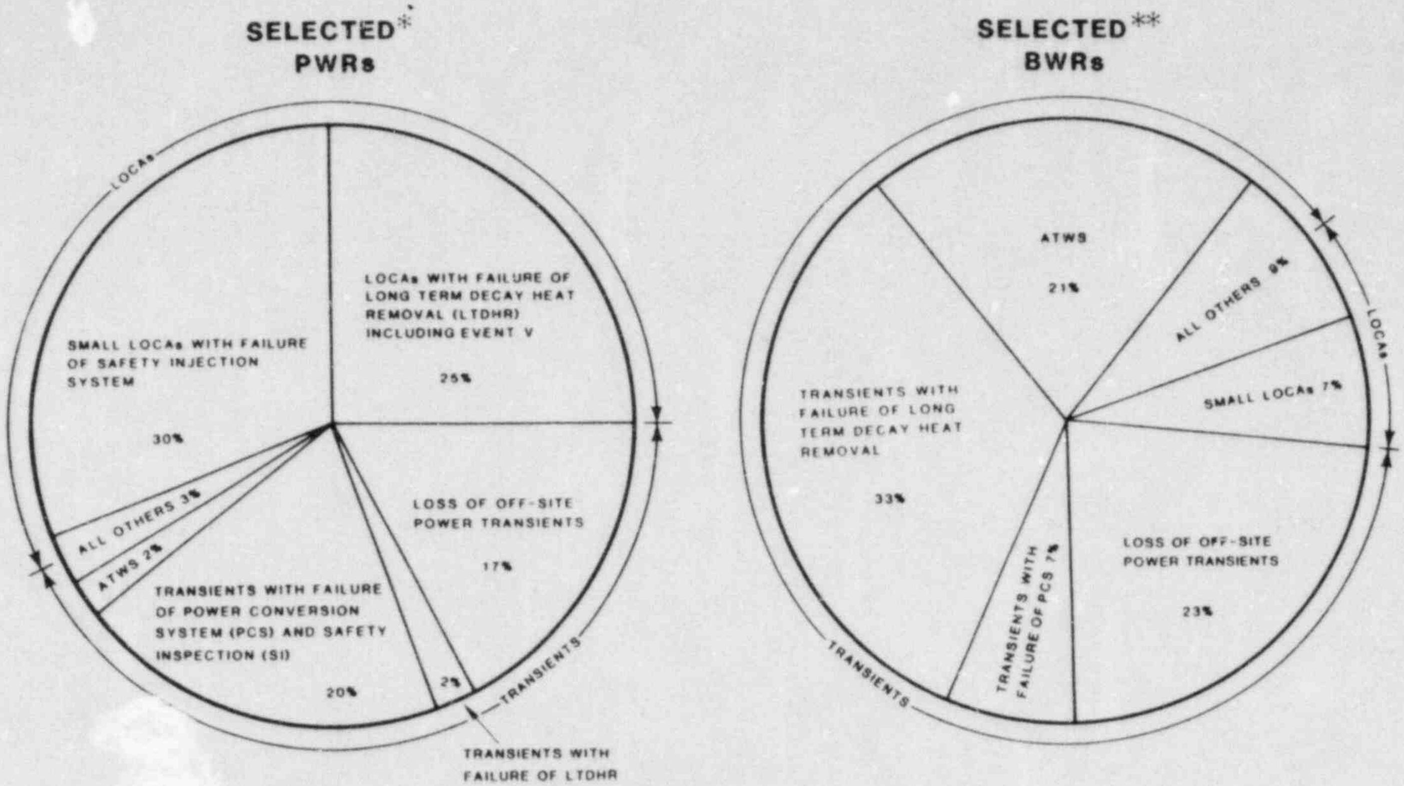
- In general, anticipated transients without scram are small contributors to core-melt frequency in PWRs but significant contributors in BWRs.

- As a group, small LOCAs with failure of long-term decay heat removal are large contributors to core-melt frequency for PWRs.

Several studies (e.g. Zion, Indian Point, Big Rock Point, Limerick, Millstone 3, Seabrook) highlighted the importance of a probabilistic treatment of such external events as earthquakes, fires, and floods. Part of the reason for the high contribution from external events found in these studies is related to the considerable uncertainty associated with their frequency of occurrence as well as the structural and containment responses to such events. These uncertainties, by and large, are attributable to the state of knowledge and ability to model. It is believed that as both knowledge and modeling improve, their risk significance is likely to change. This subject is discussed further in B.1.4.

B.1.2 Radionuclide Releases

The RSS indicated that accident sequences that dominated the core-melt frequency often did not result in large offsite consequences for the PWR studied because the predominant failure



* Arkansas-1, Oconee-3, Sequoyah-1, Surry, Zion

** Grand Gulf, Limerick, Peach Bottom-2

"All Others" contain roughly equal mixes of LOCA and transients

NOMENCLATURE:

LOCA	Loss of Coolant Accident	PCS	Power Conversion System
SI	Safety Injection	LTDHR	Long Term Decay Heat Removal
ATWS	Anticipated Transients Without Scram	Event V	Interfacing Systems LOCA

Figure B-1. Relative Core-Melt Frequency Contributions mode of the containment was basemat melt-through, which led to relatively small releases of radioactive material. The results of some studies performed shortly after the RSS indicated that if each core-melt sequence led to a containment failure with a fairly high likelihood of a large radionuclide release to the atmosphere, the dominant core-melt and dominant radionuclide release sequences would essentially coincide. However, more recent studies indicate that not all the dominant core-melt accident sequences involve early containment failure and therefore, the risk-dominant sequences may not coincide with those that most influence the frequency of core melting.

The studies surveyed generally show that public risk is less sensitive to plant-system unavailabilities than is the core-melt frequency. This is because risk is controlled more by the capability of the containment to withstand challenges to its integrity than by the unavailabilities of the safety systems that protect the core integrity. The frequency of significant radionuclide releases tends to decrease as the containments are assessed to be stronger in the more recent studies.

The accident sequences that appear to emerge as dominant contributors to release are those in which radioactive material bypasses the containment or in which the containment fails concurrently with (or shortly after) core melt. This early containment failure may be caused by major common-cause initiating events, such as large earthquakes. Such sequences are not necessarily the dominant contributors to core-melt frequency (e.g., interfacing-system LOCA). An example ranking of core-melt and significant release sequences is shown in Table B-3.

Figure B-2 provides ranges for categorized radionuclide-release fractions from selected PRA studies. Figure B-3 displays the same type of information but with more detail showing the results of individual plant studies in terms of iodine release only. Three illustrative cases are displayed: (1) severe containment-failure modes (i.e., early overpressurization or containment bypass), (2) late containment failure, and (3) containment remains intact despite core melt. Only the nuclides most important from the standpoint of health effects are included--the noble gases (Xe, Kr), iodine (I), cesium (Cs), and tellurium (Te).

Figure B-2 graphically displays some of the insights about source terms gained since publication of the RSS. The following points emerge:

- Source-term predictions generally have ignored several potential processes and phenomena that would reduce atmospheric releases and are, therefore, likely to be overestimates.

Table B-3

Comparison of Core-Melt and Release Sequences

Sequence	Core-Melt Ranking	Significant-Release Ranking
ZION STUDY		
Small LOCA: LTDHR failure	1	4
Seismic ac power loss	2	1
Loss of ac power and AFWS failure	13	2
Interfacing-system LOCA	16	3
INDIAN POINT-2		
Seismic loss of control or power	1	3
Fires in electrical tunnel and switchgear room	2	4
Seismic (direct) containment failure	21	1
Interfacing-system LOCA	24	2
INDIAN POINT-3		
Small LOCA failure of high-pressure recirculation	1	4
Fires in switchgear room and cable-spreading room	2	3
Interfacing-system LOCA	15	1
Seismic containment failure	37	2

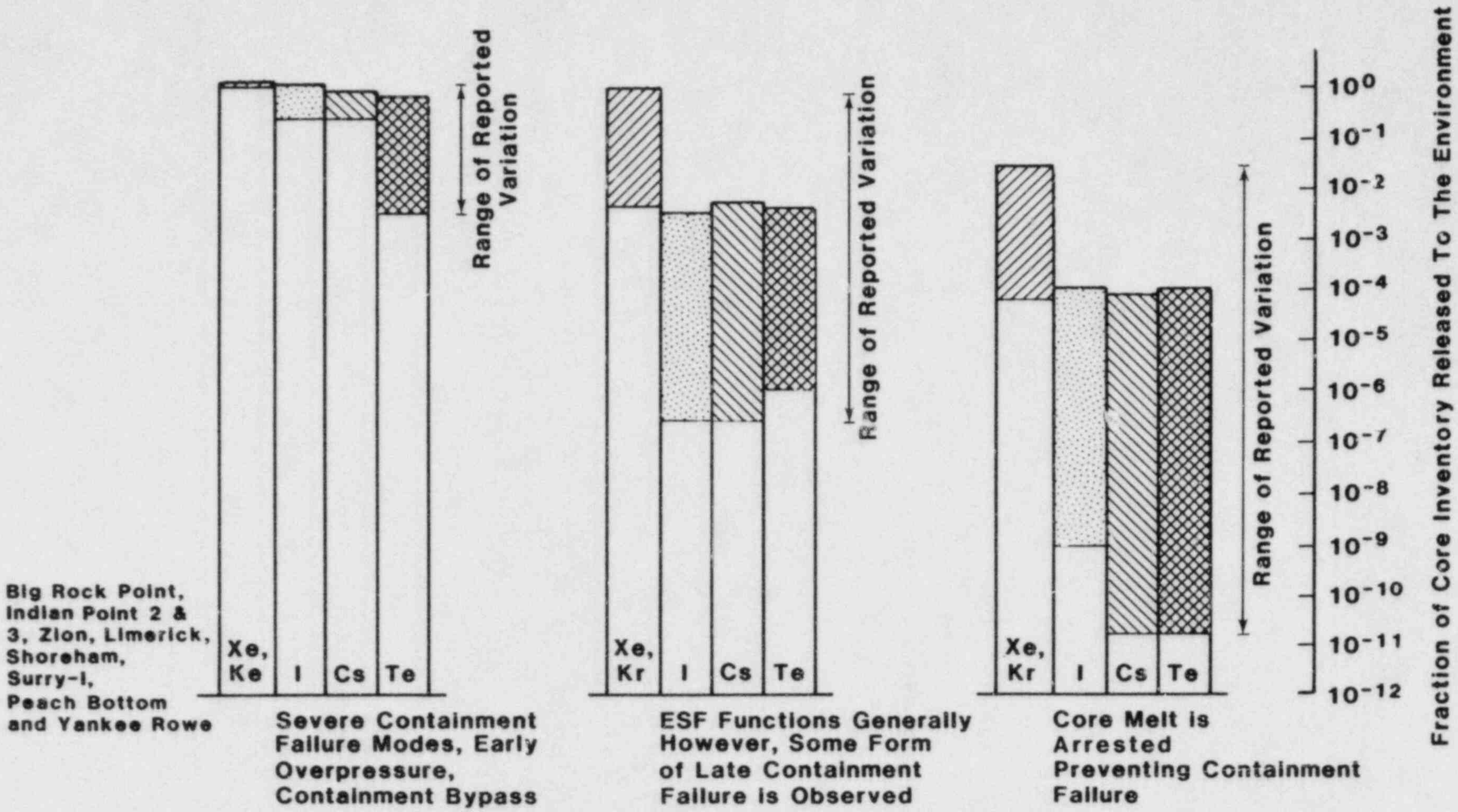


Figure B-2. Range of Radionuclide Release Fractions from Listed PRA Studies

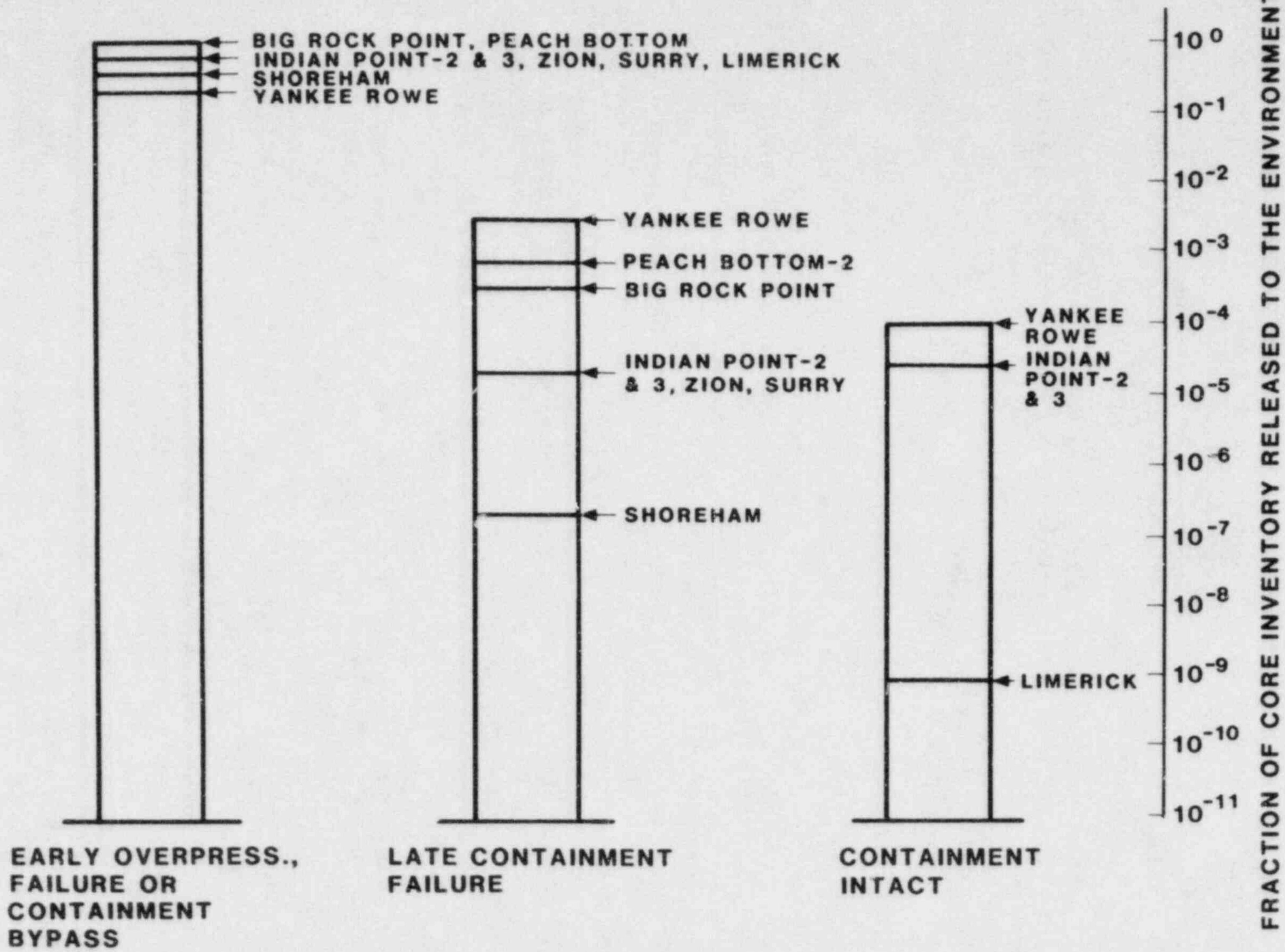


Figure B-3. Iodine Release Fractions from Listed PRA Studies

- For those core melts that do not fail the containment, the retention properties of the containment are substantial.

- If the containment fails a long time after core melt, only small-to-moderate release fractions result. The range between the predictions of various studies is extremely wide for these cases, and further resolution from current analytical and/or experimental programs is expected.

- Only containment bypass, early overpressurization sequences, or sequences involving common-cause containment and core-cooling failures lead to large releases. Because of the existence of dose thresholds, the occurrence of early health effects is generally limited to these containment failure modes.

B.1.3 Offsite Consequences

PRA studies have provided a number of significant insights into severe reactor accident offsite consequences. Several of these were listed in Section 3.3 of the main report. Clearly, all consequences are sensitive to the amount of radioactive material that could be released during an accident (the source term). However, early fatalities and injuries are particularly sensitive because of the existence of dose thresholds for these effects. If potential source terms for the most severe accidents are substantially smaller than previously assessed (by at least one order of magnitude), then the risk of early health effects generally would no longer be a principal concern. Nonetheless, the consequences of such accidents could still be large; the nature of the risk, however, would be different. Focus would shift to latent health effects and to the more localized problem of land contamination. Land contamination is roughly proportional to the quantity of long-lived radionuclides (mainly cesium) released. Tradeoffs between decontaminating an area, barring its use (interdiction), and a possible increased risk of cancer would need to be considered. In the limit, release of only the noble gases (krypton and xenon) could still result in significant offsite radiation exposures.

In addition to the source-term magnitude, the estimated number of early health effects is very sensitive to assumptions about the nature and effectiveness of potential emergency protective measures. For large releases of radioactive material, prompt evacuation and sheltering are potentially effective means of reducing the numbers of early health effects. Latent-cancer fatalities are not as sensitive to emergency-response assumptions because larger areas and longer exposure times are involved.

The weather (wind speed, rain, or dry weather) at the time of the accident can have a very large effect on offsite consequences. The variation in weather from site to site does not appear to affect the total risk appreciably, because the probabilities of weather types that contribute the most to variation in consequences are not significantly different in different climates. However, total risk depends strongly on site characteristics (e.g., population density, land use); these considerations are important for reactor siting.

B.1.4 Externally Initiated Accidents

PRA studies have provided a new understanding of the importance of externally initiated events to public risk. In addition, specific insights into system response and methodology application have been derived. Some of the most significant insights are summarized below.

The impact of externally initiated events appears to be <u>mainly plant-specific</u>. For seismic events, the specifics of one plant's PRA results do not seem to be transferable to another plant, even though the plants may be similar. Although the specifics are different, the general character of fires is similar; major cable or control areas are involved, and multiple redundant safety systems are affected. For flooding events, the results likewise do not seem transferable from plant to plant.

Detailed analyses of external events have identified some accident sequences initiated by these events as important contributors either to core-melt frequency or to risk. Thus, the conclusion in the RSS that external events contributed only about 25% to plant risk has not been widely borne out, but this is difficult to confirm conclusively because of the uncertainties in analysis of external events, as well as plant-to-plant variations.

For seismic events the following insights are indicated:

- Earthquakes significantly larger than the safe-shutdown earthquake (SSE) are the significant seismic contributors to plant risk.
- Local ground and subsoil conditions have been an important issue in all PRAs investigating seismic events.
- Earthquakes usually result in the loss of offsite power, which affects the availability of systems important to safety.

Most of the fires found to be important to risk are those whose likelihood and/or severity are substantially reduced by the new NRC regulatory approach now being implemented and associated regulatory guides and standards (10 CFR 50, Appendix R).

For high winds, metal-sided structures are more fragile than other structures and most equipment, and are more likely to fail and compromise overall plant safety. Like earthquakes, high winds generally cause losses of offsite power, affecting system availabilities.

B.2 Dominant Accident Sequences

The RSS showed that the risk posed by the two plants that had been studied stemmed primarily from a few accident sequences. The relevance of these dominant accident sequences was immediately recognized. Uncertainties in the frequency or consequences estimated for these sequences would have the greatest effect on risk estimates. To achieve a significant reduction in risk, potential backfits or improvements in future designs would have to reduce either the frequency or the consequences of the dominant accident sequences. Thus, the understanding of risk, and the ability to effectively reduce risk, hinges on an understanding of the accident sequences that dominate risk.

Shortly after the RSS, a program was instituted by the NRC to address, among other things, the similarities of dominant accident sequences for PWRs and BWRs. The results of the program indicated that the dominant accident sequences were <u>not</u> consistent in detail across broad plant classes, such as all PWRs or all BWRs. In fact, the plant features and operational characteristics that gave rise to specific dominant accident sequences were not of a nature that would lead to the conclusion that dominant accident sequences would be similar, even for smaller classes such as "all B&W PWRs." Characteristics that determined what accidents were dominant were often dependent on the design of support systems (electric power, service water, etc.), which vary significantly from plant to plant, or reflected individual utility practices, such as what check valves were tested before returning to power after shutdown or, if tested, how they were tested. Thus, the consensus that began to form in the late 70s was that the specific dominant accident sequences for plants across the industry could be quite different in detail, and therefore the task of reducing the existing plant risk through generic decisions (as opposed to plant-specific decisions) would be more difficult than had been hoped.

Many more risk assessments have now been done, and the results of these studies have tended to confirm this earlier conclusion and to add new insights. Though each plant is unique and may exhibit accident sequences that are specific to the design and operation of the plant, it is still possible to identify broad accident characteristics of plants that lead to the high frequencies (dominance) of specific accident-sequence categories. Based on these characteristics, plants can be placed into classes such that each member of the class would be expected to have dominant accident sequences in similar categories. The principal observations from such categorization are the following:

- Dominant accident sequences can be expected to differ for different plants and have relatively wide frequency ranges as a result of differences in plant design, operation, and siting.

- Despite plant differences that affect sequence frequencies, generic studies that support regulatory decision-making can be performed effectively by assigning plants to categories with similar dominant accident sequences.

The remainder of this section defines the relevant safety functions and then discusses the dominant functional sequences for PWRs and BWRs, respectively.

The plant functions used to prevent core-melt or mitigate consequences differ with the initiating event, which is usually a LOCA or a transient. LOCAs are component or piping failures that result in a loss of cooling water from the reactor-coolant system. For LOCAs, the common set of functions performed by the mitigating systems is as follows:

(1) Render reactor subcritical.

(2) Remove decay heat (core cooling).

(3) Protect containment from overpressure caused by steam evolution.

(4) Scrub radioactive material from the containment atmosphere.

Transient events, as the term is used in PRA, are events that cause one or more physical parameters of the plant to exceed the normal operating range and for which prompt achievement of reactor subcriticality (scram) is desired. For transients, the common set of functions performed by the mitigating systems is as follows:

(1) Render reactor subcritical.

(2) Remove core decay heat (core cooling).

(3) Protect reactor-coolant system from overpressure failure.

(4) Protect containment from overpressure caused by steam evolution.

(5) Scrub radioactive material from the containment atmosphere.

Functional accident sequences can be defined in terms of the initiating event (transient or LOCA) and then by the subsequent functional failures. This approach was used in the Accident Sequence Evaluation Program (ASEP). Tables B-4 and B-5 provide listings of the functional sequences obtained. The tables also show the range of accident-sequence frequencies that have been reported as central estimates in past PRAs. Some of the major design differences and uncertainties that contribute to the wide variations in frequencies among PRAs are also provided, together with a commentary.

B.3 Important Dependences, Systems, and Human Interactions

In addition to identifying the dominant accident sequences, PRA studies provide valuable information on the individual constituents in these sequences. They indicate which aspects of plant design, operation, and siting are important and how they are related. These constituents include important dependences and human interactions. These can assist in decisions regarding potential risk-reduction modifications, the assignment of reliability-assurance priorities, technical specification requirements, etc. Exhaustive amounts of information can be compiled on these subjects. The information described below is intended solely for illustrative purposes.

B.3.1 Dependences Between Frontline and Support Systems

Systems important to performing the safety functions in nuclear power plants fall into two broad groups, often referred to as the frontline systems and support systems. The frontline systems are designed to directly perform the safety functions. Support systems provide power, control, cooling, or other supportive needs to the frontline systems.

Frontline systems differ from plant to plant. Furthermore, different vendors or utilities may give very similar systems slightly different names. Sometimes, the names reflect different uses of the systems; other times, the different names reflect no more than a preference. The situation is further complicated by the fact that the same system may be given different names within a given plant to reflect different functions it serves when aligned for different modes of operation. For example, the low-pressure injection system (LPIS) and low-pressure recirculation system (LPRS) may represent nearly the same set of components only realigned to different water sources. Tables B-6 and B-7 list some of the frontline systems currently being used in LWRs.

Table B-4

Functional Accident-Sequence Categories for PWRs

Sequence Category	Frequency Range ($\times 10^{-6}$)	Major Uncertainties	Comment
Transient Loss of reactor sub-criticality	1 - 60	RPS reliability; RCS ability to withstand pressure spike	ATWS rule pending
Transient Loss of integrity Loss of core cooling	<1 - 30	PORV demand rate; HPIS availability; necessity to switch-over to recirculation	TMI fixes (raising PORV set point and anticipatory AFWS start signal) should reduce sequence frequency
Transient Loss of core cooling	0.1 - 1000	Feed-and-bleed capability; AFWS availability	TMI fixes have called for many improvements in AFWS availability
Transient Loss of core cooling Loss of containment heat removal	0.2 - 140	Redundancy of ac power sources; battery, CST depletion x possibility of induced RCS pump-seal leak; long-term ventilation loss effects; AFWS availability	NRC position statement-forthcoming
LOCA Loss of core cooling	<0.4 - 200	LOCA frequency; ECCS success criteria; ECCS redundancy	Small LOCA may be higher than thought due to RCP seal leaks; TMI fixes stressed better procedures for small LOCA
LOCA Loss of core cooling Loss of containment heat removal	<1 - 6	LOCA frequency; ECCS success criteria; ECCS redundancy	Small LOCA may be higher than thought due to RCP seal leaks; TMI fixes stressed better procedures for small LOCA

Table B-5

Functional Accident-Sequence Categories for BWRs

Sequence Category	Frequency Range (x 10^{-6})	Major Uncertainties	Comment
Transient Loss of reactor subcriticality	0.1 - 50	RPS reliability; adequacy of ECCS; unknown phenomenology in RCS ability of open to control water level	ATWS rule pending
Transient Loss of RCS integrity Loss of core cooling	<0.2 - 70	ECCS availability; operator procedures for ADS SRV demand rate ADS; SRV demand rate	
Transient Loss of RCS integrity Loss of containment cooling	0.1 - 1000	RHR availability; SHV demand rate	Estimated time to core melt appears longer than previously expected, thus longer times for recovery
Transient Loss of core cooling	0.2 - 700	ECCS availability; operator procedure for ADS	Station blackout rules pending
Transients Loss of containment cooling	<0.4 - 100	RHR availability; ECCS success criteria; ECCS redundancy	Estimated time to core melt appears longer than previously expected, thus longer times for recovery
LOCA Loss of containment cooling	<0.1 - 5	RHR availability; time avail- for recovery	Estimated time to core melt appears longer than previously expected, thus longer times for recovery

Table B-6

Typical Frontline Systems for PWRs

Initiating Event/Function	Frontline Systems
LOCA	
Render reactor subcritical	Reactor protection system (RPS)
Remove core decay heat	High-pressure injection system (HPIS) Low-pressure injection system (LPIS) High-pressure recirculation system (HPRS) Low-pressure recirculation system (LPRS) Core flood tanks (CFT) Auxiliary feedwater system (AFWS) Power Conversion System (PCS)
Prevent containment overpressure	Reactor building spray injection system Reactor building spray recirculation system Reactor building fan coolers Ice condensers
Scrub radioactive materials	Reactor building spray injection system Reactor building spray recirculation system Ice condensers
Transients	
Render reactor subcritical	Reactor protection system (RPS) Chemical volume and control system (CVCS) High-pressure injection system (HPIS)
Remove core decay heat	Auxiliary feedwater system (AFWS) Power conversion system (PCS) High-pressure injection system (HPIS) Power-operated relief valves (PORV)
Prevent containment overpressure	Containment spray injection system (CSIS) Containment spray recirculation system (CSRS) Containment fan cooling system Ice condensers
Scrub radioactive materials	Containment spray injection system (CSIS) Containment spray recirculation system (CSRS) Ice condenser

Table B-7

Typical Frontline Systems for BWRs

Initiating Event/Function	Frontline Systems
LOCA	
Render reactor subcritical	Reactor protection system
Remove core decay heat	Main feedwater system Low-pressure coolant injection (LPCI) system Low-pressure core spray system (LPCS) Automatic pressure relief system (APRS) High-pressure coolant injection (HPCI) system Reactor core isolation system
Prevent containment overpressure	Suppression pool Residual heat removal system (RHRS) Containment spray injection system (CSIS)
Scrub Radioactive materials	Suppression pool Containment spray injection system (CSIS)
Transients	
Render reactor subcritical	Reactor protection system (RPS) Standby liquid control system
Remove core decay heat	Power conversion system (PCS) High-pressure core spray system High-pressure coolant injection (HPCI) system Low-pressure core spray system (LPCS) Low-pressure coolant injection (LPCI) system Reactor core isolation cooling system (RCIC) Feedwater coolant injection Standby coolant supply system Isolation condensers (IC) Control rod drive system (CRDS) Condensate pumps
Prevent reactor-coolant system overpressure	Safety relief valves (SRV) Power conversion system (PCS) Isolation condensers (IC)
Prevent containment overpressure	Residual heat removal system (SRV) Shutdown cooling system Containment spray injection system (CSIS)
Scrub Radioactive materials	Suppression pool Containment spray injection system (CSIS)

Support systems, which provide power, control, cooling, or other supportive needs to frontline systems, also differ considerably from plant to plant. In general they may be electrical systems, water systems, or air systems. Most frontline systems will require some form of support systems to operate. Notable exceptions are the reactor protection system (RPS) and core flood tanks (CFT), which require none. Table B-8 displays a typical set of frontline systems and the support systems needed for each. This table was taken from a PRA of the Arkansas Nuclear One, Unit 1 power plant.

Table B-8

ANO-1 Frontline vs Support System Dependences

FRONT LINE SYSTEMS \ SUPPORT SYSTEMS	OFFSITE AC POWER	DIESEL AC GENERATORS	125V DC POWER	ENGINEERED SAFEGUARDS ACTUATION SYSTEM	EMERGENCY FEEDWATER INITIATION AND CONTROL SYSTEM	SERVICE WATER SYSTEM	INSTRUMENT AIR SYSTEM	INTEGRATED CONTROL SYSTEM	INTERMEDINTE COOLING SYSTEM	AC SWITCHGEAR ROOM COOLING	DC SWITCHGEAR ROOM COOLING	HIGH PRESSURE PUMP ROOM COOLING	LOW PRESSURE/SPRAY PUMP ROOM COOLING	NON-NUCLEAR INSTRUMENTATION POWER
REACTOR PROTECTION SYSTEMS														
CORE FLOOD SYSTEM														
HIGH PRESSURE INJECTION/RECIRCULATION	●	●	●	●		●				●	●	●		
LOW PRESSURE INJECTION/RECIRCULATION DECAY HEAT REMOVAL	●	●	●	●		●				●	●		●	
REACTOR BUILDING SPRAY INJECTION/RECIRCULATION	●	●	●	●		●				●	●		●	
REACTOR BUILDING COOLING SYSTEM	●	●	●	●		●				●	●			
POWER CONVERSION SYSTEM	●		●		●	●	●	●	●	●	●			●
EMERGENCY FEEDWATER SYSTEM	●	●	●		●	●				●	●			
PRESSURIZER SAFETY RELIEF VALVES														

NOTE: ALL REQUIREMENTS FOR DIESEL GENERATORS ASSUME LOSS OF STATION POWER

Table B-9, taken from the same report, reflects that support systems often require yet another support system. Thus, a typical power plant is a complex set of interdependent systems that perform a range of functions that are important to prevention of core-melt and reduction of public risk.

Table B-9

ANO-1 Support vs Support System Dependences

SUPPORT SYSTEMS \ SUPPORT SYSTEMS	OFFSITE AC POWER	DIESEL AC GENERATORS	125V DC POWER	ENGINEERED SAFEGUARDS ACTUATION SYSTEM	EMERGENCY FEEDWATER INITIATION AND CONTROL SYSTEM	SERVICE WATER SYSTEM	INSTRUMENT AIR SYSTEM	INTEGRATED CONTROL SYSTEM	INTERMEDIATE COOLING SYSTEM	AC SWITCHGEAR ROOM COOLING	DC SWITCHGEAR ROOM COOLING	HIGH PRESSURE PUMP ROOM COOLING	PRESSURE/SPRAY PUMP ROOM COOLING	NON-NUCLEAR INSTRUMENTATION POWER
OFF SITE AC POWER	■													
DIESEL AC GENERATORS		■	●	●		●				●	●			
125V DC POWER	●	●	■					●			●			
ENGINEERED SAFEGUARDS ACTUATION SYSTEM	●	●	●	■						●				
EMERGENCY FEEDWATER INITIATION AND CONTROL SYSTEM	●	●	●		■					●	●			
SERVICE WATER SYSTEM	●	●	●	●		■				●	●			
INSTRUMENT AIR SYSTEM	●		●			●	■		●	●				
INTEGRATED CONTROL SYSTEM	●	●	●					■		●	●			
INTERMEDIATE COOLING SYSTEM	●		●	●		●			■	●	●			
AC SWITCHGEAR ROOM COOLING	●	●				●				■				
DC SWITCHGEAR ROOM COOLING	●	●				●				●	■			
HIGH PRESSURE PUMP ROOM COOLING	●	●		●		●				●		■		
LOW PRESSURE/SPRAY PUMP ROOM COOLING	●	●		●		●				●			■	
NON-NUCLEAR INSTRUMENTATION POWER	●	●	●								●			■

Many of the contributors to core-melt frequency or risk result from interactions among systems, events, and phenomena. Additional insights into dependences and their treatment in PRAs are as follows:

- The dependence of multiple systems on a common service such as pump cooling or room cooling is a major contributor to accident sequences. However, in these sequences a long time is generally available before the release of radioactive material, which gives the operator the opportunity to recover from initial support-system failures.

- The importance of recirculation failures to core-melt frequency in PWRs depends on the ability to use high-pressure and low-pressure systems independently and the mode of switchover to recirculation (manual or automatic). The potential for human error in switchover from injection to recirculation under LOCA conditions is an important consideration.

- Some systems that are cross-connected between units at multiple-unit sites improve the availability of support systems because of improved flexibility and thus diminish the effect of support-system failures on accident-sequence frequencies.

- For BWRs, the loss of long-term containment heat removal was considered important in past PRAs because it eventually resulted in the failure of coolant makeup systems. However, because of the long times involved, the operators have considerable time for recovery actions, which could reduce the importance of these accidents to core melt.

- Operator error is often a significant contributor to coolant-injection failures in the case of transients and small LOCAs in BWRs. This happens because the operator may fail to initiate depressurization if the high-pressure systems are unavailable, and automatic depressurization may occur too late to protect the core.

- High-pressure events contribute more to overall risk than do low-pressure events, particularly in PWRs.

- In BWRs, the progression of low-pressure events is much slower than it is in PWRs.

- The risk of low-pressure events in BWRs can be reduced significantly by recovery actions.

B.3.2 Relative Importance of Systems

In investigating design alternatives and in establishing surveillance programs, decisionmakers must understand which systems are the most important. It is very difficult to establish the relative importance of systems because (1) many ways exist for defining importance, and the appropriate measure should be chosen in light of the objective for which the measure will be used, (2) the importance of systems depends on the dominant accident sequences, which differ for different plants, and (3) the systems are interdependent, particularly the support systems that provide electric power, cooling, control, and other functions that support the main systems.

Nevertheless, attempts have been made to clarify the subject. Under NRC sponsorship, a report (NUREG/CR-3385) was issued that addresses two risk-importance measures to evaluate a feature's importance in further reducing the risk and its importance in maintaining the risk level. One of the importance measures, called the feature's "risk-reduction worth," was developed for use in assigning priorities to future improvements. The second type of importance measure, called the feature's "risk-achievement worth," was developed for assigning priorities to features that are most important in reliability assurance and risk maintenance.

This study applied the risk-worth measures to the four plants studied in the Reactor Safety Study Methodology Applications Program (RSSMAP): Oconee, Grand Gulf, Calvert Cliffs, and Sequoyah. The four plants employ light-water reactors of the two major types (BWR and PWR), the four types of nuclear steam supply systems (General Electric, Westinghouse, Babcock & Wilcox, and Combustion Engineering), and three containment types (large dry, Mark III BWR, and ice condenser). The four studies provided a good opportunity for comparing the importance of systems because the PRA methods for the studies were generally similar.

Figure B-4 shows the risk-achievement ratios and the risk-reduction ratios for the Sequoyah plant, with core-melt frequency as the risk measure. The risk-achievement ratios are graphed above the dividing line and indicate the factor by which core-melt frequency would increase if the system had a failure probability of unity (that is, it was never operable). The risk-reduction worths are graphed below the dividing line and indicate the factor by which core-melt frequency could be reduced at the plant by improving system reliability. Also shown is human action, identified by RSSMAP as having the largest risk-achievement worth.

Figure B-4 shows that a very significant increase in core-melt frequency could occur if the reliability of important plant systems were allowed to deteriorate below that predicted by PRAs. The figure thus emphasizes the need for a sound reliability-assurance program to ensure that this deterioration does not occur.

Another important study, performed under the sponsorship of the Office of Nuclear Reactor Regulation, reviewed 15 published PRAs and estimated the relative importance of systems from their contribution to the dominant accident sequences in Figure B-4. Both BWRs and PWRs were considered. The results are shown in Figures B-5 and B-6. The arrows indicate that each system was not involved in the dominant accident sequences in at least one PRA. The explanations of the system abbreviations (in the order of their appearance, first in Figure B-5 and then Figure B-6) are:

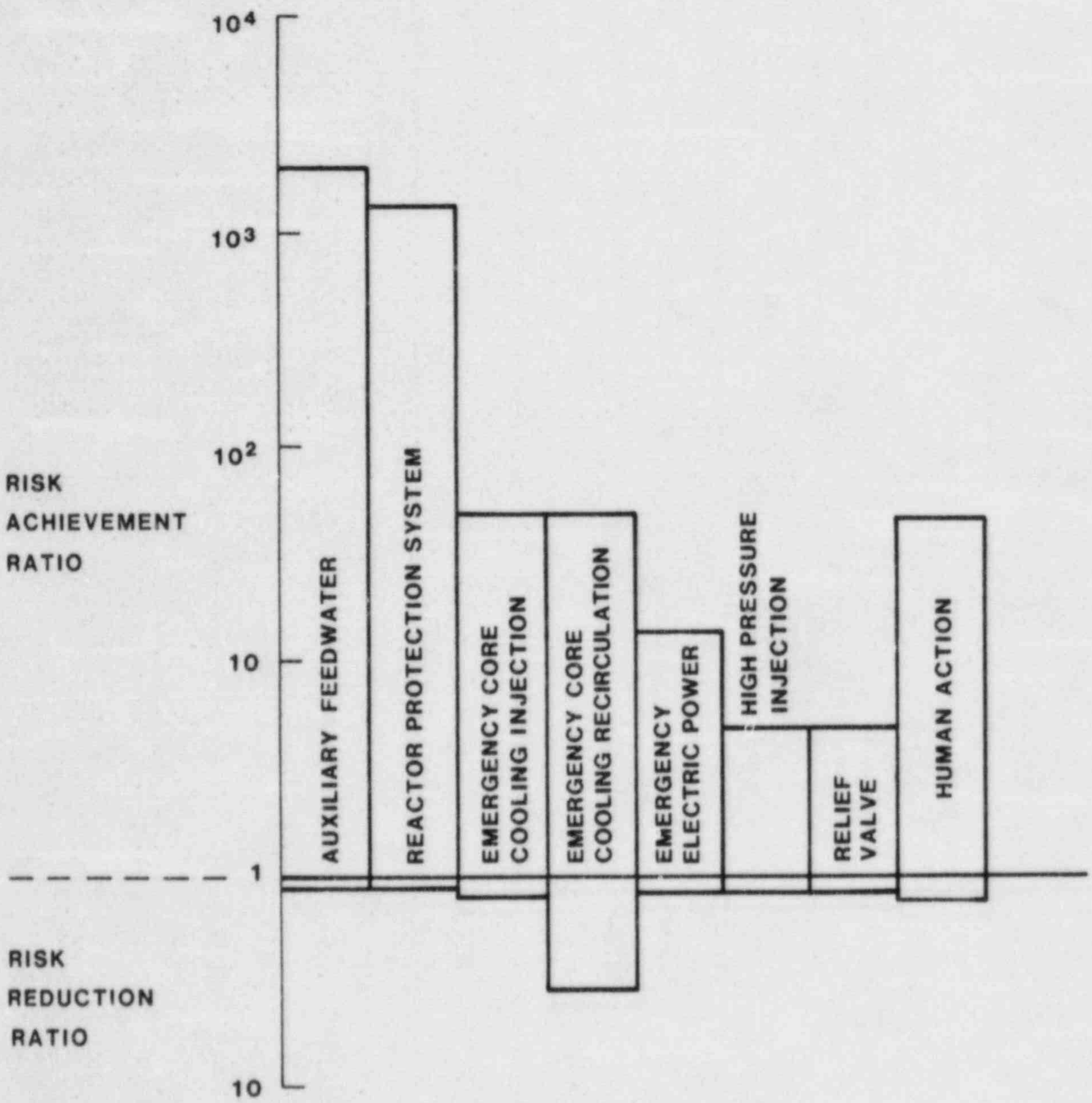


Figure B-4. Risk-Worth Ratios for Sequoyah Safety Systems with Regard to Core-Melt Frequency

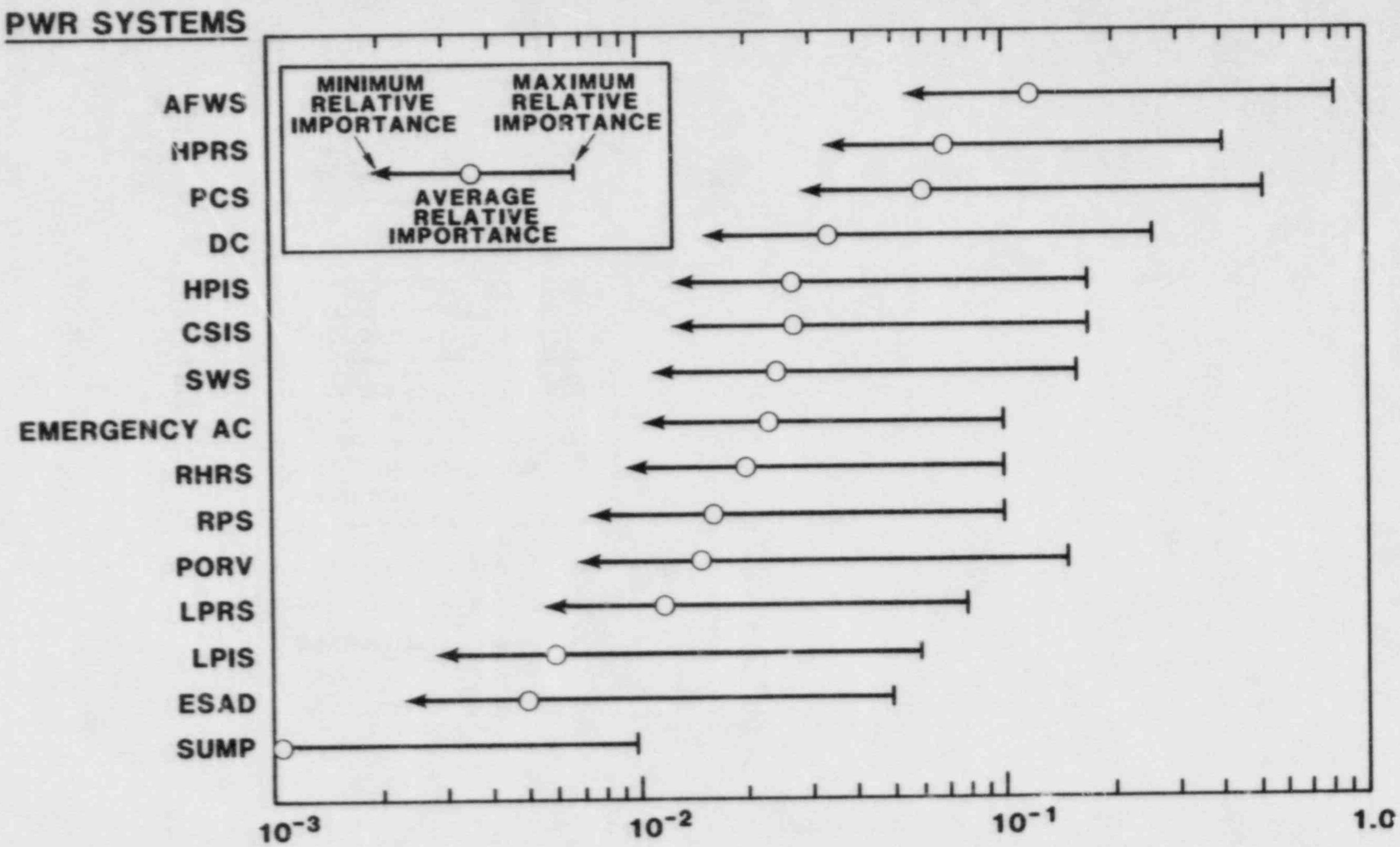


Figure B-5. Relative Importance of PWR Systems Considering Dominant Accident Sequences from 15 PRAs

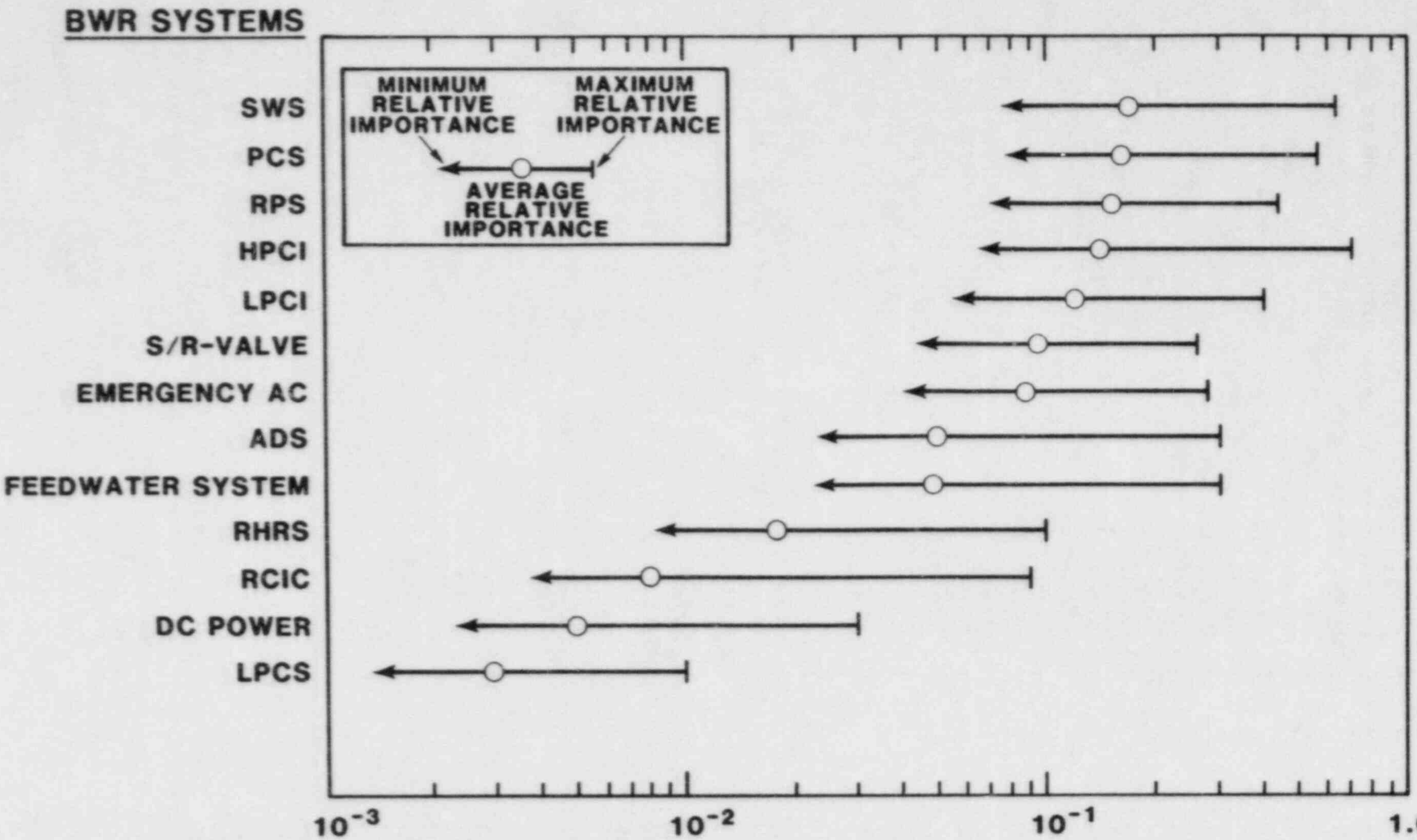


Figure B-6. Relative Importance of BWR Systems Considering Dominant Accident Sequences from 15 PRAs

AFWS	Auxiliary feedwater system
HPRS	High-pressure recirculation system
PCS	Power-conversion system
DC	Direct current power
HPIS	High-pressure injection system
CSIS	Containment spray injection system
SWS	Service water system
Emergency AC	Emergency ac power
RHRS	Residual-heat-removal system
RPS	Reactor-protection system
PORV	Power-operated relief valve
LPRS	Low-pressure recirculation system
LPIS	Low-pressure injection system
ESAD	(To be defined)
SUMP	Containment sump
HPCI	High-pressure coolant injection system
LPCI	Low-pressure coolant injection system
S/R-VALVE	Safety/relief valve
ADS	Automatic depressurization system
RCIC	Reactor-core isolation cooling system
LPCS	Low-pressure core spray system

The industry degraded core rulemaking (IDCOR) program has also arrived at some generic conclusions about the relative importance of systems. For PWRs, the following systems are fairly consistently most important for all plants:

(1) Auxiliary feedwater system
(2) High-pressure injection system
(3) Low-pressure recirculation system

For BWRs, less consistency was found but, in general, the following systems often appeared important:

(1) Power-conversion system
(2) High-pressure injection system
(3) Reactor-core isolation cooling system
(4) Reactor-protection system
(5) Residual-heat-removal system

B.3.3 Human Interactions

Human-plant interactions constitute an important link in the operation, control, maintenance, and testing of equipment in virtually all industrial activities. These beneficial interactions often enable various typical systems to achieve an extremely high availability. However, a dichotomy exists. Although such human interactions are largely responsible for maintaining high availability, the human contribution to accidents that do occur has been estimated to be as high as 90% in the cases of the airline (NUREG/CR-2744) and chemical industries (Joschek, 1982).

The experience of the nuclear industry also shows the importance of human interactions. For example, the NRC-sponsored Accident Sequence Precursor Study of Licensee Event Reports (Minarick, 1982) examined 19,400 such reports, submitted from 1969 to 1979, of which 529 were selected for detailed review. One hundred and sixty-nine were defined as significant accident precursors. Human errors were found to be significant contributors in 38% of these. The key categories of human errors were maintenance, operations during transients, use of procedures, and errors related to testing.

Assessments made in various PRA studies provide further corroboration of the importance of human interactions. For example, an examination of the RSS results showed that human errors can account for 50 to 85% of the system failures during accident sequences (NUREG/CR-0400). Likewise, an examination of the HTGR Accident Initiation and Progression Analysis (AIPA) Study found that the contribution of human actions to the frequency of core heatup was about 50% (Fleming et al, 1979). In the German risk study (DRS, 1979) human errors were reported to contribute 63% to the core-melt frequency.

Similar findings have emerged from some plant-specific PRA studies for nuclear power plants (Joksimovich et al, 1983). Past PRA studies have found that both beneficial and detrimental contributions of the human influence impact the ordering of dominant sequences and, hence, the risk profile of the plant. For example, the studies have invariably included human actions that can cause initiating events or result in the unavailability of plant systems prior to an initiating event. In some studies, human interactions that compensate for accident causes can include the diagnosis of and recovery from an accident sequence. It is clear that the PRA techniques provide a framework for assessing the importance of human interactions in a spectrum of accident sequences.

The definition of specific accident sequences in PRA studies provides the analysts with a tool for investigating more clearly where the human might influence the risk. For example, the uncertainties in the quantitative impact can be assessed, the ways that humans affect the course of an accident can be described, and the importance of humans in a particular sequence can be quantified. The two human interactions that appear consistently to be important in PRAs are failure to properly switch over to recirculation during the PWR LOCA sequences and failure to initiate the automatic depressurization system manually after the failure of high-pressure injection in small LOCAs in BWRs.

B.4 Reliability Assurance

A PRA study presents a "snapshot" of the risk profile at a given plant at a given time. As time progresses, modifications to plant equipment or procedures (i.e., operating or maintenance practices) can change the risk profile. Furthermore, as operating experience accumulates, the improved information base may suggest that the generic failure rates used for some components should be modified or that the potential for dependent failures differs from the potential previously assessed. Thus, there is a need to update the analyses and to make the PRA essentially a "living" document that reflects the impact of plant modifications and recently acquired data.

There are techniques that permit an analyst to measure the incremental effect of a degradation in a given safety function, system, or component. Such analyses permit the plant owner and the NRC to focus inspection and quality-assurance activities on the plant features that could conceivably increase the core-melt frequency or risk estimates of the PRA. The features identified by such an analysis may not necessarily be those that are major contributors to risk. Rather, they are the features that could become dominant if their failure characteristics are degraded significantly in relation to those used in the analysis.

The availability of an updated PRA would also make possible a means for interpreting the significance to risk (or core-melt frequency) of variations in component-failure rates as determined by acquired plant-specific data. Similarly, plant models could be compared with actual occurrences to ensure that they reflect the best information on plant performance and interactions among systems and components.

The use of PRA techniques alone would not necessarily constitute an adequate reliability-assurance program. PRA techniques at present have limited application to such potential problems as faulty installation or improper specifications of performance requirements. Thus, PRA techniques could be integrated with appropriate quality-assurance and quality-control approaches for a comprehensive reliability- or safety-assurance program, with the PRA techniques providing key information about the risk impacts of reliability-assurance alternatives.

B.5 Plant Safety Enhancements

Next to an explicit quantification of public risk or core-melt frequency, the identification of specific safety concerns and the evaluation of possible solutions to implement risk management are probably the best-recognized and most widely used applications of PRA. The performance of a PRA naturally leads to significant improvements in the understanding of the design and operation of the various systems, the response of the containment, and the role of plant operators under accident conditions. This understanding, in turn, often reveals design or procedural modifications and training programs that can enhance safety. There are numerous examples of changes that have been made or are under active consideration because of PRA studies performed to date. Some are briefly summarized below.

- The Big Rock Point study showed that several of the changes proposed under the post-TMI action plan and SEP did little to reduce the risk or were not cost-effective, but the same analysis also revealed several other areas where enhancements could be made. The study recommended that seven changes (six design and one procedural) be made.

- During the Shoreham study, two design changes were recommended, and others were slated for further evaluation. One of the implemented changes was to modify the design of viewing windows on containment hatches so that their ultimate strength matched that of other structures in the containment. Even though these windows were previously rated for design-basis accident pressures, they would have failed at lower pressures than other parts of the containment for dominant risk sequences. Another implemented change was in the trip setpoint of the RCIC system that permits the system to operate during a LOCA.

- The Zion study analyzed the relative risk-reduction benefits of both large- and small-scale proposed design modifications. These modifications included a refractory core ladle, a filtered-vented containment, and the addition of hydrogen recombiners, all of which had been selected for consideration prior to the performance of the PRA. In the course of the PRA, it was readily identified that a fourth option, a diesel-driven containment spray pump modified to be independent of ac power, not only would cost considerably less, but would effect a greater reduction in an already very low risk level than the three costly alternatives that had been proposed prior to the PRA. More importantly, the results supported the decision option to leave the plant the way it was.

- Indian Point study insights led to a number of plant modifications including an upgrade of the charging pump alternate-shutdown power supply to reduce the probability of reactor-coolant pump-seal failure, and replacement of manual valves with motor-operated ones in fan-cooler service-water lines.

- In the aftermath of the TMI accident, the NRC mandated that the Midland plant utility install an additional auxiliary feedwater pump at each unit of the two-unit plant. The detailed analysis of dependent failures involving support systems in this PRA determined that the number and type of pumps in the original (two-pump) design, which included one motor-driven and one turbine-driven pump, was not the key to this system's contribution to risk reduction. The key was the fact that both pumps were dependent on an electrically powered chilled-water system. A third pump was installed in the turbine building to be independent of the chilled-water system.

- The PRA for Indian Point identified seismic events as an important contributor to core-melt frequency and latent health effects. The failure mode of greatest importance involved the loss of plant control as a result of disabling the control room. The sequence of events included a strong motion earthquake and the subsequent interaction of the control-room building roof line with an adjoining structure. The result was a possible collapse of the control-room roof and the inaccessibility of plant controls. An analysis of this scenario identified an effective modification. It involved increasing the gap between the two buildings and installing rubber bumpers. This relatively inexpensive modification increased the seismic capacity substantially. As a result, the core-melt frequency due to seismic events was reduced by about a factor of 10. A similar reduction was achieved for the latent health effects.

- Several changes were recommended as a result of the RSSMAP and Integrated Reliability Evaluation Program (IREP) studies. These are summarized in Table B-10.

Table B-10

Examples of Plant Modifications Made or Committed to Based on PRA Insights

Plant	Plant Modification	Program
Sequoyah	Procedures changed to insure upper compartment drain plugs removed after refueling	RSSMAP
Oconee	Procedure and hardware changes made to reduce frequency of interfacing system LOCA	RSSMAP
ANO-1	Station battery test scheduling changed to reduce common-mode failure probability	IREP
ANO-1	Test procedure for ac and dc switch-gear room cooler actuation circuitry established	IREP
Millstone	Logic changes made to emergency ac power-load sequencer to eliminate single failure	IREP

Generic insights regarding plant system design and maintenance procedures generally evolve when a plant-specific conclusion is replicated over a number of plants. For example, the importance of the interfacing-system LOCA was originally identified in the RSS and was replicated for the plants analyzed in RSSMAP. This implied the need for increased attention to maintenance procedures for the interfacing system check valves. In general, the results obtained in the Severe Accident Risk Reduction Program (SARRP) and the IDCOR program indicate that a modest overall reduction in core-melt frequency may be possible from specific hardware or maintenance improvements to existing systems. Such improvements include modifications to the auxiliary feedwater systems, improvements in emergency ac power systems, modifications to the reactor-protection system, improved maintenance for ice-condenser floor drains, etc.

Insights about operating procedures for severe accidents generally come from PRA findings regarding the progression of dominant accident sequences and the role of the operator during these sequences. For example, the following types of operator interactions have been found to be important in many PRAs:

- Failure to realign the emergency core-cooling system manually from the injection mode to the recirculation mode when the water inventory in the refueling water storage tank falls below a set level (PWRs).

- Failure to initiate the feed-and-bleed mode in PWRs or to actuate the automatic depressurization system in BWRs when the reactor-coolant system is at high pressure during accidents initiated by transients.

- Failure to initiate the liquid-poison injection system or to insert control rods manually during accidents involving a failure of the reactor-protection system in BWRs.

Recognition of the importance of specific operator actions can be a vital first step toward defining both appropriate procedures for the management of severe accidents and appropriate approaches to operator training. To date, PRA insights into man-machine interfaces have not been used as effectively as they could be.

Insights about consequence-mitigation systems draw from PRA findings about the types of loading that pose the most serious threats to containment integrity. Currently, the uncertainties regarding containment loading and response are large; various task forces and projects at the NRC and within the industry are addressing the problem.

An example of how PRA results can be used to obtain useful information even in the face of large uncertainties is presented below.

The risk of a reactor plant has an overall uncertainty which is the integrated effect of uncertainties emanating from a number of sources. The various contributors to risk uncertainty can perhaps best be visualized when the risk of a given sequence for a specific containment failure mode is expanded as the product of the frequency of a given accident sequence, times the probability of a containment failure mode given the sequence, times the magnitude of the consequence given that failure mode. To obtain the total risk, this process is continued to consider all containment failure modes and all accident sequences.

Uncertainties in any of these factors will have an effect on the overall uncertainty in the resultant risk.

When considering plant modifications that have the potential for reducing risk, and for which the risk-reduction benefit must be weighed against the cost of implementation, it is convenient to generalize the risk equation above to a "financial risk" equation. Financial risk may be defined as the risk times the cost, summed over all sequences and all possible consequences. Four measures of financial risk that have been used in cost-benefit analyses of plant modifications are

(1) Offsite Financial Risk -- The mean financial risk resulting from the offsite consequences of severe accidents (e.g., offsite property damage and the cost of early and latent fatalities).

(2) Onsite Financial Risk -- The mean financial risk resulting from onsite consequences (e.g., replacement power and cleanup costs).

(3) Total Financing Risk -- The sum of offsite and onsite financial risks.

(4) Financial Risk ALARA Guideline -- The financial risk from population dose, evaluated at $1,000 per person-rem.

To demonstrate how uncertainties in financial risk may be evaluated and how plant modifications can be identified to reduce these uncertainties, consider as an example a PWR with an ice-condenser containment. In the original PRA for this plant (NUREG/CR-1659), the following types of accident sequences were determined to contribute significantly to offsite risk:

- Transient or LOCA followed by failure to cool the core (e.g., S_2D, S_2H, and TMLU) with containment failure resulting from a hydrogen burn.
- LOCA followed by common-mode failure of emergency core cooling and containment sprays in the recirculation mode (e.g., S_2HF) with containment failure resulting from a hydrogen burn, a steam spike, or a gradual overpressurization. The interruption of recirculation is caused by human failure to reopen the upper compartment floor drains after a refueling outage.
- Low-pressure injection-system check-valve failure (sequence V) leading to a LOCA outside containment.

The discussion above can be interpreted to demonstrate a value for controlling hydrogen in the ice-condenser containment and for improving maintenance procedures for the floor drains and the LPIS check valves. Since the PRA, some measures have been taken to address these issues, i.e., a deliberate ignition system has been installed, and closer attention is being paid during maintenance operations to the drains and check valves. Analyses are currently being performed to determine whether these measures are effective for the sequences enumerated above.

Figure B-7 shows some preliminary estimates of offsite and total financial risk for the ice-condenser plant, first without the design and procedural modifications just mentioned, and then with these modifications. For this example, we have assumed that the modifications reduce the threats from hydrogen burning, drain blockage, and check-valve failure by 99% for the sequences in question, while recognizing that achievement of this high reliability may require modifications beyond those currently in place.

Four uncertainty bands are illustrated for each case. The first (A) examines the effects of fission-product source-term uncertainties on the financial risk, holding other variables at their mean or nominal values. The others add to each previous band the uncertainties associated with (B) containment-failure-mode probabilities, (C) sequence frequencies, and (D) financial costs. Sources for the information used to generate the figure are summarized in Table B-11.

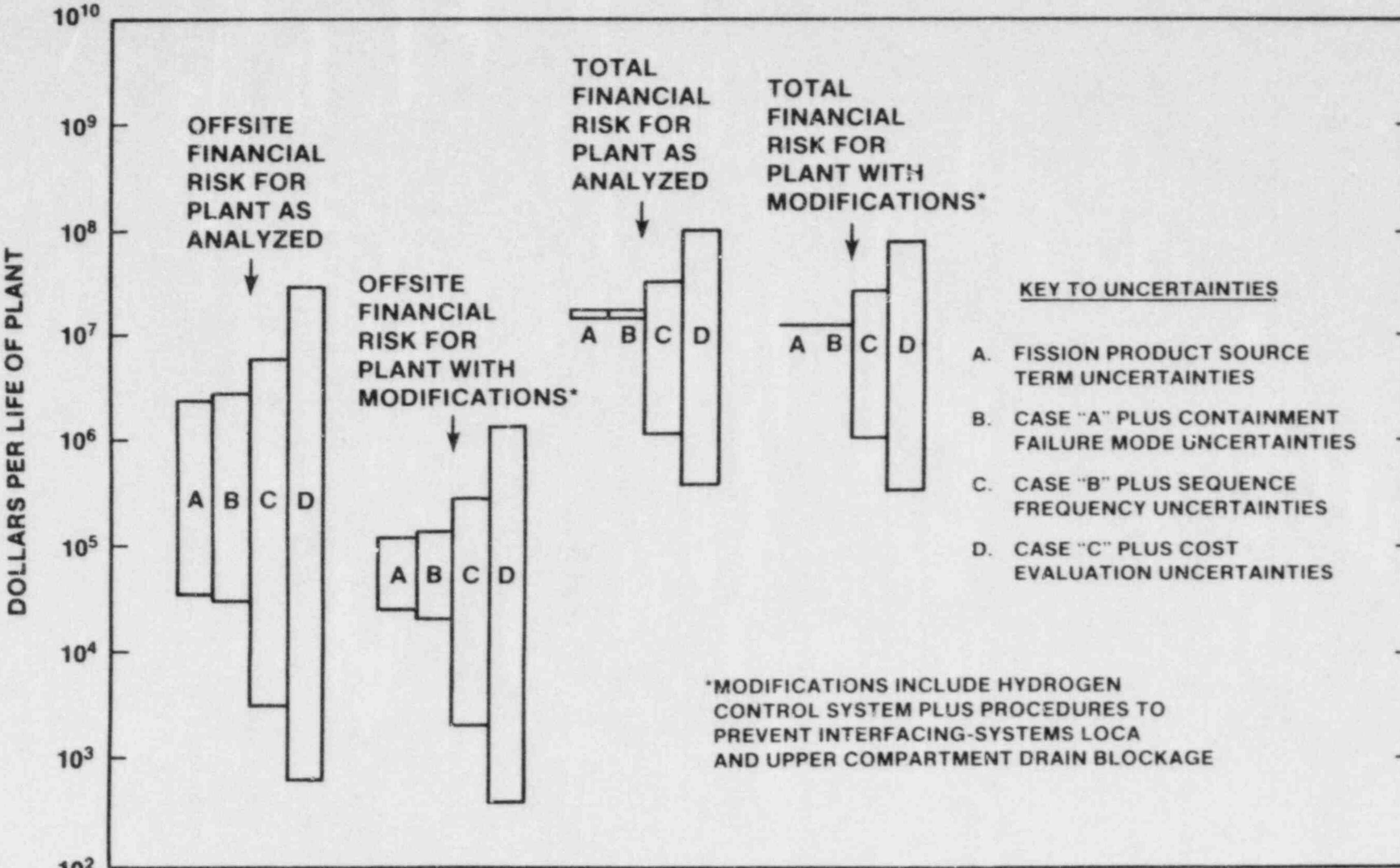


Figure B-7. Preliminary Estimates of Effect of Postulated Safety Improvements on Off-site and Total Financial Risks for a PWR Ice-Condenser Plant

Table B-11

Sources for Demonstration of Uncertainty Reduction

Risk Parameter	Sources of Information
Frequency	Medians from NUREG/CR-1659, partially rebaselined by ASEP (to be published). Bounds based on NUREG-75/014.
Probability of containment failure	Upper bounds from NUREG/CR-16[illegible]. Lower bounds based on reduced hydrogen generation from M. Rogovin, otherwise same as NUREG/CR-1659
Fission-product release	Upper bounds from NUREG-0773. Lower bounds based on 99% reduction of nonvolatile releases.
Consequences	Means and bounds from NUREG/CR-2239.
Cost	Means and bounds from NUREG/CR-2723 and NUREG/CR-3673.

It is apparent from Figure B-7 that the <u>total</u> financial risk for this plant is considerably larger than the <u>offsite</u> financial risk, indicating the importance of onsite costs such as power replacement and cleanup. The overall <u>uncertainty</u> in the total financial risk, however, is considerably smaller than that for offsite financial risk, because the onsite costs are basically independent of containment-failure mode and fission-product source term. Reduction of the uncertainty in total financial risk requires safety features that reduce the uncertainty in core-melt frequency. Reduction of the uncertainty in offsite financial risk can be accomplished by safety features that reduce the uncertainty in either the core-melt frequency or the fission-product releases given a core melt.

The postulated hydrogen-control and procedural modifications reduce the uncertainty in the offsite financial risk by about an order of magnitude while having little effect on the total financial risk. This result occurs because the modifications are designed to reduce the likelihood of accidents involving high fission-product releases to the environment, without necessarily affecting the accidents that are higher in probability but significantly lower in radioactive releases.

It should be pointed out that the assumptions used in this example were selected for purposes of demonstration only, and the uncertainty bands displayed in Figure B-7 are not associated with any particular confidence levels. Further, they do not incorporate all the information now becoming available from ongoing working groups and programs. They are based on bounding estimates and models that have previously been published in the open literature.

B.6 Insights from Precursor Studies

An ongoing study is examining operating experience data and assessing plant safety as it is reflected by the operating experience. A report based on analyses of operating data reported from 1969 to 1979 was published in 1982 and subjected to intensive peer review. Analyses of later operational events are continuing.

The work performed to date, viewed in light of the comments submitted during the peer review, supports the following insights:

- Accident precursors can generally be assigned to one or another of the generic-accident sequence classes previously identified in PRAs. However, the precursors may include unique or unusual failures or interactions. This suggests that the limit of resolution of the PRA methodology may be at the system or component-failure level, with a more limited capability to evaluate specific component-failure modes.

- Many of the initiating-event frequencies and function unavailabilities developed from operating experience agree reasonably well with PRA results.

- No evidence exists that the rate of occurrence of significant precursors varies with plant age.

- The number of potential precursors does not vary significantly among reactor vendors or architect-engineers.

- Human errors are involved in a significant percentage of major precursors. Operator errors of commission are not modeled well in PRAs.

- Losses of offsite power and losses of feedwater contribute significantly to core-melt frequency, as predicted by PRAs. However, LOCAs do not seem to be as important as predicted by PRAs.

REFERENCES

Commonwealth Edison Co., "Zion Probabilistic Safety Study," 1981.

Consolidated Edison Co. and New York State Power Authority, "Indian Point Probabilistic Safety Study," 1982.

DRS, Deutsche Risikostudie Kernkraftwerke, "Eine Untersuchung zu dem durch Störfalle in Kerndraftwerken verursachten Risiko," Der Bundesminister für Forschung and Technologie, Verlag TUV-Rheinland, 1979.

Fleming, K. N., F. A. Silaby, and G. W. Hannaman, Treatment of Operations in HGTR Risk Assessment Study, General Atomics Co., GA-A-15499, 1979.

Garrick, B. J., "Current Experience in Risk Assessment," paper presented at 1983 meeting of American Institute of Metallurgical Engineers (AIME), October 1983.

Joksimovich, V., M. Frank, G. W. Hannaman, and D. D. Orvis, "A Review of Some Early Large Scale Probabilistic Risk Assessments," EPRI NP-3265, Project 2171-1, Electric Power Research Institute, Palo Alto, CA.

Joschek, H. I., "Risk Assessment in the Chemical Industry," in Proceedings, Internations ANS/ENS Topical Meeting in Probabilistic Risk Assessment, Port Chester, NY, September 1982.

NUREG-75/014, "Reactor Safety Study," WASH-1400, October 1975.

NUREG-0773, "The Development of Severe Reactor Accident Source Terms: 1957-1981," November 1982.

NUREG/CR-0400, "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," September 1978.

NUREG/CR-1659, "Reactor Safety Study Methodology Applications Program: Sequoyah #1 PWR Power Plant," Vol. 1, Sandia National Laboratories, February 1981.

NUREG/CR-2239, "Technical Guidance for Siting Criteria Development," Sandia National Laboratories, 1982.

NUREG/CR-2723, "Estimates of the Financial Consequences of Nuclear Power Reactor Accidents," Sandia National Laboratories, September 1982.

NUREG/CR-2744, "Human Reliability Data Bank for Nuclear Power Plant Operations," Vol. 1, Sandia National Laboratories, March 1983.

NUREG/CR-3385, "Measures of Risk Importance and Their Applications," Battelle Columbus Laboratories, July 1983.

NUREG/CR-3673, "The Economic Risks of Nuclear Power Reactor Accidents," Sandia National Laboratories, April 1984.

Rogovin, M. and G. Frampton, Jr., Three Mile Island, A Report to the Commissioners and to the Public, US Nuclear Regulatory Commission Special Inquiry Group, January 1980.

APPENDIX C

PROBABILISTIC STUDIES OF LIMITED SCOPE

APPENDIX C

CONTENTS

APPENDIX C

CONTENTS (continued)

APPENDIX C

PROBABILISTIC STUDIES OF LIMITED SCOPE

Many special-issue studies have used probabilistic risk assessment (PRA) techniques to provide reliability or risk-based information for decisionmaking on a wide variety of topics. As discussed in Chapter 3, these limited studies, most of which have drawn on the information base of the larger PRA studies, are becoming an increasingly important tool in the regulatory process. Many of the studies were done within the Nuclear Regulatory Commission (NRC) and have not been formally documented. A brief description of 21 limited-study subjects is presented below to illustrate the breadth of issues to which PRA methods can be applied. The list is not meant to be all-inclusive.

C.1 <u>Risk-Based Categorization of NRC Technical and Generic Issues</u>

Perhaps the first well-known use of PRA insights in the regulatory process occurred in 1978 when the Probabilistic Analysis Staff performed a study (SECY/78-7616) to categorize the existing technical and generic issues facing the NRC. The primary objective was to assist in identifying the task-action plan issues that have the greatest safety significance on a relative risk basis. One hundred thirty-three task-action items were reviewed and assigned to four broad categories ranging from those having high-risk significance to those not directly relevant to risk. Of the 133 items, 16 fell in the high-risk categories. The ranking aided the selection of the generic issues designated "unresolved safety issues" (USI). This effort was recently redone by the NRC's Office of Nuclear Reactor Regulation (NRR) to include all Three Mile Island (TMI) action-plan issues and all issues identified since the TMI accident (NUREG/CR-2800). The most recent effort, similar to the earlier effort, developed and quantified the accident sequences associated with each issue.

C.2 <u>Value-Impact Assessment of Alternative Containment Concepts</u>

Another regulatory use of PRA techniques also occurred in 1978. The NRC was then considering the underground siting of nuclear power plants, an issue that had been raised by environmental organizations. Under the sponsorship of the NRR, a study was undertaken to compare the relative value and cost of alternative containment concepts "between the present regulations and underground siting that could add to plant safety" (NUREG/CR-0165). Using insights from the Reactor Safety Study, NUREG/CR-0165 considered nine alternative designs as the "logical alternatives." Filtered atmospheric venting was the design alternative found to be most promising on a value-impact scale. This study contributed to the subsequent focusing of containment research on filtered vents and the diminution of interest in the underground siting of nuclear power plants.

C.3 NRC Auxiliary Feedwater Studies

After the TMI accident, the NRR sponsored a series of studies to review the design of auxiliary feedwater systems in U.S. PWRs (NUREG-0667, -0635, -0611). These studies used PRA techniques to identify potential failures, including the station blackout sequence, that could dominate the unreliability of auxiliary feedwater systems during transients caused by a loss of main feedwater. (The ability to cope with the station blackout sequence had not been a licensing requirement for the earlier licensed plants.) This study, which demonstrated the value of applying PRA techniques at the system level, led to changes in the safety review process. A quantitative requirement on auxiliary-feedwater availability was added to the standard review plan, and studies of auxiliary-feedwater reliability became a routine requirement for licensing.

C.4 Analysis of dc Power Supply Requirements

This study was undertaken as part of the NRC's generic safety task A-30, "Adequacy of Safety Related dc Power Supplies" (NUREG-0666). The issue stemmed from the dependence of decay-heat-removal systems on dc power supply systems, which nominally meet the single-failure criterion. The failure of dc power supplies affects the ability to cool the reactor core. It was found that dc power-related accident sequences could represent a significant contribution to the total core-damage frequency. It was also found that this contribution could be substantially reduced by the implementation of design and procedural requirements including the prohibition of certain design features and operational practices, augmentation of test and maintenance activities, and staggered test and maintenance activities to reduce human errors.

C.5 Station Blackout

Two studies addressed USI A-44, "Station Blackout." Together they provide the technical base for resolving the A-44 issue. The first study, "The Reliability of Emergency ac Power Systems in Nuclear Power Plants," (NUREG/CR-2989), when combined with the relevant loss-of-offsite-power frequency, provided estimates of station-blackout frequencies for 18 nuclear power plants and 10 generic designs. The study also identified the design and operational features that are most important to the reliability of ac power systems.

The second study, "Station Blackout Accident Analysis," (NUREG/CR-3226) focused on the relative importance to risk of station-blackout events and on the plant design and operational features that would reduce this risk.

The technical base supplied by these PRA-type special-issue studies is currently being used to formulate the NRC strategy for resolving the station-blackout issue.

C.6 Precursors to Potential Severe Core-Damage Accidents

This study (NUREG/CR-2497) is applying PRA techniques to operating experience to identify the high-risk features of plant design and operation. The operating-experience base is derived from the licensee event reports (LERs) of operational events that have occurred in U.S. nuclear power plants. The events of interest are multiple events that, when coupled with postulated events, cause plant conditions that could eventually result in severe core damage.

The precursor study is a long-range study that is still under way. In the first 2-1/2 years, 169 significant precursors were identified for the 432 reactor-years of operating experience represented by the LERs submitted from 1969 to 1979; preliminary findings show 56 precursors for 126 reactor-years of operating experience for 1980-81. The results were used to analyze accident sequences and to estimate core-melt frequencies for operating plants. One objective of the precursor study is to compare these results with the estimates made in existing PRAs.

C.7 Anticipated Transients without Scram (ATWS)

The NRC staff evaluation of ATWS in NUREG-0460 was one of the first applications of PRA techniques to a USI. The evaluation highlighted the relative frequency of severe ATWS events for various reactor types and estimated the expected reduction in frequency for various postulated plant modifications. The study also proposed quantitative goals for resolving this issue.

Other notable examples of PRA application to the ATWS issue are the NRC-sponsored survey and critique of the reactor protection system (RPS) (SAI, 1982), the quantitative evaluation of proposed ATWS-related modifications sponsored by a consortium of U.S. utilities (SAI, 1981), and the ATWS Task Force report summarized in SECY-83-293. The RPS survey reviewed 16 reliability studies, most of them published PRAs, to compare the predicted failure probability per unit demand, the anticipated-transient frequency, and the primary influences on RPS unavailability. There was a surprising degree of agreement among the 16 studies. The second study quantified the relative improvement to be gained by implementing a set of recommendations proposed by the utility consortium in an ATWS petition to the NRC. The third study, a valve-impact evaluation of the risk reduction of generic plant classes, provided the basis for a final rule on ATWS (SECY-83-293).

C.8 Pressurized Thermal Shock

In addressing pressurized thermal shock (USI A-49), probabilistic assessments were used to derive screening criteria to identify operating plants in need of modification. The owners groups that were associated with the different PWR designs submitted estimates of severe overcooling event frequencies (Kinsley, O.; Combustion Engineering; Babcock & Wilcox). The Westinghouse assessment was evaluated by the staff in SECY-82-465. Analytical efforts using PRA techniques continue to evaluate the risk significance of this issue.

C.9 Addition of Pilot-Operated Relief Valves to Combustion Engineering Plants

The purpose of this study was to determine the change in risk between Combustion Engineering plants with pilot-operated relief valves (PORVs) and plants without PORVs (SECY-84-134). The study indicated that for certain plants an appreciable fraction (40 to 50%) of the risk reduction came from the additional pressure relief for ATWS sequences. The remainder came from the addition of feed-and-bleed capability, which reduced the frequency of core-melt sequences involving the loss of decay-heat-removal capability.

C.10 BWR Water Level--Inadequate Core Cooling

PRA techniques were used in the analysis of TMI Action Item II.F.2, BWR Water Level--Inadequate Core Cooling. The results indicated that additional instrumentation to detect inadequate core cooling in the BWRs is unnecessary. The study showed that after implementing improvements in existing systems for water-level measurement as well as in operator performance (Shoreham and Limerick), the predicted core-damage frequency from failure in water-level measurements in the plants analyzed would be small compared to the total core-damage frequency predicted in recent PRAs for BWRs.

C.11 Scram Discharge Volume

An analysis of pipe breaks in the BWR scram system, in response to draft NUREG-0785 published by the Office of Analysis and Evaluation of Operational Data, indicated that the postulated sequence of events is not a dominant contributor to core-melt frequency (NUREG-0803). The analysis was based on the assumptions that the failure frequency of the scram discharge volume (SDV) pipe is about 10^{-4} per plant-year and that the operability of required mitigation equipment is not degraded by the resultant adverse environment.

C.12 TMI Action-Plan Items II.K.3.2 and II.K.3.17

PRA provided tools for the analysis of TMI action-items II.K.3.2, the frequencies of LOCAs caused by stuck-open pressurizer PORVs, and II.K.3.17, outages of ECCS.

The results of II.K.3.2 indicated that the frequency of small LOCAs from stuck-open PORVs, with the PORVs operated as they are at present, was in the range of the small-LOCA frequency in the RSS and that no additional measures to reduce the PORV-LOCA frequency are required. The purpose of the data collection under item II.K.3.17 was to determine whether cumulative outage requirements were needed in the technical specifications and which plants had a significantly greater than average cumulative ECCS outage time.

C.13 Evaluation of Exemptions from Limiting Conditions for Operation, Technical Specification Changes, and Surveillance Requirements

Probabilistic models have been used by the NRC staff to perform sensitivity studies for providing insights into the bases for limiting conditions for operation (LCOs), LCO extensions, and testing and maintenance requirements. Some specific examples include allowed outage times for auxiliary feedwater systems and diesel-generator LCO extensions. A typical report, WCAP-10271, has been proposed as a basis to revise reactor protection system testing requirements (WEC, 1983).

C.14 Waterhammer

USI A-1 considers the potential impact of waterhammer events in operating reactors. A fairly large number of reported waterhammer events in recent years have caused concern regarding the ability of plant systems and safety features to respond adequately. Several existing plant-specific risk assessments were reevaluated to determine the risk importance of this issue. The study showed that the inclusion of waterhammer data caused virtually no change in the quantification of dominant accident sequences (NUREG-0927). These results were used as part of a value-impact analysis in support of the resolution of issue A-1, which will be documented shortly.

C.15 Toughness of Supports for Steam Generators and Reactor-Coolant Pumps

The low-fracture toughness of the supports for steam generators and reactor-coolant pumps is USI A-12. PRA techniques were used to simulate support-structure failures during an earthquake. The results showed that backfits to operating plants were unwarranted and that the regulatory requirements in Standard Review Plan 5.3.4 for new plants are cost effective (NUREG-0577).

C.16 Seismic Design Criteria

USI A-40 addresses new seismic criteria for the Standard Review Plan. PRA techniques were used to estimate the incremental risk from changes in seismic criteria. The results showed that proposed changes would not affect the plant risk significantly. However, there also is no additional cost associated with implementing the proposed changes (NUREG/CR-1161).

C.17 Containment Sump Performance

As part of its effort to resolve USI A-43, the NRC staff performed a limited risk assessment to gain insights into the potential for risk reduction. Issue A-43 concerns the possibility that, after a LOCA in a PWR, the recirculation sump will be blocked by debris from damaged pipe insulation. A parametric study was performed for various frequencies of sump blockage and was then coupled with an engineering evaluation of debris generation in a high-energy pipe break. The study plans to provide realistic estimates of the core-melt contribution from USI A-43. Preliminary results indicate that the risk-reduction potential is very dependent on plant-specific design features such as the type and location of insulation. The resolution of this issue was documented in NUREG-0897.

C.18 Selected Topics in the Systematic Evaluation Program

To support the integrated assessment phase of the Systematic Evaluation Program (SEP), analyses were performed to determine the risk significance of selected SEP topics. Proposed modifications that would upgrade the plant to current licensing criteria were evaluated to determine their effect on core-melt frequency and risk. The results were considered in the plant-specific backfit decisions. Many issues, such as loose-parts monitoring and RCS leak detection, were found to have low-risk importance for virtually all the plants reviewed. Other issues (e.g., dc power availability, fire protection, and recirculation switchover in PWRs) were often found to have high-risk importance. These studies have provided useful insights and allowed resources to be applied to the areas where the greatest reduction in risk could be achieved (NUREG-0820 through -0828).

C.19 Emergency Planning and Response

Several studies have been performed to provide guidance on emergency planning and response (NUREG-0396, -0654). Their results formed the basis for the implementation of emergency planning zones for the plume-exposure pathway and for NRC staff recommendations regarding the use of thyroid-blocking agents.

C.20 Reactor Siting

A study was performed to develop bases for formulating new regulations for siting nuclear power plants (NUREG/CR-2239). Generic and site-specific calculations were performed to evaluate the sensitivity of predicted consequences to variations in source terms, population distribution, weather conditions, and emergency response.

C.21 Economic Risks

Several studies have examined economic consequences and risks (NUREG/CR-3673, -2723, -2925). Their results indicate that economic risks are dominated by relatively high-frequency forced outages and that the economic losses predicted for the owners of the plant generally exceed offsite economic consequences.

REFERENCES

Babcock and Wilcox, "B & W Owners Group Probabilistic Evaluation of Pressurized Thermal Shock, Phase 1 Report," BAW-1791, June 1982.

Combustion Engineering, "An Assessment of the Probability of Overcooling Transients at Nuclear Steam Supply System," CEN-2012, June 1981.

Kinsley, O. (Westinghouse Owners Group) Letter to H. Denton (NRC), on "Summary of Evaluations Related to Reactor Vessel Integrity," May 28, 1983.

NUREG-0396, "Planning Basis For the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants," December 1978.

NUREG-0460, "Analytical Transients Without Scram for Light Water Reactors, Volumes 1-4," 1978-1980.

NUREG-0577, "Potential for Low Fracture Toughness and Lamellar Tearing in PWR Steam Generator and Reactor Coolant Pump Supports," Rev. 1, October 1983.

NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants," January 1980.

NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants," February 1980.

NUREG-0654, "Criteria For Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," Rev. 1, November 1980.

NUREG-0666, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," April 1981.

NUREG-0667, "Transient Response of Babcock & Wilcox-Designed Reactors," May 1980.

NUREG-0803, "Generic Safety Evaluation Report: Integrity of BWR Scram Discharge Piping," August 1981.

NUREG-0820, "Integrated Safety Assessment Program - Systematic Evaluation Program, Palisades Plant," November 1983.

NUREG-0821, "Integrated Safety Assessment Program - Systematic Evaluation Program, R. E. Ginna Nuclear Power Plant," August 1983.

NUREG-0822, "Integrated Safety Assessment Program - Systematic Evaluation Program, Oyster Creek Nuclear Generating Station," January 1983.

NUREG-0823, "Integrated Safety Assessment Program - Systematic Evaluation Program, Dresden Nuclear Power Station, Unit 2," February 1983.

NUREG-0824, "Integrated Safety Assessment Program - Systematic Evaluation Program, Millstone Nuclear Power Station, Unit 1," February 1983.

NUREG-0825, "Integrated Safety Assessment Program - Systematic Evaluation Program, Yankee Nuclear Power Station," June 1983.

NUREG-0826, "Integrated Safety Assessment Program - Systematic Evaluation Program, Haddam Neck Plant," June 1983.

NUREG-0827, "Integrated Safety Assessment Program - Systematic Evaluation Program, Lacrosse Boiling Water Reactor," June 1983.

NUREG-0828, "Integrated Safety Assessment Program - Systematic Evaluation Program, Big Rock Point Plant," September 1983.

NUREG-0897, "Containment Energy Sump Performance, Technical Findings Related to USI A-43," for comment, April 1983.

NUREG-0927, "Evaluation of Waterhammer Occurrence in Nuclear Power Plants," Rev. 1, March 1984.

NUREG/CR-0165, "A Value-Impact Assessment of Alternative Containment Concepts," Sandia National Laboratories, 1978.

NUREG/CR-1161, "Recommended Revisions to Nuclear Regulatory Commission Seismic Design Criteria," Lawrence Livermore Laboratory, May 1980.

NUREG/CR-2239, "Technical Guidance for Siting Criteria Development," Sandia National Laboratories, December 1982.

NUREG/CR-2497, Vol. I, "Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report," Science Applications, Inc., June 1982.

NUREG/CR-2723, "Estimates of the Financial Consequences of Nuclear Power Reactor Accidents," Sandia National Laboratories, November 1982.

NUREG/CR-2800, "Guidelines for Nuclear Power Plant Safety Issue Prioritization Information Development," Battelle Memorial Institute, February 1983.

NUREG/CR-2925, "In-Plant Considerations for Optimal Offsite Response to Reactor Accidents," Sandia National Laboratories, March 1983.

NUREG/CR-2989, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," Oak Ridge National Laboratory, July 1983.

NUREG/CR-3226, "Station Blackout Accident Analyses (Part of NRC Task Action Plan A-44)," Sandia National Laboratories, May 1983.

NUREG/CR-3673, "Economic Risks of Nuclear Power Plant Accidents," Sandia National Laboratories, April 1984.

Science Applications, Inc., "Survey and Critique of RPS Reliability Studies," (Draft) 1-220-03-637-00, October 1982.

Science Applications, Inc., "Technical Support For the Utility Group on ATWS," SAI-011-82-SJ, December 1981.

SECY/78-616, U.S. Nuclear Regulatory Commission, 1978.

SECY-82-465, Pressurized Thermal Shock (PTS), November 23, 1982.

SECY-84-134, Power Operated Relief Valves For Combustion Engineering Plants, March 23, 1984.

Westinghouse Electric Corporation, "Evaluation of Surveillance Frequencies and Out of Service Times For the Reactor Protection Instrumentation System," January 1983.

NRC FORM 335
(11-81)

U.S. NUCLEAR REGULATORY COMMISSION
BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG-1050

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
Probabilistic Risk Assessment (PRA) Reference Document, Final Report

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)

5. DATE REPORT COMPLETED

MONTH	YEAR
August	1984

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

DATE REPORT ISSUED

MONTH	YEAR
September	1984

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.

13. TYPE OF REPORT
Final

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

The Commission's Safety Goal Policy Statement in NUREG-0880, Rev. 1, directs the staff "...to collect available information on PRA studies and prepare a reference document that describes the current status of knowledge concerning the risk of plants licensed in the U.S." The document discusses the purpose and content of a PRA and identifies the PRAs and other probabilistic studies performed to date. It then discusses the level of development and uncertainties associated with the various elements of PRA methodology as well as those generic insights derived from studies performed. Finally, potential uses of PRA in regulation are evaluated.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Probabilistic risk assessment
PRA
Risk assessment

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

20. SECURITY CLASS *(This page)*
Unclassified

21. NO. OF PAGES

22. PRICE
$

NRC FORM 335 (11-81)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FOURTH-CLASS MAIL
POSTAGE & FEES PAID
USNRC
WASH. D. C.
PERMIT No. G 67

120555078877 1 1AN
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555