NUREG/CR-2300
Vol. 1

PRA PROCEDURES GUIDE

A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants

Final Report
Vol. 1 - Chapters 1-8
Vol. 2 - Chapters 9-13 and Appendices A-G

Jan. '83

Prepared under the auspices of
The American Nuclear Society and
The Institute of Electrical and Electronics Engineers

Under a Grant from
The U.S. Nuclear Regulatory Commission

GPO Printed copy price: $11.00

NUREG/CR-2300
Vol. 1

PRA PROCEDURES GUIDE

A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants

Final Report
Vol. 1 - Chapters 1-8
Vol. 2 - Chapters 9-13 and Appendices A-G

Manuscript Completed: December 1982
Date Published: January 1983

Prepared under the auspices of:
The American Nuclear Society
LaGrange Park, IL 60525
NRC Grant No. G-04-81-001

The Institute of Electrical and Electronics Engineers
New York, NY 10017
NRC Grant No. G-04-81-05

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Foreword

The development of safety design requirements for nuclear power plants in the last 20 to 25 years took place in a subjective, deterministic framework. Little use was made of the techniques of quantitative probabilistic risk assessment (PRA), largely because these techniques were not fully developed for analyzing nuclear power plants. It was F. R. Farmer who introduced the idea of reactor safety based on the reliability of consequence-limiting equipment in the early 1960s. The first major application of PRA techniques was the Reactor Safety Study (WASH-1400), which demonstrated that a nuclear power plant could be analyzed in a systematic fashion by PRA techniques. Since the completion of the Study in 1975, the Nuclear Regulatory Commission (NRC) has been exploring ways of systematically applying probabilistic analysis to nuclear power plants, and the use of PRA techniques has been rapidly becoming more widespread in the nuclear community.

Contributing to these developments has been a growing appreciation of the wisdom of the strong recommendations made by the Lewis Committee to use PRA techniques for reexamining the fabric of NRC's regulatory processes to make them more rational.* After the accident at Three Mile Island, these recommendations were reinforced by the Kemeny† and Rogovin reports,‡ which also encouraged the use of these techniques. As Lewis stated in his March 1981 Scientific American article,§ "the Three Mile Island incident illustrates graphically how important it is to quantify both the probability and the consequences of an accident, and to generate some public awareness of these issues.... This is an issue that goes to the heart of many regulatory and safety decisions, where one must have some measure of the risks one is willing to accept on as quantitative a basis as the expert community can provide."

The NRC has recently raised questions about potential accident risks for nuclear plants near high population concentrations. To answer these questions, the industry has performed PRAs for the Indian Point, Limerick, and Zion plants. Moreover, the utilities themselves are showing considerable interest in taking advantage of the safety and availability insights afforded by risk assessments. As a result of these forces, an increasing number of PRAs are either under way or being planned. Finally, the NRC is contemplating a future program (National Reliability Evaluation Program, NREP) in which many licensed nuclear power plants will be required to perform a probabilistic risk assessment.

---

*H. W. Lewis et al., Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, USNRC Report NUREG/CR-0400, 1978.

†J. G. Kemeny et al., Report of the President's Commission on the Accident at Three Mile Island, Pergamon Press, 1979.

‡M. Rogovin, Three Mile Island: A Report to the Commissioners and to the Public, USNRC Report NUREG/CR-1250 (Vol. 1), 1979.

§H. W. Lewis, "The Safety of Fission Reactors," Scientific American, March 1981.

Because of this increasing application of PRA techniques within the industry and the regulatory process, there is a need for technical guidance on methods and procedures. It was this need that led to the creation of the PRA Procedures Guide project and ultimately to this document.

The objective of this project was to compile a procedures guide describing the principal methods now used in PRAs. To accomplish these objectives, a Steering Committee and a Technical Writing Group were formed. Funding has been provided by the NRC, the Department of Energy (DOE), and the Electric Power Research Institute (EPRI), and expertise was contributed by the nuclear industry.

The group responsible for the document is the Steering Committee. The Committee includes representatives from the American Nuclear Society, the Institute of Electrical and Electronics Engineers, the NRC, the DOE, the Atomic Industrial Forum, EPRI, and utilities (see Chapter 1 and Appendix B for the membership list). The Technical Writing Group, whose members were selected by the Steering Committee (see Appendix B), consists of technical specialists experienced in the application of probabilistic and reliability techniques to the analysis of nuclear power plants.

To obtain the wide peer review desired for the Procedures Guide, the Steering Committee decided on two mechanisms: criticism by a carefully selected peer review group and open review in two conferences. The objective in establishing the peer review group was to bring additional technical expertise and, in some instances, alternative viewpoints to the project. An effort was also made to include experts who are not members of the nuclear community. Candidates for the peer group were proposed by the Steering Committee and members of the Technical Writing Group; those who were finally selected are listed in Appendix B.

The first of the two conferences, held on October 26-28, 1981, included a series of workshops in risk assessment. It was sponsored by the Institute of Electrical and Electronics Engineers. The second was held on April 4-7, 1982, by the American Nuclear Society. These meetings have allowed the Steering Committee to obtain comments from a large number of experts in disciplines related to probabilistic risk assessment as well as potential users of the Procedures Guide. The disposition of these comments, like those of the peer review group, has been resolved by the Technical Writing Group under the guidance of the Steering Committee.

Actual writing of the Procedures Guide by the Technical Writing Group began only in April 1981, and by July a working draft was produced for review by the Steering Committee. It was followed by a review draft that was distributed for peer review and discussion at the October 1981 conference. The October 1981 conference was heavily attended, and many comments were submitted to the Steering Committee. A major revision of the Procedures Guide resulted in a second draft, published in April 1982 for the attendees of the ANS Executive Conference, which reflected many, but not all, of the comments.

After the ANS Executive Conference, a final revision was made, and this document resulted. Thus, the methods described herein have received broad review from both PRA practitioners and potential users of PRA techniques.

Upon completion of the PRA Procedures Guide project, the Steering Committee, which has guided the project, was disbanded. Future questions or comments on the Guide should be directed to Robert M. Bernero, Division of Risk Analysis, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555.

Contents

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

VOLUME 2

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

List of Figures

LIST OF FIGURES (Continued)

LIST OF FIGURES (Continued)

LIST OF FIGURES (Continued)

LIST OF FIGURES (Continued)

List of Tables

LIST OF TABLES (Continued)

VOLUME 2

LIST OF TABLES (Continued)

Chapter 1
Introduction

This document, the PRA Procedures Guide, is intended to provide an overview of the risk-assessment field as it exists today and to identify acceptable techniques for the systematic assessment of the risk from nuclear power plants. This chapter describes the objectives and the scope of the PRA Procedures Guide and its uses. Also discussed briefly are the guidelines followed in selecting the methods described in the Guide, the objectives and uses of probabilistic risk assessments, and the treatment of dependent failures. The chapter ends with a summary of the contents of this document and of the individual chapters.

1.1 CHARTER AND ORGANIZATION

The PRA Procedures Guide project was started at the behest of the U.S. Nuclear Regulatory Commission (NRC) to gain the advice and participation of many competent parties before settling upon any specific procedures guide for its use. The complete charter for the project is provided in Appendix A.

The charter called for procedures that would address the following subjects: (1) system reliability analysis, (2) accident-sequence classification, (3) the assessment of frequencies for classes of accident sequences, (4) the estimation of radionuclide release fractions for core-melt accident sequences, and (5) consequence analysis. For each of these subject areas, the procedures guide was to delineate (1) acceptable analytical techniques; (2) acceptable assumptions and modeling approximations, including the treatment of statistical data, common-cause failures, and human errors; (3) the treatment of uncertainties; (4) acceptable standards for documentation; and (5) the assurance of technical quality.

The organization of this project was intended to enable the NRC and the nuclear industry to work closely with two technical societies, the Institute of Electrical and Electronics Engineers (IEEE) and the American Nuclear Society (ANS), in cosponsoring their activities in a coordinated scheme of action. The project was directed by a Steering Committee under the joint chairmanship of two representatives of the technical societies; namely, Saul Levine for the ANS and Richard Gowen for the IEEE. The Steering Committee had representatives from the NRC, IEEE, ANS, the Department of Energy, the Atomic Industrial Forum, and other organizations within the nuclear industry. A list of the Steering Committee members follows.

STEERING COMMITTEE

Saul Levine, Co-Chairman
NUS Corporation
910 Clopper Road
Gaithersburg, Maryland 20878

Robert M. Bernero
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Guy A. Arlotto
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Malcolm L. Ernst
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Andrew C. Millunzi
U.S. Department of Energy
NE-540
Washington, D.C. 20545

Edward P. O'Donnell
Ebasco Services, Inc.
2 World Trade Center, 89th Floor
New York, New York 10048

Robert J. Breen*
Nuclear Safety Analysis Center
Electric Power Research Institute
P.O. Box 10412
Palo Alto, California 94303

Ian B. Wall
Electric Power Research Institute
P.O. Box 10412
Palo Alto, California 94303

Wayne L. Stiede
Commonwealth Edison Company
72 West Adams Street
P.O. Box 767
Chicago, Illinois 60690

Richard J. Gowen, Co-Chairman
Institute of Electrical and
Electronics Engineers, Inc.
South Dakota School of Mining
and Technology
Rapid City, South Dakota 57701

Kenneth S. Canady
Duke Power Company
P.O. Box 33189
Charlotte, North Carolina 28242

James F. Mallay
Babcock & Wilcox Company
P.O. Box 1260
Lynchburg, Virginia 24505

Alfred Torri
Pickard, Lowe & Garrick, Inc.
17840 Skypark Boulevard
Irvine, California 92714

John T. Boettger
Public Service Electric & Gas Company
80 Park Plaza
Newark, New Jersey 07101

Sava I. Sherr
Institute of Electrical and
Electronics Engineers, Inc.
345 East 47th Street
New York, New York 10017

Robert E. Larson
Systems Control, Inc.
1801 Page Mill Road
Palo Alto, California 94303

---

*Replaced Edwin Zebroski as representative of the Nuclear Safety Analysis Center.

The Steering Committee appointed a Technical Writing Group to develop the Procedures Guide. The members of the Technical Writing Group were selected on the basis of their expertise in PRA methods. They came from the nuclear industry, the national laboratories, and the NRC. A listing of the members of the Technical Writing Group can be found in Appendix B.

1.2 OBJECTIVES AND SCOPE OF THE PRA PROCEDURES GUIDE

The main objective of the PRA Procedures Guide is to provide general assistance in the performance of probabilistic risk assessments for nuclear power plants. The Guide has been prepared in accordance with the following guidelines set by the Steering Committee:

1. Although the procedures in whole or in part may have wider application, the thrust of the Guide will be toward performing probabilistic risk assessments of light-water-reactor (LWR) nuclear power plants.

2. The procedures will be suitable for use by the nuclear industry. This implies, among other things, that the techniques described will not require the use of expertise, computer codes, or methods not readily available to the nuclear industry or its contractors.

3. The procedures will be suitable for use in the regulatory process. The Guide will contain sufficient detail for the information base, analytical methods, assumptions, uncertainties, and results to be readily understandable.

4. The Guide will be in sufficient detail to be suitable for use by small teams of persons with a firm grasp of engineering principles, probabilistic methods, and the design and operation of LWR nuclear power plants.

5. The Guide will, where appropriate, provide major alternative procedures or methods and, in doing so, describe the different applications, advantages, and disadvantages of the alternatives.

Since the ultimate user of the Procedures Guide was envisioned to be a risk-assessment team with the necessary expertise, it was decided that the Guide should not attempt to teach risk assessment, engineering, or LWR principles. Rather, the Guide is intended to outline the procedures for applying these principles to assessing the risk of an LWR nuclear power plant. To accommodate the readers who are not deeply involved in risk assessment, the document has been written in a style that makes it understandable to members of the technical community in general.

In general, it was desired to provide sufficient detail to define unambiguously the methods that can be used while avoiding prescriptive detail at a level that would inhibit the flexibility of the user in applying available

resources, recognizing that the resources available to various studies will vary widely. Furthermore, since the PRA field is developing rapidly, an approach that is too prescriptive might inhibit useful developments.

Risk assessments, both past and present, vary widely in scope, depending on the available time and resources as well as the purpose of the study. It was therefore decided that the Guide should cover a range of levels in scope, and three discrete levels, described more fully in Chapter 2, were selected:

1. System analysis. An assessment of this type would consist of the definition and quantification of accident sequences, component data, and human reliability.

2. System and containment analysis. An assessment of this scope would include all of the subjects covered in level 1 as well as the physical processes of core-melt accidents and radionuclide release and transport.

3. System, containment, and consequence analysis. A study of this scope would include all of the subjects covered in levels 1 and 2 as well as environmental transport and consequence analyses.

An analysis of external events may be included in any of the three levels described above.

1.3 USES AND LIMITATIONS OF THE GUIDE

The users of the Procedures Guide are expected to fall into three categories:

1. Persons requesting a probabilistic risk assessment or contracting to perform one.

2. Persons performing a probabilistic risk assessment.

3. Persons interested in improving their understanding of probabilistic risk assessments.

It is expected that the Guide will be used mainly as a reference document by government agencies or private organizations when requesting, or contracting for, the performance of a probabilistic risk assessment. It was partly for this reason that the Guide has been structured to serve different levels of scope and to provide descriptions of different methods. In using the Guide as a reference document for specifying scope levels and methods, the user will have to establish the desired level of scope and, in some cases, select a particular method. To help in making these choices, the Guide describes the attributes of the various levels of scope as well as the disadvantages and advantages of various methods under particular circumstances.

Persons who use the Guide in performing a probabilistic risk assessment will have to make similar choices, unless the choices are specified by a client or a requesting agency.

Persons using the Guide to improve their understanding of the procedures used in probabilistic risk assessments will find the document useful in many respects. It should be noted, however, that the Guide is not a training manual or a textbook. It does not, in general, provide the theoretical background or the fundamentals needed to understand the methods.

Finally, and most important, the user must recognize that the probabilistic risk assessment of nuclear power plants is a relatively new field that is rapidly changing. Any guide for such studies can, at best, represent the state of the art for only a brief period of time and should be updated as necessary.

1.4 METHODS SELECTED

Perhaps the most difficult and important task in preparing this document was the selection of the methods to be described. It was recognized that in some cases the method is selected to suit available resources or the objectives of the study, but in some instances the choice between two or more equally appropriate methods may be completely arbitrary. The Guide therefore identifies the methods that are most appropriate under particular circumstances when it is possible to do so. When more than one method is described, the Guide discusses the attributes of each and, where possible, gives the conditions under which they are most suitable.

The methods selected for description in the Guide are methods that have been fully developed and used, although not necessarily in the nuclear industry. By its charter, the Guide is not intended either to propose or to develop new methods. Its function is to describe procedures for using state-of-the-art methods in performing a risk assessment.

1.5 THE OBJECTIVES AND USES OF PROBABILISTIC RISK ASSESSMENTS

The probabilistic risk assessment is an analytical technique for integrating diverse aspects of design and operation in order to assess the risk of a particular nuclear power plant and to develop an information base for analyzing plant-specific and generic issues. In achieving these objectives, probabilistic risk assessments serve many purposes.

An assessment of the plant-specific risk provides both a measure of potential accident risks to the public and insights into the adequacy of plant design and operation.

The assessment of the adequacy of plant design and operation is achieved by identifying those sequences of potential events that dominate risk and establishing which features of the plant contribute most to the frequency of such sequences. These plant features may be potential hardware failures, common-mode failures, human errors during testing and maintenance, or procedural inadequacies leading to human errors. Thus a probabilistic analysis reveals the features of a plant that may merit close attention and provides a focus for improving safety.

The other objective achieved by a probabilistic risk assessment is the development of an information base for analyzing plant-specific and generic issues. This information base identifies dominant accident sequences and plant features contributing significantly to risk; it also contains the models of the plant developed during the study. Knowledge of the most probable severe accidents could assist the utility and the Nuclear Regulatory Commission in developing strategies for coping with accidents beyond the current design-basis accidents. This information could provide a focus for training operators to deal with such accidents. Emphasis could be placed on diagnosing the most-probable severe accident sequences and on providing information and guidance to the operators on how to cope with such accidents. In addition, the timing and location of containment failure and the magnitude of the potential release and radioactive material are estimated for each accident sequence. This information could be used in developing emergency-response plans.

Information developed in the assessment could help in making decisions about the allocation of resources for safety improvements, by directing attention to the features that dominate plant risk. The analysis may uncover new issues potentially generic to the industry. The Nuclear Regulatory Commission could use this information to focus its resources on investigating problems most important to safety and eliminating or reducing requirements and the expenditure of resources on issues not important to safety.

The plant models developed in the assessment can serve a wide spectrum of uses. They can be used to assess the safety significance of operational occurrences at the plant; they can also be used to assess the applicability and significance of occurrences at other plants. The models provide a basis for evaluating alternative design changes to improve safety.

The utility may well find the information and models developed in the study to be useful in training personnel. The analysis draws together diverse aspects of plant design and operation into an integrated model that could provide plant operators and utility engineers with a different perspective that could prove useful in the training of both.

In a broader sense, the Nuclear Regulatory Commission has used a collection of PRA studies to evaluate the potential safety value of contemplated regulatory changes and to evaluate generic safety issues.

Thus, probabilistic risk assessments provide not only a technique for assessing the safety of a particular facility but also an information base that is applicable to a wide variety of issues and decisions.

1.6 TREATMENT OF DEPENDENT FAILURES

In risk analysis, the treatment of dependences in the identification and quantification of accident sequences is referred to as "dependent-failure analysis." The identification and analysis of such failures are extremely important in PRA studies because dependences tend to increase the frequency of multiple concurrent failures. Several terms have been used to describe specific types of dependent failures, such as "common-mode failures" and "propagating failures." In this Guide, the term "dependent failure" is used to encompass all of these. Dependent failures are divided into several categories, which are discussed in Section 3.7.

The treatment of dependent failures is not a single step performed during the PRA; it must be considered throughout the analysis and thus has many steps. For this reason, the treatment of dependent failures is discussed in several chapters of this Guide. The treatment of dependent failures in the development of accident sequences and system models is covered in Section 3.7, and data sources for dependent failures can be found in Section 5.6. The dependences of human errors are discussed in Chapter 4. Earthquake, fire, and flood initiators that give rise to dependent failures are included in Chapter 11.

1.7 ORGANIZATION

A probabilistic risk assessment for a nuclear power plant is a complex project with special requirements. The organization and management of such a project are discussed in Chapter 2, which covers such topics as the sequencing and scheduling of PRA tasks, resource requirements, documentation, the assurance of technical quality, and manpower needs. Chapters 3 through 6 present the procedures for performing a level 1 PRA study. The first of these chapters describes procedures for identifying accident sequences; the next, Chapter 4, handles human reliability, discussing acceptable methods for determining the scope of human errors that is appropriate for the study as well as methods for determining human-error rates. Chapter 5 covers the development of component data and describes how component-failure probabilities are developed from generic and plant data. Chapter 6 describes the methods for quantifying the accident sequences.

Chapters 7 and 8 guide the reader through the containment analyses needed for a level 2 risk assessment. The former describes the physical processes of core-melt accidents; the latter gives the procedures for analyzing the release and transport of radionuclides. For a level 3 PRA study, Chapter 9 must be added to the preceding. It covers the transport of radionuclides through environmental pathways and describes the methods that can be used for determining the radiation doses that would be delivered to the public. It also explains how to calculate the health effects that would later develop in the exposed population and to quantify the economic impacts. Finally, it shows how to estimate public risk.

Chapters 10 and 11 are concerned with the topics needed to make the preceding efforts a full risk assessment: analyses of external events. Chapter 10 presents guidance on the selection of external events for evaluation and procedures for performing the pertinent analyses. Chapter 11 is concerned with seismic, fire, and flood analyses. Beginning with Chapter 3, each of these chapters covers the appropriate analytical techniques, the appropriate assumptions and approximations, methods of documentation, and assurance.

The last two chapters cover uncertainty analysis (Chapter 12) and the development and interpretation of results (Chapter 13). The appendices contain the charter of the PRA Procedures Guide project, the names of persons involved in producing and reviewing the Guide, and supporting technical data.

Chapter 2

PRA Organization

Probabilistic risk assessments (PRAs) are complex projects requiring considerable commitments of time and manpower. Depending on the objectives, they may range in scope from an analysis of engineered systems to a full risk assessment. After discussing the definition of objectives, the timing of the analysis, and the various levels of scope (Section 2.1), this chapter presents an overview of the tasks performed in PRAs of various levels (Section 2.2). It then describes the management of a PRA project (Section 2.3) and estimates manpower and schedule requirements, covering also the important points of report preparation (Section 2.4).

2.1 DEFINITION OF OBJECTIVES, TIMING, SCOPE, AND RESULTS

2.1.1 DEFINITION OF OBJECTIVES

Probabilistic risk assessments may have various objectives. Since the objectives of the analysis determine the scope of the PRA to be performed, an important first step in organizing a PRA is to clearly define the objectives of the study.

While the primary motivation for performing the study should be clear, an organization undertaking a PRA may wish to consider other possible uses for the information generated in the analysis. By properly structuring the analysis, it may be possible to produce, with only minimal extra effort, a study useful in many ways beyond the primary purpose.

Given a clear understanding of the objectives and potential uses of the study, the scope of the analysis can be delineated and the effort organized as discussed in the rest of this chapter.

2.1.2 TIMING OF THE ANALYSIS

A probabilistic risk assessment can be performed at any stage of plant life. The timing of the analysis may not preclude any of the objectives of the study, but it will affect the certainty of the design, the availability of plant-specific data, and hence the level of detail in the analysis. Furthermore, it will affect the flexibility for making design improvements that might be suggested by the analysis.

The analysis could be performed after the initial plant design, before construction. Such an analysis could be particularly useful in improving the designers' understanding of the safety significance of plant design features and in identifying design weaknesses. However, because the design

may not yet be firm, the analysis could be made more complex by the need to incorporate design changes as the analysis progresses. This problem occurs regardless of the status of the plant, but it is especially difficult for an analysis performed before the final plant design is established. The analysts generally must specify a date beyond which plant design modifications are not included. An analysis at this stage would not be able to use plant-specific component data; it would rely on generic industry data or, perhaps, on data from other plants in the utility's system. Similar limitations would apply to operating procedures. Nonetheless, despite these limitations, an analysis at this stage may well provide valuable input for design decisions and operating procedures.

The analysis could be performed just before plant startup. An analysis at this time could be particularly useful in identifying procedural inadequacies, since procedures will have been written but not used in plant operation. The analysis could be performed in full detail, but plant-specific component data would still be lacking, and there may still be last-minute design modifications and procedural changes to include. An analysis at this stage allows more detailed decisions to be made regarding plant design and operation.

An analysis of an operating plant can use plant-specific component data and an established design, although modifications are frequently made to operating plants. It can incorporate peculiarities of the particular plant that may become apparent only after operating experience. While a PRA performed at this stage may yield the most complete and applicable results, the design inadequacies identified by the analysis may be more difficult to correct. It is, of course, desirable to correct any serious deficiencies before plant operation. To the extent that the PRA might identify such problems, it is desirable to perform the analysis before plant operation.

2.1.3 SCOPE AND RESULTS OF THE ANALYSIS

Probabilistic risk assessments can be performed at many levels of scope, depending on the objectives of the study, the perspective sought in the study (i.e., whether just the core-melt frequency is important or whether a measure of risk is desired), and the availability of time and manpower. For the purposes of this guide, three discrete levels of scope are described:

1. Systems analysis.
2. Systems and containment analysis.
3. Systems, containment, and consequence analysis.

A level 1 PRA, described in Chapters 3 through 6 of this guide, consists of an analysis of plant design and operation focused on the accident sequences that could lead to a core melt, their basic causes, and their frequencies. It does not investigate the frequency or the mode of containment failure or the consequences of radionuclide releases. External events, such as fires, floods, and earthquakes, may or may not be included. The results are a list of the most probable core-melt sequences and insight into their causes. An analysis of such scope provides an assessment of plant safety,

an assessment of design and procedural adequacy, and plant models from the perspective of preventing core melt, but it does not permit an assessment of the risk associated with the plant. Nor can the core-melt sequences be differentiated into those with potentially high consequences and those with lower consequences.

A level 2 PRA, described in Chapters 3 through 8, consists of an analysis of the physical processes of the accident and the response of the containment in addition to the analysis performed in a level 1 PRA. Besides estimating the frequencies of core-melt sequences, it predicts the time and the mode of containment failure as well as the inventories of radionuclides released to the environment. As a result, core-melt accidents can be categorized by the severity of the release. Such an analysis adds information and perspective to a level 1 PRA, but it still does not provide sufficient information for a full assessment of plant risk. Some insight into risk, however, is provided by the relative frequencies of various release categories. The risk assessments of the Reactor Safety Study Methodology Applications Program, sponsored by the Nuclear Regulatory Commission (Carlson et al., 1981), are of this scope.

A level 3 PRA, discussed in Chapters 3 through 9, analyzes the transport of radionuclides through the environment and assesses the public-health and economic consequences of the accident in addition to performing the tasks of a level 2 PRA. An analysis of this scope does permit an assessment of plant risk since it estimates both the consequences and the frequencies of various accident sequences. The results are generally presented in the form of a "risk curve" depicting the frequency of various consequences. The Reactor Safety Study (USNRC, 1975) was of this scope.

An analysis of external events may be included in any of the three levels of PRA described above. The external events that are selected for analysis depend on the site, but they include such events as plant fires, internal and external floods, and earthquakes. These subjects are discussed in Chapters 10 and 11.

2.2 METHODS AND TASKS

Probabilistic risk assessment involves developing a set of possible accident sequences and determining their outcomes. To this end, several sets of models are developed and analyzed.

The development of sequences for the analysis can be broken down into two sets of models: those relating to plant systems and those relating to the containment. Plant-system models generally consist of event trees, which depict initiating events and combinations of system successes and failures, and fault trees, which depict ways in which the system failures represented in the event tree can occur. These models are analyzed to assess the frequency of each accident sequence.

The containment models represent the events occurring after the accident but before the release of radioactive material from containment.

They cover the physical processes induced in the containment by each accident sequence as well as the transport and deposition of radionuclides released within containment. The analysis examines the response of the containment to these processes, including possible failure modes, and evaluates the releases of radionuclides to the environment.

The outcome of the accident in terms of public-health effects and economic losses is assessed by means of environmental transport and consequence models. These models use site-specific 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 risk-assessment process is an uncertainty analysis. It involves not only uncertainties in the data but also uncertainties arising from modeling assumptions. The results of the risk assessment are analyzed and interpreted to identify the plant features that are the most significant contributors to risk.

Throughout the analysis, it is important to use realistic assumptions and criteria. When information is lacking or controversy exists, it may be necessary to introduce conservatisms or evaluate bounds, but the goal of the PRA should be to produce as realistic an analysis as possible.

The sections that follow discuss the tasks associated with risk assessments of various scopes. Each task is briefly described, and the relationships between tasks are discussed. The steps involved in the analysis are shown in Figure 2-1.

2.2.1 INITIAL INFORMATION COLLECTION

Probabilistic risk assessments are broad, integrated studies requiring large amounts of information. The information that is required depends on the scope of the analysis and falls into three broad categories:

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

A level 1 analysis requires the final safety analysis report; piping, electrical, and instrumentation drawings; descriptive information about the systems of interest; and test, maintenance, operating, and administrative procedures. This information is needed to give the analyst a set of documents on plant design and operation that is as complete as possible. Other studies performed on the plant may also prove useful. Most important are discussions with design engineers and plant personnel, which should be held throughout the PRA to ensure that the information used in the analysis is accurate. In addition to design information, analysts need both generic and plant-specific data on the occurrence of initiating events, component failures, and human errors. As already mentioned, the time at which the PRA study is done will influence both the amount and the detail of the available

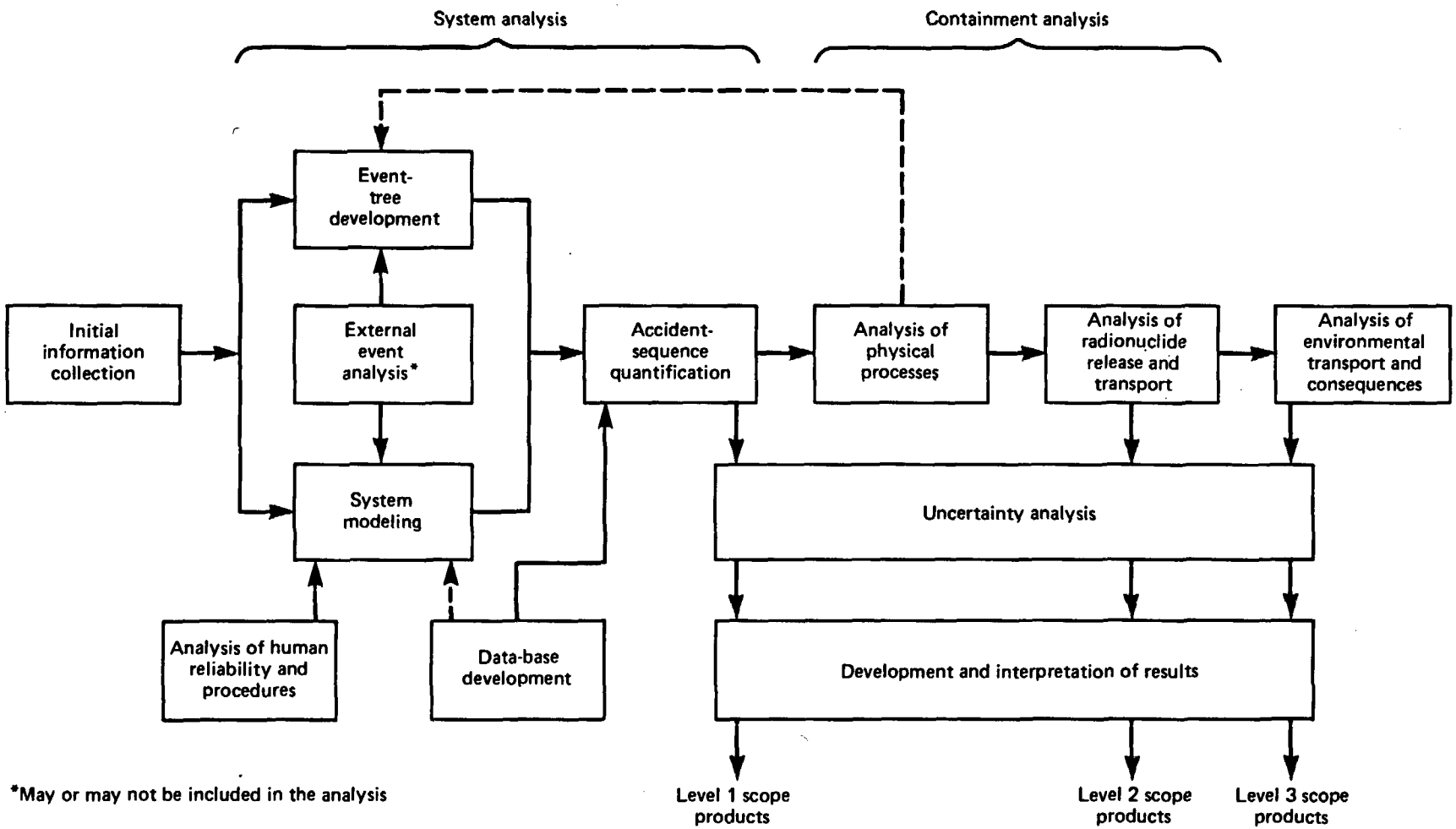


Figure 2-1. Risk-assessment procedure.

information. The analysts should also have this procedures guide or other methods documents providing guidance on the performance of the analysis.

The additional information needed for a level 2 analysis includes more-detailed design information on the reactor-coolant system and the containment. The information on the structural design of the containment should include dimensions, masses, and materials.

A level 3 analysis requires site-specific meteorological data for the environmental-transport calculations. If topographic data are pertinent and available, they may be also included. Local population densities and health-effects models are necessary for site-specific consequence calculations, and evacuation plans may be considered as well.

If external events are to be analyzed, considerably more information will be needed, depending on the external events to be included. For instance, detailed structural information as well as data on the seismic design of the plant and the seismicity of the site are needed for a seismic analysis. Information about the compartmentalization of the plant is necessary to analyze susceptibility to fires and floods.

The information needs of each part of the risk assessment are discussed in detail in the pertinent chapters of this guide.

2.2.2 SYSTEM ANALYSIS

This task involves the definition of accident sequences; an analysis of plant systems and their operation, the development of a data base for initiating events, component failures, and human errors; and an assessment of accident-sequence frequencies. It constitutes a major portion of the risk assessment and hence is divided into the several subtasks discussed below. Although the subtasks are presented sequentially, the performance of the plant-system and accident-sequence analysis requires considerable iteration. The results of this analysis--the frequencies of accident sequences and insights into their causes--constitute the products of a level 1 PRA. They are also used in the subsequent tasks of more-extensive risk assessments.

2.2.2.1 Event-Tree Development

The event-tree development subtask delineates the various accident sequences--that is, combinations of initiating events and the successes or failures of systems--to be analyzed. This activity includes an identification of initiating events and the systems that respond to each initiating event. The scope of the event tree depends on the scope of the analysis. Systems that only serve to mitigate, but do not contribute to the prevention of a core-melt accident may not be included in a level 1 PRA. The analysts developing the event trees should consult with those familiar with the analysis of physical processes inside the containment to define system dependences arising from interactions related to the physical phenomena induced by the accident. Separate event trees are generally constructed for each

initiating event or class of initiating events having a unique event-tree structure.

2.2.2.2 System Modeling

This subtask involves the construction of models for the plant systems covered in the risk assessment. The systems to be analyzed and their success criteria are identified in conjunction with event-tree development in an iterative process. Assistance from thermal-hydraulics 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. Thus, there is some interface with the data-base-development subtask discussed later. In addition, human errors associated with the testing, maintenance, or operation of the systems are included in the system model, and thus system modeling interfaces directly with the analysis of human reliability and procedures. Common-cause contributors and potential systems interactions should also be included to ensure proper integration into the analysis.

2.2.2.3 Analysis of Human Reliability and Procedures

Past PRAs have shown the importance of operator error. These human errors are included in the plant-system models. The analysis performed in this 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.

2.2.2.4 Data-Base Development

The quantification of accident sequences requires a component-data base, which is developed by compiling data, selecting appropriate reliability models, establishing the parameters for those models, and then estimating the probabilities of component failures and the frequencies of initiating events. The data used in this subtask may be generic industry data or plant-specific data, or a combination of both. Guidance from the data analyst will assist in determining the level of detail to which to develop the plant-system models.

2.2.2.5 Accident-Sequence Quantification

In order to quantify the frequencies of the accident sequences delineated in the event trees, failure rates are assigned to each plant-system model and frequencies are assigned to 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. A computer code assists the analyst in identifying and quantifying combinations of events (initiating events, component failures, and human errors) that result in the accident sequence.

The size of the fault trees developed in the system-modeling subtask may cause problems in running the computer codes. In such an event, the sequence quantifier should work closely with the systems analyst to resolve the difficulties.

2.2.3 CONTAINMENT ANALYSIS

Probabilistic risk assessments performed at levels 2 and 3 include an analysis of the containment. This analysis is important for differentiating among the consequences of various core-melt accident sequences and consists of two subtasks. The results of this analysis--an identification of containment-failure modes and a prediction of the radionuclide inventory released to the environment for each accident sequence--constitute the products of a level 2 PRA. They are also used in the subsequent tasks of more-extensive risk assessments.

2.2.3.1 Analysis of Physical Processes

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 are insights into the phenomena associated with the accident sequence and a prediction of whether the containment fails.

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. Insights from this analysis may be used in the iterative process of constructing system event trees if accident phenomena affect system performance.

2.2.3.2 Analysis of Radionuclide Release and Transport

For each core-melt accident that is postulated to breach the containment, it is necessary to estimate the inventory of radionuclides that would be available for release to the environment. In this subtask the analyst uses a computer model to analyze the radionuclides released from the reactor fuel during the accident and to assess their transport and deposition inside the containment before containment failure. The results of this analysis

are a prediction of the radionuclide inventory released into the environment at the time of containment failure for each accident sequence.

2.2.4 ANALYSIS OF ENVIRONMENTAL TRANSPORT AND CONSEQUENCES

To assess the risk associated with the plant, it is necessary to calculate the consequences of the release in addition to the frequency of the accident and the inventory of released radionuclides. Consequences are generally expressed in terms of early fatalities, latent-cancer fatalities, and property damage. To perform this task, the analyst uses a computer model that begins with the inventory of radionuclides 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 population density are then used to calculate the radiation doses delivered to the population, and a health-effects model is used to estimate health effects. The economic consequences that are estimated are those resulting from a relocation of the population and the interdiction or decontamination of the land. The results of the analysis--consequence distributions (i.e., plots of the predicted frequency for consequences of varying magnitudes) for each accident release category--constitute the products of a level 3 PRA.

2.2.5 ANALYSIS OF EXTERNAL EVENTS

External events, frequently excluded from risk assessments, include fires, earthquakes, and floods. This task uses the models developed in the plant-system analysis. The models are either analyzed independently from the perspective of external events or else they are modified to reflect external events explicitly. Additional event trees are developed to delineate the external event sequences to be analyzed.

The results of the external events analysis are incorporated into the accident-sequence analysis. In addition, external events may influence the containment analysis. The subsequent steps of the risk assessment are the same as those discussed above. The final result is a more complete risk assessment.

2.2.6 UNCERTAINTY ANALYSIS

Uncertainty analysis is an integral part of a risk assessment regardless of scope. There are uncertainties in every step of a PRA, and some of them may be large. Whether qualitative or quantitative in nature, the analysis considers uncertainties in the data base, uncertainties arising from assumptions in modeling, and the completeness of the analysis. To the extent possible, these uncertainties are propagated through the analysis. Where this is impractical, a sensitivity analysis provides insight into the possible range of results.

2.2.7 DEVELOPMENT AND INTERPRETATION OF RESULTS

The final step in performing PRAs of various scopes is to integrate the data obtained in the various tasks of the analysis and to 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.

2.2.8 DOCUMENTATION OF RESULTS

The results of the analysis must be substantiated and fully documented. This is a substantial task for an analysis of this magnitude. All major assumptions made in the analysis should be discussed. Where possible, supporting analyses in the literature should be referenced. The report should describe all tasks of the analysis in sufficient detail to permit the reader to understand how the plant systems work, to independently calculate the frequencies of the dominant accident sequences, and to calculate or at least understand the derivation of quantities that are important in the assessment of public risk, such as the magnitude of the radionuclide source terms and the interval between the awareness of an impending core melt and the start of radionuclide release to the environment.

2.3 PRA MANAGEMENT

As discussed previously, probabilistic risk assessments are broad, integrated plant analyses. As such, they require analysts with diverse backgrounds. The success of the project will depend largely on assembling persons with the proper backgrounds and properly managing and integrating their efforts.

2.3.1 THE ANALYSIS TEAM: EXPERTISE AND COMPOSITION

The expertise needed for a risk assessment depends on the level of the analysis. A certain core of expertise is, however, required for all such analyses--namely, the expertise needed for a level 1 PRA. Probabilistic risk assessments of greater scope require people with additional expertise.

For each of the three levels, at least one person having thorough familiarity with that level of analysis should have a prominent role in the technical direction of the team. A person familiar with the relationship among the levels is also required. Equally important is the contribution of at least one person who is thoroughly conversant with the design and the operation of the plant. He, too, should have a prominent role in the technical direction of the study.

It is important, however, that the team work under the direction of one individual. This team leader provides perspective and direction to the effort. His primary technical role in the study is to integrate the various portions of the analysis. Probabilistic risk assessments involve considerable judgment since many issues as yet unresolved in the technical community must be treated in the analysis. The team leader must weigh differing viewpoints and decide how the analysis will be performed. This is often a matter of judgment, but will depend heavily on the objectives of the study and what portions need to be emphasized. In the course of the analysis, questions involving subtleties in modeling will arise; guidance will be needed as to the level of detail at which to terminate modeling. The team leader must assume responsibility for the analysis and make these and other judgments.

Although project personnel may come from a variety of organizations--contractors, consultants, and several in-house utility organizations--strong utility-management commitment is essential, and it is essential that utility personnel be intimately involved in the project. Such involvement can be expected in most projects since utilities are likely to be the most frequent sponsors of PRAs. The role of the utility in any PRA is, however, very important. The success of the project requires intimate familiarity with the plant, which can be best provided by utility personnel. The utility can provide people capable of making unique contributions to the analysis. Among them should be someone thoroughly familiar with the operation of the plant. He should understand how the plant will be operated under accident conditions and should be familiar with control-room operation, plant equipment, and plant layout. Utility personnel can also provide the necessary knowledge of testing and maintenance procedures as well as the accompanying administrative controls. The analysis team should also have access to plant personnel familiar with specialized aspects of plant design, such as instrumentation and control.

In addition to providing unique capabilities to the team, utility personnel serve as focal points for the gathering of information from the plant and the transmittal to the utility of information pertaining to the analysis. They also ensure that the assumptions made in the analysis accurately reflect the design of the plant and help to ensure that the analysis is realistic.

The major portion of a level 1 PRA is performed by systems analysts, several of whom will be needed on the team. The analysts should be familiar with system design and operation, although they need not necessarily be familiar with probabilistic risk assessments. The systems analysts are responsible for developing the event-tree and system models for the plant. A PRA project therefore needs analysts who can provide the systems overview needed for event-tree construction and who can analyze both fluid and electrical systems.

Persons with expertise in human-reliability and data analysis are desirable members of the team. The human-factors analyst assists the systems analyst in identifying the human errors to be included in the plant models and provides the insights needed to quantify these errors. The analyst need not have special training in the human-factors field, although such training is certainly desirable. The data analyst compiles and uses generic and plant-specific data to estimate component-failure rates and initiating-event frequencies for the quantification of accident sequences. He should have experience in using various data sources and selecting the proper failure rate for the event in question.

The models involved in the quantification of accident sequences are often too large to be analyzed by hand. Rather, the analysis requires the use of computer codes for manipulating logic expressions. The analysis team should include a person familiar with the preparation of input and the operation of the chosen code.

A team with the above-delineated expertise should be able to perform a level 1 PRA. The team for a level 2 PRA should include persons familiar with the analysis of physical processes occurring inside the containment after an accident, structural analysis, and the thermal-hydraulics analysis of the behavior of the reactor-coolant system under accident conditions. The analysts use computer codes to calculate the phenomena occurring in the containment and to assess the release of radionuclides from the core, the transport and deposition of these radionuclides inside the containment, and the radionuclide inventory released at the time of containment failure. Analysts familiar with the physics involved in the analysis, the running of the appropriate codes, and the interpretation of the results are needed on the analysis team.

A level 3 PRA requires analysts familiar with the environmental transport of radionuclides and the consequences to the public. Once again, computer codes assist in the analysis, and analysts familiar with the physics involved, the running of the codes, and the interpretation of the results should be included in the team. Utility or local civil-defense personnel could be of assistance by providing detailed information on local emergency-response plans and evacuation routes.

If external events are to be included in the analysis, the team will need personnel with expertise in analyzing these events. The particular expertise required will depend on the events evaluated in the study. For example, if seismic events are included in the analysis, the PRA study team should include a qualified seismologist and engineers experienced in seismic hazard analysis, seismic structural and subsystem analyses, structural and mechanical design, and seismic qualification testing.

2.3.2 PROJECT MANAGEMENT

The day-to-day management of the analysis is the responsibility of the team leader. He provides the technical direction and directs the activities of the team members. To keep the team on schedule and within budget, the team leader must anticipate and ensure the timely resolution of problems as

they arise. The team leader also must review all work products for technical accuracy, prepare periodic briefings for corporate management, and coordinate the preparation of all reports.

Corporate management must provide the analysis team and the team leader the support they need. They are responsible for providing office space and facilities, and for initiating and managing any required contracts with outside organizations. Corporate management must also provide the manpower necessary for the analysis and ensure the timely availability of support personnel. They should also review the results of the analysis and ensure that facilities are available to produce the reports.

2.3.3 ASSURANCE OF TECHNICAL QUALITY

The assurance of technical quality refers only to the assurance of quality for the PRA itself. Theoretically, a PRA has quality when it represents real life, but this attribute cannot be measured. Therefore, a PRA is said to have quality when the insights or risk profiles it produces reflect the appropriate use of risk-assessment methods as well as information about the plant and the site--and when the resulting documentation clearly and accurately conveys the resulting insights and risk profiles as well as their bases.

There is no simple or certain formula for the quality of a PRA. The assurance of quality is not a function that can be separated from the performance of a PRA. There are, however, several steps that can be taken to enhance quality or to facilitate its achievement. The most noteworthy, described in this section, are (1) steps that can be taken by management or program planners, (2) practices that should be followed by the study participants, and (3) levels of review that can take place during or on completion of the study.

2.3.3.1 Program Definition and Initial Planning

The care taken in the initial planning of the program will have a great effect on the quality of the study. Although many decisions will affect the outcome of the work, five areas stand out as most important: (1) definition of objectives, (2) delineation of scope, (3) organization and selection of participants, (4) funding, and (5) scheduling.

Definition of Objectives. The purpose for which the study will be used should be identified. From this should follow the specific stated objectives of the study. Where judgments or assumptions must be made during the study, as always happens, having stated objectives will facilitate judgment and the selection of assumptions that best meet the intended purpose of the study.

Delineation of Scope and Depth of Detail. From the stated objectives of the study should follow a definition of the total scope and depth of detail for the study. This definition should reflect not only the purpose

of the study but also available funding and time. The pursuit of areas of study unnecessary to the program objectives will, in general, reduce the resources available for pursuing necessary areas. By focusing resources on the most important areas, the careful definition of scope and depth of detail will enhance the quality of the results.

Organization and Selection of Participants. The appropriate use of risk-assessment methods and information requires people who are both knowledgeable and experienced in the required disciplines; it also requires well-defined responsibilities and interfaces. The team leader should be carefully selected and his authority well defined. This guide has attempted to provide guidance in these areas.

Funding and Scheduling. As in any other project, the quickest road to inadequate quality is the inadequate allocation of funding or time. This guide has attempted to provide guidance in these areas.

2.3.3.2 PRA Practices

Without question, the most important contribution to quality comes from the practices followed by the team conducting the PRA. These practices fall into five general areas: planning, methods, internal review, documentation, and computer codes. Success in achieving quality at this level depends primarily on the team leader.

Planning. Each team member should be assigned specific tasks with well-defined responsibilities and products. The interfaces between tasks and therefore individuals should also be carefully defined.

Methods. The methods to be used need to be well defined to ensure consistency between team members and appropriateness of intermediate products for use in subsequent tasks. The methods and information sources should also have reasonably broad acceptance to enhance the acceptability of the insights and risk profiles produced by the study. This document has attempted to provide guidance in this area.

Internal Review. Mechanisms should be established to ensure the internal review of all analyses and products.

Documentation. Engineering notebooks, correspondence files, or similar records should be kept daily to enhance the traceability of information sources, assumption bases, and calculation results. Formal or published documentation should be sufficiently complete for the reproducibility of results, the identification of all information sources, and an understanding of the bases of judgments and assumptions. This documentation and computer calculations should be retained for a few years for future use and as a resource when questions arise.

Computer Codes. Several activities associated with the use of a computer code in a PRA can help to ensure a quality analysis. First, the user must ensure that, once he has obtained a code, it is running properly on his machine. To do this, the user should reproduce samples of input and output from the code developer. These samples should cover all areas of the code

that are likely to be used in the PRA. Second, the user often has to rely heavily on the presumed competence of the developer of the code. The user should read the code manual and associated literature with a critical eye, noting the sources cited for the various models and the justifications given for their use. He should not hesitate to query the code developer if there is any reason for doubting that the coding represents good practice. Third, if the user alters the code he has obtained, to improve the modeling, he should describe the reasons for the alterations and reference them. He should also carry out independent calculations (e.g., hand calculations) to ascertain that the new modeling is working correctly and compare them with experimental results, if available. Fourth, if the literature contains examples of calculations carried out by other code developers, or if there has been some sort of benchmark exercise, it is both desirable and instructive to compare results with those of other codes. If the results lie within an envelope generated by other modelers, well and good; if not, the code must be examined to see why the results differ. If the user wishes to stand by his modeling, he must know his code well enough to determine the reasons for the difference and to justify the modeling or parameters that cause the difference. Fifth, once the code is put to use in a specific PRA, the problem of assuring technical quality is mainly dependent on the justification of the input data used. This can be done by carefully referencing the sources of data and by using an independent reviewer to ensure that the collected set of data is actually correctly input to the code. Finally, it is desirable to rerun the standard sample problems from time to time to make sure that there has been no deterioration in the code over a period of time.

2.3.3.3 PRA Reviews

To achieve quality in general, PRAs should be reviewed at four levels: study team, plant operating personnel, peers, and management.

Study-Team Review. The review of all work done should be carried out by the team leader and an internal peer group. Although this review should cover all aspects of the study, it is at this level that methodological mistakes are identified with the greatest confidence.

Review by Plant Operating Personnel. It is desirable to have the PRA reviewed by persons most familiar with the plant design, operation, and utility operating practices. It is at this level that technical mistakes concerning representation of the plant and site characteristics are identified with the greatest confidence.

Peer Review. This review should be carried out by true peers; that is, persons who are not involved in the study but have capabilities essentially equivalent to those of the persons performing the study. The peers should span the range of disciplines required for the study. In general, this review should concentrate on the appropriateness of methods, information sources, judgments, and assumptions.

Management Review. The level of review should concentrate on perspective, scope, and product suitability in meeting program objectives. The reports from the peer review should be a part of the management review.

2.3.4 SUPPORT PERSONNEL AND SPECIAL NEEDS

Probabilistic risk assessments generate substantial quantities of paper and drawings. Several typists, preferably using word-processing equipment, are needed to produce the reports. Draftsmen or graphic artists are useful for producing the many drawings and fault trees incorporated into the reports.

Several computer codes are used in the analysis. The particular codes that are used depend on the scope of the analysis and the preference of the analysts. Computers compatible with the programs must be available to the analysis team.

Members of the team occasionally may need access to the plant to view equipment, to observe tests, and to become familiar with the layout of certain equipment. Plant personnel should be available on these occasions to escort the analysts and answer questions they may have.

It is desirable for the analysis team to be in the same location. This improves communication among the members of the team and facilitates consistency in approach and assumptions. Adequate office space and accommodations should be secured before the beginning of the study.

2.4 SCHEDULE, MANPOWER, AND REPORTING

A PRA consists of many tasks and subtasks, as discussed in Section 2.2. Several of the tasks can be performed in parallel; others depend on the products of a previous task and hence must be performed sequentially. This section presents estimates of the manpower needed for each subtask. The estimates were obtained from the authors of the various chapters of this guide and are based on the assumption that this procedures guide is being used. As such, no time is allocated for developing PRA methods. It is also assumed that the necessary computer codes are up and running and that the team contains persons familiar with their use. No time for the special training of personnel is included; it is assumed that they bring the requisite skills to the analysis and can learn anything more on the job. Finally, the estimates pertain to a one-time-only PRA; no estimates are included for updating the PRA to reflect new design changes. Without knowing the total manpower available, it is not possible to develop a timetable for the completion of the analysis. Section 2.4.2 presents two possible schedules--one a "minimum" timetable and one more representative of other analyses. Logical reporting points in the analysis and the manpower and time required for compiling the reports are discussed in Section 2.4.3.

Several other factors may affect the effort needed to conduct the analyses. Among these are the age of the plant, its operational status, and the available documentation; peculiarities of containment design; the availability of similar analyses on similar plants; and the level of PRA experience of the particular team.

Given these qualifying remarks, manpower and schedule estimates are presented here. They are intended merely for information; any organization considering a PRA must develop its own estimates pertinent to the particular project.

2.4.1 SCHEDULE AND MANPOWER

The PRA is broken into the major tasks and subtasks discussed in Section 2.2. The estimates of manpower needed to perform each task are given in Table 2-1. Table 2-2 presents estimates for PRAs of different scopes, including reporting, the assurance of technical quality, and management. Each is discussed below.

Table 2-1. Estimated manpower per task

Task	Manpower estimate (man-months)	
Initial information collection	1-2	Level 1 = 51-89
Event-tree development and system modeling	29-38	
Analysis of human reliability and procedures	2-6	
Data-base development	5-6	
Accident-sequence quantification	9-12	
External event analysis[a]	14-18	
Uncertainty analysis	3-4	
Development and interpretation of results	2-3	
Analysis of physical processes	15-137	Level 2 = 75-288
Analysis of radionuclide release and transport	5-20	
External event analysis[a]	3-4	
Uncertainty analysis (additional)	2-8	
Development and interpretation of results (additional)	2-30	
Analysis of environmental transport and consequences	3-4	Level 3 = 80-298
External event analysis[a]	1-2	
Uncertainty analysis (additional)	1-2	
Development and interpretation of results (additional)	1-2	

[a]May or may not be included in the analysis.

Table 2-2. Estimated total manpower for PRAs of various levels

Function	Manpower estimate (man-months) Level 1	Level 2	Level 3
Analysis	51-89	75-288	80-298
Reporting	11-22	19-38	23-43
Assurance of technical quality	7-12	10-20	11-21
Management	14-19	19-21	21-24
Total	83-142	123-367	135-386

2.4.1.1 Level 1 PRA

Task 1, initial information collection, begins on deciding to perform the PRA. It is important that the analysis team have available a substantial amount of information on beginning the analysis to avoid delays and misinformation. The information-collection task is an activity that continues throughout the PRA, and as the analysis proceeds, more information will be needed regarding specific aspects of plant design and operation. For the initial accumulation of information, however, it is estimated that 1 to 2 man-months will be needed.

The development of plant models and particular analyses germane to this development may proceed in parallel. Event-tree development (subtask 2a) and system modeling (subtask 2b) use much of the same information. The models are generally separate, although some insights from each development may influence the other. In particular, the development of event trees helps to clearly define the events to be modeled in system modeling. The effort required for event-tree development and the development of models representing all systems included in the analysis is estimated to be 29 to 38 man-months.

The development of plant models is supported by an analysis of human reliability and operating procedures (subtask 2c) and the development of a data base (subtask 2d) for assessing component reliabilities and initiating-event frequencies. Both activities are performed in parallel with the model development. This ensures that human errors are incorporated into the models. The data-base-development subtask assists in establishing the appropriate level of detail for the models and provides data for accident-sequence quantification. The human-factors analyst assisting in the analysis of human reliability and procedures is estimated to need 2 to 6 man-months; the development of a data base, 5 to 6 man-months.

The accident-sequence quantification (subtask 2e) integrates the plant models and data to quantify accident sequences. This subtask follows the plant-modeling effort and the development of the data base. Considerable iteration can be expected during this activity. The manpower needed to complete this task is estimated to be 9 to 12 man-months.

If an external events analysis is included, it proceeds concurrently with the development of plant models and uses information contained therein. The system analysis is completed before the quantification of accident sequences to permit the inclusion of its results in the accident-sequence analysis. Manpower needs depend on the number and the type of external events considered. If seismic, fire, and flood analyses are performed, it is estimated that 14 to 18 man-months will be needed for this task.

An uncertainty analysis is performed in a level 1 PRA. The manpower needs depend on the depth of this analysis, but 3 to 4 man-months is a representative figure. An additional effort of 2 to 3 man-months is estimated for the development and interpretation of results.

The above tasks constitute a PRA of level 1. Their performance is estimated to require 51 to 89 man-months. In addition to these technical tasks, however, the PRA requires program management, assurance of technical quality, and report preparation. Program management is estimated to require an additional person working full time; the team responsible for ensuring technical quality is assumed to need 7 to 12 man-months. Report preparation for a level 1 PRA is estimated to require 11 to 22 additional man-months (see Section 2.4.3). Given a representative schedule (see Section 2.4.2.2), the total manpower needed to perform, review, and publish a level 1 PRA is estimated to be 83 to 142 man-months.

2.4.1.2 Level 2 PRA

Two additional tasks are performed in a level 2 PRA: the analysis of the physical processes of accidents and the analysis of radionuclide releases to the environment. These tasks generally require people with substantially different backgrounds and expertise from those involved in the level 1 PRA.

Some analysis of physical accident processes is required early in the PRA effort to support the activities of task 2 related to event-tree development and system modeling. This is a comparatively small effort that is required in a level 1 as well as a level 2 PRA. After the identification of specific system sequences in subtask 2b, the progression of accident sequences must be analyzed in order to be able to estimate their radiological consequences. Because of the large number of system sequences identified, it is not practical to analyze the physical processes of every sequence. Either the sequences must be ranked in importance through quantification, or they must be grouped according to similar behavior, with only representative sequences analyzed. In either case, the analysis of accident processes should not be completed before subtask 2e, the quantification of accident sequences, since some iteration may be required as the dominant contributors to risk become apparent. The other major effort required in the physical-processes task is the development and quantification of the containment event tree, which describes the different possible pathways for the release of radionuclides from containment for an accident sequence.

The amount of effort required for the analysis of accident processes can vary substantially (15 to 137 man-months), depending on the expected use

of the PRA and the amount of previous experience in the analysis of a particular plant design. The state of the art of physical-process analysis is not at the point where specific computer codes can be used in the analysis without extensive checking and evaluation. The analysis of physical processes, particularly in relation to the likelihood and the time of containment failure, can, however, appreciably affect the overall risk. The high end of the estimate range is characteristic of the effort required in the Zion probabilistic risk assessment (Commonwealth Edison Company, 1981) without accounting for extensive model development. (Such model development, if required, may require as much as 20 to 25 man-months.)

The analysis of radionuclide release and transport (subtask 3b) depends on and follows the analysis of physical processes. The final product of this task is the assignment of accident sequences to release categories that describe the timing and quantity of radionuclide releases from the containment. The manpower needed for this analysis is estimated to be 5 to 20 man-months.

If external events are included in the analysis, it will be necessary to perform an analysis of the containment under the conditions of each type of external event. Such analyses are estimated to require 3 to 4 additional man-months.

The development and interpretation of results may take 2 to 4 man-months if a good correlation to previously published containment event tree(s) is obtained or if a qualitative statement is sufficient. If a detailed containment event tree is developed, up to 30 man-months should be allocated for development and quantification.

Additional uncertainty analysis is performed in a level 2 PRA, reflecting the additional modeling involved. Uncertainty analysis follows subtasks 3a and 3b, and is estimated to take 2 to 8 man-months more than it does in a level 1 PRA.

The performance of a level 2 PRA is estimated to require an additional 24 to 199 man-months of technical work beyond a level 1 PRA. Additional program management, assurance of technical quality, and reporting requirements are estimated to entail another 16 to 26 man-months. Thus, the total manpower for performing, reviewing, and publishing a level 2 PRA is estimated to be 123 to 367 man-months.

2.4.1.3 Level 3 PRA

A level 3 PRA includes an analysis of the environmental transport and consequences of radionuclide releases for each accident sequence (task 4). The collection of meteorological, topographic (if pertinent), and demographic data occurs concurrently with the radionuclide release and transport analysis. This ensures that the analysis can be performed immediately after the identification of release categories. The manpower for the analysis is estimated to be 3 to 4 man-months, with an additional 1 to 2 man-months needed should external events be considered, and 2 to 4 man-months for the uncertainty analysis and the development of results.

The performance of a level 3 PRA, then, requires an additional estimated 5 to 10 man-months of technical work. Additional requirements for management, reporting, and the assurance of technical quality are estimated to entail 7 to 9 man-months. A level 3 PRA is therefore estimated to require 135 to 386 man-months to produce, review, and manage.

2.4.2 EXAMPLES OF SCHEDULES

As already discussed, it is difficult to estimate the time required for a risk assessment without knowing how many people are devoted to the job and their particular expertise. Presented below are two schedules. The first is a "minimum schedule," that is, a schedule for a project performed by the maximum number of people of the right expertise. The second is more typical of risk assessments that have been performed.

2.4.2.1 Minimum Schedule

The tasks requiring the most man-months are those related to the development of plant models and, should it be included in the scope, the analysis of external events. Thus, to minimize the time required for the analysis, it is necessary to maximize the number of systems analysts. The analysis of front-line systems generally precedes the analysis of supporting systems. Thus, the maximum number of systems analysts would be one for each front-line system.

To complete the analysis in the shortest time, the analysis team is assumed to consist of the following:

1	team leader/integrator	Level 1
7	systems analysts	
1	human-reliability specialist	
2	data analysts	
2	sequence-quantification specialists	
3	physical process analysts	Level 2
1	structural analyst	
2	radionuclide-transport analysts	
2	environmental transport specialists	Level 3
8	external event analysts (if included)	

This 29-member team should be able to perform the technical analysis for a complete risk assessment in approximately 12 months. If such an ambitious schedule is undertaken, a great deal of effort must be expected of the team leader to ensure consistency and to clarify interfaces among the many analysts.

Of course, the team and the schedule depend on the scope of the analysis. The technical analysis for a level 1 PRA could be performed in approximately 10 months with the 13-member team specified above. The technical analysis for a level 2 PRA would require at least 19 team members (more if a highly involved containment analysis were performed) and could be

accomplished in approximately 11 months. The technical analysis for level 3 would take approximately 12 months. The team would consist of 21 members. If external events are included, eight additional team members are assumed. The schedules would be the same, however, since the external event analysis would not be on the critical path.

The schedule could be shortened somewhat by involving more people in the accident-sequence quantification. This, however, may not be desirable in that more inconsistencies could be introduced into the quantification by increasing the number of analysts. Because of the importance of this task, it is highly desirable to minimize the inconsistencies. This consideration took precedence over shortening the time for this schedule.

The 12-month "minimum schedule" is shown in Figure 2-2.

An additional month would be required to draft the document and another month for producing the draft. Three more months should be added to the schedule for reviewing and revising the draft. An additional month for printing the final report gives an 18-month minimum for producing a complete risk assessment in final form. A similar 6-month document-preparation time should be added to the estimates for PRAs of other levels. Hence, the minimum times for producing PRAs of various levels are estimated to be as follows:

PRA level	Months
1	16
2	17
3	18

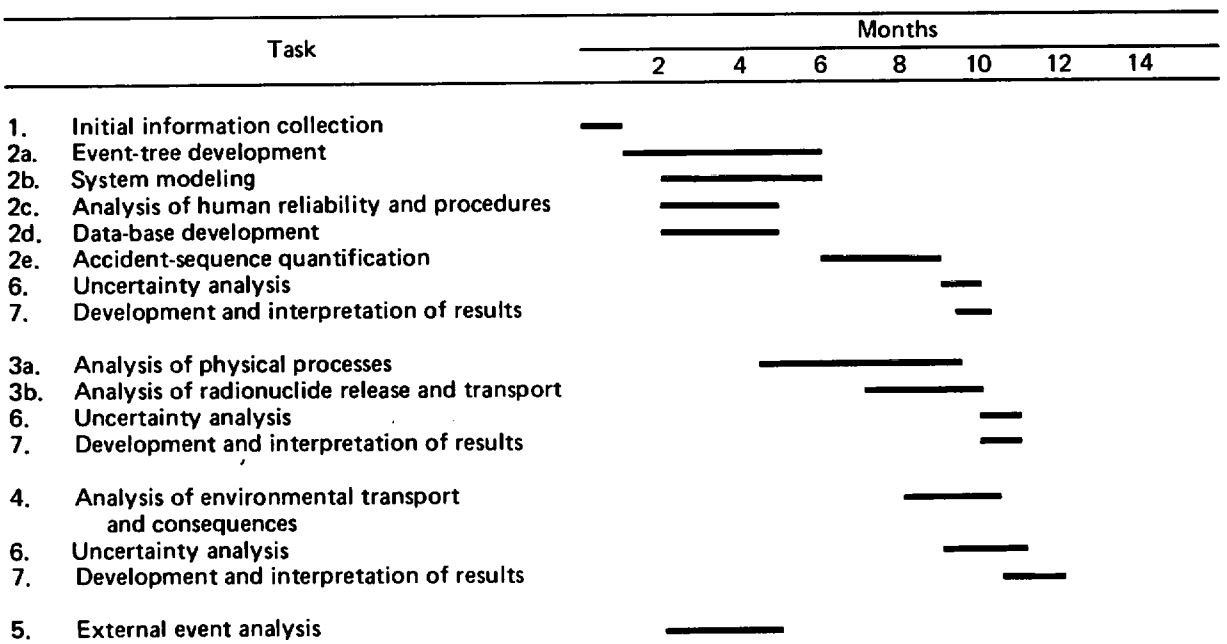


Figure 2-2. Minimum technical schedule. For report preparation and publication, another 6 months should be added.

2.4.2.2 Representative PRA Schedule

A more representative PRA team would not include as many systems analysts. This would diminish the difficulty of finding the required number of analysts and increase the consistency of the analysis. The fewer the analysts, the easier it is to achieve consistency among the analyses.

A representative PRA team is assumed to consist of the following:

1	team leader/integrator	Level 1
4	systems analysts	Level 1
1	human-reliability specialist	Level 1
1	data analyst	Level 1
2	sequence-quantification specialists	Level 1
3	physical process analysts	Level 2
1	structural analyst	Level 2
2	radionuclide-transport analyst	Level 2
2	environmental transport specialists	Level 3
4	external event analysts (if included)	

This 21-member team should be able to perform the technical analysis for a complete risk assessment in approximately 17 months. A 17-month schedule for the representative PRA is shown in Figure 2-3.

Because of the increased work required of each analyst, an additional month would be required to write and produce a draft report. To write and produce the draft, to review and revise it, and to produce the final report would take approximately 7 months. Thus, the complete risk assessment would require approximately 24 months to produce.

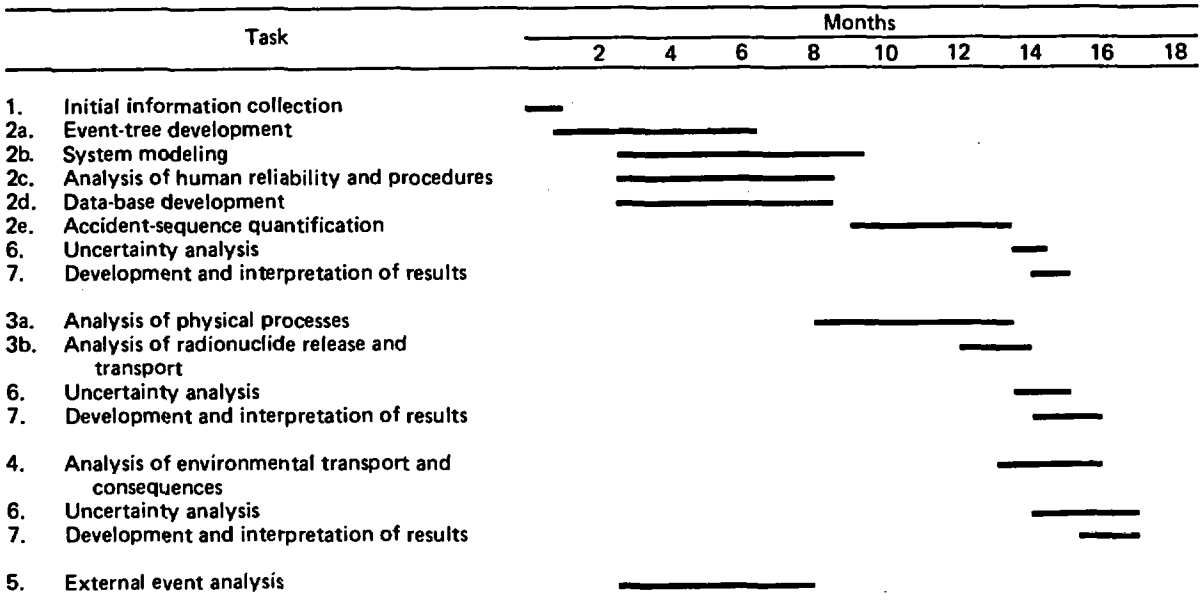


Figure 2-3. Representative technical schedule. For report preparation and publication, another 7 months should be added.

The representative schedules for PRAs of various levels are estimated to be as follows:

PRA level	Months
1	22
2	23
3	24

These schedules are only meant to provide general guidance. Each organization undertaking a probabilistic risk assessment must assess the scope of the project, the required time scales, and the availability of proper manpower in developing its own schedule.

2.4.3 REPORTING

The documentation associated with a probabilistic risk assessment is substantial. Large amounts of information are used in the analysis, and many assumptions are made. All this needs to be well documented to permit an adequate technical review of the work and to ensure that the final document is understandable and usable.

Two different strategies can be employed: (1) reports can be written at the conclusion of each major portion of the analysis or (2) the reporting may be delayed until all technical work is complete. The first approach makes it possible for the work to be reviewed by management and those responsible for ensuring technical quality as the project unfolds. Erroneous assumptions or misinformation can be corrected before proceeding. This approach, however, may interrupt the continuity of the analysis. The second approach ensures uninterrupted focus on the technical analysis, but errors may not be found until it is difficult to correct them, and certain assumptions made during the analysis may have been forgotten and left out of the final report. Reporting at the completion of each major product therefore appears to be the more desirable approach. To minimize the effort needed for preparing the final report, each interim report should, to the extent possible, reflect the detail, content, and format of the appropriate section of the final report.

Given this approach, interim reports are appropriate for the following tasks:

1. Event-tree development.
2. System modeling, including human-reliability analysis and database development.
3. Accident-sequence quantification.
4. Containment analysis.
5. Environmental transport and consequence analysis.
6. External event analysis.

In addition, a draft final report is compiled for review, and, after revision, a final report is published.

Each interim report is reviewed by those responsible for ensuring technical quality. The review of event trees focuses on the number of groupings of initiating events, the inclusion of appropriate systems in the headings, the proper reflection of system dependences, and the appropriateness of assumptions about physical phenomena. The review of system models focuses on the appropriateness of the top events, the correctness of the logic structure, and the appropriateness of the level of detail. The review of the accident-sequence quantification focuses on the techniques, on the appropriateness of truncation values, and on the accuracy of the frequencies of the dominant or near-dominant accident sequences. Reviews of the containment analysis, the environmental transport and consequence analysis, and the external event analysis focus on the assumptions, the data used in the analysis, and the accuracy of the final results.

Given appropriate attention to the interim products and the subsequent comments, the review of the draft report can focus on the emphasis placed on the results, on the interpretation of the results, and on verifying that the document is comprehensible and usable. To achieve the latter, it is necessary to ensure that all assumptions are clearly stated, data sources are given, and the results presented are reproducible.

The production of reports is a substantial task. Each analyst can expect to spend 1 to 2 man-months documenting his work. An additional month may be spent incorporating peer comments for the final report. Reports are typically several thousand pages long, and sufficient typing support to produce a draft in one month is desirable. Word-processing equipment is invaluable in this task. Several draftsmen are needed to produce the many drawings needed for the report. These include several event trees, simplified schematics and logic models for each system analyzed, and risk curves for the final product (if desired) in addition to any figures germane to a particular portion of the analysis. A fault-tree graphics capability is highly desirable. Otherwise, the drafting of fault trees may be prohibitively expensive and time consuming.

Estimates of the manpower involved in producing reports for each level of PRA are as follows:

Level	Technical	Support
1	11-22	2-5
2	19-38	4-8
3	23-43	5-9

This chapter has discussed the general approach to, and the management of, probabilistic risk assessments of varying levels. The subsequent chapters of this guide discuss each step of the analysis in detail.

REFERENCES

Carlson, D. D., W. R. Crammond, J. W. Hickman, S. V. Asselin, and P. Cybulskis, 1981. Reactor Safety Study Methodology Applications Program: Sequoyah #1 PWR Power Plant, USNRC Report NUREG/CR-1659.

Commonwealth Edison Company, 1981. Zion Probabilistic Safety Study, Chicago, Ill.

USNRC (U.S. Nuclear Regulatory Commission), 1975. Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), Washington, D.C.

Chapter 3

Accident-Sequence Definition and System Modeling

3.1 INTRODUCTION

This chapter describes methods for the definition of potential accident sequences and the development of system models. The event-tree method is described as a method for modeling plant-level sequences that may lead to public risk. The approach to event-tree development and application is generalized and can be adapted to specific study objectives. The event-tree method has been used in some form in all recent risk assessments for light-water reactors. It is a most suitable means for modeling complex plant-level sequences, and it permits these sequences to be evaluated in an efficient manner.

Several methods for system modeling are described, with emphasis on fault-tree analysis. Fault trees are used in many industrial applications and have proved to be a widely accepted means for evaluating the failure potential of systems. Moreover, the results of system fault-tree models can be easily communicated to technical and management groups.

The integration of event trees and fault trees provides an analytical approach capable of handling the complexities associated with modeling potential accident sequences. It is a proved means for defining and understanding plant design and operation in a manner that leads to the quantification of public risk.

Numerous analytical approaches and a variety of techniques are associated with the combined event- and fault-tree method. Section 3.2 provides an overview of the procedures for accident-sequence definition and system modeling. Sections 3.3 through 3.7 discuss the methods for performing individual analytical tasks. The methods are presented in the approximate order the tasks would be performed in a probabilistic risk assessment (PRA), from plant familiarization through the incorporation of dependent failures into the plant and system models. Section 3.8 summarizes procedures for incorporating the described methods into a coherent approach for a PRA. Section 3.9 discusses the treatment of uncertainty, and Section 3.10 describes provisions for the assurance of technical quality.

The accident-sequence definition task described in this chapter provides a framework for the entire risk assessment. It delineates the set of events that can initiate accident sequences and describes the plant functions that can arrest or control those sequences. Because of its central role in a PRA project, the work of accident-sequence definition must interface directly with the analyses of human reliability (Chapter 4), the physical processes of core-melt accidents (Chapter 7), and external events (Chapters 10 and 11). Furthermore, the models must be developed in a form suitable for the application of numerical input data (Chapter 5) and the methods used in the accident-sequence quantification (Chapter 6).

3.2 OVERVIEW

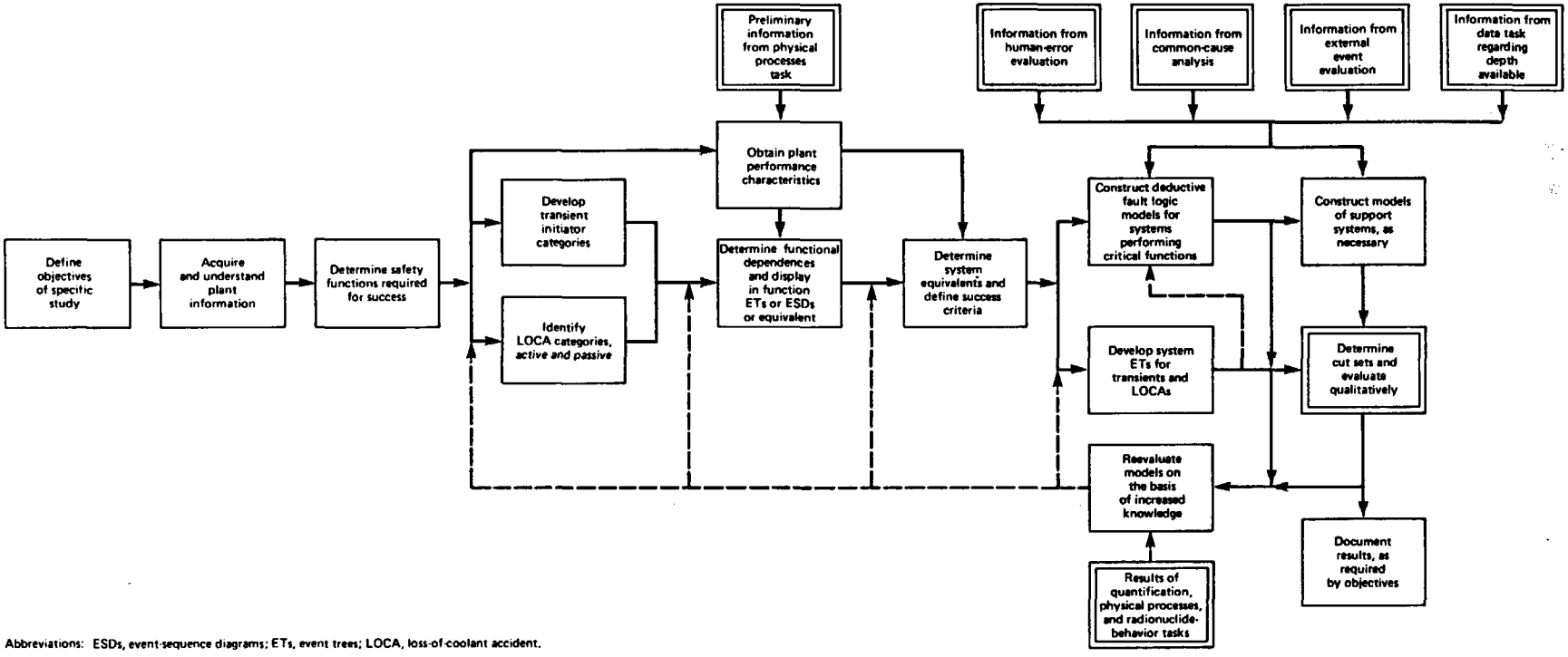
The first step in performing a probabilistic risk assessment is the task of accident-sequence definition and system modeling. This task begins with a definition of the objectives of the study and the acquisition of a substantial amount of information on plant design and operation. It progresses through the generation of plant models, both inductive and deductive, to the identification of possible accident sequences. The process includes the identification of the accident-initiating events, component failures, procedural faults, human errors, and dependent-failure mechanisms that could cause these accident sequences to occur.

This chapter discusses several methods for defining accident sequences and constructing system models. The method selected for sequence identification must produce an inductive plant model that is consistent with the methods chosen for detailed system modeling and for quantifying the frequency and the consequences of the sequences. This is discussed further in the subsequent detailed discussion of the various inductive modeling techniques.

The process of identifying accident sequences is shown in Figure 3-1. This process is iterative, as the construction of the models increases the analyst's knowledge and understanding of plant design and performance characteristics.

The task of defining potential accident sequences must begin with a clear understanding of the objectives of the study. These, in turn, will be used to define the depth of the analysis and to establish bounds on the failure modes considered. For example, it should be recognized at the start that a study used for design optimization or for the selection of optimal testing frequencies may differ substantially from one whose objective is to estimate the risk associated with the given design. Similarly, a study intended to estimate public risk and to provide information on the value of plant modifications aimed at reducing the risk will also differ substantially from those mentioned above. Thus, the level of the risk assessment, as defined in Chapter 2, strongly influences the structure of the models. This is so because the levels of truncation for the analyses of various systems and sequences will depend on the desired product. If the risk assessment includes external events, the system models constructed during this task should include the information necessary to incorporate the common failure modes associated with fires, floods, or earthquakes. Plant characteristics, such as equipment location, should be included in the models, and care must be taken that components with a low probability of random failure (e.g., pipe sections) are not eliminated by a probability truncation. The selection of limits on the analyses must be made on a case-by-case basis, with careful thought given to ensure that the methods used will satisfy the specific objectives of the analysis. It is desirable to keep the models as flexible as possible to accommodate changes or additions to study objectives.

Once the objectives of the study have been defined, the task of familiarization with the plant begins. Plant information must be acquired, and the PRA analysts must become familiar with the details of plant design and



Abbreviations: ESDs, event-sequence diagrams; ETs, event trees; LOCA, loss-of-coolant accident.

Figure 3-1. The process of accident-sequence definition.

operation. This consists of acquiring and analyzing detailed information on the design and operation of the plant and of evaluating experience data and analyses performed for similar plants. The information collected should be retained in a retrievable form, such as plant notebooks. Key features pertinent to the analysis can be collected and displayed as part of preliminary system-analysis descriptions. Details on the type of information needed, contents of the plant notebooks, and the activities performed during this familiarization process are presented in Section 3.3.

Probabilistic risk assessments can be performed at any stage of the development of nuclear plants. They naturally vary in terms of the level of completeness, information available for the analysis, and the intended use of study results. A PRA study performed during the conceptual design phase is generally aimed at comparing competing design concepts and of necessity must be restricted to a low level of detail. Studies conducted during the preliminary or final design phase are aimed at providing additional insights into plant-design features and information on the relative safety or risk of well-formulated designs. Basic information such as design descriptions, preliminary safety analysis reports, and piping and instrumentation diagrams is available, but the lack of detailed design and operational information limits the level of detail that can be included in the study. Detailed information on support-system requirements, instrumentation parameters, and operational and maintenance procedures is typical of information that may be in a preliminary form or not available if a study is performed before the plant is completed.

It is necessary in any PRA study to define a "freeze point," a time after which design or operational changes, if any are made, are not incorporated into the PRA until it is finished the first time. Experience has shown that plant design can change too fast for the PRA to keep up with it. Since a PRA is, by its nature, design specific, if there is no final design, there can be no final PRA. This does not mean that plants in the earlier phases of design cannot be assessed. It means that, no matter what the stage of plant design, the design must be frozen in a particular configuration in order to do the PRA. If the PRA is done early in plant design, more of it will have to be based on assumptions (leading to higher uncertainties) rather than on plant-specific drawings. Even these assumptions will have to be frozen to complete the PRA.

Having or declaring a freeze point does not eliminate the responsibility for finally updating the PRA to include subsequent design changes. For this reason the PRA team should develop models and keep records in a way that facilitates this updating and makes it as convenient as possible.

Having developed an understanding of plant design and method of operation, the analyst defines the required safety functions and initiating events, and develops appropriate groupings of accident-initiating events. These can be listed in various levels of specificity, depending on the analytical techniques and study objectives. If they are used in general terms, the root causes of the initiating event should also be investigated and may be presented appropriately in a fault tree or an equivalent logic

model. This can be done deductively, using a fault-tree approach, or the information can be obtained from a failure modes and effects analysis of system interfaces. In any event, it needs to be presented in a form suitable for documentation that indicates the level of completeness of the analysis.

Initiating events should be grouped by the design features associated with each safety function. Typically, initiating events are divided into two general categories--transients and loss-of-coolant accidents (LOCAs)--and these categories are further subdivided in terms of general characteristics of the plant response. The decision on how finely to subdivide these categories again depends on the degree of detail in the plant model and, to some extent, on the methods used in later stages of the process. Event trees are typically developed for groups of initiating events with similar characteristics rather than individual initiating events. The grouping of initiators defines the number of event trees required and simplifies the analytical process.

The analysts then must evaluate the response of the plant to the identified group of initiating events. Detailed information on safety functions, systems, and operational schemes is required to identify responses and define criteria for successfully meeting the challenges to plant safety. During this phase of the work there is a strong interaction between the analysts developing the accident sequences and those analyzing the physical processes of core-melt accidents.

Using the transient and LOCA grouping of initiating events, the knowledge gained on plant performance characteristics, and preliminary information from the physical processes task described in Chapter 7, the analyst determines functional dependences and constructs function event trees or event-sequence diagrams for the various groups of initiating events. Event trees and event-sequence diagrams are devices that depict the current state of the analyst's knowledge about function and system dependences. Their construction is an inductive process requiring considerable iteration.

It is necessary to convert the function models to system models. This is done by identifying the systems that satisfy the various functions and reconstructing the event tree accordingly. The system event trees can be presented solely in terms of the systems that directly perform the safety functions, or they can include the support systems that are required for the successful operation of the systems performing safety functions. If the former option is chosen, the supporting systems are included in the deductive system logic models. If the latter option is chosen, care must be taken that all known system dependences involving support systems are adequately depicted on the system event tree.

Having constructed system event trees, the analyst should compare the accident sequences thus generated with those identified in previous studies and with operating experience. Using engineering judgment, the event trees are reevaluated to establish that the identified accident sequences are valid and that all important sequences are represented.

Success (or failure) states for systems depicted on the event trees must then be defined to allow the development of the system models. Deterministic analyses may be required in some cases to define the success states realistically since much of the prior analysis of the plant may have been based on the conservative assumptions required by the licensing process. To the extent possible within time and funding constraints, success definitions should be realistic. These definitions, converted to statements of undesired events, constitute the top events of the logic models used to analyze specific system-failure modes.

Deductive system logic models are constructed to determine the causes of system failure. The fault trees, or equivalent logic models, must include not only component failures but also the effects of testing, maintenance, and human errors on system performance. The trees must be constructed in the context of the evaluation being performed. Thus, the depth of analysis depends on both the availability of appropriate data and the objectives of the study. The structure of the trees is also influenced by the techniques used for dependent-failure analysis and the scope of the overall analysis. For example, the faults modeled may differ if it is known that the trees will be used for studies of external hazards like earthquakes or flooding. Details on the various techniques used are presented in Sections 3.5 through 3.7.

The fault tree for any given system must include interfaces with various supporting systems (e.g., ac power, dc power, auxiliary cooling-water systems, heating, ventilation, and air-conditioning systems) unless these are explicitly included in the event-tree model. If supporting systems are considered in the deductive logic models, it is generally more convenient to construct separate fault trees (or equivalent logic models) for the supporting systems. Care must be taken, of course, to ensure that the supporting-system models are developed in the context of the boundary conditions and that plant components are uniquely identified. The nature of this modeling will be affected by the structure of the inductive event-tree models of plant performance.

The construction of fault trees will lead the analyst to a much improved understanding of plant design and method of operation. Therefore, the analyst should reevaluate the work done previously, particularly the event-tree development, to determine whether system-to-system and function-to-function dependences are properly modeled. The search for dependent failures should be performed as described in Section 3.7 and incorporated as appropriate into the plant and system models. As already noted, the event tree is developed inductively and must be subjected to iteration as a more detailed understanding of plant responses and system interactions is acquired.

The interrelationships among specific accident sequences, the physical processes of core-melt accidents (Chapter 7), and radionuclide behavior (Chapter 8) are most important. These involve timing, temperatures, and pressures at the time of core melt as well as the operability of containment safeguards and other systems. Given the complexity of the plant-containment interface, an early effort at defining "plant states," accident-sequence conditions important to the containment analysis, is particularly useful.

The definition of such states will have a definite effect on the configuration of the event trees.

The result of the modeling activity is a set of plant and system models--event trees and fault trees--that are used to characterize the potential outcomes of postulated accident-initiating events. These models can then be evaluated in a manner commensurate with study objectives. Chapter 5 provides information on the development and application of the numerical input data required to quantify the models. Chapter 6, "Accident-Sequence Quantification," describes the methods and approaches for evaluating the plant and system models. There is a strong interaction between the tasks of model development, data development, and quantification.

Two approaches to quantification are described in Chapter 6. In both cases, once the logic models are constructed, the equivalent Boolean expressions are obtained for the various system fault trees and combined to generate equations for the accident sequences identified on the event trees. In one case, however, these are processed to find the minimal cut sets--that is, the minimum number of fault-event combinations that can lead to a given accident sequence. If this approach is taken, it is often useful to obtain a qualitative idea of failure importance by ordering the minimum cut sets according to their size. Because the failure probabilities often decrease by orders of magnitude as the size of the cut set increases, this ranking gives a gross indication of the importance of a cut set. The qualitative evaluation of these accident-sequence cut sets produces valuable information on the nature of potential accident causes, even without detailed quantification, and can be useful in developing system modifications or in improving operating procedures. The analyst must remain aware, however, that common dependences might well cause higher-order cut sets to become important contributors. Thus, the qualitative evaluation is incomplete and must be regarded as such.

This initial qualitative evaluation identifies in a preliminary way the components for which failure-rate information is necessary and defines the context for the quantitative evaluation. Thus, it provides initial input to the data-analysis task described in Chapter 5. The cut sets and accident sequences provide the basic input to the quantification task.

After this type of initial screening process, it is necessary to re-evaluate the fault and event trees through the application of more definitive data, human-reliability and dependent-failure analyses, and, if available, information from the analyses of physical processes and radionuclide behavior. The analyst should iterate, as necessary, to ensure that the plant model reflects the current state of knowledge of the plant.

The accident sequences that are thought to be important must be subjected to a detailed engineering review. This review requires that the postulated phenomena be closely examined and that proper credit be given for the ability of the operator and his staff to cope with, or recover from, the incident. Again, if necessary, the models of the plant should be modified.

The results of the combined accident-sequence definition and system-modeling tasks should be documented in such a way that all assumptions are

clearly delineated. The output information required for other tasks should be tabulated in a convenient form. As always, the specific nature of the documentation depends strongly on the objectives and needs of the study.

3.3 PLANT FAMILIARIZATION

Before the detailed analytical work can begin, it is necessary for the PRA team to become familiar with the design, operation, and maintenance of the plant. All team members should become as familiar as possible with all aspects of the plant to help ensure that function and system dependences are appropriately considered throughout the PRA activity.

A large amount of plant information must be collected and organized for a risk assessment. To facilitate this task, a formalized system for data acquisition and tracking should be established. It is preferable to assign data management to one team member who has overall responsibility for cataloging data, controlling the information within the PRA project team, as well as documenting all requests for additional information and correlating responses.

A focal point for coordinating information on plant operation should also be designated. This should preferably be a person who is a senior employee of the operating utility and is located at the plant site. This person will coordinate all data requests with cognizant onsite personnel and assist in expediting the collection of operational and maintenance information.

Much of the detailed information is needed for review only; it is reduced or reformatted for specific uses during the analysis. Information on overall plant functions and performance that is synthesized from the overall data set should be collected in a single information source supporting event-tree development and the integrated assessment. Information on individual systems should be organized, updated, and retained in the system-analysis notebooks.

Specific types of plant documentation that are necessary for the analysis can be defined at the outset. This information is supplemented by detailed data requests formulated as the study progresses. An important part of the information is obtained from plant visits and interviews with operations and maintenance personnel. These visits should be coordinated to optimize the flow of information to the PRA study team and its use in specific study activities.

A partial list of the sources of information needed to support the task of accident-sequence definition is given in Table 3-1. An attempt was made to relate the data to three major study activities, even though many of the data sources have a general application. The safety analysis report for the plant contains a significant amount of information pertinent to a PRA. However, the use of this information must be carefully considered, particularly in those areas where minimum requirements for equipment

Table 3-1. Sources of the information needed for the definition of accident sequences

Task	Information sources
Plant familiarization and accident review	Operator training manuals Complete final safety analysis report (FSAR) Plant layout drawings Reviews with operating staff Emergency procedures Plant visits
Event-tree development	FSAR Chapters 6 and 15 EPRI NP-2230[a] Licensee event reports from specific plants or sister plants, plant incident reports Performance capability of the emergency core-cooling system and other systems considered in developing system-success criteria Analyses documenting system performance Plant visits
Fault-tree development	FSAR chapters on individual systems and instrumentation System descriptions Piping and instrumentation diagrams Control logic diagrams Drawings of instrumentation power supplies Piping location and routing drawings Power-source documents Drawings of the offsite and onsite power-distribution systems One-line diagrams of the electrical system Circuit diagrams and trip criteria for the electrical bus protection system Normal operating procedures for systems Chapter 16 of the FSAR (i.e., technical specifications) Testing and maintenance procedures and intervals Annunciated system parameters System-response parameters (valve opening times, pump start times) Environments for all essential sensors, detectors, and indicators under normal and accident conditions Any existing failure modes and effects analyses on plant systems Plant visits

[a]ATWS: A Reappraisal, Part 3, "Frequency of Anticipated Transients," Electric Power Research Institute, 1982.

configurations or criteria for meeting functional requirements are derived. Requirements reflecting licensing criteria may be overly conservative for a realistic PRA. Conversely, in important activities like defining success criteria, care must be exercised not to use information that cannot be properly documented and justified.

Additional sources of valuable information are documented risk assessments of similar nuclear power plants. An attempt should be made to obtain available documentation of applicable PRAs. Care should be exercised, however, in reviewing and applying such information because the specific objectives, analytical assumptions, or analytical approaches of another study may have been different.

The information sources in Table 3-1 provide a foundation for study and initial plant-modeling activities. All team members should become familiar with the basic safety functions necessary to prevent core damage or to mitigate its consequences and the systems that perform these functions. They must also know the events that initiate potential accident sequences as well as the success criteria for functions and systems. During the plant-familiarization process, the PRA team investigates those plant-level characteristics to become thoroughly familiar with the key elements (i.e., safety functions, initiating events, function and system criteria) that are fundamental to all subsequent study activities.

As already mentioned, a PRA entails a substantial effort in information collection and management. The appointment of a data manager and an organized method for cataloging and controlling information will greatly enhance the efficiency and orderly conduct of the study.

The plant-familiarization process cannot be strictly specified, as it consists of numerous activities all aimed at gaining an understanding of the plant and its operation. However, some generalized tasks and documentation activities can be pointed out.

An early task in any PRA is the identification and listing of the front-line systems (i.e., the systems that directly perform the safety functions and thereby have a direct impact on the course of a potential accident) and the support, or auxiliary, systems that are associated with each front-line system. Since an understanding of the interactions between systems and the dependence of one system on another is vitally important to any PRA activity, an overview of system operations should be performed to identify dependences between front-line and support systems.

Initial information on accident-initiating events can be obtained from generic lists and the operating history of the plant. The operational responses of the plant, as documented in safety analysis reports and available transient analyses, should be carefully reviewed. All of the information can be brought together in the plant and systems notebook, which will be updated as the study progresses.

In addition, it may be desirable to systematically perform a preliminary qualitative analysis of each system that might either initiate or affect accident sequences. A comprehensive list of plant systems is drawn up, and a partial analysis is performed for each system on the list.

A detailed analysis should be made later only for selected systems found to be important through further analysis. Some systems that are not important to mitigation can initiate accident sequences. A preliminary systems analysis can thus be a vital step in the search for initiators, helping to ensure completeness in the definition of accident sequences.

If this approach--a preliminary qualitative analysis--is taken, a partial system description (PSD) is written for each system. These PSDs document the information on which the importance of the system (i.e., its role in the initiation and mitigation of sequences) is based. The PSDs for systems found to be not important need not be developed any further. The PSDs for systems that are analyzed in detail will become part of a complete system-description notebook.

Plant familiarization provides baseline information for starting the definition of accident sequences and the modeling of plant systems. Initial requirements for the types and number of event trees should be developed and documented, key systems should be identified, and their success criteria should be defined. The team of analysts will be loosely divided into two groups, one concerned with sequence definition and the other with system modeling. These activities can begin concurrently, with maximum attention given to interaction and communication between the two groups. Although the two activities are distinct, an analyst may be involved in both of them, further enhancing his overall understanding of the assessment.

It is during the plant-familiarization process that the PRA team becomes familiar not only with the plant but also with the different analytical tasks to be performed and the role that each team member will play. It is important that team members understand the basic methods associated with their portion of the assessment and how their activity is integrated into the overall PRA process.

3.4 EVENT-TREE DEVELOPMENT

Quantification of the risk associated with a commercial nuclear power plant requires the delineation of a large number of possible accident sequences. Because nuclear systems are complex, it is not feasible to write down by inspection a listing of important sequences. A systematic and orderly approach is required to properly understand and accommodate the many factors that could influence the course of potential accidents.

The event tree in Figure 3-2 illustrates by example the logic used in developing an event tree. Its purpose is not to show a typical function or system tree, but rather to show the general event-tree process and how events of various types are reordered and evaluated as a result of the process. The initiating event is assumed to be a LOCA associated with a simple imaginary reactor system. The various event possibilities representing the systems or functions necessary to mitigate the consequences of the accident are listed across the top of the event tree.

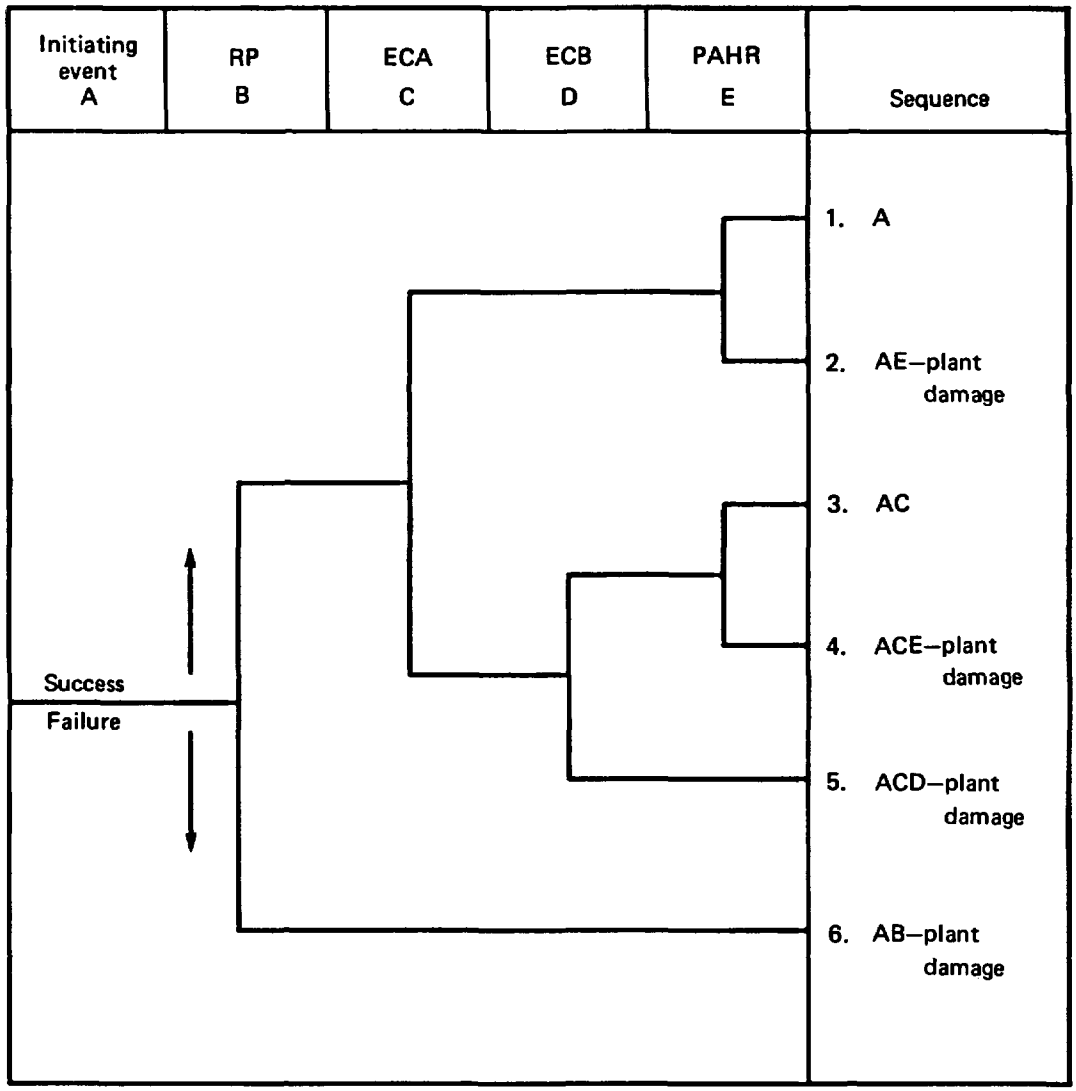


Figure 3-2. An example of a simple event tree. (See page 3-13 for an explanation of symbols.)

In an actual event tree, either systems or functions can serve as event-tree headings. There is considerable latitude as to the definition of event headings. The example in Figure 3-2 shows components, systems, and functions on the same tree in order to illustrate the variety of event-tree headings.

The end result of each sequence is assumed to be either the safe termination of the postulated sequence of events or some plant-damage state. In developing event trees for a specific plant, care must be taken in specifying the expected plant-damage state. Simple assumptions of core melt or no core melt should be avoided.

Care must be exercised to ensure that the event headings are consistent with actual plant-response modes and to ensure that the heading can be

precisely related to system-success criteria that can be translated to top events for system-fault modeling. For the example selected, the initiating event is a pipe break in the reactor-coolant system. The other headings are as follows:

RP = Operation of the reactor-protection system to shut down the reactor

ECA = Injection of emergency coolant by pump A

ECB = Injection of emergency coolant by pump B

PAHR = Post-accident decay-heat removal

The placement of these events across the tree is based on either the time sequence in which they occur, proceeding from left to right, or some other logical order reflecting operational interdependence. Consequently, the initiating event is shown first and the PAHR function is shown last.

The various sequences are represented by the paths developed by following the vertical and horizontal lines beneath the events. At a junction between a horizontal and vertical line, the system is successful if the path is upward; the system fails if the path is downward. The column at the far right of the tree identifies the various sequences. For example, sequence AE would be the sequence starting with the initiating event, A, and ending with failure of the PAHR function, E.

For this sample event tree, it was assumed that either emergency coolant pump A or B is sufficient to satisfy the emergency coolant requirement. With this in mind, each of the sequences shown is briefly described below to explain why there are no success or failure options for some of the sequences.

In sequence A, as in all sequences, it is assumed that the pipe break has occurred. The reactor-protection system is successful, emergency coolant pump A is successful, and the PAHR systems are successful. No success or failure path need be shown for emergency coolant pump B (event D): since pump A is sufficient for the cooling requirements, the success or failure of pump B makes no difference.

Sequence AE is the same as sequence A, except that the PAHR function (event E) has failed. This sequence is assumed to result in a plant-damage state.

In sequence AC, pump A (event C) has failed; however, pump B (event D) is successful, and no plant damage occurs.

Sequence ACE is the same as AC, except that the PAHR function (event E) has failed. This failure results in a plant-damage state.

In sequence ACD, both pumps A and B (events C and D) have failed. Because this combination of events is assumed to result in a plant-damage

state, the success or failure of PAHR is of no concern. Consequently, no success or failure option is shown for event E.

In sequence AB, the reactor-protection system has failed and the success or failure of the remaining events is not considered, as a plant-damage state is assumed to occur.

Because headings ECA and ECB result in the same consequences and do not result in different boundary conditions on the downstream systems, they could have been included in one event-tree heading.

Figure 3-2 illustrates the method of accounting for the time relationships and system interfaces that follow a given accident. It also demonstrates how the number of possible sequences to be analyzed can be reduced. The total number of possible sequences in the sample problem is 16. By using the event tree, this number has been reduced to only four core-melt sequences that need to be evaluated in more detail. In general, if there are no event headings representing system functional responses, there are 2^n potential sequences associated with each initiating event. Because of the logic inherent in the event-tree process, only meaningful sequences are retained for further evaluation and illogical sequences are eliminated during the development of the tree, thus greatly reducing the total number of sequences to be evaluated.

The event tree is the basic analytical tool that has been most frequently used for the organization and characterization of potential accidents. Two general types of event trees are used in PRAs: system event trees and containment event trees. System event trees, discussed in this section, are developed to relate system responses to identified initiating events and represent distinct system accident sequences. A system accident sequence consists of an initiating event and a combination of various system successes and failures that lead to an identifiable plant state. Containment event trees, described in Chapter 7, are developed to relate possible containment responses to those plant states that could lead to a release of radionuclides.

For a level 1 PRA, only the system accident sequences are developed. A level 1 PRA identifies the potential accident sequences that may lead to core damage. No attempt is made to define the consequences of identified accident sequences other than determining whether or not the sequences would lead to core damage. The containment analysis for a level 1 PRA is limited to an analysis of containment systems to determine impacts on sequences leading to core damage.

Level 2 and 3 PRAs must include a detailed evaluation of containment response to system accident sequences. When such PRAs are performed, both system event trees and containment event trees are used to describe complete accident sequences.

Figure 3-3 shows the basic elements involved in the development of system event trees. Task elements 1 through 5 are central to any approach taken for event-tree development. Acceptable methods for performing the various individual tasks are described below.

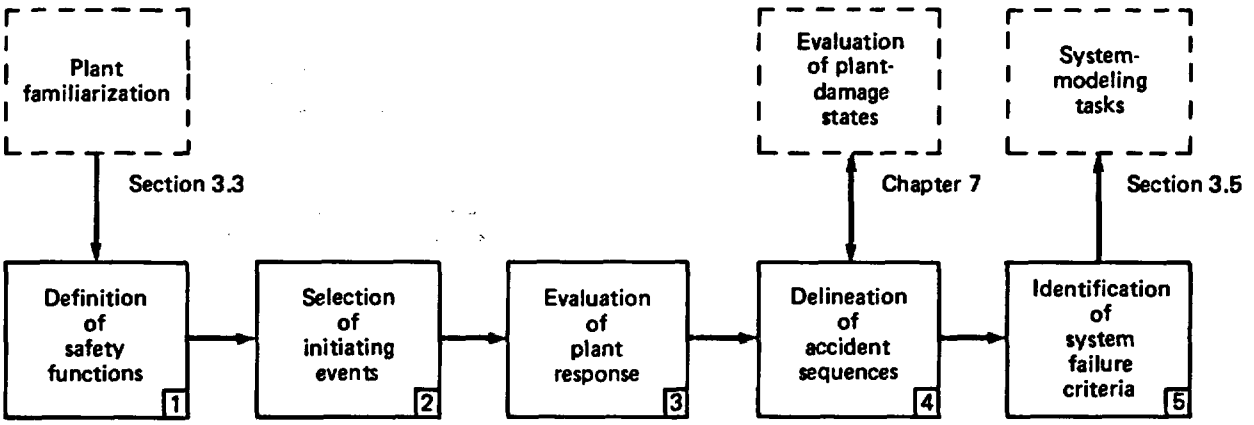


Figure 3-3. Generalized process of event-tree development.

3.4.1 DEFINITION OF SAFETY FUNCTIONS

The functions that must be performed to control the sources of energy in the plant and the radiation hazard are called "safety functions." The concept of safety functions forms the basis for selecting accident-initiating events and delineating potential plant responses. Generally, safety functions are defined by a group of actions that prevent core melting, prevent containment failure, or minimize radionuclide releases. Such actions can result from the automatic or manual actuation of a system, from passive system performance, or from the natural feedback inherent in the design of the plant.

Safety functions can be defined in many different ways, depending on the plant type, the system design, the timing of system responses, and the preference of the analyst. Table 3-2 shows one grouping of typical safety functions and their intended purposes.

Typically, safety functions can be considered within a certain hierarchical framework. Reactivity control is the foremost function because the amount of heat that must be removed from the core depends on how well this function is accomplished. Next in precedence are the functions for appropriately cooling the core. Core cooling requires the performance of actions needed to provide fluid flow through the core, to maintain an adequate inventory in the reactor-coolant system (RCS), and to maintain an appropriate RCS pressure. If the core heat is not removed, then the removal of heat from the RCS is irrelevant. This kind of logic illustrates the logic used in structuring the basic safety functions for the plant under evaluation.

Definition of the necessary safety functions forms the preliminary basis for grouping accident-initiating events. It also provides the structure for defining and grouping systems in order to define a complete set of system responses and interactions for each class of accident-initiating events.

Table 3-2. Safety-function purposes[a]

Safety function	Purpose
Reactivity control	Shut reactor down to reduce heat production
Reactor-coolant-system inventory control	Maintain a coolant medium around the core
Reactor-coolant-system pressure control	Maintain the coolant in the proper state
Core-heat removal	Transfer heat from the core to a coolant
Reactor-coolant-system heat removal	Transfer heat from the core coolant
Containment isolation	Close openings in containment to prevent radionuclide releases
Containment temperature and pressure control	Keep from damaging containment and equipment
Combustible-gas control	Remove and redistribute hydrogen to prevent an explosion inside containment

[a]From Corcoran et al. (1980).

Additional distinction may be needed in the definition of safety functions to differentiate between classes of initiating events. The function of controlling the reactor-coolant inventory, for example, may include the maintenance of RCS integrity for most transients, but for LOCAs the control of coolant inventory depends primarily on makeup.

3.4.2 SELECTION OF ACCIDENT-INITIATING EVENTS

The objective of event-tree development is to define a comprehensive set of accident sequences that encompasses the effects of all realistic and physically possible potential accidents involving the reactor core. By definition, an initiating event is the beginning point in the sequence. Hence, a comprehensive list of accident-initiating events must be compiled to ensure that the event trees properly depict all important sequences.

The selection of initiating events for inclusion in event trees consists of two steps:

1. Definition of possible events.

2. Grouping of identified initiating events by the safety function to be performed or combinations of system responses.

A clear understanding of the general safety functions and features incorporated into the plant design, supplemented by the preliminary system reviews, will provide the initial information necessary to select and group the initiating events.

Two approaches can be taken in identifying the accident-initiating events. One is a comprehensive engineering evaluation, taking into consideration information from previous risk assessments, documentation reflecting operating histories, and plant-specific design data. The information is evaluated and a list of initiating events is compiled, based on the engineering judgment derived from the evaluation. Another approach is to more formally organize the search for initiating events by constructing a top-level logic model and then deducing the appropriate set of initiating events. Portions of each approach can be effectively used as appropriate to define and display the accident-initiating events. The two approaches are described below in Sections 3.4.2.1 and 3.4.2.2.

3.4.2.1 Comprehensive Engineering Evaluation

The focus of a PRA for a nuclear power plant is the release of radionuclides from a damaged core. There are two major types of accidents with the potential for core damage in light-water reactors: transient events and LOCAs. The identification of accident-initiating events can be done by making a list of potential plant-specific events for each of the two types of potential accidents.

Although each type of accident can be treated separately in developing a list of initiating events, it must be recognized that certain transient sequences can result in the loss of RCS inventory. The distinction between LOCAs and transient events has been carried over from licensing-type evaluations and is used only for convenience in a PRA study. It is retained in this discussion only for the sake of tradition.

The reactor-coolant system and its interfaces with other systems should be surveyed to determine all possible breaks that could result in a loss of reactor-vessel inventory. A complete spectrum of LOCA sizes, or breaks, in the reactor-coolant system should be considered. Typically the number of LOCA types can be reduced to three or four break sizes, grouped by mitigation requirements, each requiring a separate event tree. The size and the location of the break are the two important parameters to be considered in selecting LOCA-initiating events.

In addition to the search for pipe breaks, it is also important to survey the reactor-coolant system for the potential of coolant-inventory loss by other means. A systematic search of the reactor-coolant pressure boundary should be performed to identify any active elements that could fail or be operated in such a manner as to result in an uncontrolled loss of coolant. Particular attention should be paid to elements, such as safety relief valves, whose failure to reclose could result in a loss of RCS inventory that might be induced by a transient. Figure 3-4 shows the format that can be used for a summary documentation of the search for active components whose failure can result in an event that results in a loss of RCS inventory.

Transient initiators are more complex events and thus more difficult to characterize for event-tree development. The EPRI report on anticipated

LOCA site	Description	Effective break size	Primary system symptoms	Effects on other systems	Automatic compensating action	Comments
FCV 74-67 Coolant recirculation and RHR injection line Vessel penetrations H2F, H2G, H2H, H2J, H2K	If the check-valve function of FCV 74-68 fails, the inadvertent opening of FCV 74-67 exposes low-pressure RHR piping to reactor operating pressure	3.14 ft^2 (24-in. diameter) Water break	1. Rapidly decreasing reactor water level 2. Rapidly decreasing reactor pressure 3. Drywell pressure unaffected	Rupture of RHR	Reactor scram on low water level	
FCV 74-47 Coolant recirculation and RHR return line Vessel penetrations H2F, H2G, H2H, H2J, H2K, H1A, H15	If FCV 74-47 and FCV 74-48 are inadvertently opened, low-pressure piping is exposed to reactor operating pressure	2.18 ft^2 (20-in. diameter) Water break	See FCV 74-67	Rupture of RHR	Reactor scram on low water level	
FCV 74-53 Coolant recirculation and RHR injection line	If the check-valve function of FCV 74-54 fails, the inadvertent opening of FCV 74-53 exposes low-pressure piping to reactor operating pressure	3.14 ft^2 (24-in. diameter) Water break	See FCV 74-67	Rupture of RHR	Reactor scram on low water level	
13 PCVs 1-41, 1-80, 1-42, 1-30, 1-31, 1-34, 1-18, 1-19, 1-22, 1-23, 1-4, 1-179, 1-5	Inadvertent opening of any of these PCVs results in a LOCA that discharges primary coolant into the suppression chamber	0.20 ft^2 each (6-in. diameter) Steam break	1. Turbine-pressure regulator will attempt to control pressure 2. Pressure and water-level responses are unknown--depend on the number of valves that open	Temperature of the suppression pool will increase	Time and signal of reactor scram undetermined--depend on number of valves opening	

Figure 3-4. Example of format for documenting the search for an active component whose failure can induce a loss of RCS inventory.

transients without scram (EPRI, 1982) provides a starting point by describing initiating events from the operating histories of both BWRs and PWRs. Tables 3-3 and 3-4 summarize potential initiating events for each reactor type. Although these tables are purported to contain events that have led to reactor trips, some of the entries represent complex events that include failures that occurred after a reactor trip. Hence, in using such a list, care must be taken to ensure that the events chosen are properly defined for the grouping and modeling of potential accident sequences. Any such generic list must be checked for applicability to a specific plant before it is used and should not be regarded as a complete or exhaustive set of potential initiating events. If the plant under consideration has a history of operation, all available information on the occurrence of transient events should be used to supplement the generic data.

Table 3-3. List of BWR transient initiating events[a]

1.	Electric load rejection
2.	Electric load rejection with turbine bypass valve failure
3.	Turbine trip
4.	Turbine trip with turbine bypass valve failure
5.	Main-steam isolation valve (MSIV) closure
6.	Inadvertent closure of one MSIV
7.	Partial MSIV closure
8.	Loss of normal condenser vacuum
9.	Pressure regulator fails open
10.	Pressure regulator fails closed
11.	Inadvertent opening of a safety/relief valve (stuck)
12.	Turbine bypass fails open
13.	Turbine bypass or control valves cause increase in pressure (closed)
14.	Recirculation control failure--increasing flow
15.	Recirculation control failure--decreasing flow
16.	Trip of one recirculation pump
17.	Trip of all recirculation pumps
18.	Abnormal startup of idle recirculation pump
19.	Recirculation pump seizure
20.	Feedwater--increasing flow at power
21.	Loss of feedwater heater
22.	Loss of all feedwater flow
23.	Trip of one feedwater pump (or condensate pump)
24.	Feedwater--low flow
25.	Low feedwater flow during startup or shutdown
26.	High feedwater flow during startup or shutdown
27.	Rod withdrawal at power
28.	High flux due to rod withdrawal at startup
29.	Inadvertent insertion of control rod or rods
30.	Detected fault in reactor protection system
31.	Loss of offsite power
32.	Loss of auxiliary power (loss of auxiliary transformer)
33.	Inadvertent startup of HPCI/HPCS
34.	Scram due to plant occurrences
35.	Spurious trip via instrumentation, RPS fault
36.	Manual scram--no out-of-tolerance condition

[a]From ATWS: A Reappraisal, Part 3 (EPRI, 1982).

Table 3-4. List of PWR transient initiating events[a]

1.	Loss of RCS flow (one loop)
2.	Uncontrolled rod withdrawal
3.	Problems with control-rod drive mechanism and/or rod drop
4.	Leakage from control rods
5.	Leakage in primary system
6.	Low pressurizer pressure
7.	Pressurizer leakage
8.	High pressurizer pressure
9.	Inadvertent safety injection signal
10.	Containment pressure problems
11.	CVCS malfunction--boron dilution
12.	Pressure, temperature, power imbalance--rod-position error
13.	Startup of inactive coolant pump
14.	Total loss of RCS flow
15.	Loss or reduction in feedwater flow (one loop)
16.	Total loss of feedwater flow (all loops)
17.	Full or partial closure of MSIV (one loop)
18.	Closure of all MSIVs
19.	Increase in feedwater flow (one loop)
20.	Increase in feedwater flow (all loops)
21.	Feedwater flow instability--operator error
22.	Feedwater flow instability--miscellaneous mechanical causes
23.	Loss of condensate pumps (one loop)
24.	Loss of condensate pumps (all loops)
25.	Loss of condenser vacuum
26.	Steam-generator leakage
27.	Condenser leakage
28.	Miscellaneous leakage in secondary system
29.	Sudden opening of steam relief valves
30.	Loss of circulating water
31.	Loss of component cooling
32.	Loss of service-water system
33.	Turbine trip, throttle valve closure, EHC problems
34.	Generator trip or generator-caused faults
35.	Loss of all offsite power
36.	Pressurizer spray failure
37.	Loss of power to necessary plant systems
38.	Spurious trips--cause unknown
39.	Automatic trip--no transient condition
40.	Manual trip--no transient condition
41.	Fire within plant

[a]From ATWS: A Reappraisal, Part 3 (EPRI, 1982).

The accident-initiating events must be grouped by safety function or system response. This reduces the number of event trees needed to represent all initiating events. All initiating events in a given group would require the same set of system actions. The groups of events can be further refined by examining specific system responses and associated temporal considerations. Event-tree development is very much an iterative process. The identification and grouping of initiating events will be modified and updated as information from subsequent task elements is refined.

3.4.2.2 Master Logic Diagram

A summary fault tree, or master logic diagram (MLD), can be constructed to guide the selection and grouping of accident-initiating events and to ensure completeness. An example of one possible master logic diagram is shown in Figure 3-5.

The event "excessive offsite release" of radionuclides is the top event. The events in the MLD are identified by the level they appear in the tree, with the top being level 1. The use of levels is an ordering technique to assist in locating events by approach to an offsite release. The strategy is to achieve completeness of events by level.

"Excessive offsite release," level 1, can result from either (OR gate) an excessive direct release or an excessive indirect release. Since these and only these release paths exist at a nuclear power plant, level 2 is complete. An excessive direct release, from the spent-fuel pool and the like, is usually an insignificant contributor to risk. An excessive indirect release would require extensive core damage, failure of the RCS pressure boundary, and containment failure (AND gate); level 3 in the sample MLD is therefore also complete. For these three events to occur, some of the safety functions listed in Table 3-2 would have to fail. Therefore, the inclusion of safety functions completes level 4.

When the diagram reaches level 5, equipment failures or misoperations that could threaten each safety function are identified. A comprehensive listing of such events should define all important accident-initiating events.

The initiating events defined by the MLD are already grouped by the safety function they most threaten. However, "safety function most threatened" is usually not sufficiently descriptive to serve as the sole means for grouping initiators. Usually, a further breakdown according to more specific mitigating-system requirements is necessary. Table 3-5 is a summary listing of some of the safety functions, initiating events, and system-response groupings derived from the MLD shown in Figure 3-5.

3.4.3 EVALUATION OF PLANT RESPONSE

Once accident-initiating events have been identified and grouped, it is necessary to determine the response of the plant to each group. Two distinct methods for evaluating plant response are described here. One uses a function event tree as an intermediate analytical step for sorting out the complex relationships between accident initiators and system responses. The other method employs a detailed event-sequence analysis to explicitly define the response of key plant systems.

Detailed information on plant functions, systems, and operational schemes is required to identify expected responses and define criteria for successfully meeting the identified challenges. The plant-response evaluation determines how realistic or conservative the study will be. If

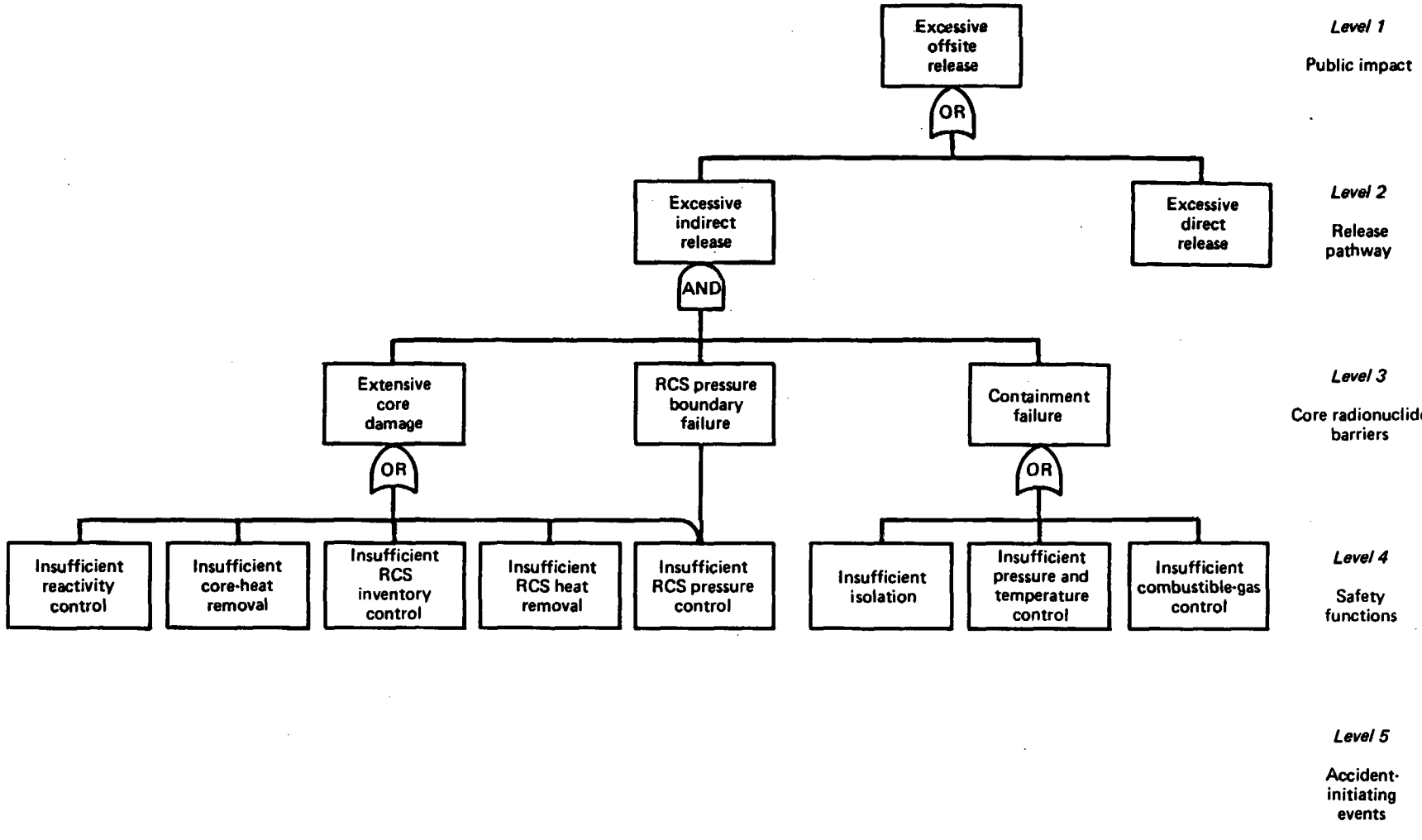


Figure 3–5. Master logic diagram. See Table 3–5 for a summary listing of the safety functions, initiating events, and system-response groupings derived from this master logic diagram.

Table 3-5. Examples of initiating events from a master logic diagram

Threatened safety function	Threatening effect	Front-line source of threat (initiating event)	Examples of cause of threat
Reactivity control	Rapid insertion of positive reactivity	1. Excessive rod-group withdrawal	CRDCS failure
		2. Excessive rod withdrawal	ICS imbalance on auto-to-manual switchover
	Rapid insertion of positive reactivity + small loss of RCS inventory	Control-rod ejection	CRD weld failure
	Rapid insertion of a little negative reactivity	Control-rod drop; control-rod-group drop	CRD power-supply failure
	Slow insertion of negative reactivity	Inadvertent boration	LDPS malfunction
	Slow insertion of positive reactivity	Inadvertent deboration	LDPS malfunction
	Rapid insertion of a lot of negative reactivity	Inadvertent reactor trip	Instrumentation noise; inadvertent or intentional manual scram; RPS test errors; inadvertent fast transfer to CT1; xenon oscillation
RCS inventory control	Small loss of RCS inventory (nonisolatable, inside containment)	1. Small RCS pipe breaks	
		2. Inadvertent PSV opening	
		3. RCS seal failure	Loss of seal cooling
		4. CRDM seal leakage	
	Intermediate loss of RCS inventory (nonisolatable, inside containment)	Medium RCS pipe breaks	
	Large loss of RCS inventory (nonisolatable, inside containment)	Large RCS pipe breaks	
	Isolatable RCS-inventory loss inside containment	Inadvertent PORV opening	Control system failure
	Isolatable RCS-inventory loss outside containment	Letdown or sample-line break; letdown relief valve opening	
	Loss of RCS inventory and ECCS flow to core	Reactor-vessel rupture	
	Loss of RCS inventory to steam generator	Steam-generator tube leak	
	Decrease in RCS inventory without coolant spillage	Charging < letdown	LPDS malfunctions
	Increase in RCS inventory	Charging > letdown	LPDS malfunctions; inadvertent HPI actuation
RCS pressure control	Increase or decrease in RCS pressure with no change in inventory	Pressurizer heater fails on	Control-system malfunction
Core-heat removal	Decrease in flow rate through core	1. RCP trip	Low-flow indication--real or spurious
		2. RCP shaft seizure/break	Loss of lubricating-oil cooling
	Decrease in flow rate through core; no RCP speed change	Core internals vent valve seizes open	
	Change in flow distribution; no RCP speed change	Core flow blockage	Corrosion; crud buildup
RCS heat removal	Increase in steam flow, no loss of inventory, isolatable	1. Turbine control valve open	TBV power failure; momentary decrease in condenser vacuum; turbine pressure failure; ICS malfunction; increase in electrical demand
		2. Inadvertent opening of TBV	
	Large increase in steam flow, no loss of inventory, isolatable	Inadvertent opening of all TBVs	ICS failure

information from the safety analysis report is used, its conservative bias must be taken into account. It is important to apply the most realistic information available in terms of the pressure, temperature, flow rates, and timing characteristics associated with systems designed to respond to accident-initiating events. Such information can be derived from analyses of transients by the utility or vendor-supplied thermal-hydraulics calculations that can be justified and referenced.

It should be noted that in some PRAs a formally documented evaluation of plant responses was omitted, and system event trees were developed directly from the information described in the preceding sections. This usually can be done only by analysts who are very familiar with plant design and responses to accident-initiating events. Such engineering judgment is very valuable to the risk-assessment process, but a typical PRA would benefit from a formally documented approach, as described in the sections that follow.

3.4.3.1 Analysis of Function Event Trees

The use of function event trees to evaluate plant responses requires the development of an event tree that orders and depicts safety functions according to the mitigating requirements of each group of initiating events. The headings of the function event tree are statements of safety functions that can be translated in terms of the systems performing each function. Success criteria are then defined for each of these systems. This stepwise process provides the information needed for preparing the more detailed system event trees that delineate the system accident sequences.

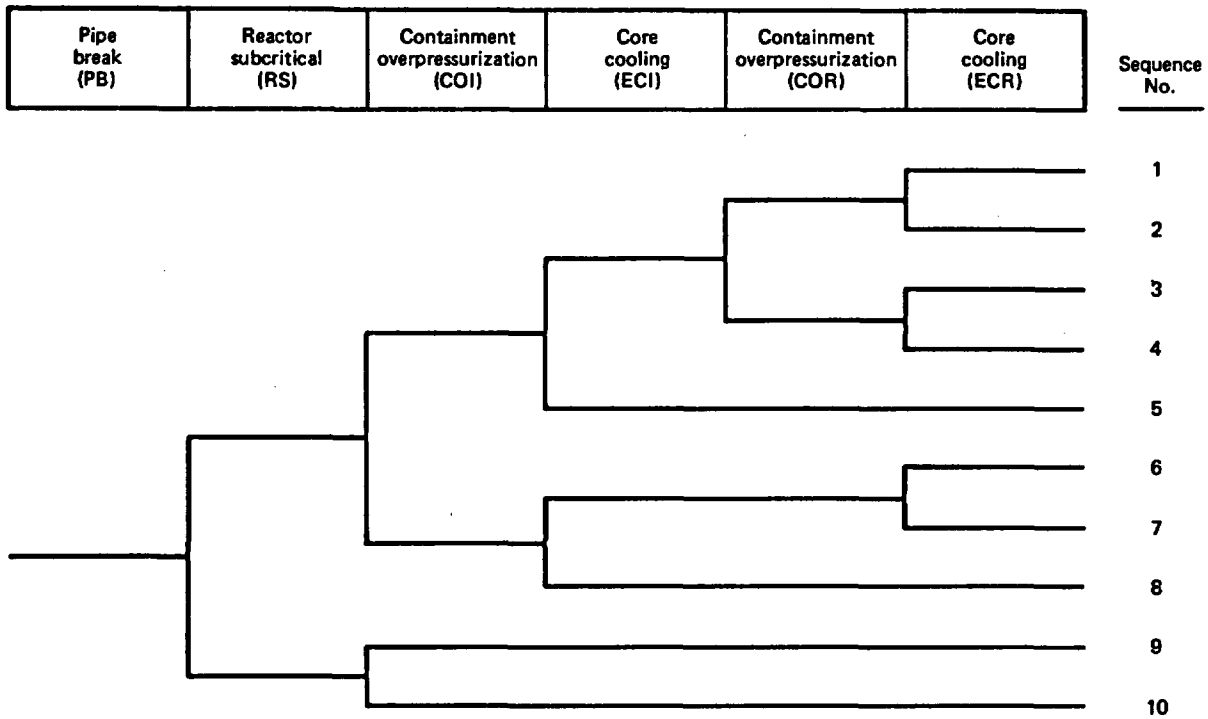
Function event trees are developed for each group of initiators because each group generates a distinctly different plant response. The function event tree is not an end product; it is an intermediate step that provides a baseline of information and permits a stepwise approach to sorting out the complex relationships between potential initiating events and the response of mitigating features. It is the initial step in structuring plant responses to accident conditions in a temporal format. The top events of function event trees are eventually decomposed into statements of system operation or unavailability that can be quantitatively measured.

In constructing the event tree, the analyst considers the functions required to prevent core damage, potential consequences, and the relationships between safety functions. For example, if the RCS inventory is not maintained, then RCS heat removal cannot be accomplished. This could result in eliminating the choice for RCS heat-removal sequences where the RCS inventory is not successfully maintained.

Figure 3-6 shows a typical function event tree for a large LOCA. The functions considered in developing this event tree are as follows:

1. Reactor subcritical (RS): termination of the fission process.

2. Containment overpressure (COI): initial suppression of blowdown by steam condensation only.



Seq. No.	RS	COI	ECI	COR	ECR	Remarks
1						Core cooled
2					f	Slow melt
3				f		Core cooled
4				f	f	Slow melt
5			f	NA	NA	Melt
6		f		NA		Core cooled
7		f		NA	f	Slow melt
8		f	f	NA	NA	Melt
9	f		NA	NA	NA	Melt
10	f	f	NA	NA	NA	Melt

f = function failure; NA = not applicable.

Figure 3-6. Example of a function event tree for a large-break LOCA.

3. Core cooling (ECI): initial removal of core heat by coolant-inventory makeup only.

4. Containment overpressure (COR): containment temperature and pressure control by steam suppression and heat rejection.

5. Core cooling (ECR): addition of heat rejection to coolant makeup.

The function event tree serves as a guide for the development of system event trees. The determination of potential core damage and/or consequences in the system trees must be consistent with the basic results of the function event trees.

Each safety function that is an event-tree heading is performed by a collection of systems. Some systems may perform more than one function or

portions of several functions, depending on plant design. It is necessary to determine which systems are required to successfully perform each safety function to establish the headings of the system event tree. Figure 3-7 is an example of documentation for function-success criteria, in terms of mitigating systems, for a large LOCA.

Some safety functions will be performed by different systems, depending on the accident. Information about the level of detail to which the systems are specified is fed iteratively back into the classification of accidents. For example, the control of reactor-coolant inventory may require only high-pressure coolant-injection systems for a small LOCA and only low-pressure coolant-injection systems for a large LOCA.

The definition of functional success in terms of systems will include primarily the engineered safety features of the plant. However, other systems may also provide necessary or backup mitigating actions. For example, the power-conversion system could contribute to the RCS heat-removal function for transients and very small LOCAs and therefore would be included among the systems that perform this safety function.

Support systems, such as component-cooling water and electric power, do not directly perform the required safety functions. However, they could significantly contribute to the unavailability of a system or group of systems that perform safety functions. Therefore, it is necessary to define the support systems for each front-line system and to include them in the system analysis.

Specific success criteria for each system that performs safety or support functions must be established. In addition to a performance definition (e.g., flow rate, response time, trip limits), these success criteria must be stated in discrete hardware terms, such as the number of required pumps, flow paths, instrument trains, or power buses. This hardware definition will support the fault-tree analysis of systems and the construction of the system event trees. The system-success criteria should also, as appropriate, address the joint operation of systems. For example, for some initiating events at a BWR, low-pressure makeup systems can be used only in conjunction with depressurization systems.

Definitions of joint operation will assist in eliminating meaningless sequences. Response-time definitions will help determine the order of the headings. The required complement of equipment for each system will reveal when failure in one mode of system operation will not induce a failure in a subsequent mode. This system-success information along with the functional relationships will determine which sequences are to be included in the system event tree.

3.4.3.2 Event-Sequence Analysis

Event-sequence analysis is another method used to identify the complex relationships between accident-initiating events and detailed system responses. Event-sequence diagrams (ESDs) are developed for each group of initiating events. The ESD is an analytical tool intended to facilitate

Break type and size	Reactor subcritical	Coolant injection		Coolant recirculation	
		Containment overpressure	Core cooling[a]	Containment overpressure	Core cooling
BREAK LOCATION: SUCTION					
Water, 0.3 to 4.3 ft^2	No more than 30 rods scattered throughout the core not fully inserted OR No more than 5 adjacent rods not fully inserted	Adequate suppression-pool level and no bypass leakage from drywell to wetwell	2 of 2 core-spray loops and 2 of 4 LPCI pumps OR 1 of 4 LPCI pumps OR 1 of 2 core-spray loops and 2 of 4 LPCI pumps (one LPCI pump per injection loop)	1 of 2 CADS trains	2 of 4 RHR pumps with associated heat exchangers
BREAK LOCATION: DISCHARGE					
Steam, 1.4 to 4.1 ft^2			2 of 2 core-spray loops OR 1 of 2 core-spray loops and 1 of 4 LPCI pumps 2 of 2 core-spray loops OR 4 of 4 LPCI pumps OR 1 of 2 core-spray loops and 1 of 4 LPCI pumps		

[a]A core-spray loop is defined as the rated two-pump flow from that loop.

Figure 3-7. Example of format for documenting function-success criteria, in terms of mitigating systems, for a large-break LOCA.

the collection and display of information required for developing system event trees. Its objective is to illustrate all possible success paths from a particular accident-initiating event to a safe-shutdown condition. The ESDs tend to include a significant amount of design and operational information relative to the potential success paths. Their construction is an iterative process with input from various PRA team members, particularly those who have transient analysis, operational, and simulator experience.

One useful aspect of the ESD is its capability to document the assumptions used in an event-tree analysis. The ESD can be very detailed, explicitly showing all the sequence options considered by the analyst. When simplifying assumptions are made in the event trees to facilitate quantification and to render the logic more tractable, the ESD can be used to demonstrate why such assumptions are believed to be bounding (conservative) or probabilistically justified.

In accomplishing a safety function, the effectiveness of a particular success path noted on an ESD depends in general on what systems are operable in the plant and on whether or not the process variables are within the design range of the particular system or subsystem. The method of accomplishing a safety function depends on the state of the plant at the time of an event, as affected by the event, the operator, and system actions.

Figure 3-8 shows a portion of one type of ESD. Each block represents a system performing a mitigating action, as indicated by the description on the right. Each action is initiated by the signals shown in the circles coming into the block from the left. Manual actuation of the system is indicated by the "M" in the bottom of the action block. Blocks without an "M" indicate automatic actuation. All actions appear in approximate temporal order.

The line that branches off from the heavy line above each block in Figure 3-8 indicates an alternative success path given that the expected mitigating action has failed or has failed to be performed. As many possible alternative success paths as are available are shown to the right of each expected action. After the various alternatives (usually safety and nonsafety actions within the normal design bases) are tried and none succeed, then an oval is used to indicate special conditions like "failure to scram" or "excessive cooldown." The systems required to mitigate these special conditions are shown on another page of the ESD, as indicated by the transfer symbol on the oval.

In addition to documenting the agreement on the expected plant response to each initiating event, event-sequence analysis delineates the required operator/system interactions for the human-factors evaluation. The ESDs also help disseminate information to all project participants about how the plant has been assumed to respond to initiating events and helps in coordinating the development of accident sequences by documenting for the systems analyst which systems in the system event trees must be further analyzed.

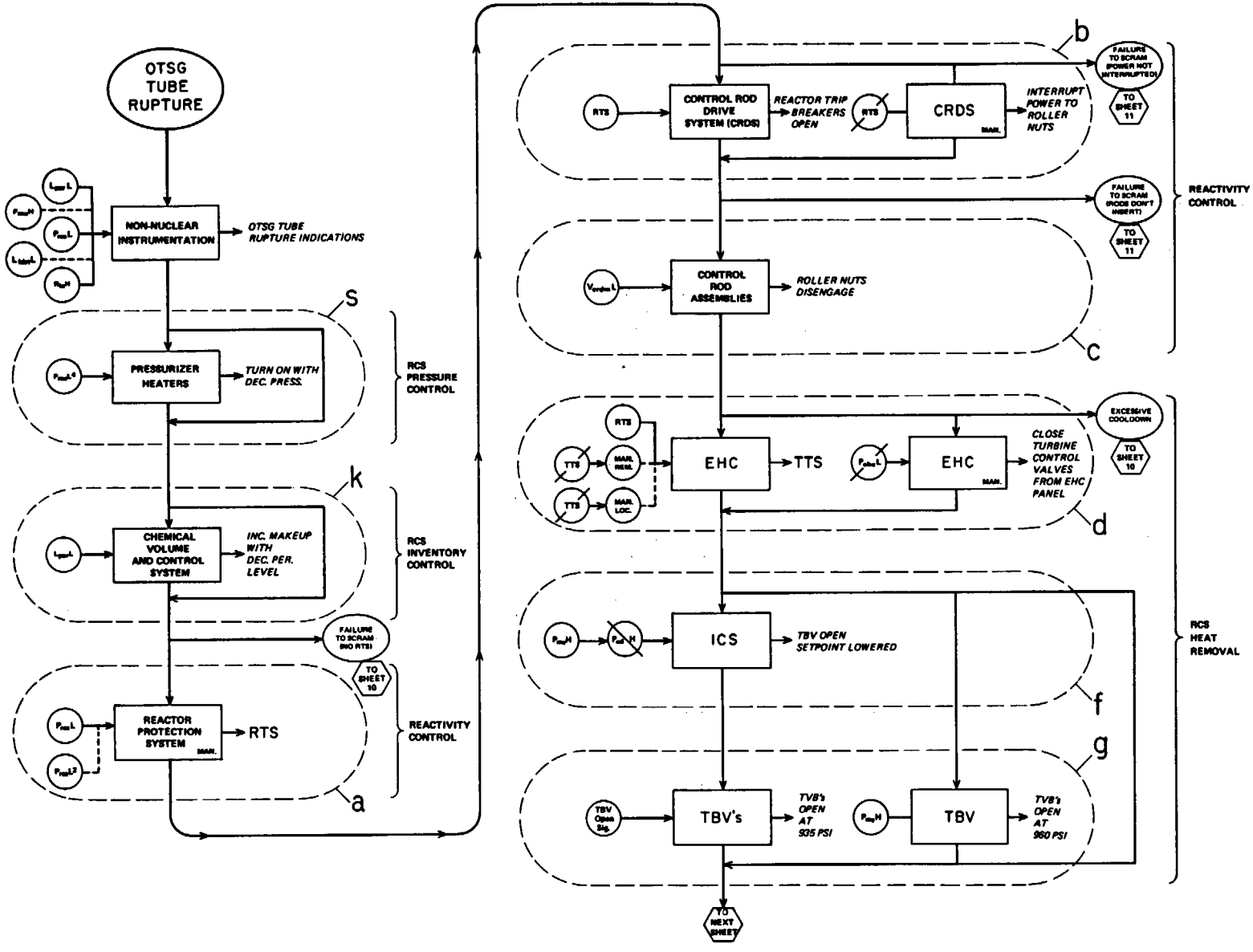


Figure 3-8. Excerpt from an event-sequence diagram.

3.4.4 DELINEATION OF ACCIDENT SEQUENCES

The accident sequences associated with each initiating event can be fully delineated on the basis of a clear understanding and evaluation of the plant response to each type of initiating event. This delineation of sequences is accomplished by developing detailed system event trees. As described in this section, system event trees can be developed from either function event trees or event-sequence diagrams, but the method used for accident-sequence quantification (Chapter 6) depends on the approach followed in developing the trees. Event trees developed from function event trees are quantified by the method of fault-tree linking, whereas event trees developed from sequence diagrams are quantified by using the method of event trees with boundary conditions.

3.4.4.1 System Event Trees Developed from Function Event Trees

The number of system event trees that must be evaluated is determined by the classification of potential accidents, based on unique groups of systems that can perform the required safety functions. Each unique set of required systems is evaluated by means of a system event tree.

The classification of accidents by safety function is the starting point for classification by mitigating system. However, because of the factors listed below, classification by system usually produces more accident classes than does classification by safety function. The factors responsible for this are the following:

1. Design capability of systems. Although the same set of safety functions may be required for two sets of initiating events, different systems may be employed to perform the same function because of the nature of the initiating event. For example, a distinction will be made between LOCAs if they require a different complement of systems for RCS inventory control.

2. Interactions between initiating events and systems. Some initiating events will affect either the function or the availability of potential mitigating systems. Therefore, the set of systems available for mitigating these events will differ from that available for initiating events that are not involved in such interactions. A most obvious example is the following situation, which can occur at many plants: a loss of offsite power makes the power-conversion system unavailable for RCS heat removal. In addition, this loss-of-power initiator affects the availability of the remaining systems because emergency power becomes the only source of electric power for the mitigating systems.

The system event trees will use the information on the effects of loss of various safety functions identified in the function event trees. However, it is likely that the sequences in the system event trees will differ somewhat from the function event trees. This is due to the fact that in some cases system faults may fail multiple functions or system operation may be of interest because of its impact on consequences.

Each system event tree will have a specific system or group of systems as the heading. The exact order of the headings is not crucial to the analytical results, but can be very important to the efficiency and brevity of the analysis. The number of sequences can be reduced by a judicious ordering of the headings. Three factors will assist in the initial ordering--temporal, functional, and hardware relationships--but only an event-tree analysis can determine the "best" order. A good starting point is the time of response: the systems are arrayed in the order in which they are expected to respond to an accident. Thus, systems responding immediately (e.g., the reactor-protection system) are placed first, and those responding later are listed in order of response (e.g., the high-pressure injection then high-pressure recirculation). However, the time of response alone is not a sufficient basis for ordering headings.

Functional and hardware relationships between systems should also be considered in selecting the order of event-tree headings. Systems that depend on the operation of other systems to perform their function should be listed after the other systems. For example, the decay-heat-removal system may require the successful operation of containment sprays and thus may be listed after containment sprays on the event tree. Hardware dependences also may affect the order, as in the case of a system with multiple modes of operation. Since failure in one mode may imply failure in other modes, subsequent dependent modes should be listed later.

The event-tree analysis proceeds by postulating the success or failure of each system in the context of all the boundary conditions established by the previous system states. Only those unique combinations of success and failure states that have physical meaning are included in the event tree. This understanding of the implications of each event-tree sequence comes from the previous steps of the event-tree-development process. For each potential system success or failure state in the event tree, a decision is made to postulate both states or to eliminate the choice and proceed to the next point. Only the system success or failure states that may affect the outcome of the accident sequence or subsequent system operation and physical reality are explicitly shown on the event tree.

Success or failure choices in the event tree can be eliminated if all of the following questions can be answered in the negative:

1. Does the success or failure of the system affect the outcome (e.g., plant-damage state, radionuclide release, containment response)?

2. Does the operation of this system contribute to a safety function in this context?

3. Does the operation of this system at this point affect the need for, or the operation of, other systems?

If any of the responses are positive, the particular success or failure state of the system should be explicitly included in the event tree. It is important to examine each question in the context of each potential accident sequence because the importance or physical impact of a system success or failure can change, depending on the states of other systems.

Figure 3-9 shows the development of the system event tree for a large-LOCA initiating event.

The sample system event tree in Figure 3-9 indicates the relationship between the functional evaluation of plant response and associated systems. Each event-tree heading represents specific system-success criteria as described in Section 3.4.3.1. The system-success criteria for each complement of equipment will be translated into specific failure criteria (described in Section 3.4.5) to facilitate the detailed system evaluations or assignment of failure data that will be needed for the eventual quantification of the system accident sequences.

3.4.4.2 System Event Trees Developed from Event-Sequence Diagrams

After extensive review by operational and administrative personnel, the actions noted on the ESDs are grouped to define event-tree headings. The headings are selected for the following reasons:

1. To show what safety function or system failures will produce each plant-damage state.

2. To display important dependences.

3. To group plant systems to facilitate the calculation of accident-sequence frequencies.

In deciding how to group the ESD actions into event-tree headings, the following guidelines are applied:

1. Use a minimum number of event-tree headings consistent with the reasons for choosing the headings as described above.

2. If an event-tree heading affects only one other heading, roll them together into a single heading.

3. Have only one failure effect come from each event-tree heading.

4. If an event-tree heading significantly affects the boundary conditions on two or more other headings, keep it separate.

Figure 3-10 shows an example of the ESD actions grouped for a typical "failure to trip the reactor" event-tree heading (RT). Failure to trip the reactor is usually a heading because it drastically changes the boundary conditions on at least two other subsequent headings (see item 4 above).

As an example of a heading leading to a change in boundary conditions, consider the following case. A transient leads to turbine trip followed by reactor trip and to an increase in RCS pressure. The opening of the pilot-operated relief valve (PORV) provides sufficient relief capacity to arrest the pressure increase. Thus, the boundary conditions on an RCS relief heading would be such that any RCS relief valve opening would be enough. If, however, the reactor fails to trip after the turbine trips, then one PORV opening will not be enough anymore, the boundary conditions on the RCS

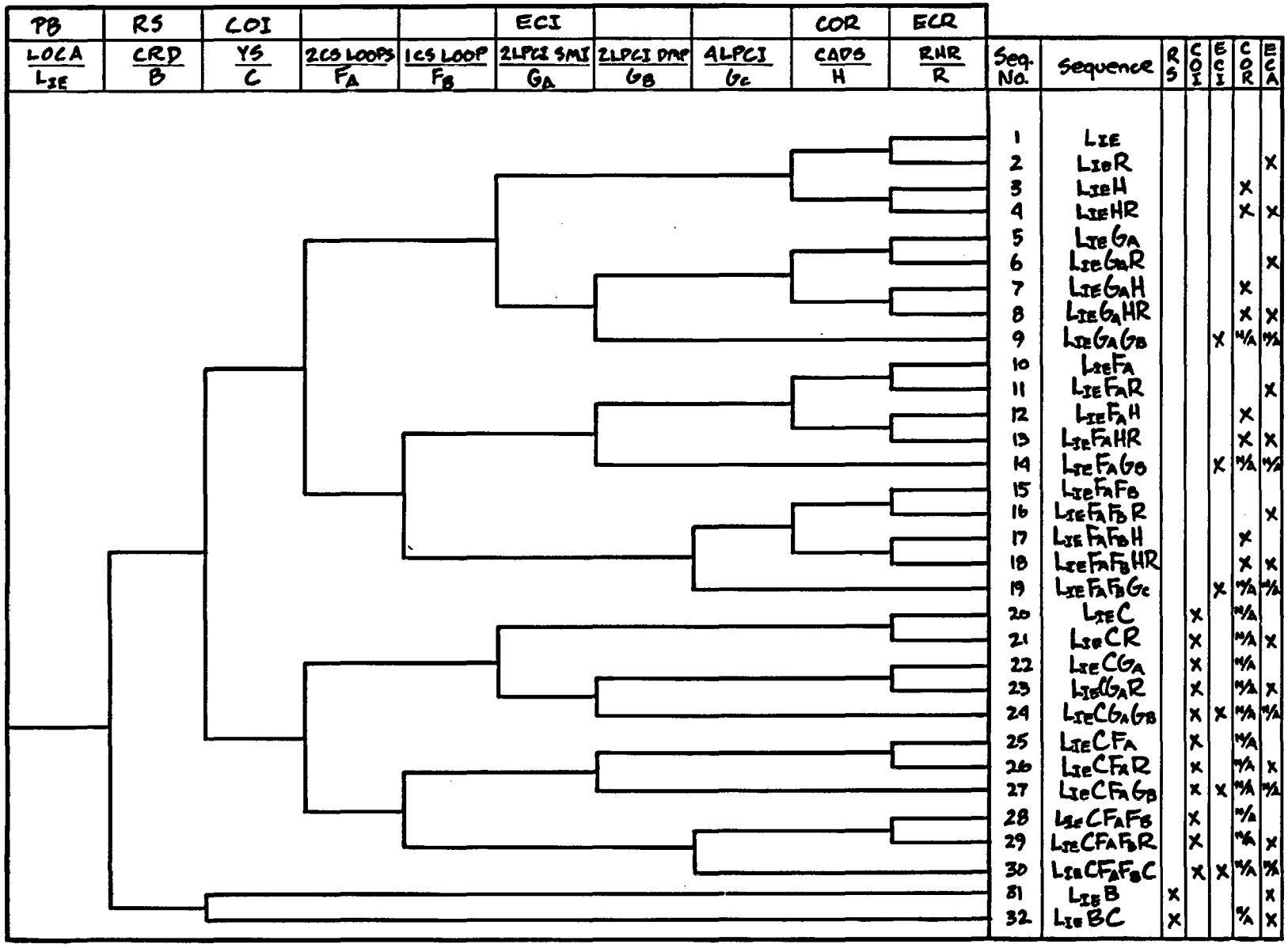


Figure 3-9. System event tree for a large LOCA.

relief heading have changed, and now two of three or three of three relief valves might be required to open.

The actions shown in Figure 3-10 could be arranged into three top events consistent with the three types of failure shown by the ovals: failure to generate a reactor-trip signal (RTF-I), failure to interrupt power to the control rods (RTF-II), and failure to insert the control rods (RTF-III). Although it is usually not necessary to do so, all three have, at different times in the past, been treated as separate headings.

For instance, it would be important to show the impact of an RPS failure (failure to generate a reactor-trip signal) if that failure changes the boundary conditions on more than one other heading. Such a case would arise if the reactor-trip signal is the predominant input to actuate some other important system. In this case, RTF-I should be kept as a separate heading.

If there is not much time for operator action and the interruption of power to the rods on loss of onsite power will significantly increase the likelihood that the rods get inserted, then RTF-II should be a separate heading. The process illustrated in Figure 3-10 for reactor-trip failure is then repeated for all actions in the ESD.

Usually the event-tree headings are single systems or parts of systems, either front-line or supporting, as this allows the effect of the failure of each system to be more clearly defined. Sometimes, in an effort to simplify the tree, the heading may be "too much" or "too little" of a safety function (e.g., excessive RCS heat removal). The reason for including more than one system in a heading is to minimize the number of event-tree branch points from which both branches lead to the same plant-damage state. This helps to minimize the number of branches in the event tree. Minimizing the number of branches generally clarifies the message transmitted by the event tree.

Since the ESD has been used, before the development of the event tree, to trace out each sequence on a system level, the event tree does not have to be used for this purpose. Most of the failures that are important to core damage have already been identified on the ESD, and the important ones can be summarized on the event tree.

Figure 3-11 is an example of an event tree that was derived from an ESD in the manner discussed above. The systems included in each event-tree heading will be indicated by free-form circles on the ESD as is RT in Figure 3-10. Symbols like RO-1 are used to indicate, for example, heading RO (relief valves open), boundary condition 1.

In addition to its being derived from an ESD, the event tree has some other interesting features. Some specific points to be noted on Figure 3-11 include the following:

1. The nominal (expected) plant performance is shown at the top of the tree as a straight line. Each sequence, as it becomes more complicated, drops toward the bottom of the drawing. If no failures occur, the sequence line remains straight.

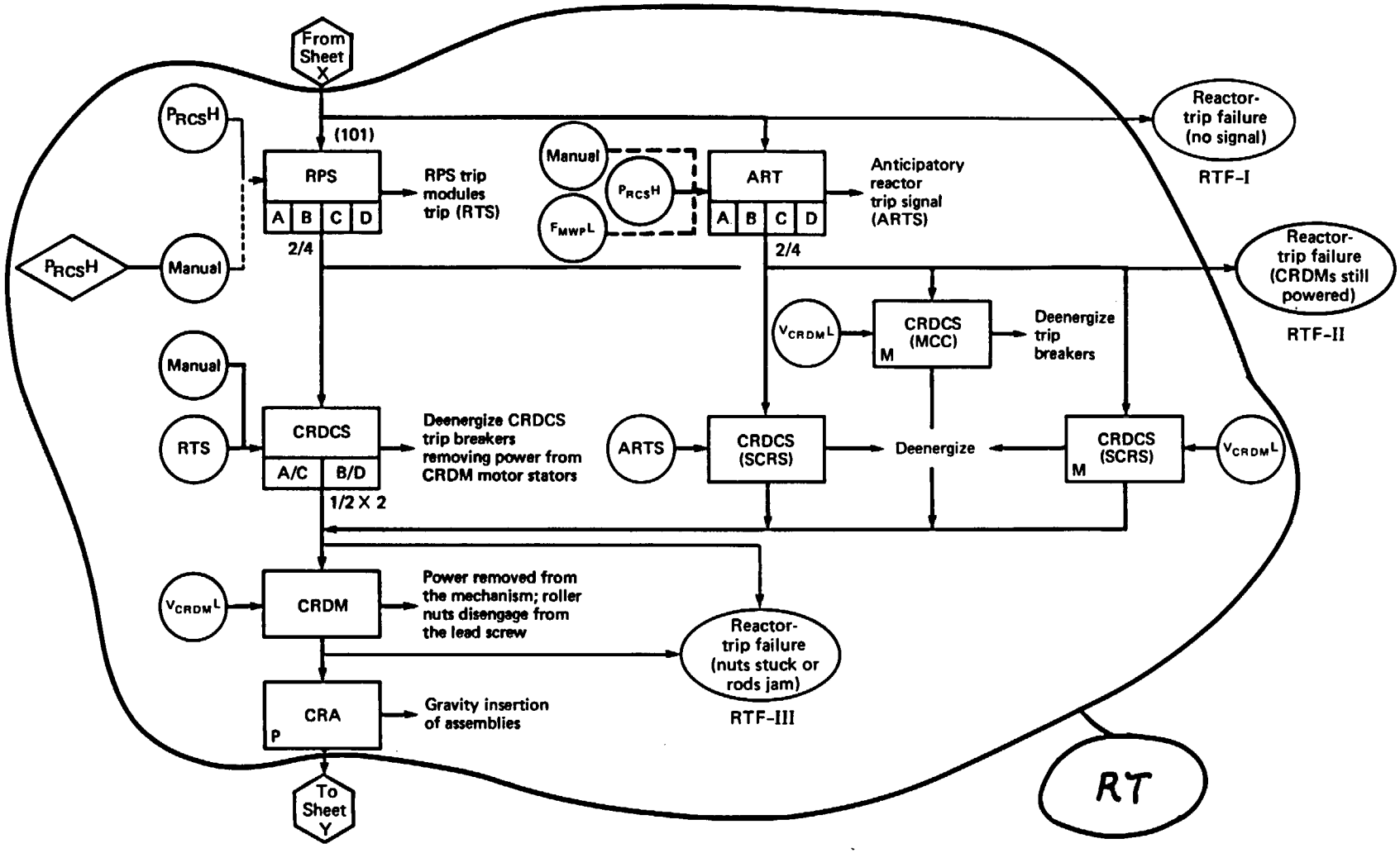
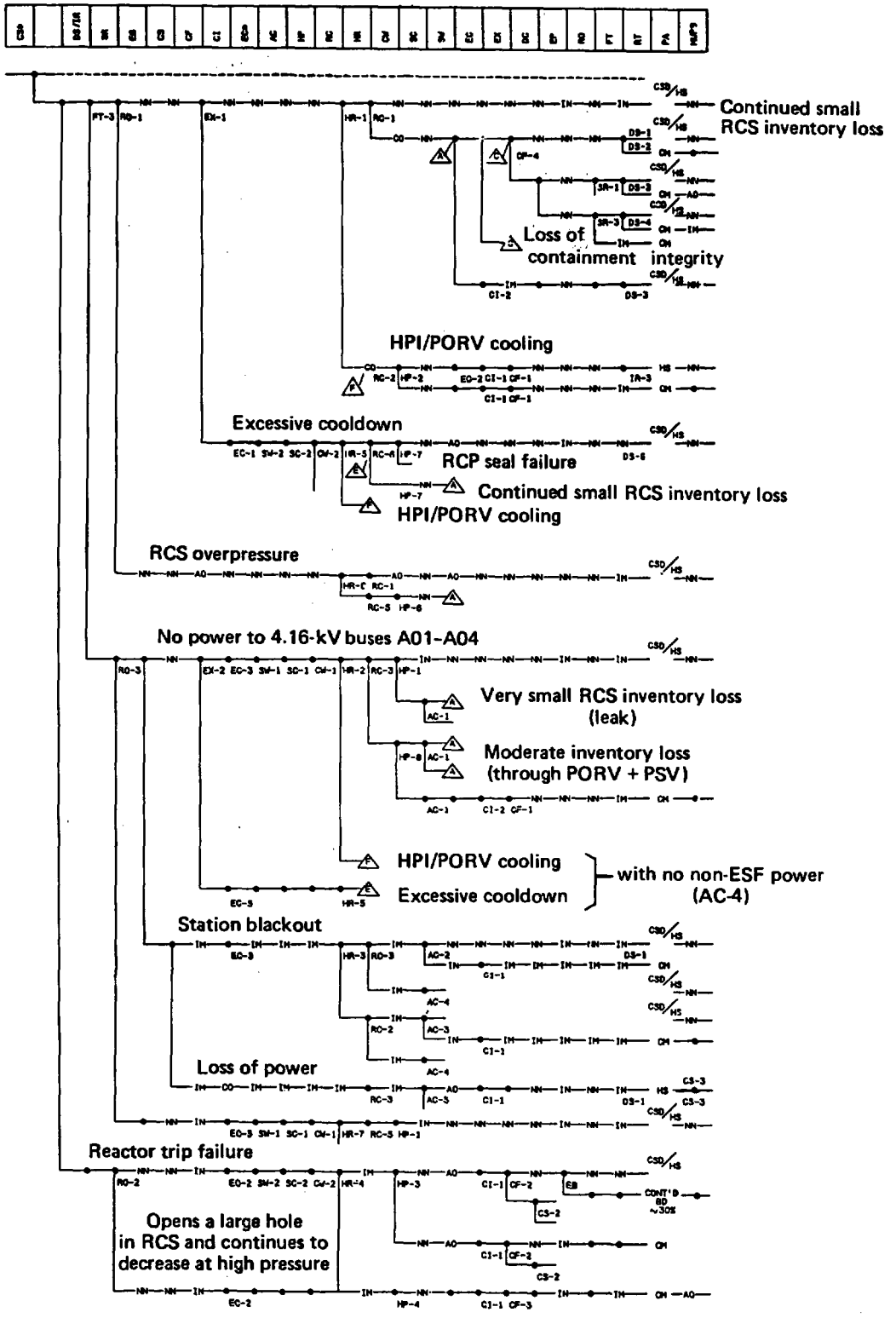


Figure 3–10. Reactor-trip actions.



Key to headings: PA, early preventive action; RT, reactor trip; FT, fast transfer; RO, primary pressure integrity; EP, emergency power; DC, dc power; EX, excessive heat removal by secondary system; EC, emergency cooldown actuation signal; SW, service water; SC, safeguards chilled water; CW, component-cooling water; HR, just enough heat removed from RCS; RC, reclosure of primary relief valves; HP, high-pressure injection; AC, restoration of electric power; CI, containment isolation; CF, fan coolers; CS, containment sprays; EB, emergency boration; SR, suction from containment sump; DS/IR, recirculation or cooling to cold shutdown; CS*, containment sprays actuated at core damage. The blank box represents the outcome of the scenario.

Figure 3-11. Event tree for the malfunctioning of the makeup and purge system.

2. The reasons for the line not branching are explained at each point where it could. For instance, if a line does not branch because the system is not called on to operate, the letters "NN" (system not necessary) appear.

3. The different boundary conditions at each branch point are indicated explicitly.

4. Only the branches that are of interest are shown; others are just indicated by a solid circle (●). Branches are added to (or removed from) the tree as the dominance (in terms of frequency and damage) of each sequence becomes known.

The structure of this tree is unrelated to the fact that it was derived from an ESD except that the names of the sequences, such as "reactor-trip failure," correspond to the ovals on the ESD.

3.4.5 DEFINITION OF SYSTEM-FAILURE CRITERIA

Each heading in the system event trees must eventually be quantified. In many cases, detailed system models must be developed to determine the likelihood of system failure. To support the detailed system modeling, each event-tree heading that is to be further developed must be translated from the system-success criteria previously developed (Section 3.4.3.1) to a statement defining the criteria for system failure.

The system models for event-tree headings require exactly defined failure criteria, which are based on the success criteria defined for each event-tree heading. In this context, failure and success criteria are not exact opposites of each other, because previous failures in the accident sequence may dictate that either some part of the system is already unavailable or that different system components must operate. Each system-failure criterion is defined as part of an event-tree sequence, consisting of the previous successes or failures of other systems, that leads to the definition of boundary conditions on the system's operation. Sometimes these boundary conditions affect the fault-tree top event and thus the fault-tree logic. Therefore, different system-failure criteria may have to be identified for each event-tree heading under each boundary condition on the system(s) in that heading.

The system-success criteria are based on a combined neutronics and thermal-hydraulics calculation of the plant response to postulated conditions. Such calculations are made to determine how much flow, for instance, a high-pressure injection (HPI) system must deliver to prevent the uncovering of the core in a particular accident sequence. Having this much flow or more becomes the success criterion for the HPI system in this particular sequence. In other sequences more flow might be required to keep the core covered or one HPI pump might not be available because of the failure of a diesel to start. In either of these two cases, the definition of the failure criterion will change.

Data are required to support the adoption of specific success or failure criteria. The best sources of such data are those thermal-hydraulics analyses that have been done under realistic assumptions about system performance and are as close as possible to the accident sequence being considered. The latest versions of RETRAN or RELAP are examples of best-estimate computer codes that may assist in defining reasonably realistic success criteria. In the absence of such analyses, either FSAR analyses (from FSAR Chapter 6 or 15) or FSAR success criteria may be used. For some sequences, these generally conservative success criteria are acceptable estimates; for others they can mislead by introducing physically unrealistic assumptions. Such unrealistic assumptions must be treated very carefully so that they do not eventually carry the whole sequence or impact a complete assessment in an unrealistic conservative direction.

Other information may also be used to help define supportable and realistic success and failure criteria. One source of such information is the work done on special issues (e.g., anticipated transients without scram, vessel beltline fracture on excessive cooldown) or for emergency procedure guidelines in response to the accident at Three Mile Island. Another alternative source is persons who have extensive experience in thermal-hydraulics analyses or who have operated plants through numerous accident sequences. Data from this second source must be carefully documented in order to ensure that the judgments are supportable.

It is important to clearly understand the relationship of the systems denoted in the event-tree headings and their support systems. Each front-line system should be reviewed in context with its identified failure criteria to determine the required support elements.

System event trees can generally accommodate the support system in two different ways. One way is to define event-tree headings that are more composite in nature and to determine the impact of support-system failures through system modeling. The other way is to define more discrete event-tree headings wherein the support systems are broken out and explicitly included in the event tree itself.

3.5 SYSTEM MODELING

A general objective of risk assessment is to determine the susceptibility of a system or of groups of systems to conditions of design, operation, test, and maintenance that could lead to failure. This objective can be realized through system modeling, for which a variety of analytical techniques can be used. To be of greatest value to the overall PRA process, however, the techniques used in system modeling should have the following characteristics:

1. The technique should be capable of predicting the unavailability of complex systems in a manner that can be employed by a variety of practitioners.

2. The technique should be proceduralized to the extent that it can be used for a wide variety of systems in a manner that is traceable, repeatable, and verifiable.

3. The technique should provide reasonable assurance of completeness.

4. The technique should enhance understanding, communication, and the use of results.

5. The technique should produce a model that promotes understanding of the principal ways in which the system can fail and the ways in which failures can be prevented or their impact reduced.

Although no single technique completely satisfies all of these generalized criteria, the fault tree is one of the best available analytical tools for understanding how a system works and might fail. Because of its extensive use in the aerospace industry over the past 20 years and the more recent applications in the nuclear industry, the fault tree has become an important analytical method for determining critical system-fault paths and is also often used to determine the associated unavailabilities.

Other analytical tools, such as failure modes and effects analyses (FMEAs) and reliability block diagrams, can be used in conjunction with the fault tree to support the overall system-modeling process. The following discussion of system modeling points out how they can be employed in the context of the combined event- and fault-tree approach; a more detailed discussion is presented in Section 3.6.

A fundamental objective of any fault-tree process is to find the fault event combination with the highest probability of occurrence. This is usually done by finding the smallest combination of fault events that, if they all occur, will cause a selected undesired state or event to occur. This undesired event is described as the top event in the fault tree. The smallest combinations of fault events that cause the top event are the minimal cut sets. It is these minimal cut sets, represented as Boolean equations, that form the bases for the evaluation of all plant and system models. The type of the fault-tree model and the manner in which its minimal cut sets are evaluated may vary with the objectives of the study approach and the options of the PRA team.

Depending on the objectives of the study, it may be of interest to obtain a measure of safety for each individual system. In this case detailed system models are developed and evaluated individually. Minimal cut sets can be qualitatively determined and their relative importance established. The system models can also be evaluated quantitatively to determine the probabilities of minimal cut sets and system failure. Sensitivity evaluations can be performed to determine the impact of changes in the models as a function of the input data. The system models can thus be used to gauge the value of design or procedure improvements on system reliability. An alternative approach is to develop more concise system models and evaluate them only to the extent their constituent fault events contribute to specific accident sequences. In this approach, which depends on the scope and the objectives of the study as well as the availability of particular computer

programs, numerical estimates of system availability are not made; only numerical estimates of the probability of significant cut sets that contribute to certain specific accident sequences are retained.

Different event-tree modeling approaches imply variations in the complexity of the system models that may be required. If only front-line systems or combinations of systems are included as event-tree headings, the fault trees are more complex and must accommodate all dependences between front-line and support systems within the fault tree. If support systems are explicitly included as event-tree headings, more complex event trees and less complex fault trees result.

The level of the PRA determines some of the factors that must be accounted for in the system models. If the effects of external events are included, some of the effects are location dependent. Information on the elevation of a component, proximity to specific systems or components, or room location within the plant is typical of the information needed for system modeling if floods, fires, earthquakes, or similar external hazards are to be properly addressed. Decisions also are required as to the level of detail and the type of components to be included in the trees. Normally, passive failures of piping segments are omitted or lumped together. If the system models are to be used in an evaluation of seismic effects, piping segments and information on their location are included.

Figure 3-12 shows the generalized process of system fault-tree modeling. A significant amount of system-related information is generated during the plant-familiarization process. Preliminary function and system analyses will have been performed, and a basic documentation of individual system descriptions will have been prepared. This information, along with specific system-failure criteria developed for each of the event-tree headings (Section 3.4.5), forms the basis for the system modeling. The initial

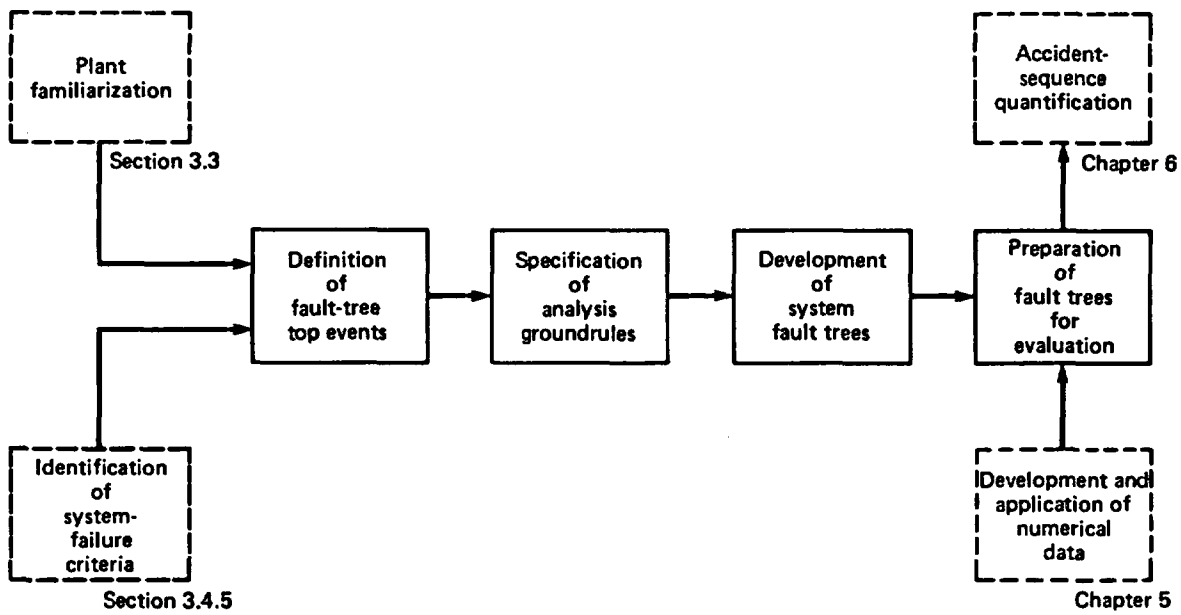


Figure 3-12. Generalized process of system modeling.

step is the definition of the top events for each fault tree; these must be consistent with the appropriate event-tree headings. When the top event has been clearly defined, the groundrules for the analysis must be clearly specified. The system under analysis must be clearly defined and its boundaries and interfaces identified. The constraints and assumptions associated with the analysis must be understood and incorporated into the model.

When this preliminary analytical work has been completed, a focused and concise system model can be developed, commensurate with the study approach. After this system model has been developed, it must be evaluated, documented, and integrated into the overall assessment activity. The desired product of the system-modeling task is a faithful representation of the system and its operational characteristics in a format allowing effective and efficient evaluation. The numerical input data required for the quantitative evaluation of the fault-tree models are described in Chapter 5. The evaluation of the models is described in Chapter 6, "Accident-Sequence Quantification."

3.5.1 DEFINITION OF FAULT-TREE TOP EVENTS

The fault-tree top event is defined after the analyst is thoroughly familiar with the system of interest, its relationship to specific safety functions, and the context in which the system is included in the analysis. Success and failure criteria are identified for each event-tree heading during the event-tree development. This information is required to define the specific system-failure modes to be deductively modeled with the fault tree.

Information from the event-sequence diagrams, if that approach is chosen, can also be used to help define the top event. After going through the ESD and grouping all actions into one event-tree top event or another, the actions can be translated into system model logic, as shown in Figure 3-13. In this case a fault-type model is used to depict the system logic. The systems analyst will probably not use this logic in exactly the form shown, but it will allow him to know exactly what front-line systems are to be included in his fault tree and to know explicitly the failure criteria for each system or group of systems.

Each system logic model is developed for a failure state postulated for the system. The top event must specifically define that failure state and when it occurs. Each system failure is postulated as part of an event-tree sequence consisting of the success or failure states of other systems. Each fault-tree top event should be defined in accordance with the boundary conditions imposed by each event-tree sequence. The boundary conditions include the status of other systems or functions that could affect the system of interest, the operating-equipment failure that constitutes a loss of system function, the operating mode of the system, the time frame of the failure, and any other conditions that might affect the development of the fault tree. The rationale associated with the selection of each boundary condition should be well documented, along with all basic considerations and assumptions about system performance and timing constraints.

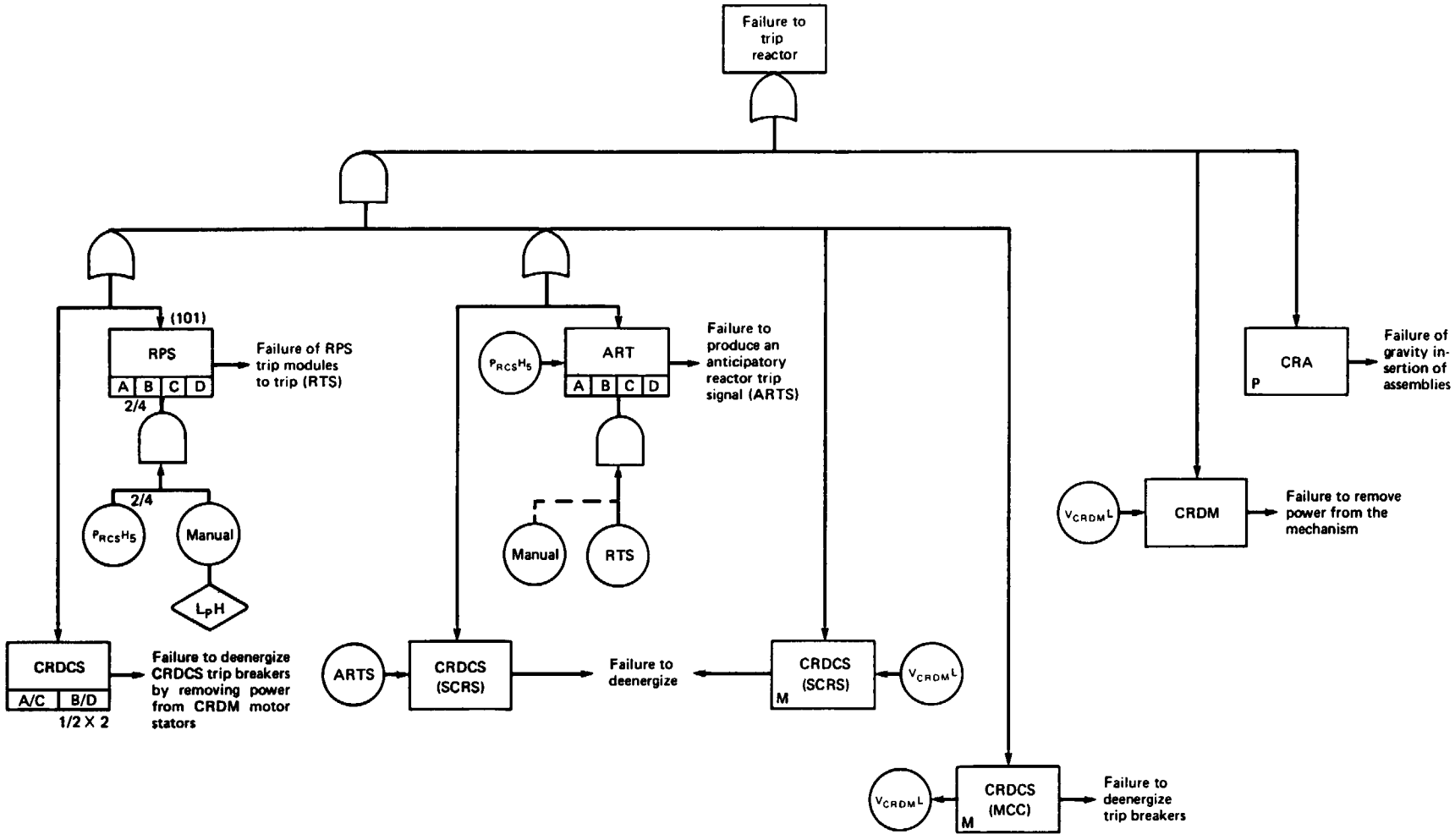


Figure 3-13. Fault-tree top events for failure to trip reactor.

3.5.2 SPECIFICATION OF ANALYSIS GROUNDRULES

Each system analysis will proceed according to certain groundrules or constraints. Some are imposed directly by the design or operational conditions attendant on the definition of the fault-tree top event; others are imposed by the limitations of the analytical process itself. All analysis groundrules that have a bearing on the completed system model must be clearly understood, incorporated into the model, and appropriately documented.

In the performance of a risk assessment, the systems to be analyzed are essentially defined at two levels. The first level of definition is a functional one; it is directly related to the function the system must perform to successfully respond to an accident condition or a transient. This definition provides insight into the overall role of the system in relation to a particular accident sequence. The second level of definition is physical; it identifies the hardware required for the system to function. This hardware definition is normally included in the statement of the top event of the fault tree and describes the minimum acceptable state of system operability. This definition provides the analytical boundaries for the various system analyses. It is important to identify and fully document the boundaries of each system. These boundaries may be different from the traditional system boundaries that are identified in information describing the system or the plant.

All support-system interfaces with the front-line system must be accounted for, and included in, the analysis. Certain system interfaces may be quite complex (i.e., instrumentation and control) and require a specific definition of the system boundaries considered in a particular analysis. Some components may be found to be within the boundaries of more than one system.

Experience has shown that the interfaces between a front-line system and its support systems may be most important to the system evaluation. In that regard a more formal search and documentation of all elements that depend on input from another source beyond the identified system boundary may be appropriate. The procedure used in the Interim Reliability Evaluation Program (IREP) included a search for, and an evaluation of, potential support-system failures that could affect the operation of front-line systems. This search and evaluation procedure resembled a failure modes and effects analysis, which is more fully described in Section 3.6. An example of the format used is shown in Figure 3-14. The level of detail shown in the FMEA example may not be necessary for all evaluations. However, the concept is important in that all areas of interface and support required for system operation are thoroughly defined and evaluated.

Although the systems analyst must make every effort to obtain and fully use all available system information in the course of the system modeling, he will inevitably have to make a number of assumptions about the details of system operation, capacities, and credible failure mechanisms. The accuracy of all assumptions should be verified, and the supporting rationale should be documented. It is extremely important that all assumptions be fully described and documented. To preserve traceability, even the assumptions that are obvious to the analyst should be explicitly stated.

Front-line system			Support system			Failure mode	Fault effect	Detection	Diagnostics	Comments
System	Div.	Comp.	System	Div.	Component					
AFWS	A	MDP-1A	AC power	A	Breaker A1131	Fail open	Concurrent failure to start or run (CFSR)	At pump test	Pump operability only	Treat as part of local pump failure
	B	MDP-1B	AC power	B	Breaker A1132	Fail open				
AFWS	A	MDP-1A	AC power	A	Bus E11	Low or zero voltage	CFSR	Prompt	Control room monitors ESG E/F 11 voltage, alarmed	Partial failure noted for future reference
	B	MDP-1B	AC power	B	Bus F12		Possible motor burnout	Prompt		
AFWS	A	MDP-1A	HVAC	A	Rx cooler 3A	No heat removal	Pump-motor burnout in 3-10 continuous service hours (CSH)	Shift walk-around	No warning for local faults	AC and SWS support systems of HVAC monitored but not HX
	B	MDP-1B	HVAC	B	Rx cooler 3B	No heat removal				
AFWS	A	MDP-1A	ESWS	A	Oil cooler S31	Loss of service water	Pump burnout in 1-3 CSH	At pump test	Local lube-oil temperature gauge, none in control room	ESWS header and pumps monitored but not lube-oil coolers; local manual valve alignment checked in maintenance procedure xx but not in periodic walk-around
	B	MDP-1B	ESWS	B	Oil cooler S32					
AFWS	A	MDP-1A	DC power	A	Bus A131	Low or zero voltage	Precludes auto or manual start, no local effect on already running pump	Prompt	Control room monitors XXX dc bus voltage--many lamps out in control room	Effect of dc power loss on ac not evaluated here; local motor controller latches on, needs dc to trip or close
	B	MDP-1B	DC power	B	Bus B132					

Figure 3-14. Example of format for a system-interaction FMEA.

3.5.3 DEVELOPMENT OF SYSTEM FAULT TREES

The actual development of the system logic model commences after the analyst has gained a thorough understanding of the system under consideration, especially about its integration into the overall accident-sequence definition process. The analytical groundrules (i.e., interfaces, assumptions, etc.) described in the introduction to Section 3.5 will guide the detailed development of the fault-tree model.

The basic concepts of fault-tree construction and analysis are well documented and need not be treated here in detail. The Fault Tree Handbook (Vesely et al., 1981) presents the latest and most comprehensive treatment of the subject. Fault Trees for Decision Making in Systems Analysis (Lambert, 1975) is also a good reference document. The remainder of this section describes the elements of a fault-tree model and addresses factors that have been shown to be important to the modeling of nuclear plant systems.

3.5.3.1 Elements of the Fault-Tree Model

In fault-tree analysis, an undesired state of a system is specified and the system is then analyzed in the context of its environment and operation to find all of the credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the top event. The fault-tree approach is a deductive process, whereby the top event is postulated and the possible means for that event to occur are systematically deduced.

A fault tree does not contain all possible component-failure modes or all possible fault events that could cause system failure. It is tailored to its top event, which corresponds to a specific system-failure mode and associated timing constraints. Hence, the fault tree includes only the fault events and logical interrelationships that contribute to the top event. Furthermore, the postulated fault events that appear on the fault tree may not be exhaustive. They can include only the events considered to be significant, as determined by the analyst. It should be noted that the choice of fault events for inclusion is not arbitrary; it is guided by detailed fault-tree procedures, information on system design and operation, operating histories, input from plant personnel, the level of detail at which basic data are available, and the experience of the analyst.

It should also be understood that the fault tree is not itself a quantitative model. Although it lends itself to quantification through the Boolean representation of its minimal cut sets, the fault tree itself is a qualitative characterization of system fault logic.

Figure 3-15 illustrates a typical fault tree. Figure 3-16 shows and explains commonly used fault-tree symbols. Primary or intermediate events (or combinations of the two) are inputs to logical operators referred to as "gates." The two basic types of fault-tree logic gates are the OR gate and the AND gate. Together with the NOT operator (commonly shown as a dot above the gate), these gates can be used to define any other specialized fault-tree gate.

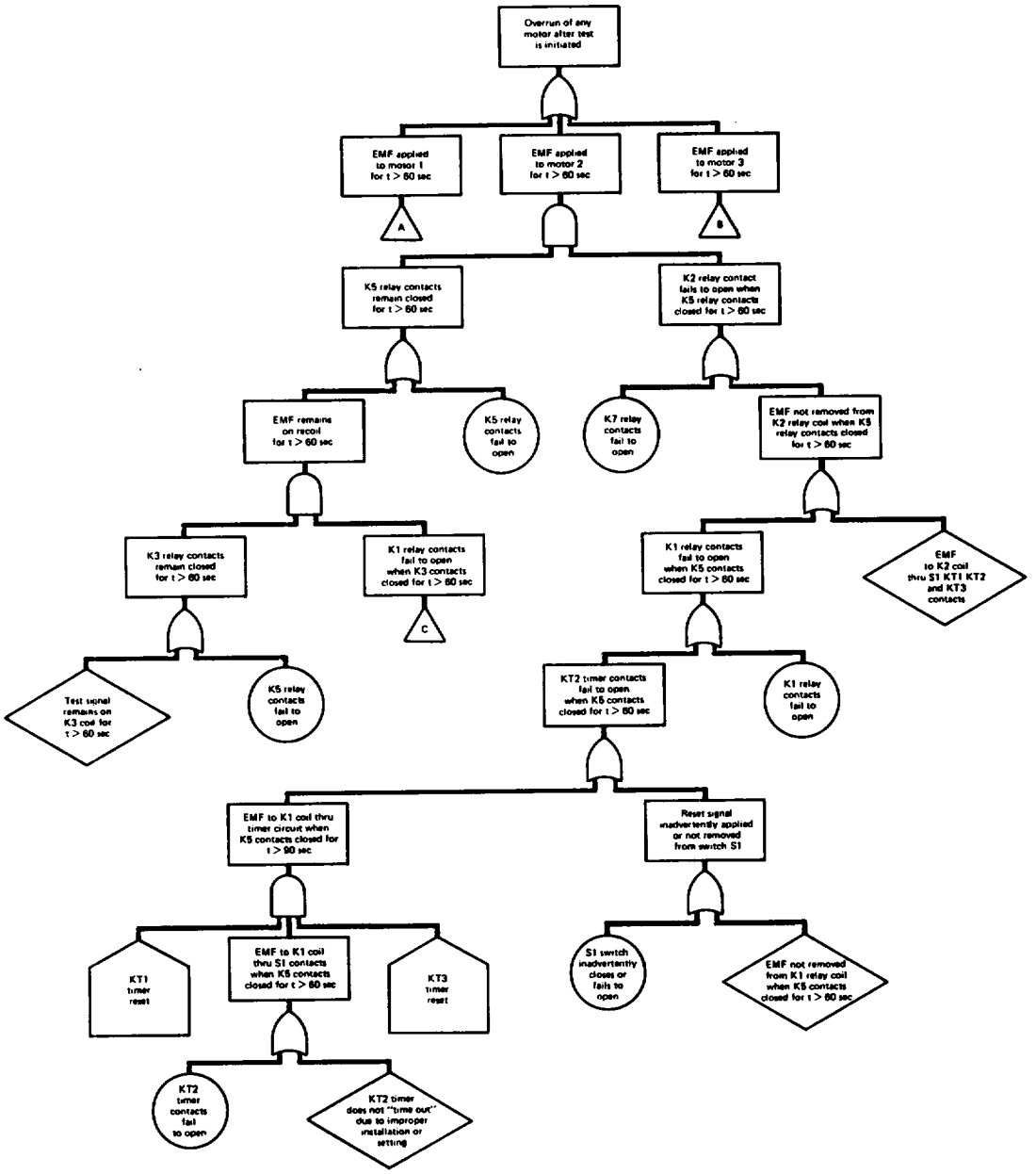
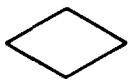


Figure 3-15. Fault tree for overrun of motor 2 (relay logic only).

In postulating a fault or failure for inclusion in a fault tree, it must be remembered that the proper definition of these events includes a specification not only of the undesirable component state but also the time it occurs. It is very important that the time be kept in mind in postulating the top event and incorporated into the analyst's thought processes when postulating all subsequent fault events. It is further useful to make a distinction between the specific term "failure" and the more general term "fault." This distinction can best be illustrated by example. If a relay closes properly when a voltage is passed across its terminals, the relay is in a state of success. If, however, the relay fails to close under these circumstances, it is in a state of failure. Another possibility is that the

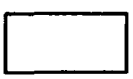
The basic event. The circle describes a basic initiating fault event that requires no further development. The circle thus signifies that the appropriate limit of resolution has been reached.



The undeveloped event. The diamond describes a specific fault event that is not further developed, either because the event is of insufficient consequence or because relevant information is not available.

The conditioning event. The ellipse is used to record any conditions or restrictions that apply to any logic gate. This symbol is used primarily with the INHIBIT and PRIORITY AND gates.

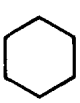
The external event, or house. The house is used to signify an event that is normally expected to occur, such as a phase change in a dynamic system. Thus, the house represents events that are not in themselves faults. This event acts as a switch by being set to 0 or 1 to reflect boundary conditions.



Intermediate event. An intermediate event is a fault event that occurs because of one or more antecedent causes acting through logic gates. It is sometimes referred to as a description box.

OR gate. The OR gate is used to show that the output event occurs if and only if one or more of the input events occur. There may be any number of inputs to an OR gate.

AND gate. The AND gate is used to show that the output event occurs if and only if all of the input events occur. There may be any number of inputs to an AND gate.



INHIBIT gate. The INHIBIT gate is a special type of AND gate. The output of this gate is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The condition that must exist is the conditional input.

EXCLUSIVE OR gate. The EXCLUSIVE OR gate is a special type of OR gate in which the output occurs only if exactly one of the inputs occurs.

PRIORITY AND gate. The PRIORITY AND gate is a special type of AND gate in which the output event occurs only if all input events occur in a specified ordered sequence. The sequence is usually shown in an ellipse drawn to the right of the gate.

Transfer symbols. Triangles are transfer symbols and are used as a matter of convenience to avoid extensive duplication in the fault tree. A line from the apex of the triangle denotes a transfer in, and a line from the side of the triangle denotes a transfer out. A transfer in attached to a gate will link to its corresponding transfer out. This transfer out, perhaps on another page, will contain a further portion of the tree describing input to the gate.

Figure 3-16. Fault-tree symbols. A circle, diamond, ellipse, or "house," represents a primary event—that is, any event that is not developed further and does not have any inputs. The two basic types of fault-tree logic gates are the OR gate and the AND gate. Together with the NOT operator (commonly shown as a dot above the gate), these gates can be used to define any other specialized fault-tree gate.

relay closes at the wrong time because of the improper functioning of some upstream component. This does not constitute a relay failure; however, the relay's closing at the wrong time may well cause the entire circuit to enter an unsatisfactory state. Such an occurrence is called a "fault." It can thus be said that, in general terms, all failures are faults, but not all faults are failures. Failures are basic abnormal occurrences, whereas faults can be described as "higher order" events.

Each fault event that appears in a fault tree contains a reference to the particular failure mode associated with that event. It is important to differentiate between the terms "failure mode," "failure mechanism," and "failure effect." When speaking of "failure effects," the only concern is with why the failure is of interest; that is, what are the effects of the failure, if any, on the system? In contrast, a "failure mode" specifies exactly which aspects of component failure are of concern. A "failure mechanism" is a statement of how a particular failure mode can occur and, perhaps, what the corresponding likelihoods of occurrence might be. In this fashion, failure mechanisms produce failures modes, which, in turn, result in certain failure effects on system operation. Each fault event should be carefully stated to ensure that it uniquely describes the condition of interest and that it is directly related to the numerical data base.

3.5.3.2 Component-Failure Characteristics

A key element of fault-tree analysis is the identification of hardware-related fault events that can contribute to the top event. To allow for a quantitative evaluation, the failure modes must be postulated in such a way that they are clearly defined and can be related to the numerical data base. In postulating component-failure modes, care should be taken to ensure that they are realistic and consistent within the context of system operational requirements and environmental factors.

All component fault events can be described by one of three failure characteristics:

1. Failure on demand. Certain components are required to start, change state, or perform a particular function at a specific instant of time. Failure to respond as needed is referred to as failure on demand.

2. Standby failure. Some systems or components are normally in standby but are required to operate on demand. Failure could occur during this nonoperational period, preventing operation when required.

3. Operational failure. A given system or component may be normally operating or may start successfully but fail to continue to operate for the required period of time. This failure characteristic is referred to as an operational failure.

Depending on the specific context of the fault tree--for example, a specific mode of system operation--the analyst should evaluate each

component in terms of the failure characteristics listed above. Chapter 5 provides additional information on the specification of failure modes for individual components and the associated numerical data.

3.5.3.3 Testing and Maintenance

In addition to the physical faults that can render a system unavailable, testing and maintenance activities can also make a significant contribution to unavailability. Unavailability due to testing or maintenance depends on the frequency and the duration of the test or maintenance act. Information on equipment unavailability due to testing can generally be obtained or derived from the technical specifications and maintenance records.

There are three general types of testing that should be considered for their potential impact on system unavailability:

1. System logic tests, which test the system control logic to ensure proper response to appropriate initiating signals.

2. System flow and operability tests, which verify the operability of such components as pumps and valves.

3. System tests that are performed after discovering the unavailability of a complementary safety system; generally referred to as tests after failure.

Testing schemes generally affect complete subsystems, and hence it is generally not necessary to consider each hardware element individually. Testing involving redundant portions of a system can be particularly important, and care should be taken that the constraints of the technical specifications are understood, evaluated, and properly accounted for in the fault tree. A complete understanding of the impact of all testing on system hardware and operational schemes is necessary for completeness and adds valuable insight into the overall operability of the system.

Maintenance activities can also make a significant contribution to system unavailability, and two types of maintenance need to be considered: scheduled and unscheduled. Scheduled, or preventive, maintenance actions are performed routinely. Information on the frequency or duration of each action can be obtained from maintenance procedures. Care should be exercised to ensure that outages associated with preventive maintenance are not already included in the time intervals assigned to testing and that the maintenance is not performed under conditions that would not contribute to system unavailability.

Unscheduled maintenance activities result when equipment failures occur and the failure is repaired or the equipment is replaced. Because these activities are not performed on a prescribed basis, the frequency and the mean duration time of the maintenance act must be determined from historical data. Chapter 5 provides information on the numerical data base for maintenance activities.

3.5.3.4 Human Errors

The impact of plant operators on the outcome of potential accident sequences is one of the most important, as well as one of the most difficult, elements of system analysis. The potential for operator error is present in virtually every phase of system operation, testing, and maintenance. Furthermore, human error may affect the design, manufacture, and inspection of nuclear plants and systems. However, certain types of human error are more amenable than others to exclusion in system modeling. For example, human errors associated with manufacturing are difficult to quantify, as are operator acts of commission because such a broad spectrum of actions would be candidates for evaluation.

The potential for human error must be considered during the detailed system analysis. Manual actions that can prevent or mitigate an accident sequence can be regarded in the same fashion as support systems like electric power or component cooling. In the context of system fault-tree analysis, human errors should be considered in terms of potential effects on individual components as well as potential effects on the operation of subsystems or systems. Each individual component should be examined to determine the potential for a human error that might disable it.

The systems analyst must consider the potential for human error (and the possibility of human intervention to recover from a faulted condition) throughout all aspects of the analysis. The analysis of human errors cannot be considered a separate task; it is an integral part of the system analysis. The systems analyst should be as familiar with the operating, maintenance, and emergency procedures for the system under analysis as he is with the equipment hardware. However, in such analyses the detailed evaluation of a given human error may be performed separately by a specialist using the techniques discussed in Chapter 4. This specialist must be thoroughly informed of all boundary conditions that may affect this analysis and be familiar with the context in which the man-induced fault is being evaluated. Thus, the human-factors specialist must be regarded as an integral member of the analytical team.

In general, human errors may be presented on the fault trees as causes of component unavailability where the error contributes to the occurrence of the accident sequence being considered (e.g., failure to realign after testing). These errors can be defined by the system analysis in terms of the availability and content of procedures, environmental conditions, and other performance-shaping factors to permit a specialist in human-reliability analysis to make an informed judgment. In contrast, human errors occurring during an accident cannot be properly evaluated on a system fault tree but must be considered as being dependent on the specific accident sequence and could be displayed on the event tree. Since human errors are accident-sequence dependent, the systems analyst must impart to the human-factors specialist a thorough understanding of the diagnostic information available to the plant staff, the procedures and precautions provided to the operator, the training of the operator in response to similar diagnostic patterns, as well as the stress, environmental, and other applicable performance-shaping factors.

To properly assess the likelihood of an accident sequence progressing to core damage or releases of radioactive material from the plant, the potential for operator recovery from the sequence should be considered. Since the probability of a successful recovery is strongly predicated on the specifics of the events that caused the accident sequence, the analysis of recovery depends not only on the sequence but also on its individual cut sets. Hence, it is not unusual for the analysis of recovery to be restricted to the dominant cut sets of the accident sequences that control the frequency of core damage or of a specified release.

It is as important that the systems analyst thoroughly understand the assumptions and judgments used by the human-factors specialist in performing the human-reliability analysis as it is that the specialist understand the specifics of the error being evaluated. The systems analyst must ascertain that the human-reliability analysis was done in the context in which it is employed in the event trees or fault trees.

If potential human errors have been defined comprehensively, an initial screening may be required to identify the more important ones. This can be done during the initial quantification and requires the assignment of numerical values to each input fault event. Initial probabilities are assigned to human-error events in a conservative manner, and the system model is evaluated to determine significant contributors. The system models are reevaluated to determine the significance of human errors, and a detailed analysis can be performed for each minimal cut set where human error was found to be significant. This reevaluation is intended to provide a more realistic appraisal of the effects of human error.

The performance of human-reliability analysis is discussed in detail in Chapter 4.

3.5.3.5 Dependent Failures

The identification and the evaluation of dependent failures are both difficult and important. Because of this importance, the subject of dependent failures is discussed in several sections of this guide. Section 3.7 defines the various types of dependent failures and discusses the methods available for their evaluation. Chapters 10 and 11 provide guidance on the development of event-specific models for evaluating common-cause events like fires, floods, and earthquakes.

The question of evaluating dependent failures extends beyond methods for the development of system models. Therefore, Section 3.7 should be referred to for detailed information on this topic. However, it should be noted that the fault tree is the principal means of accounting for functional and shared-equipment dependences between components. A well-constructed fault tree can lead to the identification of fault events that affect or interact with other components in a system and sometimes with other interfacing systems. Evaluation of the minimal cut sets for each system can identify dependences and their impact on system unavailability. Each input event on the fault tree must be accurately and consistently named or coded to facilitate the evaluation.

3.5.3.6 Level of Resolution

The question of how far to continue the analysis or to what level of detail the analysis should be taken is a general concern that must be addressed in each system-modeling project. Fault trees are developed to derive unavailabilities for event-tree headings. In some cases detailed system models are not required, and the necessary numerical data are available from historical data on a system level. It can generally be said that, for these systems to be modeled, fault events should be analyzed to the level of resolution at which applicable numerical data exist or to a level consistent with the scope predetermined by the analyst.

It should be noted, however, that there is an inherent conflict between the desire not to make an analysis any more detailed than necessary and the desire to search for dependent failures. If historical data are available for two systems, they might be applied independently. However, a detailed analysis of the two systems might uncover a subtle dependence that would invalidate the historical data for the two systems taken together. In using historical data for systems or subsystems, care must be taken to ensure that there is no potential for dependent failures that would affect the applicability of the data.

3.5.4 PREPARATION OF FAULT TREES FOR EVALUATION

The fault tree is essentially qualitative, but because of its binary logic and adaptability to Boolean expressions, it is very often quantified. Since fault trees are frequently lengthy and difficult to evaluate, they are reduced or reorganized to facilitate the quantification. By its very nature, the detailed fault tree contains many events that are insignificant in relation to other fault events or fault paths. It is desirable to include these events in the detailed tree to preserve the rigor and traceability of the analysis. However, in order to evaluate the tree, it is necessary to group or coalesce these insignificant fault events for efficiency in handling and evaluation.

The reduction can be done manually before evaluation, or it can be performed in the computerized solution of the model. Manual reduction requires an interpretation of the fault-tree logic and a gathering of the similar inputs under individual logic gates. Often the original detailed fault tree is considered a worksheet, and a reduced or reorganized version is prepared for the evaluation.

The fault-tree reduction should not result in the loss of any significant information; rather, it should provide means of focusing on the more-important events and eliminating time-consuming evaluations of meaningless combinations of insignificant events. A detailed tree can be so large that even after reduction it is difficult to evaluate the complete tree at one time. In such a case, the tree is divided into identifiable subtrees that are evaluated separately. If this approach is used, a careful search of each subtree is done to ensure that any potential common elements are identified.

Before the quantitative evaluation begins, events on the tree must be coded with an identifier unique to that event. A systematic and orderly method for coding the fault events is needed to minimize the possibility of erroneously assigning the same identifier to more than one event or of assigning different identifiers to the same event when that event appears more than once on the fault tree.

Although different fault-tree coding schemes can be used as inputs to various quantification codes, most codes accommodate an eight-digit event identifier. Coding ordinarily conveys information that readily identifies the system in which the component is located, the component type, the specific component identifier, and the failure mode. An example of a typical naming code is given in Figure 3-17. Characters in the individual fields are normally chosen from standardized tables (e.g., Tables II 2-1, 2-2, 2-3, and 2-4 of Appendix II to the Reactor Safety Study (USNRC, 1975) or derived to meet the requirements of specific evaluation codes. More-complex identifiers are required if additional information, such as location generic information for dependent-failure searches, is desired.

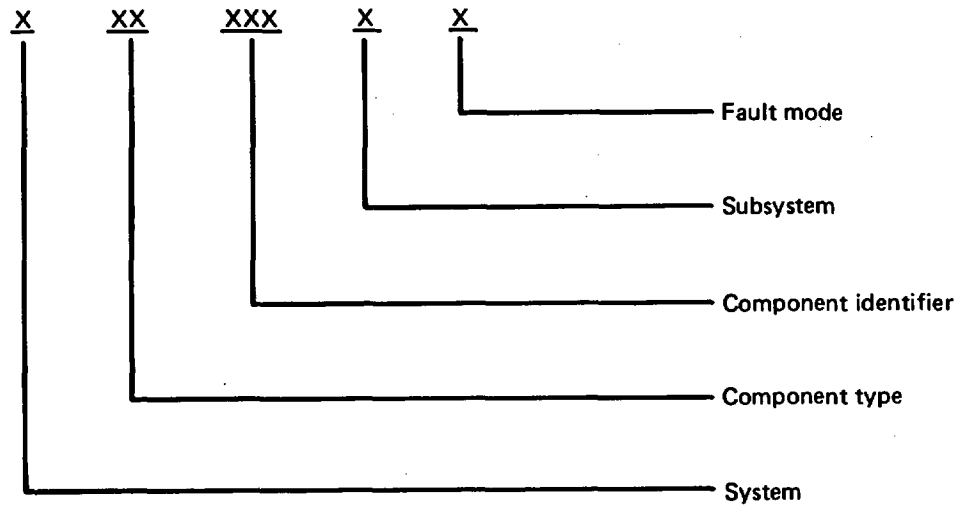


Figure 3-17. Event-naming code.

3.5.4.1 Abbreviated Fault Tree or Tabular OR Gate

In the traditional fault tree, circles represent basic component failures for which failure-rate data are expected to be available. Diamonds represent basic events that are not expanded because the event is judged to be not important, insufficient information is available, or the analyst wishes to postpone development. In any case, the event is given a name and is accountable in the Boolean expression for the fault tree. The fault tree is thus developed until basic fault states are identified for all components of the system and a binary model is obtained. Equipment-failure or human-error probabilities and appropriate time intervals can be assigned to determine probabilities for components, subsystems, and the system. During

quantification, all the information contained on the fault tree is transferred to event tables and coding sheets for ease in assigning data and for computer processing.

Since all basic-fault statements on the conventional fault tree are to be transferred to tables, one way to save effort is not to put them on the fault tree in the first place. The first step in the abbreviated method, then, is to enter all basic-fault statements directly into fault-summary tables, an example of which is shown in Figure 3-18. Only the code name of the event is shown on the fault tree.

Event name	Event component	Failure mode	Failure rate	Fault duration	Error factor	Location
HPP0000R	Pipe downstream of pumps	Rupture				
HPP0001P	Pipe 1	Plugged				
HCV0007D	Check valve 7	Does not open				
HMV0001D	Motor-operated valve 1	Does not open				
HMVCC01D	Control-circuit valve 1	Does not open valve				
ESAS-A-F	ESAS-A to valve 1	Does not open valve				
125VDCAF	125-V dc control power to valve 1	Does not open valve				
480VACAF	480-V ac power to valve 1	Does not open valve				

Figure 3-18. Example of format for a fault-summary table.

The second step is to use a new logic gate, the tabular OR gate, for listing event names on the tree rather than to show individual event statements within the conventional symbols. Typically, a system fault tree contains many events that are logically in series when reduced. The primary events are listed by code under a tabular OR gate; otherwise they can be expanded into their respective causes. The same treatment can be applied to any number of components logically in series. An abbreviated fault tree

typically shows a top undesired event, primary events listed by code name under one or more tabular OR gates, a few rectangles representing events that are inputs to chains of components and inputs to the system, a few house events, and the logic AND and OR gates used to relate the events. All other information is contained in the fault-summary table. Figure 3-19 illustrates the use of the tabular OR gate and its relationship to the traditional fault tree.

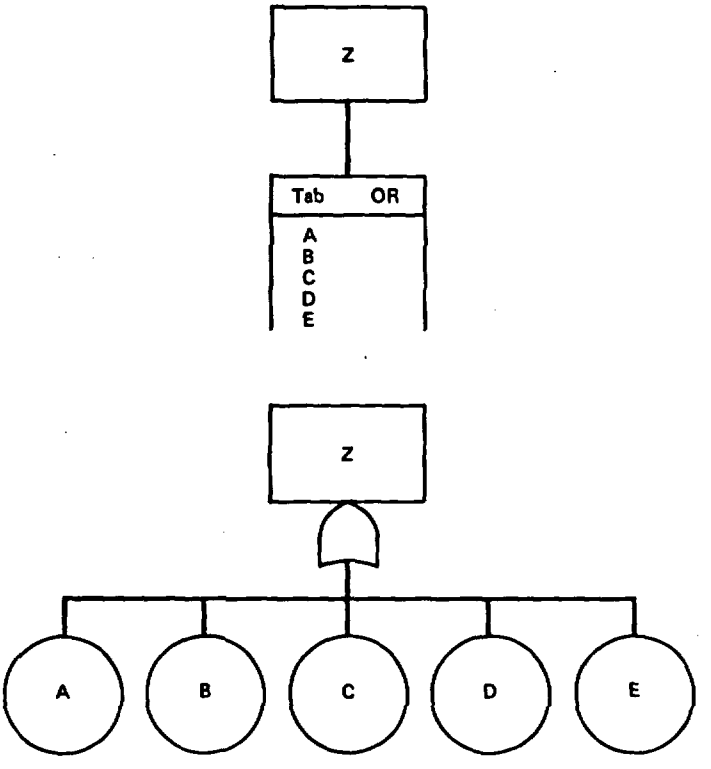


Figure 3-19. The tabular OR gate (top) and the equivalent fault-tree arrangement.

The abbreviated fault tree has several advantages over the conventional tree, all of which reduce the time and effort needed for system evaluation. It is readily restructured for each new accident situation: events can be easily added or crossed off, and blocks of events can be moved if the logic changes. Component-failure modes and their logical relationship to system failure tend to be more visible. Because of their reduced size and the greater failure-mode visibility, the abbreviated fault trees are easier to check. A typical system fault tree developed by the traditional approach may require many large sheets of paper to show all the component faults. In the abbreviated form, the same faults usually can be shown on two or three 8-1/2 by 11-inch sheets. A disadvantage of this approach is that it requires tracking both tables and figures in evaluating the tree, and the tree, being in summary form, does not provide a logic model that can be directly related to the system configuration.

3.6 OTHER METHODS

Event trees and fault trees are not the only analytical methods that can be used in performing a PRA. There are several so-called system-analysis methods that can be used in addition to, or in support of, the event- and fault-tree approach, but no other methods have been used as frequently. It should be noted, however, that methods of system analysis are constantly being developed and improved. It would be incorrect to assume that fault-tree analysis is the only or the best method. The method used depends to a large degree on the background of the analyst, the objectives of the study, and even company preference.

Often combinations of methods are desirable. For example, even though Markovian analyses are not described in detail in this chapter, they have been found useful in identifying system dependences and delineating complex sequences of events and effects of partial failures. It would also be advisable to explore ways in which other methods, such as Markovian reliability analysis, could be used to complement event and fault trees or to help in solving specific analytical problems.

A review of some of the better known methods was performed to determine whether they are applicable and whether they are being used in PRA applications (see Table 3-6). Only the methods with current applications to nuclear plant PRAs are included in the discussion presented below, which describes the basic concepts and techniques as well as their use in a nuclear plant PRA. Also discussed in this section are some recent modifications that are aimed at expediting fault-tree analysis.

3.6.1 FAILURE MODES AND EFFECTS ANALYSIS

As commonly used in reliability and safety analyses, the FMEA identifies failure modes for the components of concern and traces their effects on other components, subsystems, and systems. Emphasis is placed on identifying the problems that result from hardware failure.

To prepare for an FMEA, several steps may be useful. The system to be analyzed, including its mission and operation, should be defined, with all interfaces clearly identified. Then failure categories and environmental conditions may be specified. The extent to which each of these steps proceeds depends on the complexity of the system. Once the system and its intended use are described and understood, the FMEA can be performed.

A partial FMEA is shown in Figure 3-20 for a reactor-trip system. The column format is typical of that used to document an FMEA, but other formats can be used as well. Specific entries in the columns include a description of the component, its function and failure mode, causes of failure, possible effects, and method of failure detection. Sometimes a column for failure probability is added to provide additional information on the significance of the identified failure mode. If desired, an additional column can be added to the table and a criticality analysis can be performed to show quantitatively the effect of each component in the system.

Table 3-6. Summary of other methods

Method	Applicability	Characteristics
Phased-mission analysis	Evaluation of components, systems, or functions undergoing phased mission	Qualitative, quantitative, time-dependent; nonrepairable components only; assumes instantaneous transition
Markov analysis	Model and evaluation of components or systems	Quantitative, time-dependent, multiphased inductive; complexity increases rapidly; practical only for simple systems
GO	Evaluation of components, systems, or functions	Quantitative, time-dependent; modeling process complex; success oriented; has potential for modeling complete nuclear plant
FMEA	Identification of hazardous or dependent components or systems	Qualitative, inductive; considers only one failure at a time; simple to apply; provides orderly examination
MORT	Identification of hazards for improving safety	Qualitative; also used for accident investigation
Digraph	Model of components or systems	Qualitative; used to synthesize fault trees; complexity increases rapidly
Reliability block diagram	Model and evaluation of components or systems	Quantitative
Signal flow	Model and evaluation of components or systems	Quantitative; assumes constant failure and repair rates

The main disadvantage of FMEA is that it considers only one failure at a time and not multiple or preexisting failures. There is no limitation, however, to the number of components that can be considered simultaneously except that the number of combinations becomes prohibitively large with complex systems. The advantages of FMEA are that it is simple to apply and it provides an orderly examination of the hazardous conditions in a system.

In PRAs for nuclear power plants, the FMEA can effectively be used in several ways. As noted in Section 3.5.2, an FMEA-type of approach has been suggested as a means of searching for important failure modes associated with the reactor-coolant system. The FMEA approach can be adapted to a variety of uses. Many FMEAs are performed as part of the basic engineering process and are part of the information available to the PRA team. Such FMEAs can be effectively used as a precursor or as input information to the fault-tree models or in the identification of initiating events.

Component identification (1)	Function (2)	Failure mode (3)	Failure mechanism (4)	Effect on system (5)	Method of failure detection (6)	Remarks (7)
1. Circuit breaker 52/RTA, RTB, BYA, BYB	Trip	Fail closed	Mechanism jammed	Makes trip 1/1	Monthly test	
			UV trip attachment mechanism stuck	"	"	
			Main contacts fused	"	"	
		Fail open	Loss of dc control power	Spurious trip	Spurious trip	Immediate detection
			UV coil failure	"	"	
			Worn trip latch	"	"	
2. DC control relay	Break circuit to trip breaker UV coil on trip (de-energize to trip)	Fail closed	Contacts shorted or fused	Makes trip 1/1	Monthly test	
			Armature jammed	"	"	
			Wiring fault	"	"	
		Fail open	Loss of dc control power	Spurious trip	Spurious trip	Immediate detection
			Coil failure	Spurious trip if 2/2 fail	"	
			Broken contacts		"	
			Broken wire or loose connection	"	"	
3. AC control relay X1A, B, X2A, B, X3A, B	Break circuit to dc relays on trip (deener-gize to trip)	Fail closed	Contacts shorted or fused	Makes 1 train 2/2 vice 2/3	Monthly test	
			Armature jammed		"	
			Wiring fault	"	"	
		Fail open	Loss of ac power (instrument bus)	Spurious trip if 2/3	Spurious trip	
			Coil failure	" "	"	
			Broken contacts	" "	"	
			Broken wire or loose connection	" "	"	
4. Alarm unit PC-1,2,3	Remove ac power to relays for $P_M > P$ set	Fail off	Transformer failure	Makes both trains 1/2	Spurious trip if 2/3 fail	Partial trip alarm
			Open circuit in output section	" "	"	
			Setpoint drift	" "	"	
		Fail on	Short in output section	Makes both trains 2/2	Monthly test	
			Setpoint drift	" "	"	
5. DC power supply PQ-1,2,3	Provide power for analog current loop	Fail low or off	Transformer failure	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm
			Diode failure	" "	"	
		Fail high	Heat effects	Makes both trains 2/2	Monthly test	
			Misadjustment	" "	"	
6. Pressure transmitter PT-1,2,3	Convert pressure to analog current	Fail low	Corrosion	Makes both trains 2/2	Monthly test and compar-ison with redundant channel indicators	Possible immediate detection
			Wear	" "		
			Mechanical damage	" "		
			Heat effects	" "		
		Fail high	Misadjustment	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm

Figure 3-20. Typical format for a failure mode and effects analysis.

3.6.2 RELIABILITY BLOCK DIAGRAMS

Reliability block diagrams (RBDs) are models generated by an inductive process whereby a given system, divided into blocks representing distinct elements, is represented according to system-success pathways. The model generally is used to represent active elements in a system, in a manner that allows an exhaustive search for, and the identification of, all pathways for success.

The RBD method is commonly used in plant or system reliability predictions and allocations. In this application, the system blocks can be successively decomposed until the desired level of detail is obtained. Numerical calculations of system reliability are made, and sensitivity studies can be performed to allocate desired reliability values and optimize overall system reliability. Additional information on the development of RBDs and the numerical evaluation can be found in several texts on reliability engineering (Green and Bourne, 1972; Shooman, 1968).

Reliability block diagrams have been used to some extent in nuclear plant PRAs to facilitate and add clarity to the quantification of fault trees. A typical system analysis in RBD form is shown in Figure 3-21. The use of an RBD allows the analyst to summarize what he has learned about the importance of components in the system and facilitates the construction of Boolean expressions for estimating system unavailability.

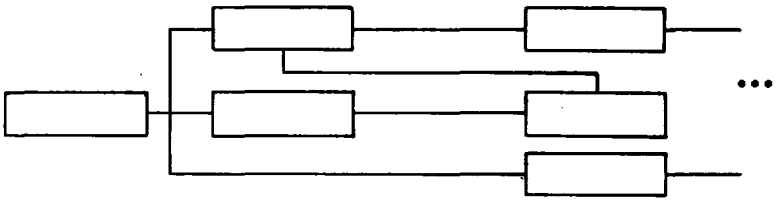
When used in the PRA process, the intent of the RBD is to combine, either directly or using the fault-tree logic as input, similar components that are in series in each system train into one supercomponent and then link together parallel supercomponents to form a summary model of the system. The selection of components whose reliability distributions are combined to produce a reliability distribution for the whole supercomponent can be based on minimal cut sets from the qualitative fault-tree evaluation. The advantage is that the combination of distributions is done step by step, making the quantification process more transparent. When used in conjunction with the cause table, discussed below, RBDs can be a powerful tool for explicitly handling dependent failures.

The set of minimal failure sets or cut sets expresses the logical relationship between the system and its components. Anything that can cause the system to fail must do so by acting through, that is to say by "causing," the failure of one or more failure sets.

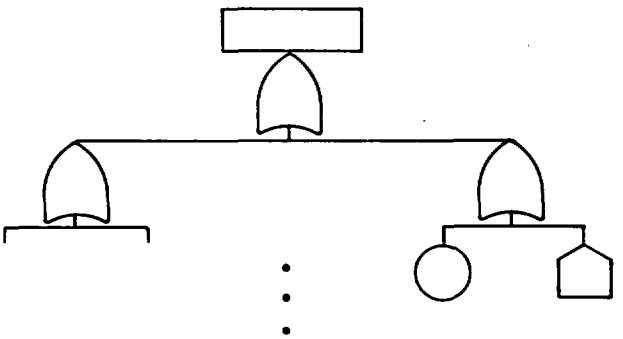
Information about what could possibly cause the failure of all components in a failure set or cut set can be summarized in a cause table. The conceptual form of this table is shown in Figure 3-21. One cause-table page is made for each order of failure set and for each boundary condition on the system. The causes of failure are listed in this table instead of being expressed as symbols in the fault tree, and therefore the RBD contains system components only. A cause table for a cut set allows the analyst to specify a single number for the contribution from each cause: random failures, testing and maintenance, human errors, etc. This number might arise from one human error disabling all the components or from one random failure of each component in the failure set. Dependent failures can therefore be handled explicitly, on the level of the failure set they affect.

System Logic

1. Block diagram



2. Fault tree



3. Failure sets (cut sets) $\{A, B\}, \{K, L, M\}...$

Cause list

Cause or cause set	Frequency	Response	Results
⋮	⋮	⋮	⋮

Analyst _____ Event tree _____ Branch point _____

Date _____ Cause table for system _____

(1) Candidate cause	(2) Occurrence fraction	(3) Operator response	(4) Response occurrence	(5) Combined occurrence	(6) Component failed	(7) System state	(8) Other systems	(9) Initiating events
CFSR								
T&M + CFSR								
Human errors								
Design errors								
Environmental factors								
Human error + CFSR								
Human error + T&M								
•								
•								
•								
Other								

Figure 3-21. Use of reliability block diagrams.

3.6.3 GO METHOD

The GO method (Gately and Williams, 1978a,b), unlike fault-tree analysis, is a success-oriented system-analysis technique. Adapted from the defense industry, it has been modified and refined for nuclear systems to incorporate some special modeling considerations, such as system interactions and man/machine interactions. Using an inductive logic to model system performance, the GO method determines system-response modes, both successes and failures.

A GO model, which consists of an arrangement of GO symbols, represents the engineering function of a component, subsystem, or system. It can generally be constructed from engineering drawings by replacing engineering elements (valves, switches, etc.) with one or more GO symbols, which are combined to represent system function and logic. The GO computer code uses the GO model to quantify system performance. The method has the capability to evaluate system reliability and availability, identify fault sequences, and rank the relative importance of the constituent elements.

Some key features of the GO method are the following: (1) models follow the normal process flow; (2) model elements have almost one-to-one correspondence with system elements and handle most component and system interactions and dependences; (3) models are compact and easy to validate; (4) outputs represent both success and failure states; (5) models can be easily altered and updated; (6) fault sets can be generated without altering the basic model; (7) system operational aspects can be incorporated; and (8) numerical errors due to truncation are known and can be controlled.

Briefly, the GO procedure uses a set of standardized operators to describe the logic operation, interaction, and combination of physical equipments. The logic for combining the inputs properly for each GO operator is defined in a series of algorithms contained in the GO computer codes. These standardized operators can be used to model most commonly encountered engineering subsystems and components. A system is modeled by selecting the GO operators that characterize the elements of the system and interrelating their inputs and outputs. The specific probabilities (point estimates) of component operation are defined separately as inputs to the computer code. At present, the analyst can use 17 standardized GO operators to develop the system models.

Figures 3-22 and 3-23 show a simple system and the associated GO chart. Each system element is represented as a compound number (1-30, 6-70, etc.). The first number represents the operator type (i.e., 1 represents a component that does or does not function properly; 6 refers to a component that needs two inputs), whereas the second number references the associated probabilities. The numbers on the connecting lines in the GO chart are called "signals" and are arbitrarily assigned to identify events whose probability of occurrence is to be estimated. Using the GO chart, the analyst inputs both model data and probability data into the computer, and the GO code calculates the probability for each signal.

A simple system like the one in Figure 3-22 can be identified as a modular block known as a supertype and combined with other supertypes to create

larger system or plant models. Figure 3-24 shows a GO chart for such a larger system.

The GO method appears to be well suited for estimating the success or failure probabilities of individual systems. The GO charts are rather easily created from system engineering drawings and follow the normal flow path. Small-system models can be efficiently evaluated, and sensitivity studies can be performed to determine the effect of changes in input parameters.

There are some disadvantages, however, to using the GO method. Complex systems require complex GO charts, which tend to become inscrutable for plant-level modeling. The ease of converting a system drawing to a GO chart and the similarity between the GO chart and a system schematic have certain drawbacks. The deductive nature of the fault tree requires an interrogatory thought process. This inquisitive rigor from a "how can it fail?" point of view provides a unique reason for using fault trees in a safety-related study. The GO method, although it can be used to construct failure models, lends itself to a direct translation from the system schematic to the logic model and is well suited for success modeling, such as system reliability and availability predictions. Moreover, the GO charts do not explicitly display hardware-failure modes. The failure-mode documentation must be done separately to complement the GO chart and allow the assignment of numerical data. Hence, the GO model can be more easily inspected for validity in representing the actual system than can a fault tree but is more difficult to review in terms of failure modes.

Several general conclusions can be drawn from some recent studies on the attributes of the GO and fault-tree methods. The GO method is ideally suited for many practical applications where the boundary conditions for the system are well defined by a system schematic or other design documents, and data can be satisfactorily applied at the component level. GO charts provide a concise model of the hardware events contributing to system success or failure. The GO chart and associated analysis tools explicitly and accurately represent most intrasystem hardware dependences of a functional or shared-equipment nature. The ability of the method to handle multiple system states makes it uniquely adaptable to analyses in which many levels of system availability are to be considered. In summary, GO is optimally applied to problems where the prime objective is to quantify the availability or reliability of a given system on the basis of a previously well-identified set of components or events.

GO is also well suited to the analysis of systems involving great numbers of hardware or hardware that is physically highly interconnected (i.e., electronic protection circuits). Because of efficiencies in the model operators, the GO chart tends to be more compact than the equivalent fault tree. Its similarity to engineering drawings aids in completeness checks, particularly if the checks are performed by design engineers. The "supertype" model provided by GO allows shortcuts in the modeling of redundant subsystems, which are frequently encountered in such systems. The algorithms of the GO codes are efficient in handling large trees; errors attributable to their tree-pruning process can be bounded.

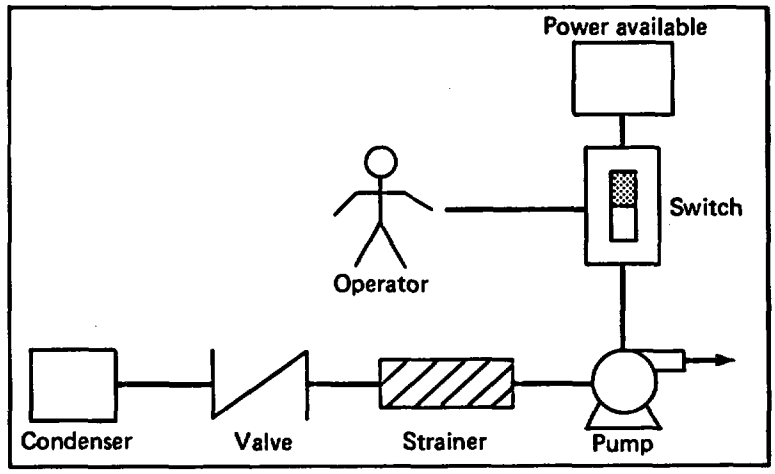


Figure 3-22. A simplified system for a GO model.

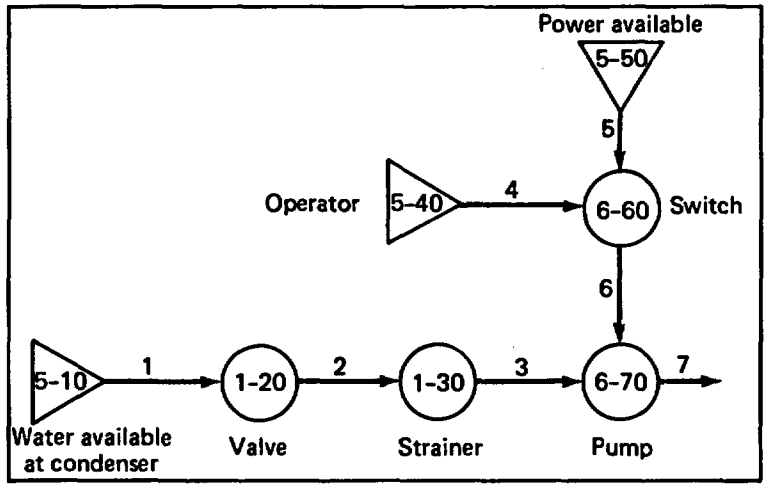


Figure 3-23. The GO chart for the system shown in Figure 3-22.
See page 3-61 for an explanation of the numbers.

Fault trees are better suited to analyses aimed at comprehensively investigating the failure modes and failure-mode combinations leading to a system top event, considering both software and hardware faults. The deductive, inquisitive nature of the fault-tree approach aids the analyst in going beyond the level of component events explicitly displayed in engineering drawings. Unlike the GO chart, which models failure modes implicitly, fault trees explicitly display and catalog the contributing faults identified by the analyst. In summary, fault trees are optimally applied to safety-analysis problems where an exhaustive cataloging of events is needed to identify primary and secondary faults and dependences beyond those explicit in a system schematic.

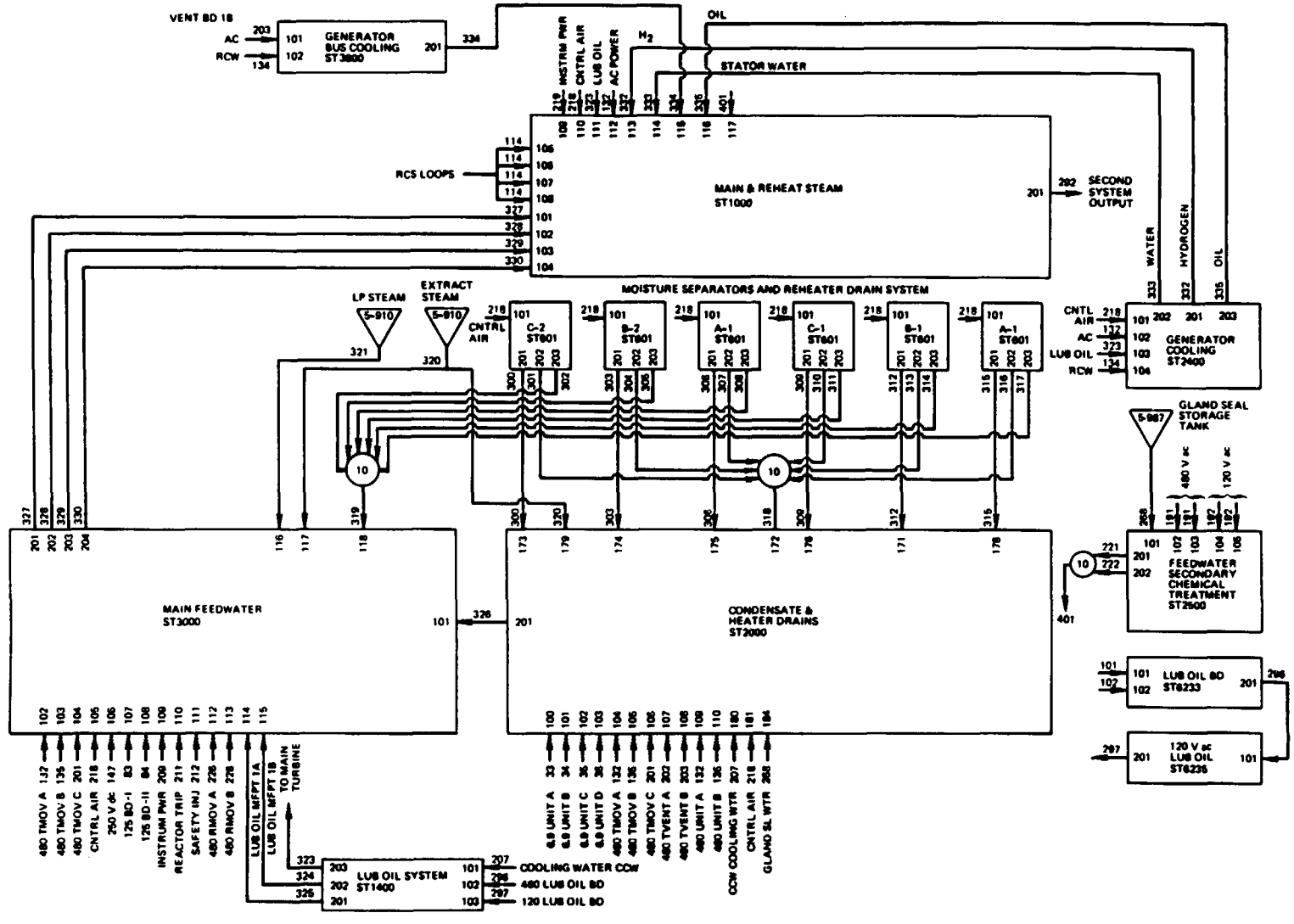


Figure 3-24. GO model for a PWR secondary loop system. Systems are shown as blocked supertypes, with only inputs and outputs showing interfaces depicted. The equipment in the supertypes has been previously modeled by means of elemental GO operators.

3.6.4 MODULAR FAULT-TREE LOGIC MODELING

Fault-tree modeling has been used in a variety of applications and has been subjected to numerous modifications. Most of these modifications have been aimed at making the modeling more efficient and reducing the more-routine documentation and evaluation activities. One such modification, currently being used in nuclear plant PRAs, is the modular fault-tree logic model.

Nuclear power plants have a number of features in common, including similar system configurations and components. As a result, the fault trees for different plants may have similar structures. Because of this, it is possible to develop modular logic models that represent the failure logic for many common plant features and to use these modules to aid in gathering the plant-specific information needed for detailed fault trees.

The approach to modular fault trees is significantly different in that the analyst selects the proper logic to fit the system and then edits pre-existing logic models. To develop the modular fault tree, the system is divided into segments, and the fault logic for the system is developed in terms of failures in the segments as defined by a set of rules. A detailed fault logic for each segment is developed through standardized subtrees that can be adjusted to properly represent the specific characteristics of each segment. Common components like valves and pumps are classified by type, and subtrees are developed for each. The analyst must edit the component tree by adding appropriate labels and deleting any events that do not apply to the particular component. Care must be taken to ensure that unique labels are applied to each component: a component must have the same label wherever it appears in trees for the plant, and no two different components can have the same label.

After the fault-tree analyst completes the fault trees for a system, he submits them to a computer analyst for conversion to computer input data. The modular logic models are stored in computer files and can be called up on a computer-graphics display system as the computer analyst selects the appropriate trees, adds the required labels, and deletes any branches not needed for the specific plant. The computer analyst will also prepare the input for trees not covered by the modular logic models and will generate plots of all the trees. The plots will be returned to the fault-tree analyst for review and correction.

Figure 3-25 shows a portion of a typical modular tree for a fluid-delivery system. It shows a modular section that can be edited to reflect an accurate system configuration. Individual contributing events are themselves modular, and the sections in which they appear can be subsequently edited to reflect an accurate characterization of the portion of the system being evaluated. The intent of this modular logic modeling is to overcome a number of the limitations commonly associated with the use of fault trees in modeling large systems. For example, it would provide the means for developing detailed trees to an analyst who has a thorough knowledge of plant systems but limited knowledge of fault-tree techniques. The modular

approach can also reduce the time required to develop specific trees and can improve consistency between analyses performed for different plants.

The use of modular fault trees may at first present some difficulties. For instance, in adapting to the rules and procedures required for the most efficient use of the technique, the analysts may generate large numbers of preliminary fault models for components of interest. Some concern has also been expressed about the potential for generating fault trees in a rather automatic mode without the required correlation of system information to the developing model. The intent of the modular approach is to reduce the amount of time the analyst must spend on routine and mundane analytical tasks. The effort conserved could then be applied to those details that are most important to the overall analysis. The approach appears to have considerable promise for specific fault-tree applications.

The modular logic approach was recently developed at Sandia National Laboratories with specific application to nuclear plant security and safeguards systems. Its first use for in-plant risk assessments occurred in the Interim Reliability Evaluation Program. The experience gained from those efforts should help to further develop the method and aid in its application on a broader scale.

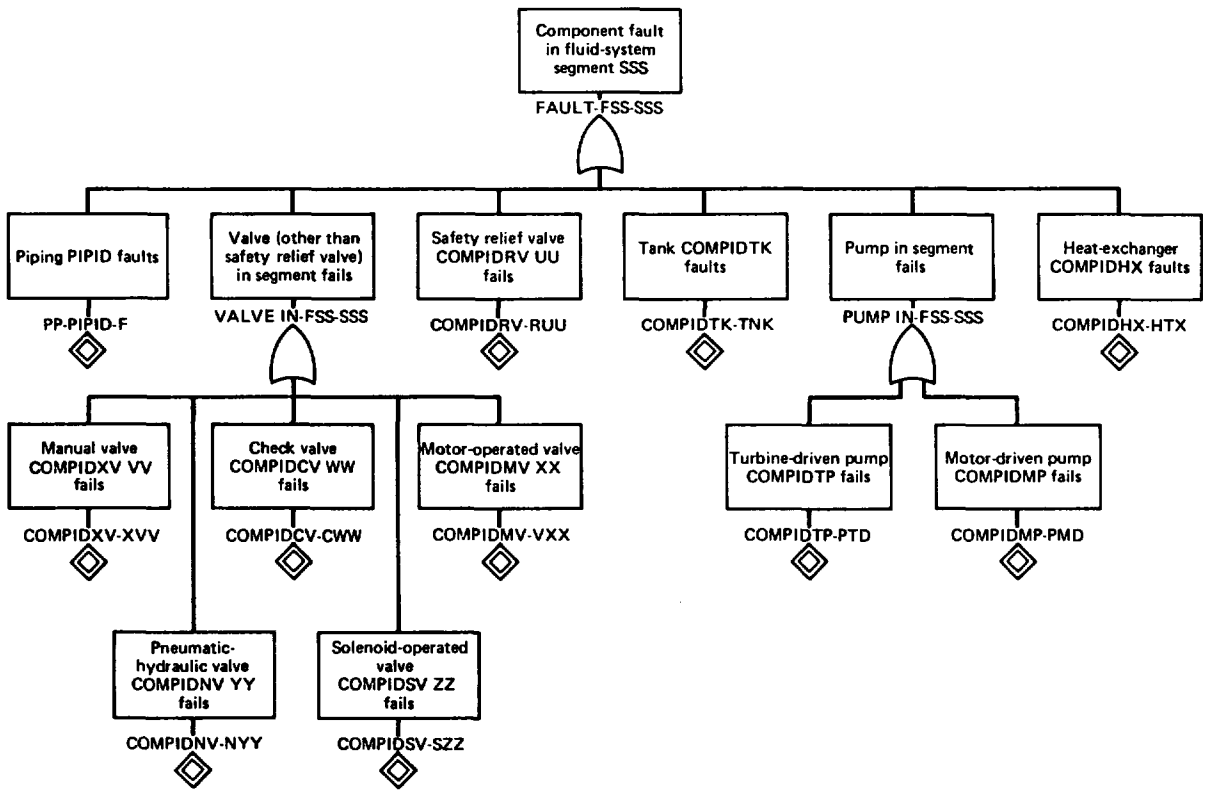


Figure 3-25. Fluid-system segment modular logic.

3.7 ANALYSIS OF DEPENDENT FAILURES

This section described the various types of dependent failures encountered in PRA studies. It defines nine different types of dependent failures and presents an integrated procedure for the analysis of each type. The procedure is a synthesis of several methods, which are described and illustrated by examples. Special considerations in the collection and interpretation of dependent-failure data are discussed. If a particular type of dependence can be treated in different ways, guidance is provided as to which method to select, depending on the information available and the scope and objectives of the PRA.

Dependent failures are extremely important in risk quantification and must be given adequate treatment to avoid a gross underestimation of risk. Risk estimates can err by many orders of magnitude if the possibilities for the so-called common-cause failures and system interactions are overlooked. Since dependent failures must be taken into account in a number of PRA tasks, several chapters in this guide cover various aspects of their analysis. However, in view of their importance, this separate section was set aside to provide a concise summary of the methods and procedures that should be used in their analysis. Where appropriate, other sections are referenced for relevant details.

3.7.1 INTRODUCTION

In risk analysis the treatment of dependences in the identification and quantification of accident sequences is called "dependent-failure analysis." Dependences tend to increase the frequency of multiple, concurrent failures. Since essentially all important accident sequences that can be postulated for nuclear reactor systems involve the hypothesized failure of multiple components, systems, and containment barriers, dependent-failure analysis is an extremely important aspect of PRA.

The failure events A and B are said to be dependent if

$$\phi(A \text{ AND } B) = \phi(A) \cdot \phi(B|A) \neq \phi(A) \cdot \phi(B)$$

In other words, the frequency of concurrent failure events A and B, $\phi(A \text{ AND } B)$, cannot be expressed simply as the product of the unconditional failure-event frequencies $\phi(A)$ and $\phi(B)$.

Several terms have been used to describe specific types of dependent failures. Common-mode failures* are multiple, concurrent, and dependent failures of identical equipment that fails in the same mode. Propagating

---

*In the Reactor Safety Study (USNRC, 1975), the term "common-mode failure" was used in a broader sense to include all the types of dependent failures defined in Section 3.7.2.

failures occur when equipment fails in a mode that causes sufficient changes in operating conditions, environments, or requirements to cause other items of equipment to fail. Common-cause failures are failures of multiple equipment items occurring from some single cause that is common to all of them. While a great many dependent failures are due to a common cause, not all can be categorized as such, propagating failures being a case in point.

Unfortunately, the above three categories of dependent failures are neither mutually exclusive nor exhaustive. This has resulted in much confusion in the literature. For our purposes the term "dependent-failure analysis" will be used to describe the assessment of all multiple, concurrent, and dependent failures. A survey of the various definitions that have been proposed for common-cause and common-mode failures has been published by Smith and Watson (1980).

3.7.2 DEFINITION OF DEPENDENT FAILURES

A number of authors have developed extensive lists of categories of dependent failures with the primary objective of design improvement. One of the more comprehensive classifications is that by Watson and Edwards (1979). The purpose here, however, is to help risk analysts select methods for their analysis, and therefore the simplified classification scheme described below is adequate.

Type 1. Common-cause initiating events (external events): external and internal events that have the potential for initiating a plant transient and increase the probability of failure in multiple systems. These events usually, but not always, cause severe environmental stresses on components and structures. Examples include fires, floods, earthquakes, losses of offsite power, aircraft crashes, and gas clouds.

Type 2. Intersystem dependences: events or failure causes that create interdependences among the probabilities of failure for multiple systems. Stated another way, intersystem dependences cause the conditional probability of failure for a given system along an accident sequence to be dependent on the success or failure of systems that precede it in the sequence. There are several subtypes of interest in risk analysis.

> Type 2A. Functional dependences: dependences among systems that follow from the plant design philosophy, system capabilities and limitations, and design bases. One example is a system that is not used or needed unless other systems have failed; another is a system that is designed to function only in conjunction with the successful operation of other systems.
>
> Type 2B. Shared-equipment dependences: dependences of multiple systems on the same components, subsystems, or auxiliary equipment. Examples are (1) a collection of pumps and valves that provide both a coolant-injection and a coolant-recirculation function when the functions appear as different events in the event tree and (2) components in different systems fed from the same electrical bus.

Type 2C. Physical interactions: failure mechanisms, similar to those in common-cause initiators, that do not necessarily cause an initiating event but nonetheless increase the probability of multiple-system failures occurring at the same time. Often they are associated with extreme environmental stresses created by the failure of one or more systems after an initiating event. For example, the failure of a set of sensors in one system can be caused by the excessive temperature resulting from the failure of a second system to provide cooling.

Type 2D. Human-interaction dependences: dependences introduced by human actions, including errors of omission and commission. The persons involved can be anyone associated with a plant-life-cycle activity, including designers, manufacturers, constructors, inspectors, operators, and maintenance personnel. A dependent failure of this type occurs, for example, when an operator turns off a system after failing to correctly diagnose the condition of the plant--an event that happened during the Three Mile Island accident when an operator turned off the emergency core-cooling system.

Type 3. Intercomponent dependences: events or failure causes that result in a dependence among the probabilities of failure for multiple components or subsystems. The multiple failures of interest in risk analysis are usually within the same system or the same minimal cut set that has been identified for a system or an entire accident sequence. Subtypes 3A, 3B, 3C, and 3D are defined to correspond with subtypes 2A, 2B, 2C, and 2D, respectively, except that the multiple failures occur at the subsystem and component level instead of at the system level.

3.7.3 METHODS FOR DEPENDENT-FAILURE ANALYSIS

3.7.3.1 Overview

Dependent failures must be taken into account in (1) the selection of initiating events, including external events; (2) the definition of accident sequences (event-tree construction); (3) system modeling (fault-tree construction); and (4) the quantification tasks described in Chapters 5 and 6. Their analysis is therefore performed by using a combination of separate methods.

The available methods for dependent-failure analysis can be categorized as either explicit, parametric, or computer aided (see Table 3-7). Explicit methods involve the identification of specific causes of dependent failures in the event- and fault-tree logic. Included in this category are the event-specific models (method a), which treat event frequencies and impacts (fragilities) in terms uniquely appropriate to each event; examples are earthquakes, fires, and floods. The human-reliability models (method e) have been set aside as a separate explicit-method category and are discussed in detail in Chapter 4.

The second category of methods, termed parametric, includes the models known as the beta factor (Fleming, 1975) and the binomial failure rate

Table 3-7. Summary of principal methods for the analysis of dependent failures

Category		Method	Applicability to steps in risk analysis: Selection of initiating events[a]	Definition of accident sequences	System modeling[b]	Quantification[c]
Explicit	a.	Event-specific models	X	X	X	X
	b.	Event-tree analysis		X	X	(d)
	c.	Fault-tree analysis	X		X	(d)
	d.	Cause-table analysis	X		X	(d)
	e.	Human-reliability analysis		X	X	X
Parametric	f.	Beta factor				X
	g.	Binomial failure rate				X
Computer aided	h.	GO		X	X	X
	i.	WAMCOM[e]	X		X	
	j.	COMCAN[e]	X		X	
	k.	BACFIRE[e]	X		X	

[a]Including external events.
[b]Includes the steps of Boolean reduction.
[c]Including the tasks described in Chapters 5 and 6.
[d]No special quantification techniques are needed for these methods.
[e]The method used by these computer codes is sometimes referred to as the "generic cause approach."

(Vesely, 1977) (methods f and g in Table 3-7). In these methods, new reliability parameters are added to the usual list to account for dependent failures. The optimal application of the beta-factor and the binomial failure-rate methods is in estimating the values for one and two dependent-failure parameters, respectively, from dependent-failure experience data. In the Limerick PRA study (Philadelphia Electric Company, 1981), conditional probabilities for the common-cause failures of diesel generators were estimated from experience data. These conditional probabilities are essentially the same as beta factors.

Computer-aided techniques for dependent-failure analysis comprise the third category of methods, which include the codes GO (Kelley and Stillwell, 1981), WAMCOM (Putney, 1981), BACFIRE (Rooney and Fussell, 1978) and COMCAN (Rasmuson et al., 1979). The latter three codes involve the search of fault-tree minimal cut sets for common susceptibilities to failure. The GO code, in addition to serving as an alternative to the fault-tree-analysis codes (e.g., WAM series, RAS), can also be used to analyze intersystem dependences in the construction and quantification of event trees.*

Table 3-8 summarizes the applicability of the various methods to different types of dependent failures. The dependences associated with common-cause initiating events are handled with event-specific models, (method a) and with the methods of event- and fault-tree analysis; details are discussed in Chapter 10. Intersystem functional dependences are normally identified in the construction of event trees. Shared-equipment dependences can be treated with a combination of event- and fault-tree methods; several variations are described in Section 3.7.3.3. Physical interactions resulting in multiple failures are treated with event-specific models and are identified in event trees and cause tables (see Section 3.6.2). All the methods except event-tree analysis are useful in the analysis of intercomponent dependences. The parametric methods (f and g) were developed and have been applied especially for the subset of intercomponent dependences known as common-cause failures. More details and illustrative examples are given in the sections that follow.

3.7.3.2 Dependent Failures of Type 1: Common-Cause Initiating Events

The first step in the analysis of common-cause initiating events, often referred to as "external events," is the selection of the respective initiating events for detailed risk analysis. The procedure for this selection is described in Chapter 10. In the case of events that occur in specific locations of the plant (e.g., fires and floods), the selection of specific locations can be accomplished with the aid of event- and fault-tree techniques. Examples are given in Chapter 11. The computer-aided methods (h through k) can aid in assigning priorities to plant locations for analysis. The GO code can be used to provide the interface between the event-specific and the event- and fault-tree logic parts of the analysis. Details are discussed in Chapter 10.

---

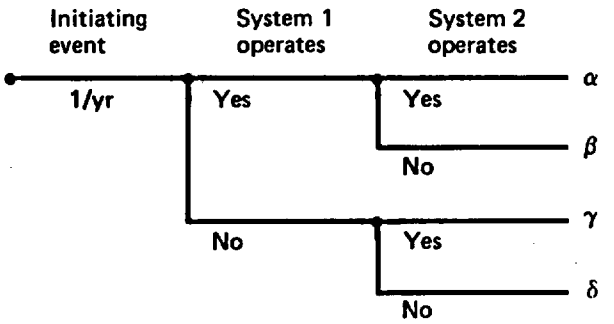
*See Section 6.6 for a description of the computer codes discussed here.

Table 3-8. Applicability of methods to types of dependent failures

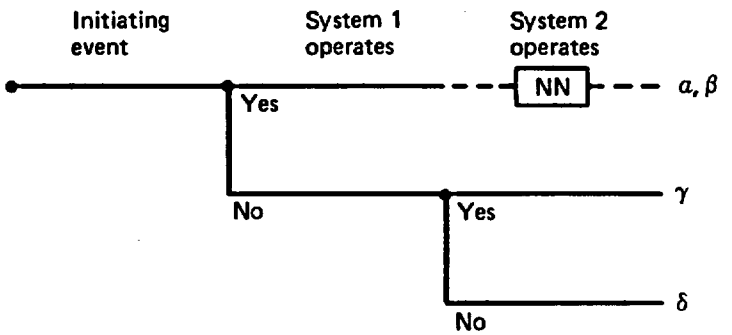
Method	Dependent-failure type: Common-cause initiating events 1	Intersystem functional dependences 2A	Intersystem shared equipment 2B	Intersystem physical interactions 2C	Intersystem human interactions 2D	Inter-component dependences 3
a. Event-specific models	X			X		X
b. Event-tree analysis	X	X	X		X	
c. Fault-tree analysis	X	X	X	X	X	X
d. Cause-table analysis				X		X
e. Human-reliability analysis				X	X	X
f. Beta factor						X
g. Binomial failure rate						X
h. GO	X		X	X		
i,j,k. WAMCOM, COMCAN, BACFIRE	X		X	X		X

3.7.3.3 Dependent Failures of Type 2: Intersystem Dependences

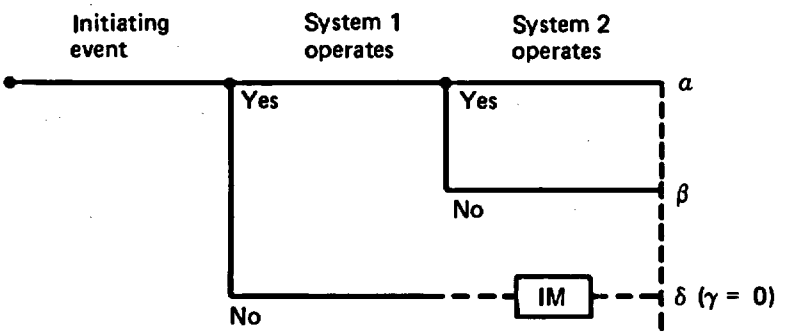
The four types of intersystem dependences (types 2A, 2B, 2C, and 2D) can be analyzed by means of event trees, fault trees, or a combination of them. The variety of approaches available can be explained in terms of a simple event tree:



To illustrate the effect of functional dependences (type 2A), suppose that system 2 is not needed unless system 1 fails. This would be reflected in the event tree as follows:

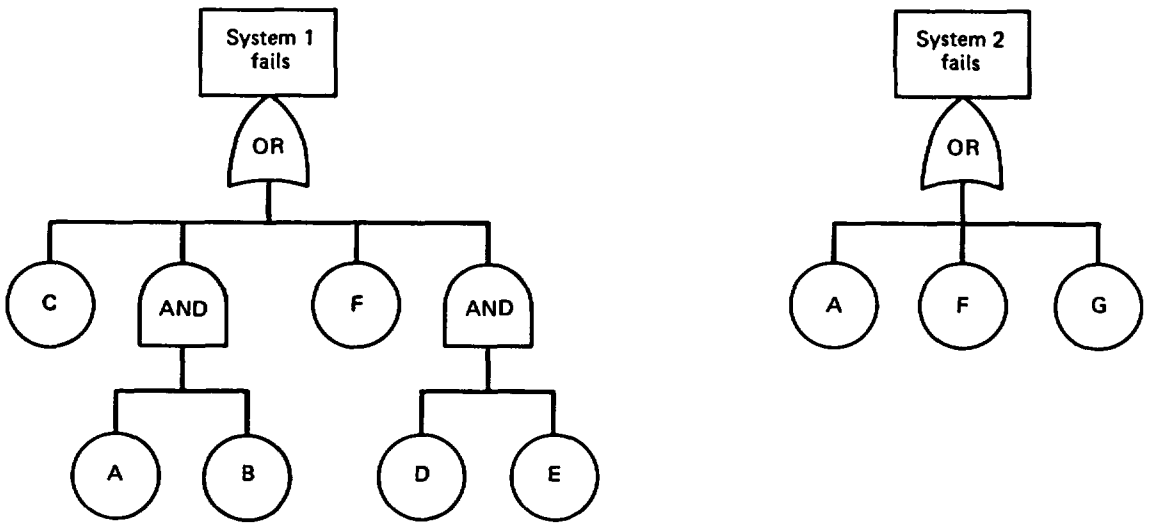


where NN denotes "not needed." Another example of a functional dependence is the case where system 2 can operate only in conjunction with the successful operation of system 1. Such a condition could result from some physical interaction (type 2C) that takes place when system 1 fails. It is reflected in the event tree as follows:

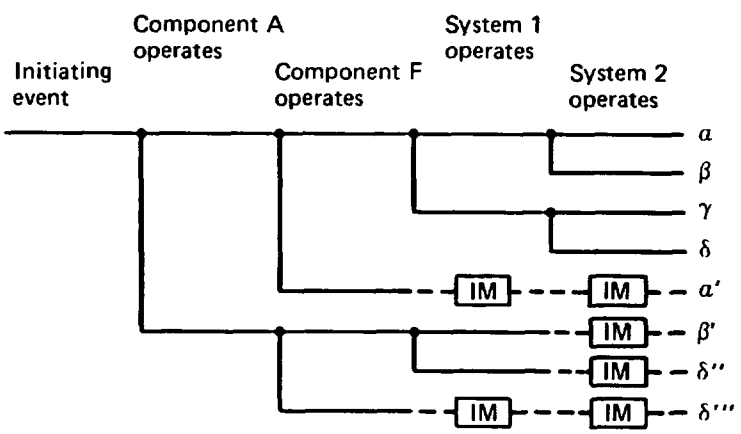


where IM denotes "impossible."

To illustrate the event-tree approach for analyzing dependences of type 2B, shared equipment, suppose that the fault trees developed for systems 1 and 2 are found to contain the same component failures, A and F, as primary events:



Components A and F have shared-equipment dependences and can be treated by incorporation into the event tree as follows:



To complete the analysis, the system fault trees are quantified as conditional on the states of A and F, which are treated as "house" events. For example, along sequence δ" the fault tree for system 1 is quantified with t(A) = 1 and P(F) = 0, which gives the conditional minimal cut sets {C, B, DE}. On the other hand, along sequence δ the conditions are P(A) = 0 and P(F) = 0, which gives the minimal cut sets for system 1 of {C, DE}. This method of analyzing shared-equipment dependences, referred to as "event trees with boundary conditions," is discussed in more detail in Chapter 6.

Another approach to treating shared-equipment dependences is to link the system fault trees together, thus developing a single large fault tree

for the entire accident sequence. In the case of sequence γ, for example, a fault tree would be constructed for the top event "system 1 fails and system 2 operates successfully." This tree would be synthesized from the respective system fault trees by linking them together with an AND gate. For each system that is postulated to operate successfully in the sequence, it is necessary to convert the failure logic in the fault tree to success logic. The fault tree for sequence γ would then look like Figure 3-26.

During the Boolean reduction of the fault tree shown in Figure 3-26, the shared-equipment dependence as well as the effect of success states are properly taken into account. It can be easily shown that, if properly evaluated, the methods of fault-tree linking and event trees with boundary conditions give identically correct results.

Note that it is not necessary to physically construct the sequence logic tree to implement the fault-tree-linking method. An alternative is to determine the minimal cut sets of each system separately and to resolve the shared-equipment dependence by using Boolean algebra to manipulate the system cut sets to find the minimal cut sets for the sequence. The Boolean logic is initially synthesized to yield

$$\gamma = 1 \text{ AND } 2$$

$$= \left[(A \text{ AND } B) \text{ OR } C \text{ OR } (D \text{ AND } E) \text{ OR } F\right] \text{ AND } \overline{(A \text{ OR } F \text{ OR } G)}$$

After Boolean reduction, the logic is simplified to the form

$$\gamma = \left[C \text{ OR } (D \text{ AND } E)\right] \text{ AND } (\bar{A} \text{ AND } \bar{F} \text{ AND } \bar{G})$$

which is equivalent to the list of minimal cut sets obtained by analyzing the synthesized fault tree:

$$\{\overline{AFG}C;\ \overline{AFG}DE\}$$

An alternative approach to the above procedure, which was used in the Interim Reliability Evaluation Program (IREP), is to link the system failures stated along each accident sequence together with an AND gate, determine the minimal cut sets of the AND gate, and compare these minimal cut sets to those of the fault trees for the system successes in the accident sequence. For the above example, the minimal cut sets for the AND gate are

$$\{AB,\ C,\ DE,\ F\}$$

After the minimal cut sets of the AND gate are determined, any minimal cut set that is a superset of a minimal cut set of a fault tree for a system success in the accident sequence is eliminated. For sequence γ in the above example, the minimal cut sets of the fault tree for the system success (system 2) are

$$\{A,\ F,\ G\}$$

Since AB is a superset of A and F is a superset of F, minimal cut sets AB and F are eliminated from the set of minimal cut sets for sequence γ.

The final set of minimal cut sets for sequence γ becomes $\{C, DE\}$. Thus, the minimal cut sets that cause system 2 to fail, contradicting the assumption that system 2 succeeds, have been eliminated.

When rigorously followed, both fault-tree linking and event trees with boundary conditions correctly model the shared-equipment dependences and both entail, apparently, comparable levels of data processing. In actual applications it is necessary to construct much larger models than that used in the preceding examples to accommodate the larger number of systems and associated dependences that must be taken into account. There is a trade-off between the level of detail in the event trees and that in the fault trees. In the method of fault-tree linking, the event trees can be kept rather small, on the order of those used in the Reactor Safety Study (USNRC, 1975), whereas the fault trees for each sequence are rather large. In contrast, the method of event trees with boundary conditions requires the use of large event trees, with correspondingly smaller fault trees for each node in the event tree. With either method, the size of the tree can become impractical if the tree is not simplified in some way. The conservative approximations that can be used with either method to reduce the size of the models for easier quantification are discussed in Chapter 6.

The method of event trees with boundary conditions has a variation that can be used to reduce the size of trees for quantification; this variation

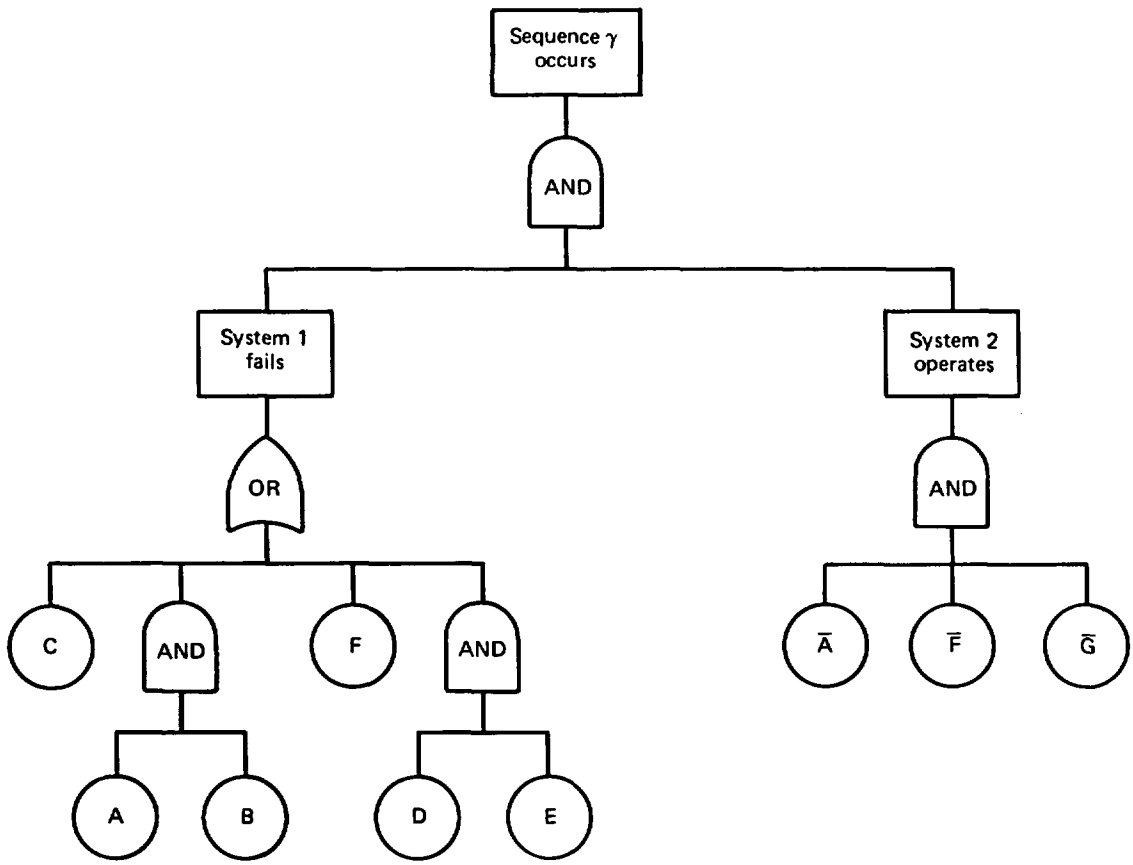


Figure 3-26. Hypothetical fault tree for sequence γ. Here X denotes failure; $\bar{X}$ denotes the successful functioning of the component.

makes use of multiple-system event trees. In practice, most shared-equipment dependences involve the dependence of front-line systems on support systems. The use of event trees with boundary conditions is made more efficient by developing a separate event tree for the support systems and separately quantifying their contributions to the risk-dominant sequences.

To illustrate the analysis of support-system dependences in separate event trees, consider the simple example of a plant that consists of three systems that must respond to some hypothetical initiating event: (1) the emergency core-cooling system (ECCS), (2) the auxiliary feedwater system (AFWS), and (3) the containment-building fan coolers (FC). Suppose also that the ECCS, AFWS, and FC systems each requires dc power, ac power, and service water as support systems. Each system is assumed to be a two-train redundant system with no cross-tie capability between divisions of front-line and support systems. It is further assumed that ac power is dependent on dc power, and service water requires both ac and dc power. The support-system event tree for this example is shown in Figure 3-27. The frequency of each sequence can be quantified by the methods described in Chapters 5 and 6. The impact of each support-system failure/success combination on the event tree is assigned an "impact vector" to describe the front-line systems that fail as a result of support-system failures. As indicated in Figure 3-27, the number of unique impact vectors is often much less than the number of sequences on the event tree. Hence, the 16 sequences result in only four unique impacts. The frequencies of each impact vector, or "support-system state," can then be obtained from

$$\phi(I_k|iE) = \sum_j \phi(I_{jk}|iE) \qquad (3\text{-}1)$$

where $\phi(I_k|iE)$ is the total frequency of unique impact vector k given the initiating event occurs and $\phi(I_{jk}|iE)$ is the frequency of the j^{th} event sequence, whose impact vector is identical with I_k given the initiating event occurs.

The analysis is completed by evaluating the front-line-system event tree--which in this example includes the ECCS, AFWS, and FC systems as event-tree headings--for each support-system state. The impact vector is used to establish the boundary conditions for the quantification of each state. The total frequency of any sequence ℓ in the front-line event tree is then obtained by using

$$\phi(\ell) = \phi(iE) \sum_{k=1}^{K} \phi(I_k|iE)\ \phi(\ell|I_k,iE)$$

where $\phi(iE)$ is the frequency of the initiating event and $\phi(\ell|I_k,iE)$ is the frequency of sequence ℓ in the front-line event tree given support-system state k and the initiating event.

The above technique was used in the Zion PRA (Commonwealth Edison Company, 1981) to analyze the dependences of plant systems on electric power. More recently, the approach has been integrated into an advanced version of the GO code (Kelley and Stillwell, 1981) that has the capability to automatically construct the event tree from a GO model of the plant and

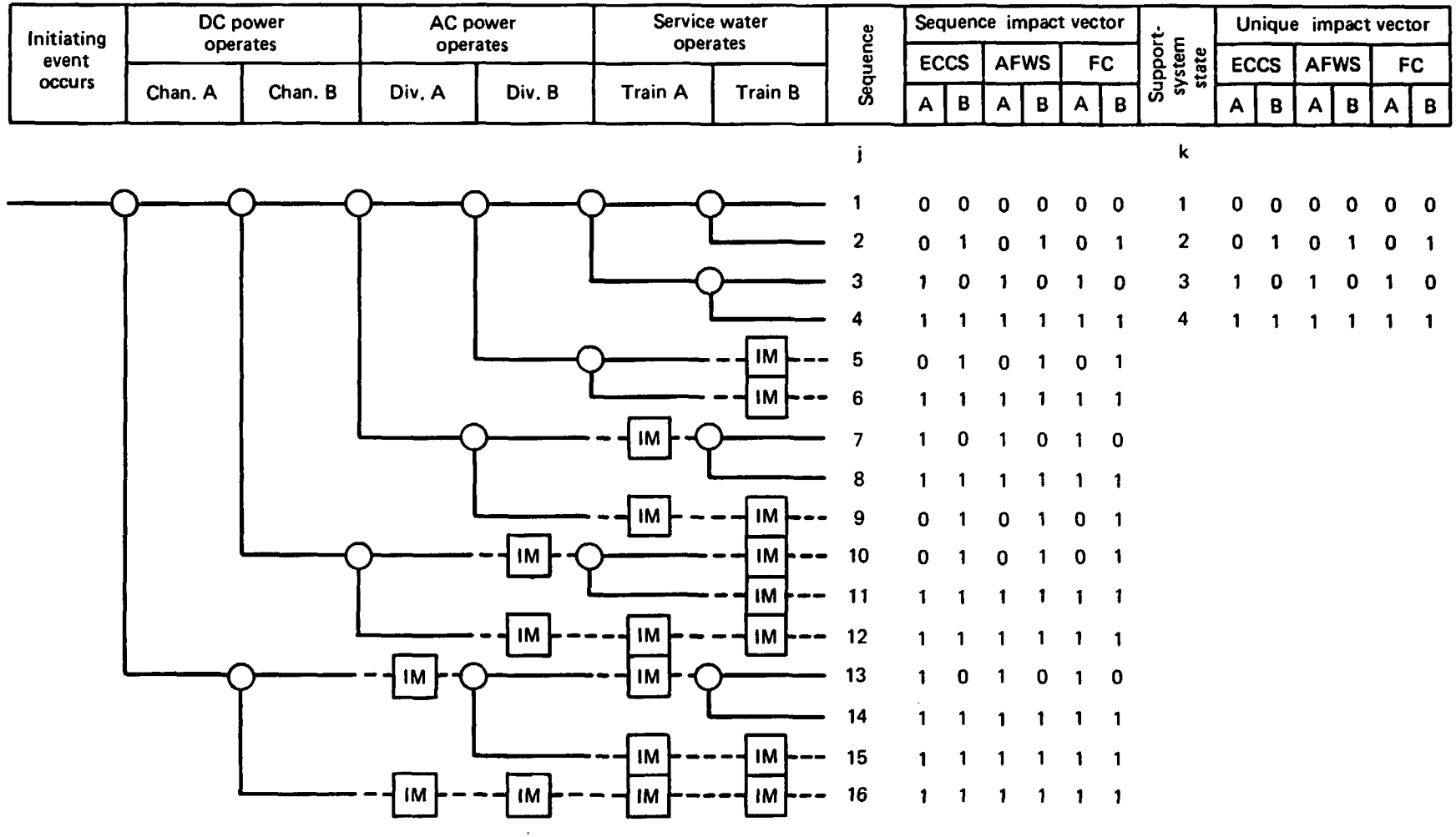


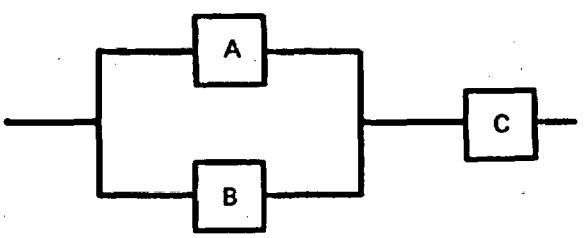
Figure 3-27. A support-system event tree with impact vectors.

system interconnections, assign impact vectors to each sequence, and perform the summation of Equation 3-1. The use of a computer-aided procedure to analyze intersystem dependences in this fashion greatly simplifies the analysis of the event trees for front-line systems. The use of computer aids for dependent-failure analysis is discussed further in Section 3.7.3.9.

The assignment of impact vectors to the support-system event trees provides an intermediate assessment of the level of damage or the consequences associated with the portion of the accident sequences that appears in the support-system event trees. Because the quantification of support-system event trees yields information about both the frequency and the damage level of each sequence, it is possible to find the risk-dominant support-system sequences, or states, without quantifying the front-line or the containment event trees. The support-system states that can be shown not to make significant contributions to risk can be "pruned" at this step, thus reducing the number of states that need to be run through the front-line event trees. Hence, a separate event-tree analysis of support systems requires less overall data processing than does either the method of fault-tree linking or the variation of the event tree-boundary condition method in which both support and front-line systems are included in the same single event tree.

3.7.3.4 Analysis of Intercomponent Dependences (Common-Cause Failures)

Once the intersystem dependences are accounted by means of one of the methods described in the preceding section, the plant logic has been developed to a level of detail corresponding with basic component-failure modes. Before the quantification of the event and fault trees can be completed, it is necessary to analyze the possibilities for dependences among the basic component failures (type 3 intercomponent dependences). A well-known category of dependent failures involving multiple components is common-cause failure (CCF): the occurrence of multiple component failures induced by a single, shared cause. The importance of CCF in system-failure analysis can be seen from the following simple example of a system with three components A, B, and C. Suppose that the reliability block diagram for this system is given by



The corresponding system unavailability Q can be expressed as

$$Q = P(A \text{ AND } B) + P(C) - P(A \text{ AND } B \text{ AND } C)$$

or alternatively as

$$Q = P(A) \cdot P(B|A)\left[1 - P(C|A \text{ AND } B)\right] + P(C)$$

where P(x) is the availability of component x and P(y|z AND t) is the unavailability of component y given components z and t are failed.

The significance of common-cause failures in this example is as follows: any cause of failure that affects any pair or all three components at the same time (or, in general, any multiple set of components in the system) will have an effect on system unavailability. When Equation 3-2 is used, these common causes show up as dependences in that the conditional component unavailabilities--for example, P(B|A)--are different from, and often significantly greater than, the respective unconditional unavailabilities; in other words, P(B|A) >> P(B). It is a well-known characteristic of common-cause failures that, if the cause or causes are shared by two or more components in the same minimal cut set, the assumption that the component unavailabilities are independent leads to optimistic predictions of system reliability. It is not so well known that, if the dependence exists between two or more units in a series system (i.e., in different minimal cut sets), the assumption of independent failures can lead to conservative predictions, depending on how the data are analyzed. However, the former effect is more important and can lead to considerably larger errors in calculations for highly reliable redundant systems.

The magnitude of the errors that result from neglecting common-cause failures can be seen by developing the model of the above three-component system in terms of sets of explicit causes of component failure. Suppose that each of the three components can fail through independent causes, denoted by A', B', and C', and further that there are additional causes of failure, denoted by D, common to components A and B, and a final set of causes, denoted by E, that are common to components B and C.

The causes of single and multicomponent failures can be represented in the format of a fault tree (see Figure 3-28) where the causes appear at the level below the basic component-failure modes.

An alternative approach is to develop the failure causes for each component-failure set in the form of a cause table (see Section 3.6.2), separately from the fault tree or the reliability diagram, which is left in terms of basic component-failure modes. In Table 3-29 this fault tree is quantified under the assumption that all the causes of single and multicomponent failures are independent for the different cases chosen to illustrate the effect of the common causes. The tree can then be quantified in the normal way with the aid of the minimal cut sets of causes rather than the minimal cut sets of component-failure modes, both of which are indicated in Figure 3-28.

Cases 1 and 2 are selected to illustrate the well-known result of a common cause shared by redundant components, in this case A and B. In each of these cases the component unavailability is held fixed at 1×10^{-3} but is distributed differently between the independent and the common causes. As the common-cause contribution is varied from 0 to 1 percent (essentially the same as varying the component beta factor from 0 to .01), the system unavailability is increased by more than a factor of 10. Of course, there are examples in which the effect of common cause is many orders of magnitude. However, these values were selected to help view the problem from a different perspective, as explained in the discussion that follows.

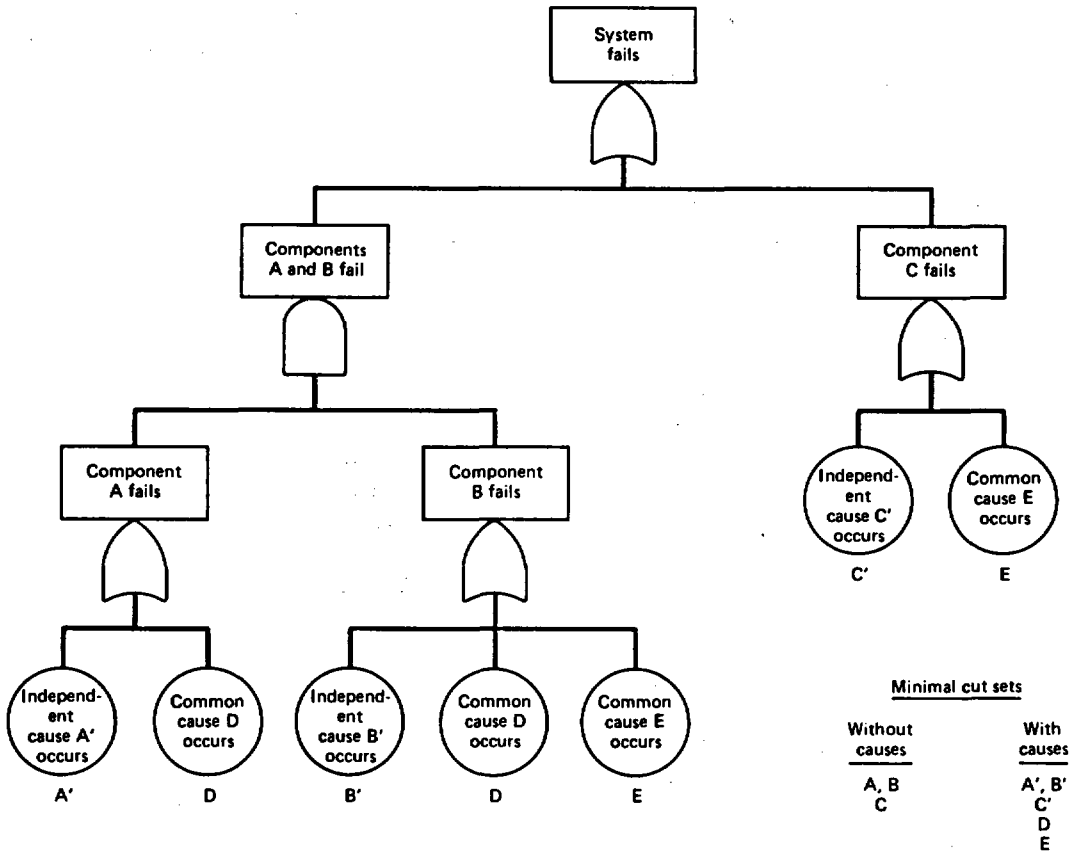


Figure 3-28. Fault tree for a three-component system with independent and common causes.

Let us examine case 1--the typical situation in which the component unavailabilities are known and it is assumed that the component-failure modes are independent. This assumption implies that all the causes of component failure, which presumably are not known in most cases, are also independent. A comparison of cases 1 and 2 shows that, in order for the result of case 1 to be "correct," it is necessary to establish that all causes of failure, which contribute to more than 99 percent of the component unavailability, are independent. (Even if only 0.1 percent of the failure-cause contribution is common, the result of case 1 is still off by a factor of 2.) This result can be generalized to the statement that, whenever independence is claimed between subsystems highly reliable redundancy, it is necessary to have an extraordinarily high level or confidence in asserting that all causes of subsystem failure are independent. The level of confidence that the independence assumption is correct must exceed the complement of the unavailability claimed for the redundant subsystem. This result is compounded for higher levels of redundancy.

Cases 3 and 4 illustrate a result that is not so well known: for a given fixed level of component unavailability, common-cause failures actually tend to improve the reliability of a system of components in series (i.e., components not in the same minimal cut set). In these two cases, the redundancy is eliminated (P(A) = 1) and the unavailabilities of components B and C are held fixed, again at 10^{-3}. As the common-cause contribution to

component unavailability increases from 0 to 50 percent (i.e., as the beta factor increases from 0 to 0.50), the system unavailability decreases by 30 percent. In most cases the common-cause fraction would be expected to be less than 50 percent, in which case the effect on the series system unavailability would be smaller. Hence, this type of common cause can usually be ignored with a small error on the conservative side. However, this example points to the fact that the existence of any cause common to any set of components in a system changes the unavailability of the system. The situation becomes even more complicated in the multisystem or plant-level models encountered in risk analysis.

The simple model and examples described above are also useful in describing some of the interrelationships between common-cause failures and their analysis--and the related issues of human reliability, data, and completeness. The role of completeness should be obvious from the quantification cases just described. The sensitivity of reliability predictions to the assumption that component failures are independent has been shown to be strongly related to the completeness of the model. Only in the ideal case, when essentially all the causes of component unavailability are identified and shown to be independent, can we be assured that the error resulting from the assumption of independence is negligible. In realistic cases, in which only some of the causes are explicitly identified, the assumption of independent failures, particularly in the case of multiple equipment items in the same cut set, should be suspect. Hence, the more complete the models are in terms of the identification of causes, the better the treatment of common-cause failures.

The relationship between human actions and common-cause failures arises from the fact that all types of system and component failures are either caused or induced by human actions. Design errors and other human acts during manufacture, installation, operation, and maintenance are among the

Table 3-9. Effect of two types of common causes on fault-tree quantification[a]

Parameter	Fault-tree quantification case			
	Case 1 No common cause, no single failures	Case 2 Common causes A and B, no single failures	Case 3 No redundancy, no common-cause failure	Case 4 No redundancy, common causes B and C
P(A')	1.0×10^{-3}	9.9×10^{-4}	1	1
P(B')	1.0×10^{-3}	9.9×10^{-4}	1.0×10^{-3}	5.0×10^{-4}
P(C')	0	0	1.0×10^{-3}	5.0×10^{-4}
P(D)	0	1.0×10^{-5}	0	0
P(E)	0	0	0	5.0×10^{-4}
Q	1.0×10^{-6}	1.1×10^{-5}	2.0×10^{-3}	1.5×10^{-3}

[a]See Figure 3-28 for the fault tree.

chief causes of multiple as well as single component failures. Of particular interest in the analysis of common-cause failures is the fact that a substantial number of human errors and shortcomings affect the entire system--or at least multiple components, as opposed to individual components singly. The dependence among error rates in a sequence of human actions is recognized as an important factor in the technique for predicting the rates of human error, which is discussed in Chapter 4.

The limitations and uncertainties associated with attempts to analyze common-cause failures can be largely attributed to a lack or a scarcity of data. For example, if sufficient applicable data were available at the system level, the unavailability and other reliability characteristics of the system could be estimated directly from the data without analyzing the system through various combinations of cause failures. The analysis of field-experience data is also the most effective and defensible way to establish the degree of dependence among the causes of multiple failures, to estimate the conditional frequencies of common-cause failures (e.g., beta factors), or to estimate multiple-failure frequencies directly, depending on the type of the model. However, many problems and limitations are associated with currently published data sources and "banks" in the context of common-cause analysis. These are discussed in Chapter 5.

There are basically three approaches to analyzing and quantifying the effects of common-cause failures in a system-failure analysis. One is to develop the causes of failure explicitly in the fault trees or the cause tables. The second and third approaches are the beta-factor and the binomial-failure-rate methods, which use parameters to quantify the effect of common causes without explicitly enumerating the causes. All three approaches require the collection and analysis of CCF experience data, as described in Chapter 5. A brief discussion and a limited comparison of the three methods are presented below.

3.7.3.5 Fault-Tree Analysis of Common-Cause Failures

One approach to the analysis of common-cause failures is to model them directly in the system fault tree or as specific entries in the cause table. The basic concepts of fault-tree construction and cause-table analysis are discussed in Sections 3.5 and 3.6.2, respectively. This approach seeks to apply experience data at the greatest level of detail available. Specific details of the modeled system-failure modes are compared with the common-cause failures experienced in similar systems to determine their applicability. The analyst must exercise judgment in this task because rarely are the systems exactly alike. For example, suppose a dependence induced two of two redundant trains to fail in one system, but the system to be analyzed has three redundant trains. The analyst must decide whether to model the cause as affecting all three trains or just two, depending on the details of the experienced event in relation to the design of the system being analyzed. While some design changes may have been specifically introduced to eliminate observed dependent failures, it is recognized that these same changes may

introduce new common-cause failures as yet not experienced. The review of past experience is therefore often augmented by systematic searches for dependences between the components of the system. Two or more components may share the same operating environment or require the same periodic maintenance actions.

These qualitative searches for sources of common-cause failure are useful for the task of design improvement but, when performed in the absence of CCF experience data, are difficult to quantify without resorting to the assignment of subjective probabilities. However, a systematic search for the common causes of failure would greatly enhance the basis for such subjective assessments. The computer-aided procedures described in Section 3.7.3.9 are useful in carrying out such systematic searches for common-cause failures.

As indicated in the sample fault-tree analysis of causes in Section 3.7.3.4, the chief weakness of this approach is the tendency to underestimate the frequencies of common-cause failures because of the incomplete enumeration of causes. If the systematic search identified the common causes of failure for each of the lowest order of minimal cut sets for the system, it would be easier to establish that the most important CCF events were accounted for. As indicated in examples given below, it would be extremely difficult to establish that any redundant system is not susceptible to common-cause failures.

It is of interest to examine some actual occurrences of dependent failures and to determine whether the search procedures would have identified them. Tables 3-10 and 3-11 describe two classes of dependent failures: those due to generic causes and those due to special conditions. The generic causes are defined as out-of-tolerance operating conditions; the special conditions refer to conditions or attributes that may be common to a number of system components. These causes and conditions form the basis for a search for dependent failures.

For example, failure data for auxiliary feedwater systems in pressurized water reactors (see the example on page 3-88) show that, in the 11 instances of multiple failures, five were due to maintenance or operator error and one was due to improper installation. This emphasizes the importance of the noted special conditions. The search procedures may have been able to assign the cause of a multiple-failure event to a common inadequately trained maintenance team. This same maintenance team, however, would be responsible for much of the plant's systems. A great many dependences could be attributed to this condition alone. All such dependent-failure causes could not possibly be included in the system's fault tree. Yet several maintenance-related errors did lead to dependent failures.

How could the analyst determine beforehand which dependences to ignore and which to include? This reveals an important limitation associated with fault-tree cause analysis. In an effort to ensure completeness, an intractable number of dependences are identified. Taken separately, these dependences can often be discounted on the basis of a perceived low occurrence probability. Experience shows, however, that as a class they cannot be dismissed. There are many accounts of dependent-failure events involving dependences once thought to be highly improbable. Table 3-12 lists just a few.

Table 3-10. Generic causes of dependent failures

Generic cause	Example of source
Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure
Vibration	Machinery in motion, earthquake
Pressure	Explosion, out-of-tolerance system changes (pump overspeed, flow blockage)
Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from control system
Moisture	Condensation, pipe rupture, rainwater
Stress	Thermal stress at welds of dissimilar metals
Temperature	Fire, lightning, welding equipment, cooling-system faults, electrical short-circuits
Freezing	Water freezing
Electromagnetic interference	Welding equipment, rotating electrical machinery, lightning, power supplies, transmission lines
Radiation damage	Neutron sources, charged-particle radiation
Conducting medium	Conductive gases
Out-of-tolerance voltage	Power surge
Out-of-tolerance current	Short-circuit, power surge
Corrosion (acid)	Boric acid from chemical control system, acid used in maintenance for rust removal and cleaning
Corrosion (oxidation)	In a water medium or around high-temperature metals (e.g., filaments)
Other chemical reactions	Galvanic corrosion; complex interactions of fuel cladding, water, oxide fuel, and fission products
Biological hazards	Poisonous gases, explosions, missiles

Table 3-11. Special conditions

Special conditions	Example of source
Calibration	Misprinted calibration instructions
Installation contractor	Same subcontractor or crew
Maintenance	Incorrect procedure, inadequately trained personnel
Operator or operation	Operator disabled or overstressed, faulty operating procedures
Proximity	Location of components in one cabinet (common location exposes all of the components to many unspecified common causes)
Test procedure	Faulty test procedures that may affect all components normally tested together

Table 3-12. Dependent failures involving subtle dependences

Plant	Description
Rancho Seco	Dropped lightbulb led to shorted instrument bus, leading to a scram and a severe transient
Three Mile Island Unit 2	Maintenance error: valves in auxiliary feedwater system left closed
Brunswick	Gasket rupture on service-water line; resulting spray failed a pressure switch
Vermont Yankee	Improper installation of insulation led to failure of three ADS valves through overheating
Trojan	Maintenance error: lifted electrical lead prevented automatic pump start
Cooper	Mechanic maintaining one service-water pump accidentally broke an adjacent pump

3.7.3.6 Beta-Factor Method

The beta-factor method (Fleming, 1975) can be used to model dependences between dissimilar and not necessarily redundant equipment. In practice, however, it is most often applied to systems for which the most data are available--systems with redundant and identical equipment. The beta-factor method models dependent failures of two types: intercomponent physical interactions (type 3C in Section 3.7.2) and human interactions (type 3D).

The model assumes that λ, the total (constant) failure rate for each unit, can be expanded into independent and dependent failure contributions:

$$\lambda = \lambda_i + \lambda_c$$

where λ_i is the unit failure rate for independent failures and λ_c is the unit failure rate for dependent failures.

For convenience, a parameter, β, is defined as the fraction of the total failure rate attributable to dependent failures:

$$\beta = \frac{\lambda_c}{\lambda_c + \lambda_i} = \frac{\lambda_c}{\lambda} \qquad (3\text{-}3)$$

so that $\lambda_c = \beta\lambda$ and $\lambda_i = (1 - \beta)\lambda$ and $0 \leq \beta \leq 1$.

For a more general case of dissimilar units, A and B, a different λ and β are defined for each unit:

$$\lambda_c = \beta_A \lambda_A = \beta_B \lambda_B$$

The above definitions can be used to derive expressions for the overall reliability or failure probability of a multiple-unit system by modeling dependent failures in series with independent failures, which are drawn in parallel in a reliability diagram. Some reliability expressions for some typical identical and redundant system configurations have been summarized by Fleming et al. (1975).

Markov models can be used in conjunction with the above definitions to develop expressions for the unavailability and reliability of repairable systems. The system probability of failure on demand, U_S, for a one-of-two system subject to independent and dependent failures is given by

$$U_S = (1 - \beta_d)^2 \lambda_d^2 (1 - \beta_d \lambda_d) + \beta_d \gamma_d \qquad (3\text{-}4)$$

where λ_d is the failure-on-demand probability for a single unit and β_d is the fraction of demand failures of each unit due to common causes.

The first term on the right-hand side of Equation 3-4 corresponds to multiple independent failures; the second term accounts for common-cause failures. For β_d and λ_d on the order of 0.1 or less, the first term can generally be neglected.

The unavailability of a one-to-two operating, repairable system, Q_S, is given by

$$Q_S = \frac{\lambda(\lambda + \mu_1)[(2 - \beta)\lambda + \beta\mu_1]}{(2 - \beta)\lambda^3 + [(3 - 2\beta)\mu_2 + 2\mu_1]\lambda^2 + [(4 - 2\beta)\mu_2 + \beta\mu_1]\mu_1\lambda + \mu + \mu_2\mu_1^2}$$

where μ_1 is the (constant) repair rate of single unit when one unit is failed, μ_2 is the (constant) repair rate of both units when the system is failed, and λ and β are as before.

For systems with more than two units, the beta-factor model does not provide a distinction between different numbers of multiple failures. This simplification can lead to conservative predictions when it is assumed that all units fail when a common-cause failure occurs. Further model developments may wish to consider dependent failures of two or three units out of a total system of n units. Note that, in general, the beta factor for the failure to continue running (β) is not necessarily equal to the beta factor for the failure to start on demand (β_d).

The strength of the beta-factor method lies in its direct use of experience data and in its flexibility. Like other dependent-failure models, subjective assessments of the parameter values must be used when data are unavailable. The beta-factor method is most useful for analyzing dependent failures in systems with limited redundancy (two or three units). It can be applied after finding the minimal cut sets of the system or incorporated directly into the fault trees. For the latter approach, a separate primary event for just the dependent failures of multiple units would be added; independent failures would be assigned their own primary events. Minimal

cut sets would then be determined, and those containing the dependent failures would be quantified by using the appropriate beta factor.

When the beta factor is incorporated directly into the fault trees, the dependences between primary events in a cut set are quantified by using the equations of the beta-factor model. If only cut sets up to a certain component order are to be quantified, components with dependent failures are counted as a single component. When the model is applied as discussed above, at the component level, judgment must be used to decide when to treat failures in a cut set as dependent or independent.

Example: PWR Auxiliary Feedwater System

Failure data for PWR auxiliary feedwater (AFW) systems have been collected from licensee event reports (Atwood, 1980a). For this collection the water supply (condensate storage tank) is defined as being outside the system. Table 3-13 identifies the number and type (e.g., turbine driven) of pumps in each train and the period of reported observation; Table 3-14 summarizes the multiple-failure instances. The reported failures include mechanical and electrical failures of pumps, valves, and strainers as well as operator and maintenance errors.

Table 3-13. Instances of multiple failures in PWR auxiliary feedwater systems[a]

Plant	Date	Number of failures and failed train type[b]	Number of trains		
			M	T	D
Calvert Cliffs Unit 1	5/76	2/T, T	0	2	0
Haddam Neck	7/76	2/T, T	0	2	0
Kewaunee Unit 1	8/74	2/M, M	2	1	0
	10/75	2/M, T	2	1	0
	11/75	3/M, M, T	2	1	0
Point Beach Unit 1	4/74	2/M, M	2	1	0
Robert F. Ginna	12/73	2/M, M	2	1	0
Trojan Unit 1	1/76	2/T, D	0	1	1
	12/77	2/T, D	0	1	1
Turkey Point Unit 3	5/74	3/T, T, T	0	3	0
Turkey Point Unit 4	6/73	2/T, T	0	3	0

[a]From Atwood (1980a).

[b]Key: M, motor-driven pumps; T, turbine-driven pumps; D, diesel-driven pumps.

Consider as a unit each train of the system, including the strainer, the pump, and the associated valves. The beta-factor method will be applied to determine a generic probability of AFW-system failure to start for systems with more than one unit. Here "start" means that at least one unit starts and runs for some short period of time. All of the incidents

Table 3-14. Summary of PWR auxiliary feedwater experience[a]

Summation of number of systems times length of service	1874 system-months[b]
Contribution to above by multiple-unit systems	1641 system-months[b]
Summation of number of units times length of service	4682 unit-months[b]
Contribution to above by multiple-unit systems	4449 unit-months[b]
Total number of single failures	69
Number of single failures in multiple-unit systems	68, N_i
Number of multiple-unit failure events	11, N_e
Number of unit failures in dependent-failure occurrences	24, N_c

[a]No distinction made between motor-, turbine-, or diesel-driven pumps.

[b]Calendar months.

collected by Atwood (1980a) can be interpreted as unit failures to start. None of the multiple-failure incidents were propagating failures. This is typical of the experience of many systems.

The beta-factor point estimate is given by

$$\beta = \frac{\lambda_c}{\lambda_c + \lambda_i} = \frac{N_c/T}{(N_c/T) + (N_i/T)} = \frac{N_c}{N_c + N_i} = \frac{24}{24 + 68} = 0.26 \qquad (3\text{-}5)$$

The number of occurrences of multiple-unit failures, N_e, should not be confused with N_c in determining β. A common error is to substitute N_e for N_c in Equation 3-5.

Assuming one complete (i.e., all units) system demand for each calendar month, the per-demand probability of failure to start for a one-of-two system is given by Equation 3-4 with

$$U = (N_i + N_c)/(T \times 1) = (68 + 24)/4492 = 0.2$$

so that

$$U_{S,2} = [(1 - .26)(.02)]^2 + (.26)(.02) = 2 \times 10^{-4} + 5.2 \times 10^{-3}$$

$$= 5.4 \times 10^{-3}$$

Note that data from both two- and three-unit systems were used to obtain a failure-probability estimate for a two-unit system. Moreover, partial as well as complete system failures were included in the model.

For a one-of-three unit system, the contribution from multiple independent failures is negligible, so that the probability of failure to start is

$$U_{S,3} = 5.2 \times 10^{-3}$$

Table 3-13 shows that 6 of the 11 multiple-failure instances resulted in total (i.e., all units) system failure. For the 1641 calendar months of system experience, a per-demand probability of system failure can be estimated to be

$$U_S = 6/1641 = 3.7 \times 10^{-3}$$

For two-unit systems alone, the data give point estimates of

$$U_{S,2} = 4/474 = 8.4 \times 10^{-3}$$

and for three-unit systems, the per-demand probability of failure to start is

$$U_{S,3} = 2/(1641 - 474) = 1.7 \times 10^{-3}$$

For this problem the beta-factor method gave a comparatively higher failure probability for three-unit systems and a slightly lower probability for two-unit systems than the values calculated directly from data.

With regard to the diversity of the AFW-system trains, the data show three total-system failures in 1373 calendar months for diverse multiple-unit systems and three total-system failures in 268 calendar months for identical multiple-unit systems. These give per-demand system-failure probabilities of $3/1373 = 2.2 \times 10^{-3}$ and $3/268 = 11.1 \times 10^{-3}$, respectively.

The beta-factor method does not provide for such distinction. Dependent failures between dissimilar or diverse trains can be modeled, but the method must be applied in two successive steps. In the first step, the two identical components are modeled; in the second step, a "supercomponent" representing the identical pair is modeled with the diverse train.

As already mentioned, the beta-factor method can also be used at the component level, rather than at the train level discussed above. This allows the results to be applied to system configurations not represented in the data base by a suitable combination of component values. There are two drawbacks to applying the model at the component level, however. First, there is less failure data for separate components than for each train as a whole. This can be partly circumvented by using data for the same components from other systems with similar environments. Second, a larger number of dependent relationships must be considered. For example, instead of the single dependence between trains, the analyst must consider dependences between the valves, the pumps, and the strainers, as well as cross-component dependences like those between the pump of one train and the valves of the others. In practice, these cross-component failures can generally be neglected or included in the count of similar components.

The failures collected by Atwood (1980a) have been assigned to one of three categories--pump, valve, or strainer failures--for this example (see Table 3-15). The estimated per-demand total failure probabilities for pumps, valves, and strainers (indicated by the subscripts p, v, and st, respectively) are

$$U_p = (40 + 15)/4449 = .012$$

$$U_v = (26 + 4)/4449 = 6.7 \times 10^{-3}$$

$$U_{st} = (1 + 5)/4449 = 1.3 \times 10^{-3}$$

The beta factors for these components are

$$\beta_p = 15/(15 + 40) = .27$$

$$\beta_v = 4/(26 + 4) = .13$$

$$\beta_{st} = 5/(5 + 1) = .83$$

The minimal cut sets for a one-of-two system with each train containing these three components are

$$V_1V_2,\ P_1P_2,\ S_1S_2$$

$$V_1P_2,\ V_1S_2$$

$$V_2P_1,\ V_2S_1$$

$$P_1S_2,\ P_2S_1$$

The total failure probability for a multiple-train system with each of the above three components in each train is then estimated by the beta-factor method to be, per demand,

$$U_S' = \beta_p\lambda_p + \beta_v\lambda_v + \beta_{st}\lambda_{st} + \left[(1 - \beta_p)U_p + (1 = \beta_v)U_v + (1 - \beta_{st})U_{st}\right]^2$$

$$= 5.4 \times 10^{-3} \qquad (3\text{-}6)$$

The last term in Equation 3-6 describes the fraction of independent failures in the total system-failure probability. The first three terms give the dependent-failure contributions. Note that for this example only dependences between similar components were modeled. As expected, the final numerical result is the same as that derived earlier with the beta-factor method at the system train level.

The above point-estimate calculations with the beta-factor method depend on the particular independent and common-cause failures. Although the experience data include events that fit the definitions of independent and common-cause failures assumed in the model, there are also events in

Table 3-15. Summary of auxiliary feedwater component categorizations

Component	Number of single-failure instances	Number of multiple-failure instances	Number of components failed in multiple-failure instances
Pump	40	7	15
Valves[a]	26	2	4
Strainers	1	2	5

[a]For our discussions all valve failures are combined, although in reality several different kinds of valve failures are included in the data.

the "gray" area, which might be termed partial or potential common-cause events. For example, one component might have actually failed, whereas the failure of a second component was found to be incipient. There is also sometimes a fine line between what might be regarded as a single failure and a common-cause failure. These factors give rise to uncertainties that must be taken into account in the analysis of common-cause failures. The methods described in Chapter 5 for estimating confidence limits in uncertainty bounds on failure rates are applicable to the beta factor as well since β is simply the ratio of failure rates as defined in Equation 3-3.

3.7.3.7 The Binomial Failure-Rate Model

The binomial failure-rate model is a special case of a more general model developed by Marshall and Olkin (1967). A system of m units can fail in 2^{m-1} ways, each represented by a vector $\underset{\sim}{x}$. The Marshall-Olkin model assumes that each failure mode $\underset{\sim}{x}$ has an exponentially distributed occurrence time given by

$$f_{\underset{\sim}{x}}(t) = \lambda_{\underset{\sim}{x}} \exp(-\lambda_{\underset{\sim}{x}} t)$$

where $\lambda_{\underset{\sim}{x}}$ is the failure rate associated with an m-dimensional vector $\underset{\sim}{x}$ consisting of 0's and 1's. For example, if m is 3, the vector (1,1,0) denotes the failure of units 1 and 2 and nonfailure of the third unit. For a system of two identical units, the probability p that both units will fail in time t is then approximately

$$p = (\lambda_1 t)^2 + \lambda_2 t \qquad (3\text{-}7)$$

where λ_1 is the single-unit failure rate, $\underset{\sim}{x} = (1,0)$ or $(0,1)$, and λ_2 is the multiple-failure rate, $\underset{\sim}{x} = (1,1)$.

Note the similarity between Equations 3-7 and 3-4. In fact, the Marshall-Olkin and beta-factor methods have been shown to be identical for two-unit systems (Fleming and Raabe, 1978).

The Marshall-Olkin model has been specialized (Vesely, 1977) for application when data are sparse. This specialization is referred to as the binomial failure-rate (BFR) model. It is assumed that the system's units are identical or at least similar, so that the failure rates λ_k depend only on the number of units failed. Each unit can fail individually with a constant failure rate λ. "Common-cause shocks are assumed to hit the system at random times. The time between shocks is exponentially distributed, with constant occurrence rate μ. Given that a shock has occurred, each unit has probability p of failure, with the same p for each unit." The term "binomial failure rate" is used because the number of failed units, given a common-cause shock, is binomially distributed with parameters m and p.

The BFR model differs from the beta-factor model in that it distinguishes between the number of multiple-unit failures in a system with more than two units. For example, different failure rates would be derived for two of three units failing versus three of three units failing. To accomplish this, however, the BFR model requires an assumption about the relationship between the failure rates, so that three parameters, U, λ, and p, need to be evaluated, no matter how many units the system has.

The applicability of the BFR model is tied to how well-observed events can be simulated by adjustments to the parameters p and μ. The shock rate μ is not directly available from the data, because shocks that do not happen to cause any failures are not observable. Also, depending on the quality of the data, single failures from common-cause shocks may not be distinguishable from single independent failures.

Consider a system of m similar units. The failure rate for one unit of the system, λ_1, is then given by

$$\lambda_1 = m\lambda + \mu(mpq^{m-1})$$

where $q = 1 - p$. The first term on the right-hand side gives the total contribution of the independent-failure rate. The second term gives the rate of single-unit failures resulting from common-cause shocks. A common-cause shock need not result in a multiple-unit failure or even a single-unit failure. The failure rate for i units of the system is given by

$$\lambda_i = \mu\left[\binom{m}{i} p^i q^{m-i}\right] \quad \text{for } i = 2, m \tag{3-8}$$

where

$$\binom{m}{i} = \frac{m!}{i!(m-i)!}$$

Any occurrences of multiple independent failures are counted as the occurrences of single failures. Given some data, the parameters m and p are selected to maximize the probability of the observed results. Define the rate of dependent multiple failures

$$\lambda_+ = \sum_{i=2}^{m} \lambda_i = \mu\left(1 - q^m - mpq^{m-1}\right) \tag{3-9}$$

and let N_i be the number of observations of i concurrent failures. Define also

$$N_+ = \sum_{i=2}^{m} N_i$$

We wish to maximize the likelihood of the observed data:

$$P_T[N_1 = n_1, N_2 = n_2, \ldots, N_m = n_m]$$

$$= P_1[N_1 = n_1]\, P_+[N_+ = n_+]\, P_m[N_2 = n_2, \ldots, N_m] = n_m \quad (N_+ = n_+) \qquad (3\text{-}10)$$

Now the variables N_1 and N_+ have Poisson distributions with parameters $\lambda_I T$ and $\lambda_+ T$, respectively. Here T is the system operating time in the observed data. Maximize the likelihood of P_1 and P_+ by estimate

$$\lambda_1 = n_1/T \quad \text{and} \quad \lambda_+ = n_+/T$$

The factor P_m of Equation 3-10 follows a multinomial distribution. Provided the independent unit failure rate $\lambda \geq 0$, then the equation that allows one to find an estimate of p that maximizes P_m is (Atwood, 1980b)

$$S = mn_+ p(1 - q^{m-1})/(1 - q^m - mpq^{m-1}) \qquad (3\text{-}11)$$

where S is the total number of units failing in multiple-failure occurrences--that is,

$$S = \sum_{i=2}^{m} in_i$$

For the special case in which m = 3, Equation 3-11 can be solved directly:

$$p = 3(S - 2n_+)/(2S - 3n_+) \qquad (3\text{-}12)$$

With λ_1, λ_+, and p, an estimate for μ can be obtained from Equation 3-9.

The above equations hold only for systems with m > 2. This is not a serious drawback because systems with m = 2 can be handled easily by the general Marshall-Olkin model or the beta-factor method. Furthermore, if independent failures can be distinguished from single failures resulting from common-cause shocks, expressions for systems with m = 2 can be easily formulated.

Example: PWR Auxiliary Feedwater System

Consider the PWR auxiliary feedwater system discussed in Section 3.7.3.6. The earlier equations in terms of failure rates are converted to

failure-to-start probabilities, assuming one system demand per calendar month. Equation 3-8 becomes

$$U_1 = \frac{N_1}{T \times 1} = \frac{68}{1641} = .0414; \quad U_+ = \frac{N_t}{T \times 1} = \frac{11}{1641} = .0067$$

Only data from three-unit systems can be used as evidence for the parameter p. The total number of units failing in multiple-failure occurrences, S, is 16 for this example. Equation 3-12 provides for an estimate of p:

$$p = 3[16 - 2(7)]/[2(16) - 3(7)] = 6/11 = .55$$

$$\hat{q} = .45$$

Then the per-demand common-cause shock rate is estimated from Equation 3-9:

$$.0067 = \hat{\mu}[1 - (.45)^3 - 3(.55)(.45)^2]$$

$$\hat{\mu} = .0118$$

Using these estimators in Equation 3-8, the per-demand system-failure probabilities for two of the three units failing and then three of the three units failing are obtained:

$$U_{S,2} = (.0118)\binom{3}{2}(.55)^2\ (.45)^{3-2} = 4.8 \times 10^{-3}$$

$$U_{S,3} = (.0118)\binom{3}{3}(.55)^3\ (.45)^{3-3} = 1.9 \times 10^{-3}$$

Uncertainties must be taken into account in estimating the parameters of the BFR model, as with any parametric method. Both Bayesian and statistical approaches have been developed for this use and published by Atwood (1980b). A computer program is also available for performing the associated calculations (Atwood and Switt, 1981). The results obtained by the beta-factor and the BFR methods are compared below.

3.7.3.8 Discussion and Comparison of the Parametric Methods

Both parametric methods use experience data to estimate common-cause rates and so are not applicable when few dependent-failure data are available or applicable.

In addition to λ, the beta-factor method estimates one extra parameter, β, while the BFR method estimates two extra parameters, μ and p. Thus the beta-factor method is the simpler, with the advantages of directness and flexibility, and the disadvantage of inapplicability to many-unit systems.

Both methods can be used after the usual procedure for fault-tree construction or incorporated into it as an integral part.

Both methods are related to the Marshall-Olkin model. In fact, the beta-factor method can be considered to be a special case of the BFR model with the parameter p set equal to 1.

Both methods require the identification of a system that is susceptible to common-cause failures. The beta-factor method is only useful for systems with a few units, so deciding on the boundaries of the system is seldom a problem. With the BFR method, there may be real difficulty. For example, should HPCI pumps be included with LPCI pumps as part of the same population susceptible to common-cause shocks?

The beta-factor method is very direct, simply estimating β. The BFR method makes stronger use of a model; for example, it estimates $U_{S,2}$ by a fairly complicated use of the data. Therefore the BFR method is probably more susceptible to departures from the assumed model, such as dissimilar units, shocks of differing severity, or shocks that do not affect all the units equally. The beta-factor method solves the problem of dissimilar units by estimating distinct beta factors. Some work has been done to accommodate dissimilar units in the BFR method (Atwood, 1980a).

With both methods, keep in mind that we are trying to understand complex reality by using quite simple methods. If the methods seem inadequate, the analyst can either live with the inadequacy or try a more complicated method (such as a more complicated Marshall-Olkin model). A consideration is the amount of data available. With a great deal of data, one can, in principle, be fairly elaborate. With only a little data, it is necessary to use simple methods. A routine part of the application of each method should be a comparison of the data with the estimates, to look for lack of fit and see whether the method used is adequate.

In the auxiliary feedwater pump example of the preceding sections, the two methods give estimates for $U_{S,2}$ and $U_{S,3}$ in two-unit and three-unit systems, shown in Figure 3-29. Note that the beta-factor method does not attempt to estimate $U_{S,2}$ in a three-unit system, but compensates by overestimating $U_{S,3}$. The BFR method estimates p entirely from the data for three-unit systems and so fits its estimates to the three-unit data almost perfectly. Both methods underestimate $U_{S,2}$ in two-unit systems, though the beta-factor method does better than the BFR method. More careful examination of the data might suggest reasons why the two-unit systems seem to have relatively greater unavailability than three-unit systems.

3.7.3.9 Computer-Aided Dependent-Failure Analysis

Qualitative search procedures have been developed to provide some assurance that the most likely common causes (believed to be the most significant type of dependent failures) are accounted for in the model. The search procedures are designed to identify system weak spots qualitatively and to optimize the features designed to protect against potential dependent failures. These search procedures make no attempt to quantify the system-failure probability.

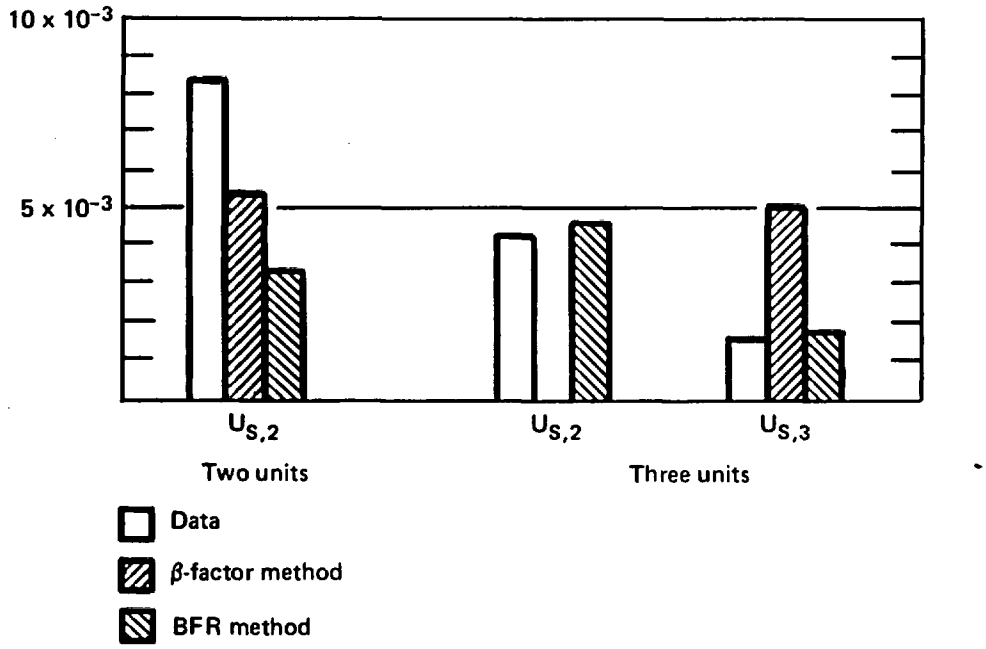


Figure 3-29. Estimated $U_{S,2}$ and $U_{S,3}$ in two- and three-unit systems.

The SETS (Worrell and Stack, 1977) code uses transformations of variables for common-cause analysis. The transformations relate common-cause events to primary events in the fault tree. Primary events that are not susceptible to any common cause may be deleted, depending on the scope of the analysis. Single common causes, multiple common causes, or combinations of common-cause events and primary events that cause the top event to occur can all be identified, depending on the type of transformation employed (Worrell and Stack, 1980). With this approach, it is not necessary to first determine the fault tree minimal cut sets, and the fault tree is not altered in any way since the procedures operate on the Boolean equations that represent the fault tree. The qualitative search procedures avoid the problems of handling fault trees of unwieldy size.

COMCAN II-A (Rasmuson et al., 1979) reorganizes the fault tree before determining common-cause dependences. The basic system fault tree is pruned so that it contains only primary events that are susceptible to a single common cause and are also in a common location. The reduced tree is then evaluated to ascertain whether any system cut sets can be constructed entirely from primary events that are susceptible to a common cause. This evaluation is then repeated for all causes and locations. Obviously, a problem with this approach is that cut sets with events that are not all susceptible to a single common cause (e.g., multiple failures) are not considered. Cut sets containing events with a common cause and one other failure may be significant.

The WAMCOM (Putney, 1981) code uses the SETS (Worrell and Stack, 1978) program to search for potential dependent failures in large fault trees. Like BACFIRE II and COMCAN II-A, it manipulates the initial system fault tree before reduction. In WAMCOM, however, the fault tree is transformed in four separate modes of succeedingly higher levels of sophistication. Each

transformation involves the replacement of a component by logic that represents both the independent and the dependent failures of the component. Dependent-failure analysis information is then used in computing the next mode. The analyst may select the number of modes implemented as his needs warrant. WAMCOM provides lists of the following:

1. All common-cause events that can fail the system by themselves.

2. All combinations of two common-cause events that can cause system failure.

3. All combinations of one common-cause event and one independent-failure event that together can cause system failure.

Currently WAMCOM is limited to determining system-dependent failures from two events or less. This is, however, an advancement over the capabilities of BACFIRE II and COMCAN II-A. Instead of including common causes as primary events, these search procedures require the analyst only to augment component-level fault trees by assigning susceptibility vectors to each component. These vectors simply indicate to which common cause the components are susceptible. Computer codes have been developed to manipulate these susceptibility vectors in accordance with the fault-tree structure to help the analyst identify significant system cut sets involving dependent failures (see, for example, Rooney and Fussell, 1978; Rasmuson et al., 1979; Putney, 1981).

Each of the computerized search procedures requires a categorized list of dependent-failure causes to be investigated (e.g., two or more periodic maintenance actions). A sample listing of causes is shown in Tables 3-10 and 3-11. The generic causes listed in Table 3-10 have domains of impact defined by physical barriers, such as fire walls, dust covers, or physical separation. The special conditions listed in Table 3-11 have domains of impact defined by plant procedural barriers. For example, the number of pressure sensors a maintenance team is permitted to calibrate would define a domain of impact for the special condition "calibration." The lists of causes are intended to be both mutually exclusive and exhaustive. Secondary causes (e.g., impact) as opposed to primary causes (e.g., pipe whip, water hammer, missiles) are listed to keep the list of causes to be searched for at a tractable number. In assigning the susceptibility vector of a system fault tree, components susceptible to water hammer or to pipe whip, in the analyst's judgment, would both be identified as susceptible to the secondary cause "impact."

After the susceptibility vector is assigned to each primary event of the system's fault tree, the analyst must describe the domains of impact for each of the causes being evaluated.

The barriers for each of the potential common causes are identified, both physical or procedural. Next the analyst assigns a location identity, relative to these barriers, to each primary event in the system fault tree and for each common cause. As one can imagine, the amount of time needed to prepare this input, especially for a complete set of causes, can be enormous. Note also that such input preparation requires an exceptional level of system-design and plant-layout detail.

There are several computer codes that can sift through the fault-tree logic to determine system minimal cut sets and identify dependences between the primary events that make up the cut sets; the dependences are identified one cause at a time. For example, BACFIRE II (Rooney and Fussell, 1978) manipulates the system fault tree to help speed the search for dependences in complex systems; this manipulation is called the "event method." Subsections of the tree that do not contain any shared dependences are replaced by single dummy events. The streamlined fault trees are then evaluated for minimal cut sets, and the dummy events are resolved. BACFIRE II allows multiple locations to be assigned to a single component (e.g., to a pipe passing through two or more rooms).

The GO code can be used in the analysis of dependent failures of type 1--common-cause initiating events.

3.7.4 RECOMMENDED PROCEDURES FOR THE ANALYSIS OF DEPENDENT FAILURES

Table 3-16 indicates that there is at least one method for each type of dependent failure defined in Section 3.7.2. In view of the advantages and disadvantages discussed in the preceding section for the various methods, and the extent to which each method has actually been applied so far in PRA studies, a recommended procedure for dependent-failure analysis was developed for use in a plant-specific risk analysis. The recommended procedure consists of a method or synthesis of methods for each type of dependent failure and is intended to reflect the current state of the art. It is recognized that risk analysis in general and dependent-failure analysis in particular are rapidly evolving in both methods and practical application and that improvements in dependent-failure analysis are both necessary and inevitable. A brief summary of these methods is presented below.

3.7.4.1 Common-Cause Initiators (Type 1)

The only feasible approach to the analysis of common-cause initiators is to treat them explicitly. In most cases (e.g., earthquakes, fires, and floods), it is necessary to employ event-specific models to aid in estimating the frequency of initiation as a function of magnitude and the conditional probability of failure for plant systems and components. In other cases, such as the loss of electric power, these models might simply consist of the statistical analysis of data from operating and maintenance experience.

Events are selected as common-cause initiators because they have the potential for initiating and influencing the progression of accident sequences. These same events can also introduce intersystem dependences, and therefore the event-specific models can also play an important role in the analysis of type 2C dependent failures.

In the case of certain common-cause initiators internal to the plant and localized to specific areas of the plant, the qualitative search procedure can greatly aid in screening the plant layout before quantification.

Table 3-16. Applications of various analytical methods to dependent failures[a]

Method of analysis	Common-cause initiators	Intersystem dependences: 2A Functional dependences	Intersystem dependences: 2B Shared equipment	Intersystem dependences: 2C Physical interactions	Intersystem dependences: 2D Human interactions	Intercomponent dependences: 3A Functional dependences	Intercomponent dependences: 3B Shared equipment	Intercomponent dependences: 3C Physical interactions	Intercomponent dependences: 3D Human interactions
a. Event specific	X			X				X	X
b. Event-tree analysis		X	X		X	(b)	(b)		
c. Fault-tree linking	X	X	X		X	(c)	(c)	(c)	(c)
d. Fault-tree cause analysis					X	(b)	(b)	X	X
e. Human reliability					X				X
f. Beta factor								X	X
g. Binomial failure rate								X	X
h. Qualitative search procedures	X			X	X			X	X

[a]See Section 3.7.2 for definitions.
[b]Accounted for by standard fault-tree and event-tree methods.
[c]Linking of fault trees implies the dependences are between systems.

This added step in the analysis will reduce the potential for overlooking important initiator locations and, at the same time, help reduce the effort spent on the analysis of locations that turn out to make negligible contributions to risk.

3.7.4.2 Intersystem Functional Dependences (Type 2A)

The recommended procedure for incorporating functional dependences among systems is one that has been used in essentially all previous and current risk studies--namely, that of explicitly incorporating the dependences into the event trees. For example, if a system is not needed along a particular accident sequence because of the success or the failure of other systems that precede it in the event tree, then the branching of the event tree at that point can be bypassed or condensed. Similarly, if along a particular sequence the failure or the success of a system is certain because of the status of preceding systems, the branch of the tree whose probability is zero can simply be eliminated.

As indicated in Table 3-16, the methods of fault-tree analysis are also capable of treating functional dependences. However, there does not seem to be any particular advantage to using this type of approach for intersystem functional dependences. In fact, there appear to be significant disadvantages to analyzing type 2A dependences at the fault-tree level. These include the need to analyze a greater number of accident sequences that do not contribute to the risk and the invisibility of these dependences for peer review in comparison with the explicit event-tree approach (method b).

3.7.4.3 Intersystem Shared-Equipment Dependences (Type 2B)

There are two methods that have been successfully applied and are therefore recommended for the analysis of shared-equipment dependences among systems: direct incorporation into event trees with defined boundary conditions for fault-tree analyses and fault-tree linking (methods b and c, respectively). As discussed in Section 3.7.3.3, each method, if appropriately used, is capable of producing the correct result, and each has its advantages and disadvantages.

The essential difference between the two approaches is that method b results in large event trees, increasing the number of event sequences to be analyzed and reducing the size of the fault trees at each branch point. By contrast, method c results in relatively small event trees, with fewer sequences but relatively large fault trees. Both approaches, if rigorously followed, appear to require the same amount of data processing; however, this has not been proved. To keep data processing at a manageable level, some sort of tree pruning is necessary with each. Variations on each method have been developed to reduce the size of the logic trees that need to be analyzed, as discussed in Section 3.7.3.3. In the case of method b, often only the most important commonalities are included in the tree and

the low-risk sequences are eliminated at some intermediate point in quantification. In method c, all the minimal cut sets of the fault trees are often not identified, and, when they are, are pruned before quantification. Such simplifications are practical necessities for both approaches. It is important that the assumptions made in their use be visibly documented to facilitate peer review.

3.7.4.4 Intersystem Physical Interactions (Type 2C)

As mentioned above, some of the event-specific models recommended for the analysis of common-cause initiators can also be used for type 2C dependent failures. In the case of seismic analysis, fragility curves are used in conjunction with event- and fault-tree models to estimate the conditional probability of multiple-system failures due to earthquakes. In the case of fires, fire-propagation models are used to help estimate effects on multiple plant systems. As in the case of common-cause initiators, the qualitative-analysis codes BACFIRE, COMCAN, and WAMCOM can be used effectively in conjunction with event-specific models for screening.

In the case of initiating events other than common-cause initiators, such as loss-of-coolant accidents and transients, the analysis of many physical interactions is embodied in the establishment of success criteria and damage limits for system components as well as in the prediction of the magnitude of environmental stress levels. It is not uncommon for these interdependences to be dealt with by the use of conservative assumptions (e.g., that the component will fail if environmental stresses exceed design limits).

3.7.4.5 Intersystem Human Interactions (Type 2D)

To the extent that human beings design, construct, operate, and maintain the plant, it is impossible to fully isolate the role of human interactions from any of the dependences discussed above in terms of hardware interactions. Hence, all of the analytical methods described above pertain directly or indirectly to human interactions.

The recommended procedure for analyzing intersystem dependences caused by human interactions is to include human errors of omission and commission explicitly in the event- and fault-tree models and to use the human-reliability methods of Chapter 4 to implement quantification. This is easier said than done. A starting point for the identification of specific errors is the analysis of operation and maintenance procedures, if they have been defined for the accident sequence being investigated. This is especially important if operator action is required to actuate a system or a collection of systems.

Of particular interest here are human interactions that involve multiple plant systems. If singular human actions are identified as failure modes for multiple systems, the logic of the dependence is much the same as the shared-equipment dependence (type 2B), and hence method b or c must be

used to avoid double accounting. Moreover, care must be taken to properly account for the dependence between multiple human errors along the same accident sequence.

It should be noted that the state of the art in modeling human interactions is limited in at least two important ways. First, there does not appear to be any method available for treating human errors of commission because of an inability to compile a reasonably complete list of things a human being can do to alter the progression of accident sequences. Second, there does not appear to be an available method or approach for treating the interdependences associated with design errors that affect multiple systems.

3.7.4.6 Intercomponent Dependences (Type 3)

The procedure recommended for analyzing dependences among components is to combine the explicit modeling of multiple-failure causes (method d) with parametric methods (f and g) to account for the effect of multiple-failure causes left out of the explicit models.

Both functional and shared-equipment dependences among components are inherently accounted for in the basic fault-tree method described in Section 3.5. Hence, apart from a thorough analysis of each system for such dependences, no special analysis of dependent failures is needed.

The parametric methods (beta factors and binomial failure rates) permit the incorporation of relevant experience data into the quantification of fault-tree models. Since they do not require the explicit identification of multiple-failure causes, the accuracy of the quantitative results and associated uncertainties is reflected in the selection of parameter values. As in estimating the values of other parameters (e.g., failure rates) from experience, care must be taken to ensure that the operating experience is relevant to the particular system and plant.

The use of both parametric methods and a detailed fault-tree analysis of causes is recommended for several reasons. First, such a procedure is conceptually more complete than either approach used singly. Because many causes of multiple failures simply do not appear in the information analyzed in a risk assessment (e.g., piping and instrumentation diagrams, the final safety analysis report, operating procedures), the fault-tree approach can identify only some of them; the examples presented in preceding sections demonstrate this point. On the other hand, a beta factor or a BFR parameter that is estimated from experience data, even if the data have been screened for applicability, may not adequately reflect the plant- and system-specific details that influence susceptibility to dependent failures. Hence, a combination of both approaches is recommended whenever possible. When both approaches are used, care should be taken to avoid double accounting. The most straightforward way to avoid this is to screen events that correspond with fault-tree events out of the data sample used to estimate the common-cause parameters.

For risk analyses carried out at a conceptual design stage, the ability to find plant-specific causes in system fault trees may be limited. In this

case, the use of the parametric methods alone may be the best that can be done.

The practical application of the above-mentioned methods for analyzing intercomponent dependences requires some judgment as to which sets of components are to be considered as potentially interdependent and which are to be treated as independent. For example, if components in one system are assumed to be independent from those in another system, apart from the intersystem dependences already discussed (types 2A through 2D), the analysis of intercomponent dependences can be localized at the level of the system fault tree. In this case, the candidates would naturally be the minimal cut sets for the system.

If, on the other hand, identical components in two different systems along the same sequence are suspected of being dependent, the candidate sets of interdependent components would more appropriately be the minimal cut sets for the entire accident sequence. As discussed in the procedure for shared-equipment dependences, in such a case fault-tree linking (method c) would seem to have an advantage over the use of event trees with boundary conditions (method b). This is because method c could entail the generation, for each entire sequence, of cut sets that would be available to screen for intercomponent dependence.

As discussed in the procedure for analyzing human interactions among systems (type 2D), all of the methods for dependent-failure analysis deal in some way with human interactions. Human interactions are implicitly accounted for by the parametric methods, since the dependent-failure data used as a basis for estimating parameter values include contributions from design errors, operator errors, and other human errors. The fault-tree analysis of causes (method d) is capable of identifying specific human causes of multiple failures. Since the human-reliability models of Chapter 4 are used to quantify these, they are also relevant to the comprehensive treatment of dependent failures in risk analysis.

A summary of the recommended procedures for the analysis of dependent failures is presented in Table 3-17.

3.7.5 DATA AND INFORMATION REQUIREMENTS

The data and information requirements for dependent-failure analysis consist of those already identified in Sections 3.2 and 6.2 as necessary for accident-sequence definition and quantification, respectively, and some additional information uniquely appropriate to the analysis of dependences. One of the most significant additional information requirements is the need for relevant experience data for use in estimating beta factors and binomial failure-rate parameters. This requires the compilation of data at the system level instead of at the component level, where most data-collection activities are focused. Fortunately, the number of dependent failures actually experienced is sufficiently small (less than three occurrences per reactor-year) to permit the incorporation of all relevant experience into any given risk analysis.

Table 3-17. Recommended methods for the analysis of dependent failures

	Dependent-failure type	Recommended method[a]
1.	Common-cause initiators	Event-specific models (a) and computer-aided CCF analysis codes (i-k)
2A.	Intersystem functional dependences	Event-tree analysis (b)
2B.	Shared-equipment dependences	Event-tree analysis (b) and fault-tree linking (c) (several variations) GO method (h)
2C.	Physical interactions	Event-specific models (a) and computer-aided CCF analysis codes (i-k)
2D.	Human interactions	Event-tree analysis (b) as well as fault-tree and cause-table analysis (c and d) Human-reliability analysis (e)
3.	Intercomponent dependences	Fault-tree and cause-table analysis (c and d) Beta factor (f) and binomial failure rate (g)

[a]Letters in parentheses are the identifiers used in Tables 3-7 and 3-8.

The types of dependent failures accounted for in the quantitative models are directly dependent on the categorization of data that support the models. Failures caused by human error must be clearly identified as being included in, or excluded from, the categorized data. For example, system manual-startup failures may be excluded from the data for these models if included elsewhere in the analysis, but maintenance-related errors occurring before system demand would generally be included. A balance between the types of dependent failures covered by these models and by the basic fault-tree methods must be established.

Any method of dependent-failure analysis should, at a minimum, account for experience data in the prediction of dependent-failure probabilities. One problem in interpreting each occurrence of multiple failures is to determine whether it represents a combination of independent failures or dependent failures. If multiple failures result from a common cause, then clearly they are dependent. It may be difficult, however, to identify the underlying common cause. Multiple, concurrent, and independent failures should be rare. If the frequency of multiple failures is high, dependences should be suspected. When more than two units are involved, both a common and an independent cause may be present, further complicating the issue.

The various methods that have been actually used in dependent-failure analysis have handled this problem in different ways. The scarcity of dependent-failure data is another problem. The data are categorized to facilitate handling in the models. In categorizing data, it is important to establish the number of units failed and the total number at risk; it is also necessary to know whether the units are identical or diverse. Dependent failures may occur between identical redundant units, diverse units, or dissimilar units that are not redundant.

Like other approaches in reliability analysis, methods for the analysis of dependent failures must adopt some level at which experience data can be categorized (e.g., plant, system, component, or part). Obviously, the higher the level of classification, the greater the amount of data available in each category. However, the application of data at a high level may be precluded because of design differences between the analyzed plant and the plants in the data base. Lower levels of classification are more responsive to a particular design but more difficult to quantify, because of the scarcity of data.

3.8 SUMMARY OF PROCEDURES FOR ACCIDENT-SEQUENCE DEFINITION AND SYSTEM MODELING

The preceding sections of this chapter provided information on available methods for performing the individual elements of the overall task of developing plant and system logic models. This section summarizes the methods for performing each task and presents them in a procedural format.

The general approach to the overall modeling process can be summarized as follows: accident-initiating events are postulated, the response of the plant to each type of initiating event is evaluated, and plant-level models are developed to identify the various sequences of events that terminate in an identified plant state. Sequences that have the potential for offsite consequences are referred to as "plant-damage states" and are grouped in plant-damage bins. This grouping is performed in conjunction with the analysis of physical processes (see Chapter 7). The individual event-tree headings are evaluated by system-modeling techniques to allow the quantification (see Chapter 6) of accident sequences that result in plant-damage states. The results of accident-sequence definition and system-modeling are a group of accident-sequence logic models that can be quantitatively or qualitatively evaluated.

3.8.1 BASIC TASKS

Figure 3-30 outlines the procedure for accident-sequence definition and system modeling. There are nine basic tasks, which lead to the end product of accident-sequence models for specific groups of accident-initiating events. As shown in Figure 3-30, analytical options are available for most of the tasks. Some of the options described are not distinctly different in substance: they reflect variations in using similar data and the preference

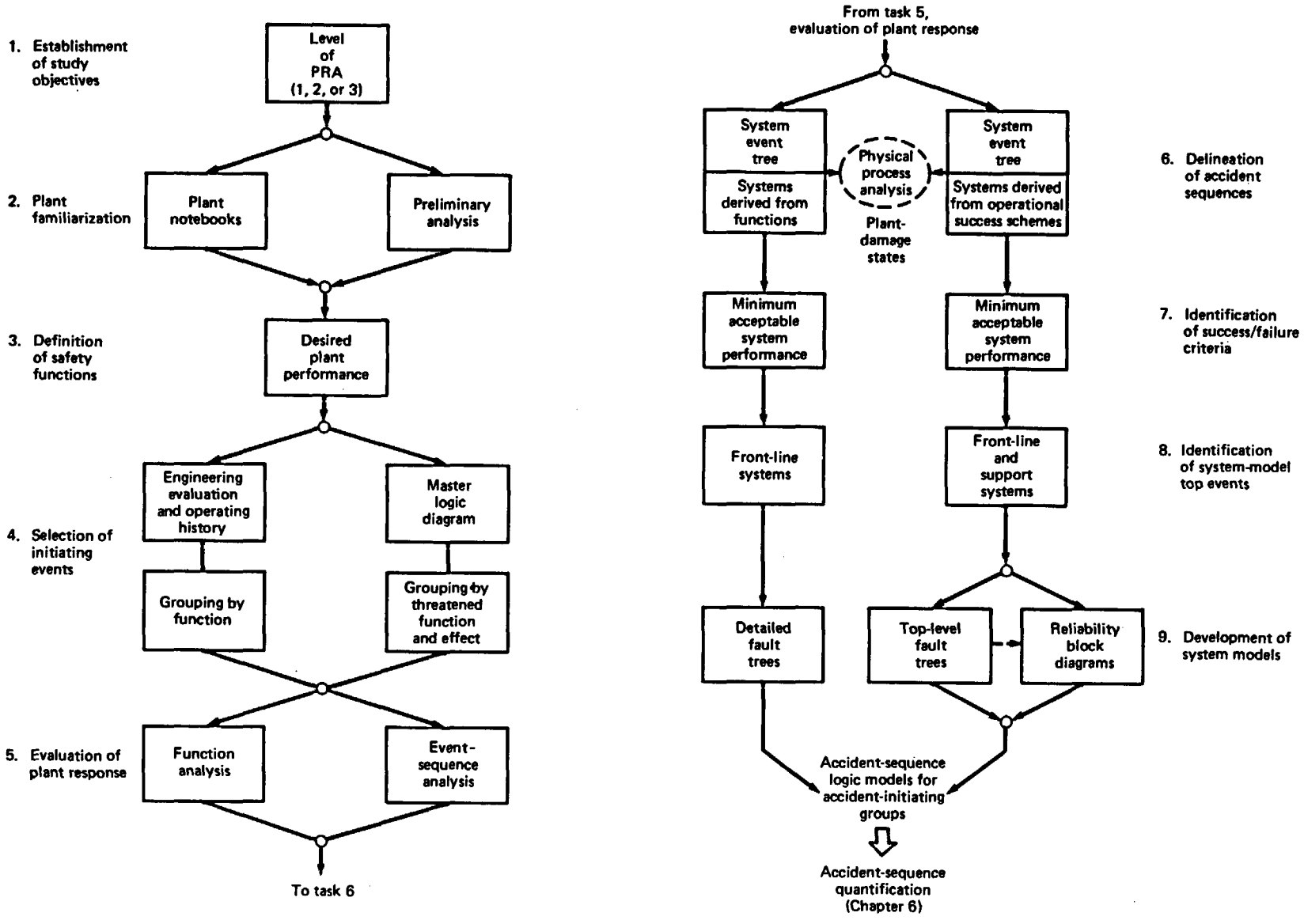


Figure 3-30. Procedure for accident-sequence definition and system modeling.

of analysts for specific techniques or model format. The selection of a particular analytical option does not necessarily preclude or limit the options for succeeding tasks. However, as noted in task 6 (see page 3-109), a significant distinction can be made between the options given at that point, and from that step forward a singular approach is dictated.

The discussion that follows briefly reviews the tasks involved in accident-sequence definition and system modeling.

Task 1: Establish Study Objectives

The first task in plant and system modeling is to determine what level of PRA will be performed. If a level 1 is selected, the accident-sequence definition will terminate in one of two stages: either a plant-damage state or the successful termination of the event sequences. If a level 2 or 3 PRA is to be performed, then additional plant-damage states are defined through interaction with the analysis of physical processes (Chapter 7). If external events are included, the system-modeling process must accommodate failure modes whose effects are location dependent.

Task 2: Plant Familiarization

Plant familiarization is fundamental to any PRA activity. It is a loosely defined task wherein all PRA team members become familiar with plant design and operation as well as with the analytical tasks required for the overall PRA process. A large amount of information is collected, synthesized, and documented to form the basis for later analytical activities. A list of plant systems is developed and reviewed for potential impacts on risk. In some PRAs, systems are identified as important, and system-analysis notebooks are developed and updated as the analysis progresses. In other PRAs, a preliminary analysis of all systems is performed and documented to an extent commensurate with the importance of each system to the overall risk assessment.

Task 3: Definition of Safety Functions

A definition and a clear understanding of safety functions are necessary in any PRA. The exact manner of definition and use may vary with the preference of the analyst; however, the definition of safety functions allows initiating events and system responses to be placed in the proper perspective and provides a starting point for the analysis.

Task 4: Selection of Initiating Events

Accident-initiating events must be identified and grouped according to similarity of plant responses. Generic lists, operating histories, and plant-specific data can be factored into a comprehensive engineering evaluation through which an exhaustive list of initiating events, including their occurrence frequency, is eventually compiled and classified. It is important to ensure that the list of initiating events considered is complete and comprehensive.

Another approach is to use a master logic diagram in order to more formally document the completeness of the search for initiating events.

A fault-tree type model is then developed to deduce all important initiating events. The identified events are grouped by the safety function that is threatened and the effects of each group of initiators. The master logic diagram helps to focus and organize the search for initiating events, but it does not ensure completeness.

Task 5: Evaluation of Plant Responses

When the groups of initiating events have been selected, the attendant response of the plant must be determined. This can be accomplished through a function analysis that defines the safety functions required for each response and orders them in a function event tree. Success criteria for each function are stated in terms of the required complement of systems for each function. Success criteria are then developed for individual systems to establish the bases for the headings of the system event tree. The value of this approach is the stepwise, ordered separation of functions by specific system. It provides a framework for the complex task of sorting system responses.

Another approach is to use an operationally oriented event-sequence analysis to organize and display an approximate time course of actions potentially available to respond to each group of initiating events. Event-sequence diagrams (ESDs) are used to assemble pertinent design and operation information in a flow-chart format. This information is used to select important responses and actions for inclusion in the system event trees. The development of the event-sequence diagrams can require a considerable expertise in plant design and operation as well as experience in system analysis.

Task 6: Delineation of Accident Sequences

The development of system event trees is a key element in accident-sequence definition. Two distinctly different ways of developing system event trees have been illustrated. The key difference between them is the manner in which support systems are accommodated. In one method the event-tree headings are defined to be composite events representing the operability states of front-line systems and the associated support systems. This approach leads to event trees with a minimum number of headings and thus facilitates the understanding of the overall accident-progression path, but it requires that support systems be included in the system models.

In the other method, support systems, functions, or operational actions are included directly in the event trees. The objective is a more accurate depiction of the various detailed accident-progression paths. This approach produces event trees with more event-tree headings and tends to display more operational information. Event trees of this type lead to system models that are less complex, as the supporting systems are already accounted for, but require considerable engineering judgment in the distinction and placement of the event-tree headings.

Task 7: Definition of Success and Failure Criteria

Each event-tree heading, whatever the type of the system event tree, must have a definite statement of the minimum acceptable complement of equipment or system performance required for success in the event described

by the event-tree heading. These criteria should be stated in discrete hardware terms, such as the number of pumps or the required flow. The basis for such criteria can be derived from licensing information, which should be recognized as inherently conservative. More realistic information can be used, such as results of particular thermal-hydraulics calculations that are supportable and documented. Care should be taken in identifying the need for more-realistic criteria, as often the difference between conservative and "more realistic" success criteria is not discernible in the results of the assessment, and the additional effort to try to justify specific criteria may not be warranted.

Task 8: Identification of System-Model Top Events

The initial step in system modeling is the definition of the top events for the system fault models. The success criteria developed in the preceding step form the basis for top-event definition. Success criteria for each event-tree heading are translated to system-failure criteria. Each top event is postulated as part of an event-tree sequence consisting of the success and failure states of other systems. These boundary conditions must be carefully carried over into the identification of system top events and subsequent model development. Both approaches shown in Figure 3-30 produce definitions of top events that account for the impact of support-system failures. In one case they are included within a composite definition of system failure; in the other, they are postulated independently.

Task 9: Development of System Models

Two approaches to system modeling are shown in Figure 3-30. As noted previously, each depends on the type of the system event trees. In one approach, detailed system fault trees are developed, including the system of interest and all required support systems. This results in large fault trees that may need to be reduced and segmented for tractability and ease of evaluation.

The other approach, with support systems explicitly included as event-tree headings, leads to more but smaller system models. Fault-tree models, reliability block diagrams, or combinations of these modeling techniques can be used to develop the necessary system models.

3.8.2 COMPARISON OF ANALYTICAL OPTIONS

As noted in Figure 3-30, several options are available for performing most tasks in the analysis, and it is difficult to recommend a specific overall approach. However, two generalized approaches can be envisioned.

In one approach, system event trees are developed from the safety functions displayed by function event trees. Each function is separated into complements of the systems that perform it, and system event trees are developed. The headings of these event trees are composite events representing the operability states of front-line systems and the required support systems. Each event-tree heading that requires model development is

evaluated by means of detailed fault trees that depict the system-failure modes, including those of support systems, that could cause failure in the identified event-tree heading.

This approach is based on the functional concept with continually increasing levels of analytical refinement. In practice, it leads to the development of function and system event trees that are correlated, leading to traceable, visible displays of the accident sequences. The system event trees are somewhat simplified because of composite event-tree headings. This approach has the disadvantage of leading to more complex system models that include support-system dependences. These dependences must be properly accounted for and often lead to large fault trees that must be segmented during development or evaluation. Very large fault trees are difficult to evaluate and validate, and care must be exercised throughout that the headings of the system event trees accurately reflect the desired function and system-operability states.

In the other approach, system event trees can be developed from operationally oriented event-sequence diagrams that include support systems and functions as individual event-tree headings. (This is but one alternative approach--there are others that could be used as well.) A significant amount of operationally specific information is included in the event trees, which leads to a greater refinement in the choices depicted on the event tree and subsequently to a large number of identified sequences. The associated system models are less complex, because they do not include support-system dependences. However, the increased complexity of the event trees requires more effort to evaluate the large number of sequences and fully understand the rationale associated with the multiple decision paths.

Whatever the approach to accident-sequence definition and system modeling, the method that is used is essentially the same, with variations in the level of detail contained in the event- and fault-tree models. One approach involves relatively small event trees (which in turn, leads to large, complex system fault trees), while the other involves more complex event trees with less complex fault trees (see Figure 3-30). Both approaches will generate equivalent results when used by skilled and experienced practitioners. Both require considerable iteration as the analyst expands his knowledge of the plant. Thus, to a large degree, the selection of an approach should be based on the preference and the experience of the analysis team. Each approach has certain advantages and disadvantages. And, like any inductive process, each is prone to error when used by inexperienced analysts or persons lacking a thorough understanding of the plant, including the various interactions that might be present.

The analytical technique illustrated on the left of Figure 3-30 first develops relatively simple functional relationships and then establishes, by a relatively straightforward procedure, which systems satisfy these functions. Support-system dependences are modeled in the fault trees. Thus, provided common-cause events are uniquely identified, the Boolean reduction of multiple fault trees that are linked together will identify common dependences on support systems or human acts that cross system boundaries. These dependences will be properly treated even if the analyst, a priori, was unaware that the dependence existed. However, this method suffers somewhat

because the root causes of multiple-fault scenarios may be submerged in the detail of the tree and not readily apparent in viewing the event or fault trees. (They are quite visible, however, in the listing of the dominant cut sets for a given accident sequence.) Furthermore, this method requires, in general, that support-system fault trees be merged with the front-line-system trees and the various merged trees be combined to determine an equivalent tree for an accident sequence. The resultant tree can be very large, requiring significant computer capacity to perform the Boolean manipulations necessary to identify the minimal sequence cut sets and to quantify the accident sequence.

The method presented on the right of Figure 3-30 displays support-system dependences explicitly on the event tree. Because the dependences are removed from the fault trees, the combination of fault trees to obtain accident-sequence trees does not require extensive Boolean manipulation. In addition, the more formalized structure of the search for initiating events may improve the completeness of the analysis. However, since system interactions (particularly regarding support systems) are treated primarily by means of the inductive thought processes of the event tree, dependences not recognized by the analyst may not be incorporated into the analysis, and complex interrelationships of multiple systems will not be identified in the tree-reduction process. Moreover, event trees that include all support-system dependences can be very large. At some point, they can become so complex that they are difficult for the reader or reviewer to understand.

3.9 UNCERTAINTY

Chapter 12 of this guide discusses methods for performing uncertainty and sensitivity analyses for a complete PRA. The process of accident-sequence definition and system modeling is a source of uncertainty in the overall PRA study. There are several areas within the plant- and system-modeling activity that give rise to uncertainty, but most are not amenable to accurate quantitative estimation or calculation. Some of those sources of uncertainty are discussed below.

3.9.1 DATA UNCERTAINTIES

In any PRA, the data needed for developing plant and system models are associated with uncertainties. Because the models should be truly representative of the plant, it is important to ensure that the latest information (e.g., piping and instrumentation diagrams, system descriptions, and operating procedures) is available to the analyst. This type of uncertainty may be of particular importance when a plant under development is being evaluated. Uncertainty in data can be reduced by actively involving plant operating personnel in the study and establishing a comprehensive method for managing and checking input data. Other uncertainties relative to basic input data are discussed in Chapter 5.

3.9.2 MODEL UNCERTAINTY

There are basic uncertainties with regard to how well the models are able to represent the actual conditions associated with the plant's design, operation, and response to accident conditions. There are obvious limitations in the ability to faithfully represent the real world by analytical models. As an example, event and fault trees are binary-type models and tend to show only discrete on-off, yes-no type situations, whereas the real plant response may be in gradations as partial failures or complex events involving degraded system operation. Model uncertainties are acknowledged and addressed by efforts to make models as realistic as possible with compensating assumptions and modeling constraints.

Some uncertainty is also associated with the manner in which the analyst applies the methods and how skillfully or accurately he is able to represent the plant or system with the adopted modeling method. There are many ways in which the analyst could improperly develop the models. These are best addressed through training, the use of consistent procedures, and proper guidance and review, as discussed in Section 3.10, "Assurance of Technical Quality."

3.9.3 COMPLETENESS UNCERTAINTY

Several specific sources of uncertainty are associated with the development and implementation of the modeling activity. The most obvious examples are the following:

1. Initiating events: Is the list of initiating events complete and exhaustive?

2. System failure: Are all of the significant contributors to system failure properly identified?

3. Accident sequences: Are all potentially significant accident sequences identified and properly characterized?

4. Plant-damage state: Are all of the plant-damage states correctly defined, and does a particular accident sequence actually result in the identified plant state?

5. System interactions: Are all dependent failures and system interactions properly accounted for?

6. Human errors: Are human actions properly accounted for in the models?

Although it appears that there are many uncertainties, only a few can exert a significant impact on the results of the overall PRA. The sensitivity analyses described in Chapter 12 aid in understanding the relative importance of specific items and their associated uncertainty.

3.10 ASSURANCE OF TECHNICAL QUALITY

A specific effort directed at ensuring accuracy and fulfilling study objectives must be maintained throughout the PRA tasks described in this chapter. Processes both external and internal to the PRA team should be established to ensure that the study is conducted in a controlled manner and that all study activities can be validated.

Adherence to the procedures described in this guide is one of the external controls that can aid in ensuring the quality and acceptability of plant and system models. Another external control is to ensure that the methods used in the study are applied in a manner consistent with other PRA studies that are considered good examples of current application. It is appropriate to perform reasonableness checks on the interim and final results of the modeling effort by comparing the structure and output of the event trees and system models with those of similar studies.

A most important control can be exerted through the management activities of the team leader and the assembling of a coherent team, all of whom are familiar with the overall PRA process. It is important that each team member know what and why particular analytical tasks are performed. Promotion of mutual understanding and team effort will greatly benefit the sequence-definition and system-modeling process. The analytical models are complex and must be properly integrated. A well-integrated team effort will substantially aid that process.

A major factor in achieving high-quality modeling is the requirement for a complete documentation of all factors that could affect the analytical results. The analysts should maintain notebooks for event-tree development and each system model. These notebooks should provide a clear picture of the analysis process, including physical and operating descriptions, assumptions, constraints, drafts of iterative modeling efforts, and any other information that provides a concise and traceable record of how the model was developed. The notebooks need not be formal documents; their primary objective is to provide a means for collecting and preserving a visible record of the study.

The team leader plays an important role in building quality into the modeling process. He should be familiar with all aspects of the analysis and personally review details of the model development. Furthermore, he should personally check the consistency of system models and their integration into the plant-level models. It is also beneficial to have individual analysts cross check the validity of the models step by step as the study progresses.

Another important means of ensuring the technical quality of the plant and system models is the participation of utility personnel familiar with the design and the operation of the plant as an integral part of the study. By reviewing the draft and final versions of the plant and system models with the analysts who developed them, these personnel provide a desirable means of verifying that the models represent the actual plant.

One area that experience has shown to be particularly susceptible to errors is the assignment of codes or identifiers to the input events of the fault models and their subsequent use throughout the evaluation process. The analysts must exercise care in assigning the correct identifiers and ensure that identical components are consistently identified in separate models. In preparing the models for evaluation, mistakes can easily be made in preparing the input data for computer evaluation. Every attempt should be made to minimize this potential for error and the attendant loss of time and resources due to erroneous computer outputs.

REFERENCES

Atwood, C. L., 1980a. Common Cause and Individual Failure and Fault Rates for Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants (draft), EGG-EA-5289, EG&G Idaho, Inc., Idaho Falls, Idaho.

Atwood, C. L., 1980b. Estimators for the Binomial Failure Rate Common Cause Model, USNRC Report NUREG/CR-1401 (EGG-EA-5112, EG&G Idaho, Inc., Idaho Falls, Idaho).

Atwood, C. L., and W. J. Switt, 1981. User's Guide to BFR, a Computer Code Based on the BFR CCF Model, EGG-EA-5502, EG&G Idaho, Inc., Idaho Falls, Idaho.

Burdick, G. R. (Ed.), 1977. Nuclear Systems Reliability Engineering and Risk Assessment, Society for Industrial and Applied Mathematics, Philadelphia, Pa.

Commonwealth Edison Company, 1981. Zion Probabilistic Safety Study, Chicago, Ill.

Corcoran, W. R., N. J. Porter, J. F. Church, M. T. Cross, and W. M. Guinn, 1980. "The Critical Safety Functions and Plant Operation," paper presented at the International Conference on Current Nuclear Power Plant Safety Issues, October 20-24, 1980, Stockholm, Sweden.

EPRI (Electric Power Research Institute), 1982. ATWS--A Reappraisal, Part 3, "Frequency of Anticipated Transients," EPRI NP-2330, Palo Alto, Calif.

Fleming, K. N., 1975. "A Reliability Model for Common Mode Failure in Redundant Safety Systems," in Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, April 23-25, 1975, GA-A13284, General Atomic Company, San Diego, Calif.

Fleming, K. N., et al., 1975. HTGR Accident Initiation and Progression Analysis Status Report, Volume II, "AIPA Risk Assessment Methodology," GA-A13617, General Atomic Company, San Diego, Calif.

Fleming, K. N., and P. H. Raabe, 1978. "A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures," in Proceedings, ANS Nuclear Reactor Safety Division on Probabilistic Analysis of Nuclear Reactor Safety, May 8-10, 1978, Los Angeles, Calif., American Nuclear Society, La Grange Park, Ill.

Gately, W. V., and R. L. Williams, 1978a. GO Methodology--Overview, EPRI NP-765, Electric Power Research Institute, Palo Alto, Calif.

Gately, W. V., and R. L. Williams, 1978b. GO Methodology--System Reliability Assessment and Computer Code Manual, EPRI NP-766, Electric Power Research Institute, Palo Alto, Calif.

Green, A. E., and A. J. Bourne, 1972. Reliability Technology, Wiley-Interscience, New York.

IEEE (Institute of Electrical and Electronics Engineers), 1975. Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems, IEEE Standard 352-1975.

Kelley, A. P., and D. W. Stillwell, 1981. Application and Comparison of the GO Methodology and Fault Tree Analysis, EPRI Research Project 818-3, Electric Power Research Institute, Palo Alto, Calif.

Lambert, H. E., 1975. Fault Trees for Decision Making in Systems Analysis, UCRL-51829, Lawrence Livermore National Laboratory, Livermore, Calif.

Marshall, A. W., and I. Olkin, 1967. "A Multivariate Exponential Distribution," Journal of American Statistics Association, Vol. 62, pp. 30-44.

Philadelphia Electric Company, 1981. Probabilistic Risk Assessment, Limerick Generating Station, Docket Nos. 50-352, 50-353, U.S. Nuclear Regulatory Commission, Washington, D.C.

Putney, B., 1981. WAMCOM, Common-Cause Methodologies Using Large Fault Trees, EPRI NP-1851, Electric Power Research Institute, Palo Alto, Calif.

Rasmuson, D. M., N. H. Marshall, J. R. Wilson, and G. R. Burdick, 1979. COMCAN II--A Computer Program for Automated Common Cause Failure Analysis, TREE-1361, EG&G Idaho, Inc., Idaho Falls, Idaho.

Rooney, J. J., and J. B. Fussell, 1978. BACFIRE II--A Computer Program for Common Cause Failure Analysis of Complex Systems, University of Tennessee, Knoxville.

Shooman, M., 1968. Probabilistic Reliability of Engineering Approach, McGraw-Hill, New York.

Smith, A. M., and I. A. Watson, 1980. "Common Cause Failures--A Dilemma in Perspective," Reliability Engineering, Vol. 1, pp. 127-142.

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

Varnado, G. B., and R. A. Haarman, 1980. "Vital Area Analysis for Nuclear Power Plants," in Proceedings of the 21st Annual Meeting, Institute of Nuclear Materials Management, Palm Beach, Fla.

Varnado, G. B., and N. R. Ortiz, 1979. Fault Tree Analysis for Vital Area Identification, USNRC Report NUREG/CR-0809 (SAND79-0946, Sandia National Laboratories, Albuquerque, N.M.).

Varnado, G. B., et al., 1980. Fault Tree Analysis Procedures for the Interim Reliability Evaluation Program, SAND81-0062 (draft), Sandia National Laboratories, Albuquerque, N.M.

Varnado, G. B., et al., 1981. "Fault Tree Analysis Using Modular Logic Models," in Proceedings of the ANS/ENS Topical Meeting on Probabilistic Risk Assessment, September 20-24, Port Chester, N.Y., American Nuclear Society, La Grange Park, Ill.

Vesely, W. E., 1977. "Estimating Common Cause Failure Probability in Reliability and Risk Analyses: Marshall-Olkin Specializations," in Proceedings, International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tenn., June 1977.

Vesely, W. E., and J. W. Johnson, 1978. "Common Mode Analysis of Valve Leakage," Proceedings, ANS Nuclear Reactor Safety Division of Probabilistic Analysis of Nuclear Safety, May 8-10, 1978, Los Angeles, Calif., American Nuclear Society, La Grange Park, Ill.

Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl, 1981. Fault Tree Handbook, USNRC Report NUREG-0492.

Watson, J. A., and G. T. Edwards, 1979. A Study of Common-Mode Failures, R-146, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, London, England.

Williams, R. V., et al., 1981. Full Scale Nuclear Power Plant Availability and Safety Models, draft report, EPRI Research Project 1842-1, Electric Power Research Institute, Palo Alto, Calif.

Worrell, R. B., and D. W. Stack, 1977. Common-Cause Analysis Using SETS, SAND77-1832, Sandia National Laboratories, Albuquerque, N.M.

Worrell, R. B., and D. W. Stack, 1978. A SETS User's Manual for the Fault Tree Analyst, SAND77-1051, Sandia National Laboratories, Albuquerque, N.M.

Worrell, R. B., and D. W. Stack, 1980. "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, Calif., pp. 363-366.

Chapter 4

Human-Reliability Analysis

4.1 INTRODUCTION

The purpose of this chapter is to provide a procedure for estimating the probabilities of human errors in the operation of nuclear power plants. This introductory section defines the scope, assumptions, limitations and uncertainties, and the product of a human-reliability analysis (HRA). The procedure for conducting a human-reliability analysis is then outlined, highlighting the major tasks involved. The recommended method is described in Section 4.3, followed by a listing of the information requirements in Section 4.4. A detailed procedure, each step of which is illustrated by example, is presented in Section 4.5. Also included in this chapter are recommendations for documentation and the display of final results (Sections 4.6 and 4.7, respectively), a discussion of uncertainty and variability (Section 4.8), and a sample of alternative methods, their strengths, and their limitations (Section 4.9). The chapter ends with recommendations on the assurance of technical quality.

For a greater understanding of the main method presented in this chapter, the reader is urged to study the practice exercises in a recent NRC publication (Bell and Swain, 1981). Additional examples, human-performance models, and estimates of generic human-error probabilities for tasks in nuclear power plants are available in the source document for most of this chapter, the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* called simply the "Handbook" in the text that follows.

4.1.1 SCOPE

The HRA methods in this chapter are intended to support probabilistic risk assessments of light-water-reactor power plants. In such an assessment, the first effort at identifying the human-related events that affect system reliability is made by the system analysts. The human-reliability analysts then determine the associated human errors that are to be defined and analyzed. Drawing from the data in the Handbook, or on better sources of data if available, these analysts then estimate probabilities for these

---

*A. D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, draft, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, October 1980. This draft will have been substantially revised by the time of its final publication in late 1982, but the authors of this chapter have attempted to keep abreast of the current revisions. It should be noted that all chapter, table, and page numbers cited here for the Handbook refer to the October 1980 draft.

system-important errors and investigate their effects on the probability of system success. Criteria for system success and failure are established by the system analysts.

In a probabilistic risk assessment, it is necessary to consider the human tasks that are performed under normal operating conditions and those performed after accidents or abnormal occurrences. In the former situation, errors might be made during or after maintenance, calibration, or testing or in the normal operation of the plant. These errors may occur in or out of the control room. In the post-accident situation, most, but not all, of the system-safety-related errors occur in the control room.

In either situation, most of the errors identified and analyzed in this guide are those made in following plant procedures (written, oral, or standard shop practice). Only occasionally are extraneous acts considered. That is, in most cases, the analyst determines whether a given response procedure is followed correctly and does not attempt to determine which uncalled-for elements are manipulated.

The HRA method recommended and most fully described in this procedures guide employs the Technique for Human Error Rate Prediction (THERP) described in the Handbook. Unless specifically stated otherwise, all qualifying assumptions and limitations apply to the alternative methods discussed in Section 4.9.

4.1.2 ASSUMPTIONS

Only human errors are dealt with--mistakes made in the performance of assigned tasks. Malevolent behavior--deliberate acts of sabotage and the like--are not considered. It is assumed that all plant personnel act in a manner they believe to be in the best interests of the plant. Any intentional deviation from standard operating procedures is made because the employee believes his method of operation to be safer, more economical, or more efficient or because he believes performance as stated in the procedure to be unnecessary.

An important aspect of a human-reliability analysis is the qualitative assessment of the sources of human error. (This calls for identifying and understanding the underlying contributors to each error and for assessing the relative importance of each of these contributors to the system-failure events being analyzed.) However, since the PRA Procedures Guide is intended for probabilistic risk assessment, this chapter deals only with the quantitative aspect. For information on qualitative application to the operations of nuclear power plants, the reader should consult the Handbook.

4.1.3 LIMITATIONS AND UNCERTAINTIES

For a complete human-reliability analysis, the risk-assessment team should include a person who is, by professional training and experience, competent in applying the techniques of human-performance analysis to complex

systems. Such a person is usually known as a human-factors specialist, an engineering psychologist, or an ergonomist. (For a more detailed description of the qualifications of a human-factors specialist, see pages 8 and 9 of NUREG-0801 (USNRC, 1981a).) To carry out the procedure described in Section 4.5 of this chapter, he must be thoroughly familiar with, and have a good understanding of, this document as well as the Handbook. For a less complete analysis (e.g., a bounding analysis) the only requirement in this respect is that the HRA analyst be familiar with this chapter and the Handbook; he need not necessarily be a human-factors specialist.

In all cases, it is presumed that the human-reliability analysis will be an integral part of the PRA project. There will be considerable and continuing interaction between those responsible for the human-reliability analysis and those working in fault-tree and system-reliability analysis. In no case should the human-reliability analyst work in isolation from the rest of the PRA team. The structure of the team should in itself facilitate the interaction necessary among the several analysts.

The major source of uncertainty in human-reliability analysis is the dearth of actuarial data on human-error probabilities (HEPs). For the most part, the Handbook presents the best available data on human performance in carrying out the tasks performed in nuclear power plants. Most of the estimates of human-error probabilities in the Handbook represent extrapolations from human-error data based on tasks performed outside, but behaviorally similar to those performed in, nuclear power plants. The tasks are behaviorally similar because they may involve the same types of cues, interpretations, response requirements, and responsibilities as those performed in nuclear power plants. Therefore, in those cases for which an analyst can find better human-performance data than those presented in the Handbook, he should use them.

It is expected that the uncertainty and speculation involved in estimating human-error probabilities for nuclear power plants will be reduced considerably in the not too distant future. Under the sponsorship of the NRC's Office of Nuclear Regulatory Research, a program plan for a human-performance data bank is being developed, and efforts are under way to collect HEP data from realistic simulator exercises for control-room tasks and from maintenance and other tasks performed outside the control room.

As explained in the Handbook, nearly all of the tabled human-error probabilities relate to routine human actions. For some operations, cognitive errors are critical (e.g., errors in evaluating display indications). There is very little information on errors of interpretation or decisionmaking (i.e., errors in the thought process). A later section (4.5.7.1) gives a general guideline for the judgments required to estimate error probabilities for post-accident decisionmaking.

The Handbook presents nominal values for the probabilities of given human actions as well as uncertainty bounds. The nominal values reflect the best estimate (based on available data and on judgment) of the probability of a particular error in a generic sense. The uncertainty bounds are considered to approximate the middle 90-percent range of the human-error probabilities to be expected under all possible scenarios for a particular action. These uncertainty bounds are based on subjective judgment rather than on actuarial data and are not meant to represent statistical confidence limits.

As discussed in the Handbook, there are several sources of uncertainty in the generic HEP values. The variability of human performance is reflected in the differences among plant personnel--differences in skill, experience, and other personal characteristics. There can be wide variation in specific environmental situations and in other physical aspects of the tasks to be performed or in the response requirements under which the operator must act. Only some of this variation in such performance-shaping factors is accounted for in the Handbook data by providing different estimates of human-error probabilities for different sets of influencing factors. The width of the uncertainty bounds surrounding each estimated nominal probability represents an attempt to account for the residual uncertainty.

Unless specifically stated otherwise, all of the probability estimates in the Handbook are based on a set of common assumptions that limit or restrict the use of the data as stated. Exceptions to these assumptions are clearly indicated. These data apply to situations in which the following hold true:

1. The plant is operating under normal conditions. There is no emergency or other state that would produce in the operators a level of stress other than the optimal.*

2. In performing the operations, the operator does not need to wear protective clothing.

3. A level of administrative control roughly equal to the average of those employed industry-wide is in effect.

4. The tasks are performed by licensed, qualified plant personnel, such as operators, maintainers, or technicians. They are assumed to be experienced--to have functioned in their present positions for at least 6 months.

5. The environment in the control room is not adverse. The levels of illumination and sound and the provisions for physical comfort are adequate even if not optimal.

The above-mentioned factors must be evaluated qualitatively for each situation being analyzed. The finding that a situation is similar to, or significantly different from, these assumed scenarios is highly judgmental. There are no absolute guidelines for establishing a plant's conformance to what is "normal" for the rest of the industry. Only with experience and exposure to several operating plants can a human-reliability analyst develop the skills necessary for performing these discriminations successfully and reliably.

---

*Most of the human-error probabilities estimated in the Handbook apply to routine human actions, often referred to as "rule-based behavior." The method for estimating the probability of human error under nonroutine (stressful) situations is unproved. Therefore, such estimates in the Handbook are characterized by wide uncertainty bounds.

It is mainly the level of detail that will differ for human-reliability analyses performed at different stages in the life cycle of a nuclear power plant. The level of detail of the procedure presented in this chapter is aimed at analyses performed for plants that are already operating. If the analysis is performed earlier (e.g., at the construction-permit stage), some of the information necessary for a detailed task analysis will not be available. Nevertheless, the procedure can still be applied as discussed in Chapter 4 of the Handbook. For analyses performed very early, much of the information needed to determine the potential for human error will have to be derived from human-reliability analyses conducted for similar plants that are already operating.

4.1.4 PRODUCT

The main result of the human-reliability analysis is, for each iteration of the analysis, a set of estimated plant- and situation-specific human-error probabilities. During quantification of the risk-significant events, these estimated human-error probabilities can be grouped into sets for incorporation into the total PRA on the basis of their effects on the reliability of a component, a whole system, or the entire response scenario required by an initiating event. The assumptions on which these sets of estimates are based are also presented to the system analysts.

4.2 OVERVIEW

Figure 4-1 shows the four phases of HRA: familiarization, qualitative assessment, quantitative assessment, and incorporation. Most HRA methods follow this general format. A block diagram illustrating the application of these phases to the procedure followed in performing a human-reliability analysis by Handbook methods is shown in Figure 4-2. The sequence of activities shown in this figure may, however, be different from that of an analysis performed in another context. Moreover, since this is a block diagram and not a flow chart of actual activities, most of the interactions between the human-reliability analyst and the rest of the PRA team are left out. This is not to suggest that they do not exist, but Figure 4-2 is meant simply to provide a schematic of the major tasks to be performed by the human-reliability analyst himself. In reading the description of these activities, it is necessary to keep in mind that the order of the various HRA activities is not a fixed one, with each activity being performed only once: the entire process is highly iterative and its parts recursive.

It is necessary to begin preparation for this analysis concurrently with the rest of the probabilistic risk assessment. Otherwise, there will not be sufficient time to perform all the activities required for an accurate assessment of the effects of human errors.

As already mentioned, a human-reliability analysis is an iterative process; various steps will be repeated as additional plant-specific or other

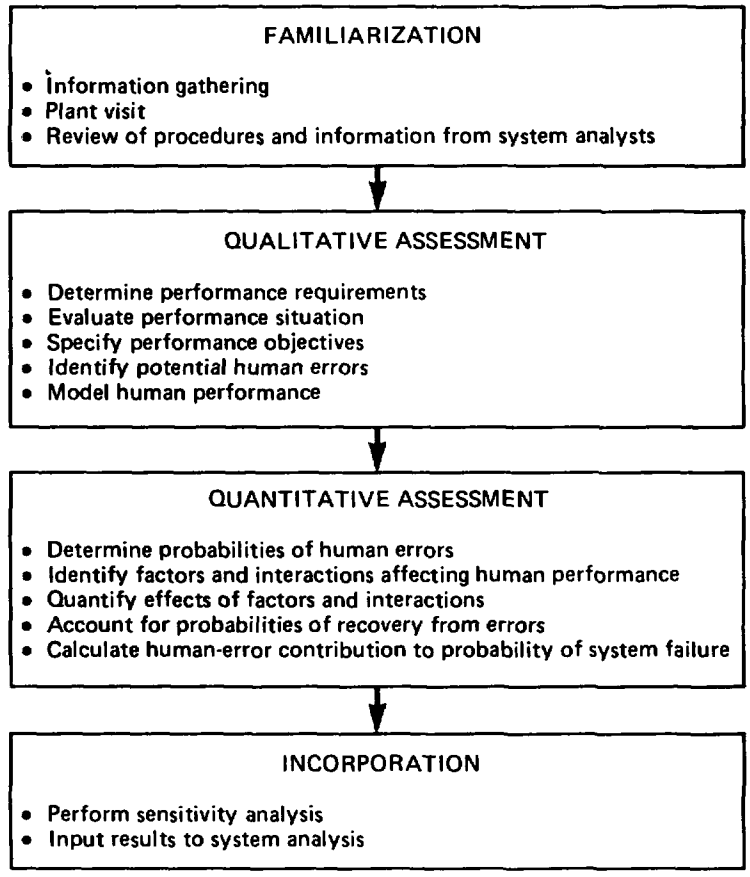


Figure 4-1. The phases of a human-reliability analysis.

information becomes available. Figure 4-2 is a block diagram for a complete analysis; for less detailed studies, such as a bounding analysis, some of the steps can be modified to reflect the appropriate level of detail and some of the steps can be eliminated. Obviously, the less plant-specific information the analyst has, the more uncertain his estimates. In a sense, the degree of uncertainty drives the level of analysis that is possible. The more uncertain an analyst's estimates, the closer his analysis is to being qualitative. A bounding analysis is more appropriate than a strictly quantitative assessment of the likelihood of any set of human errors when the information leading to the estimation of such errors is suspect.

4.2.1 PLANT VISIT

A survey of the control room during a general plant visit is an essential preliminary to the performance of a plant-specific HRA. This is to allow the analyst to become familiar with the operation of the plant. The purpose of the visit is not necessarily to evaluate the design of the control room, but rather to identify the aspects of the control room, the general plant layout, and the plant's administrative control system that affect generic human performance. No evaluation of any individual's performance is to be done. This point must be clearly understood by plant personnel if accurate and complete information is to be obtained.

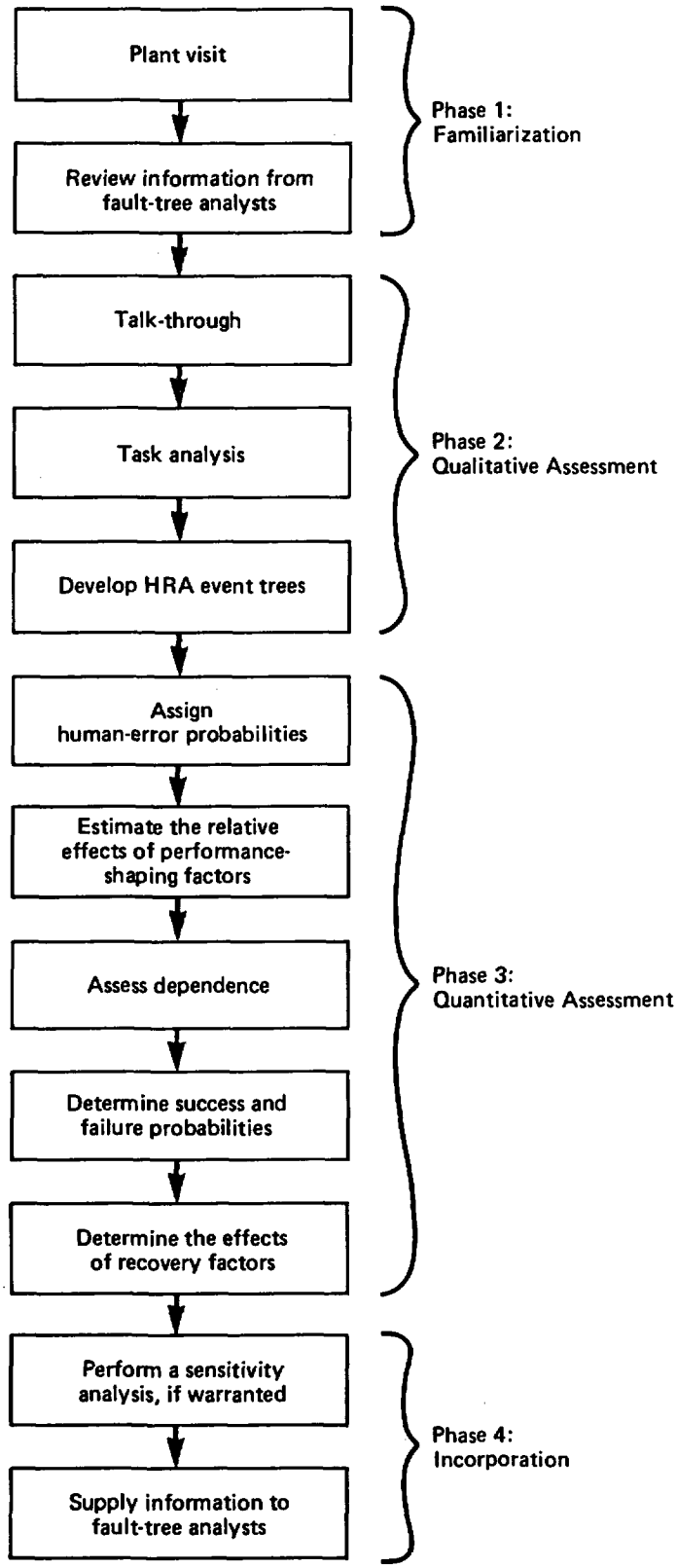


Figure 4-2. Overview of a human-reliability analysis.

4.2.2 REVIEW OF INFORMATION FROM SYSTEM ANALYSTS

For a given scenario or sequence of events, the system analysts identify human actions that directly affect the system-critical components. In light of the information obtained from the plant visit, the human-reliability analyst must review these actions in the context of their actual performance; the objective is to determine whether these actions can be affected by factors that may have been overlooked by the system analysts. For example, if performance on a noncritical element subsequently affects performance on a system-critical element, this effect must be considered, even though that task in itself is not important to the reliability of the system as defined by the system analysts.

4.2.3 TALK-THROUGH OF PROCEDURES

Sometimes performed in conjunction with the survey of the control room and sometimes at a later date during interviews with operations personnel, talk-throughs of the procedures in question are an important part of any human-reliability analysis. They are conducted by the human-reliability analyst and performed by plant operations personnel. The analyst questions the operator on points of the procedure until his understanding of the task is such that he could perform it himself or at least be able to understand fully the performance of the task. Performance specifics are identified along with any time requirements, personnel assignments, skill-of-the-craft requirements, alerting cues, and recovery factors. (The talk-through can also be performed for activities not defined by a specific plant procedure, but the effort required of the human-reliability analyst for such an analysis is greatly increased.)

The information obtained in a talk-through should enable the analyst to account for the effects of a situation's performance-shaping factors. (See Chapter 3 of the Handbook for a discussion of these factors.) Modifications made to the nominal HEP values from the Handbook will be based on information gathered here.

4.2.4 TASK ANALYSIS

At this point, a task analysis should be performed, as described in Chapter 4 of the Handbook. A "task" is defined as a quantity of activity or performance that the operator sees as a unit either because of its performance characteristics or because that activity unit is required as a whole to achieve some part of the system goal. Only the tasks that are relevant to the safety of the system are considered. A task analysis involves breaking down each task into individual units of behavior. Usually, this breakdown is done by tabulating information about each specific human action. The format of such a table is not rigid: any style that allows the information to be retrieved easily can be used. The format will reflect the level of detail as well as the type of task analysis to be performed. The analysis itself and the information it yields can be either qualitative or quantitative. Examples of task-analysis formats are presented later in this chapter.

Specific potential errors should now be identified for each unit of behavior. For every human action appearing in the task-analysis table, likely errors of omission and commission should be identified. A human action (or its absence) constitutes an error only if it has at least the potential for reducing the probability of some desired event or condition. The existence of this potential should be identified in conjunction with the system analysts. For every human action appearing in the task-analysis table, likely errors of omission and commission should be pinpointed. As mentioned earlier, extraneous acts are seldom considered. For example, the analyst may determine that, because of the control-panel layout, a selection error is possible during the manipulation of a specific switch, but his analysis will not usually predict which other element will be chosen, nor will it deal with the consequences of selecting a specific incorrect switch.

The analyst must also evaluate errors that may affect the probabilities of system success and failure but do not appear in the task analysis. Some of these can be disregarded by assuming for the entire analysis that a certain condition does or does not exist. For example, in the case of a post-maintenance test, if we are interested in the conduct of the test itself, we may arbitrarily assume that the supervisor has ordered the test. In determining which of these assumptions may be made, great care must be taken, however. In analyzing actual plant conditions, it is inappropriate to assume that something that should be done will always be done.

4.2.5 DEVELOPMENT OF HRA EVENT TREES

Each of the errors defined above should be entered as a binary branch on an HRA event tree, as described in Chapter 5 of the Handbook. The possible error events should appear on the tree in the order in which they might occur if such order is relevant. The suggested format for HRA event trees will be presented later. The product of the HRA event tree is a probabilistic statement as to the likelihood of a given sequence of events. Some PRAs deal only with the probability of successful completion of all human actions, while others take a more global approach, considering all system interactions and reactions that may contribute to the probability of system success. In either case, recovery factors usually are not included at this time. This is simply a time-saving feature of this HRA procedure. If, in a preliminary system analysis, the probability of an unrecovered human error is found not to impact system safety significantly, there is no need to expend additional time and effort on identifying and quantifying the effects of recovery factors acting on the situation.

4.2.6 ASSIGNMENT OF NOMINAL HUMAN-ERROR PROBABILITIES

An estimate of the probability of each human-error event on the HRA event tree must be derived from the data tables in the Handbook or from other sources. Tables of human-error probabilities (and the associated uncertainty bounds) for generic task descriptions are found in Chapter 20 of the Handbook.

One of the reasons the analyst should become familiar with the Handbook is the need for a thorough understanding of the assumptions and limitations of these tables. If there is no exact match between the description of a task in the Handbook and that defined by the task analysis, the estimated error probability for a similar task can be used as is, or it can be extrapolated, depending on the degree of similarity between the descriptions. "Similarity" in this context refers to the likeness of required operator behaviors. There can be a high degree of similarity between the performance of two tasks even though the equipment is dissimilar. The experience of a human-factors specialist is very valuable for this kind of judgment.

4.2.7 ESTIMATING THE RELATIVE EFFECTS OF PERFORMANCE-SHAPING FACTORS

The human-error probabilities estimated in the Handbook for a given task must now be modified to reflect the actual performance situation. For example, if the labeling scheme at a particular plant is very poor, in comparison with those described in Military Standard 1472C (U.S. Department of Defense, 1981) or NUREG-0700 (USNRC, 1981b), the probability should be increased toward the upper bound of its uncertainty bounds. If the tagging control system at a plant is particularly good, perhaps the probability for certain errors should be decreased.

Some of the performance-shaping factors (PSFs) affect a whole task or the whole procedure, whereas others affect certain types of errors, regardless of the tasks in which they occur. Still other PSFs have an overriding influence on the probability of all types of error in all conditions. Familiarity with the Handbook's treatment of PSF effects is necessary for the performance of these procedures.

4.2.8 ASSESSMENT OF DEPENDENCE

In any given situation, there may be different levels of dependence between an operator's performance on one task and on another because of the characteristics of the tasks themselves or because of the manner in which the operator was cued to perform the tasks. Dependence levels between the performances of two (or more) operators may differ, also. The analyst should keep in mind that the effect of dependence on human-error probabilities is always highly situation-specific. The concepts presented in the Handbook (the chapter on dependence) should be followed precisely.

4.2.9 ESTIMATING SUCCESS AND FAILURE PROBABILITIES

The criteria for system success and failure will be supplied by the system analysts. These criteria are used as the basis for labeling the end point of each path through an HRA event tree as a success or a failure. Multiplying the probabilities assigned to each limb in a success or failure path through the HRA event tree provides a set of success and failure

probabilities that can then be combined to estimate the total system success and failure probabilities.

4.2.10 DETERMINING THE EFFECTS OF RECOVERY FACTORS

It is often convenient to postpone consideration of the effects of recovery factors until after the total system success and failure probabilities have been determined. The estimated probabilities for a given task sequence may be sufficiently low without considering the effects of recovery factors so that the sequence does not appear as a potentially dominant failure mode. In this case, it can be dropped from further consideration.

4.2.11 PERFORMING A SENSITIVITY ANALYSIS, IF WARRANTED

To determine the effect of a single parameter on the total system-success probability, a sensitivity analysis can be performed. In this exercise, the value of a given parameter is manipulated and the resulting system-success probabilities are compared to judge the impacts of different magnitudes of change. This is not a necessary part of a human-reliability analysis in all cases, but it is extremely helpful in identifying the elements of the system that have relatively large or small effects on system safety.

4.2.12 SUPPLYING INFORMATION TO SYSTEM ANALYSTS

A copy of each HRA event tree along with a synopsis of the results, a copy of the task-analysis table, and a list of the underlying assumptions should be presented to the system analyst. The system analyst, the human-reliability analyst, and someone familiar with the actual performance of the operation should then go over the HRA event tree and the associated assumptions very carefully. This ensures that the human-reliability analyst has correctly defined the success of the system and that the system analyst does not apply the results of the HRA event tree outside the scope of its stated limitations.

4.3 METHOD

The theory, models, and data presented in this chapter are taken from the Handbook. Original sources for some of the methods (e.g., task analysis) can be found there.

The basic components of a human-reliability analysis are the task analysis and the Technique for Human Error Rate Prediction (THERP). Task analysis involves breaking down system-required human actions (or tasks) into

small units of physical or mental performance (steps) as well as identifying to the extent possible likely human actions not required by the system but having the potential for degrading certain system functions. These small units are then fully described and analyzed in terms of the PSFs that affect each function and combinations of them. The performance models and theories that make up THERP are then applied to these steps. Possible human errors are identified, and estimates of the probability of each error are derived. The end product of a human-reliability analysis is a set of system success and failure probabilities that reflect the probable effects of human errors. These system-based probabilities are in a form suitable for entering into the system fault trees by task or component.

Alternatives to THERP are discussed in Section 4.9 as well as in reports by Meister (1971), Embrey (1976), and Pew et al. (1977).

For cases in which it is necessary to use expert judgment to derive estimates of the probabilities of human error in nuclear power plants, there are a number of psychological scaling methods available. For a recent review, see Stillwell et al. (1982). In addition, the NRC, the Institute of Nuclear Power Operations, and the British National Centre of Systems Reliability (Embrey, 1981) are developing methods for psychological scaling specifically addressing nuclear power plant tasks. At present, no one method can be recommended since these studies are still under way.

4.4 INFORMATION REQUIREMENTS

After the system-analysis team has determined which system-critical events or components are to be evaluated, the human-reliability analyst should double-check to ensure that no potential human contributions have been overlooked. Procedures for performing each of the tasks involved in these events must therefore be evaluated. These procedures can be written, oral, or in the form of known standard shop practice or skill of the craft. In the case of written procedures, a copy of the procedure itself should be supplied to the human-reliability analyst; in the other two cases, the specifics required of the performance must be determined in the course of interviews with, and observations of, plant personnel.

The human-reliability analyst must become familiar with the plant, especially with the layout of the control room, and with the plant's general operating standards and administrative controls. The analyst who is not familiar with these aspects of a particular plant should make at least one visit (and preferably several) to the plant specifically for surveying the control room. Blueprints, drawings, or photographs of the consoles and control boards should be available for later reference. Personnel familiar with all phases of plant operations should be on call to provide information about control-room specifics and other features peculiar to the plant.

Human-reliability analysts need not have a thorough understanding of plant systems and functions--they need not have the same understanding of

these systems and functions as other specialists on the risk-assessment team. (Ideally each member of the PRA team would have at least a working knowledge of PRA fields other than his own; however, such people are not usually available in numbers large enough to support a full-scale PRA.) They should concern themselves primarily with actual human performance--system causes and effects are of no interest except in that they may influence an operator's perception of the urgency of a particular task. The system analysts and plant representatives are chiefly responsible for defining the impacts of human errors on the systems and functions of the plant. Their close interaction with the human-reliability analyst will ensure that the modeling of the effects of human errors is correct. In quantifying these effects, the underlying assumptions and limitations that apply to the models and data presented in the Handbook must be understood and not contradicted in their applications to a PRA.

4.5 PROCEDURE

4.5.1 INTRODUCTION

The purpose of performing a human-reliability analysis as part of the PRA described in this document is to determine the contribution of human errors to predetermined significant system failures. The object of such an analysis is to treat the relevant human actions as components in system operation and to identify error probabilities that could significantly affect system status. This section outlines an approach to be used in deriving relevant human-error probabilities along the guidelines established in the Handbook.

As already stated, the human-reliability analysis should be performed by a human-factors specialist who is familiar with the theory and techniques presented in the Handbook. For a complete human-reliability analysis, he must have an understanding of the plant's administrative-control network, some familiarity with the layout and the operating characteristics of the control room, and frequent access to plant personnel who can provide information on specific aspects of performance situations. Without sufficient plant-specific information, he will be unable to perform a human-reliability analysis that models the actual plant situation adequately in that he will not have defined all the potential human errors--nor will he have accounted for all the likely recovery factors.

This section discusses each of the major HRA tasks outlined in Section 4.2. An example of a human-reliability analysis is presented in tandem with these discussions. The description of each task is supported by an example of application to an actual human-reliability analysis.

There are several possible sequences for the elements of a human-reliability analysis. The sequence presented here is by no means absolute, but it is a sequence that served well for the Interim Reliability Evaluation Program and other PRAs. The elements themselves were derived from THERP and should be included in all complete human-reliability analyses. The

recording and reporting formats described here can be modified for the convenience of the analyst, but he should keep in mind the type and level of detail of information necessary for someone else to understand his analysis. The analysis can be used for qualitative as well as quantitative assessments, with the level of detail of the information collected reflecting that of the analysis itself. Of necessity, human-reliability analysis must depend largely on data that are extrapolations from tasks not directly related to nuclear power plants and on models that have not been verified in the strictest sense of the word. Nevertheless, this application of the theory, data, and models presented in the Handbook represents an attempt at standardizing the approach to performing human-reliability analyses for the probabilistic risk assessments of nuclear power plants.

4.5.2 PLANT VISIT

4.5.2.1 Discussion

At least one plant visit, specifically including a detailed survey of the control room, should be made at the onset of the analysis. Before this visit, the analyst should make arrangements with the plant as to the plant areas to be visited, the requirements for access, and the types of personnel to be made available for interviews. Every attempt should be made to minimize impact on the plant and on the utility as well as the disruption of plant operations.

When possible, the human-reliability analyst should meet with representatives of the plant and/or utility before visiting the plant. The objective of this meeting is to advise the plant and utility representatives about the purpose of the evaluation. More cooperation at all levels of involvement will be afforded if the concerned parties understand that the role of the human-reliability analysts is not condemnatory or judgmental. The main purpose of the visit should be stressed: the observation of plant conditions in order to provide accurate descriptions of actual performance for the analysis. The observations are to be expressed only in descriptive terms. No "solutions" to plant problems or inadequacies are to be offered.

In the initial visit to the plant, the human-reliability analyst will make notes on relevant performance-shaping factors, especially those pertinent to control-room operations. If the system analysts have already identified the plant subsystems or procedures that are of interest, these can be examined closely at this time. This visit should provide general information about the plant's operating characteristics and a "feel" for the effectiveness of the plant's administrative controls.

In surveying the control room, specifics relating to the layout of controls and displays should be noted. Copious notes should be taken on the characteristics of critical controls and displays, noting any factors that would influence their use--anything that would aid or hinder the operators in either locating, manipulating, or interpreting them. Deviations from good human-factors engineering practices, such as those noted in the previously cited military standard (U.S. Department of Defense, 1981) and NRC guidelines

(USNRC, 1981b), should be noted. Any specifics related to the operation of critical subsystems that have been pinpointed for observation by the system analysts should be recorded. If the system analysts have identified the plant procedures of interest, the time at the plant should also be used for a talk-through of these procedures (Section 4.5.4).

4.5.2.2 Example

Listed below is a set of notes similar to those that would be collected during an actual plant visit.

1. On some chart recorders the indications are hazy because of the use of nonglare glass. The operations superintendent says they are all being changed to regular glass. (The nonglare glass had been recommended by the manufacturer.)

2. Some labels for two-channel switches are sideways because of space restrictions. (Later note: When these sideways labels appear between displays, some confusion in relating a label to a display may result.)

3. Each annunciator panel is numbered, with the numbers increasing from right to left (so do the numbers for the control board and panels).

4. On the fronts of control panels CB1 and CB2, there are rows of J-handle switches, the first of which are turned inward to prevent inadvertent manipulation. This is not true for panel CB4, but its J-handle switches are not critical to plant operation. Those on panels CB1 and CB2 are for oil pumps and turbines, and their movement would cause a trip. The direction of manipulation for the reversed J-handles is the same as for the outward-facing ones.

5. Some J-handles have arrows at their bases that indicate the direction of operation; some do not. (Note: Different manufacturers?) Handles, other than the J-handles, have arrows at their bases, especially knurled or symmetrical handles. The size of these shape-coded handles is such that the arrows cannot be seen easily, especially when viewed at eye level straight on.

6. At the alarm cathode-ray tube (CRT), there are three display modes: a flashing dark-green display indicates a new, unacknowledged alarm; a steady dark-green display indicates an uncorrected but acknowledged alarm; and a steady light-green display indicates a cleared alarm (it remains on for reference only).

7. For the engineered-safety-feature (ESF) panels in the cabinets in the back (as well as other indications in the control room), display status and some parameter readings must be recorded at various intervals. (Note: Need to request a copy of "Procedures for Conducting Plant Operations" to review the checklist used versus the frequency of its use and the location of all controls checked.)

8. On the ESF panels in the control room, the color of the label for a particular item is the color of the indicator light during actuation

of the automatic safety equipment. During system response to an emergency, the operator can scan the ESF panel quickly to see whether the lights that are on are the same color as the labels for those items. A disagreement between the colors indicates that some safety system has malfunctioned or has been overridden manually for some reason.

9. Stubs from yellow tags for valve-change operations are tossed into a drawer; no record of them is in evidence. (Note: Check this out.)

10. The labels on locally operated valves are impression-printed on metal tags and, because of poor lighting, are difficult to read. No indication that designates their normal positions is present at these valves.

Obviously, there are other observations that could be made during a survey, but they have been omitted here for the sake of brevity. The levels of detail for the control-room survey and the inspection tour of the plant are at the discretion of the human-reliability analyst and should reflect the level of detail required by the risk assessment being performed. Specific information about the conduct of certain procedures identified later in the program can be supplied by plant personnel during a talk-through, with the human-reliability analyst interpreting that information in the light of knowledge gained during the plant visit.

4.5.3 REVIEW OF INFORMATION FROM SYSTEM ANALYSTS

4.5.3.1 Discussion

After the screening process the system analysts will present the human-reliability analysts with a set of scenarios to be analyzed. These will usually take the form of operator performance on a critical system element during the course of following a set of plant procedures. The system analysts will have identified system-critical components and the circumstances under which they will be manipulated. The human-reliability analysts must then determine the probability of human errors in dealing with these components. They must also determine whether human performance on other elements or in the conduct of the plant's administrative controls will affect the probability of error in operating the system-critical components.

Often, the system analysts will present the human-reliability analysts with a set of plant procedures from which they have pinpointed the steps that they feel deal directly with the operation of system-critical components. In other cases, they may have identified entire systems for which human errors must be identified and quantified. In either case, the human-reliability analyst must examine all of the plant procedures associated with these elements to determine whether they require performances on other elements that might affect the probability of error on the critical components or systems. At times, these determinations will have to be made in conjunction with the talk-throughs of the procedures (Section 4.5.4).

During this review of the information received, the critical task of the human-reliability analyst is to ensure that all human actions are

analyzed in the context of actual performance. Human actions in a nuclear power plant should not be treated as isolated entities, unaffected by other factors. There are many interactions in a nuclear power plant--between personnel and between tasks--that must be identified. Some of them will affect the assessment of levels of dependence between certain behaviors (Section 4.5.9); some of them will have a global effect on the performance of all tasks in a given procedure. The system analysts will have identified the interfaces between critical equipment items and associated human tasks. However, the interactions between these and other system elements should be identified by the human-reliability analyst, who has been trained to spot them. This extra investigative effort on the part of the human-reliability analyst must ensure that they are all identified.

In some cases, a single plant procedure will cover several sets of tasks involving critical components. For example, in restoring items of equipment after maintenance, the operators may follow a general plant procedure governing the application and removal of tags. This administrative control may apply to all tasks in which tags are used. In this case, it is the conduct of the administrative-control procedure that is analyzed, as well as the restoration act itself. The operator is actually following the control procedure rather than a set restoration procedure for a specific component. Here the human-reliability analyst can examine one procedure (the administrative-control procedure) and apply the results to all tasks involving restoration after maintenance. He must take care, however, to determine that the administrative-control procedure applies to every task he analyzes.

As he reviews the information received from the system analysts, the human-reliability analyst should search for deviations from, or inconsistencies with, the assumptions underlying the theories and models in the Handbook. The human-error probability estimates in Chapter 20 of the Handbook are based on limitations on their use--limitations that must not be contradicted. The human-reliability analyst must examine a given procedure in the context of its performance to assess its conformance to these limitations.

4.5.3.2 Example

A set of hypothetical plant procedures dealing with response to a small loss-of-coolant accident (LOCA) is presented in Figure 4-3. Only part of the procedure is given, and the steps identified by the system analysts as being critical are indicated with a double asterisk. The system analysts have assumed that the situation has been diagnosed correctly and that the operators have correctly completed the immediate actions required by the situation. These assumptions limit the nature of the human-reliability analysis because, given them, the human-reliability analyst does not have to account for errors in diagnosis or for the fact that the level of stress experienced by the operators might be higher because of their having made mistakes in the immediate actions. However, those systems that have been judged to have the potential of being degraded by human errors are those involved in the "Subsequent Activities" section of the procedures. These, therefore, are the only ones to be considered in this example. (The treatment of diagnosis errors will be discussed in a later section.)

D. SUBSEQUENT ACTIVITIES

Note: Reverify asterisked parameters in all sections, using alternative indications if available. Select proper computer functions to monitor incore thermocouples.

*If FW and RCPs are available (manual HPI actuation, no automatic actuation), proceed through Section D.
*If no FW is available, proceed to Section E.
*If FW is available but RCPs are not, proceed to Section F.

D.1 Stop all but one RCP in each loop.

Note: If ES actuation occurs before HPI can be manually established and the RCS pressure recovers, do not reset ES analog channels, since this would delay restart of actuated equipment in the event of a loss of offsite power as pressure would have to fall again to the actuation setpoint.

**D.2 Monitor RCS pressures and temperatures; maintain at least 50°F margin to saturation by holding RCS pressure near the maximum allowable pressure within the cooldown pressure-temperature curve (Figure B).

Note: If RCS pressure is not restored before the pressurizer goes solid, or if the RCS relief valve alarm remains in, the leak may be in the pressurizer steam space, and the pressurizer must be taken solid to regain RCS pressure. If such is the case, reopen ERV block valve MOV-1300 to allow ERV operation before pressurizer code safeties.

**Caution: HPI components are not to be overridden unless the following criteria are met:

1. The HPI system has been in operation for 20 min, and all hot- and cold-leg temperatures are at least 50°F below saturation temperature for the existing RCS pressure, or

2. The RCS is >50°F subcooled, and throttling of HPI is necessary or

3. The RCS is 50°F subcooled, and HPI throttling is necessary to remain within the plant cooldown pressure-temperature curve limits, or

4. DH or LPI has been operating for >20 min with total flow rates of ≥2000 gpm.

If margin to saturation drops below 50°F after HPI override, reinitiate maximum HPI until >50°F subcooled. UNDER NO CIRCUMSTANCES IS HPI TO BE OVERRIDDEN IF RCS IS NOT SUBCOOLED.

D.3 Monitor RB pressure; if pressure reaches 4 psig, verify reactor building isolation and cooling actuation (ES channels 5 & 6) and HPI & LPI actuation (channels 1, 2, 3, and 4).

Note: Proper ES actuation is verified by noting that the colors of components' indicating lamps on the ES panels ES-16 and ES-18 and CB-26 correspond to the colors of the switch nameplates. Proper flow ranges for HPI, LPI, and RB spray are marked on the meter faces. Proper penetration room ventilation is verified by noting all room isolation damper lights out, flow indicated, and negative penetration room pressure indicated....

**D.4 If RCPs and FW are available, and RCS margin to saturation is >50°F, override and throttle HPI MOVs to control system pressure if pressurizer is solid or to hold pressurizer level at setpoint while using pressurizer heaters and spray for RCS pressure control; initiate plant cooldown per Plant Procedure 12 at a rate that allows RCS pressure to be maintained within the cooldown pressure-temperature envelope.

D.5 If RCS pressure falls to within 50°F of saturation or if low margin to saturation temperature alarms are received, maintain maximum HPI flow until 50°F margin is restored.

D.6 If RCS pressure falls below secondary pressure, reduce and maintain secondary pressure at 20 lb/in. less than primary pressure and maintain maximum HPI flow until subcooled, then initiate a cooldown by decreasing secondary pressure per Plant Procedure 23.

Figure 4-3. Excerpt from the procedures for responding to a small LOCA. The critical steps are indicated by a double asterisk.

**D.7 Prepare for LPI boost to MU pump suction and RB sump recirc as follows:

D.7.1 Verify MU tank outlet MU-13 closed.

D.7.2 Open DH-7A and DH-7B, LPI discharge to MU pumps suction, verify MU pump suction crossover valves MU-14, MU-15, MU-16, and MU-17 open, and verify MU pump discharge crossover valves MU-23, MU-24, MU-25, and MU-26 open.

D.7.3 Isolate the DH rooms by closing both DH room floor drain valves, ABS-13 and ABS-14, securing room purge dampers CV-7621, CV-7622, CV-7637, and CV-7638 from ventilation control panel (east wall of 404-foot ventilation room) and closing watertight doors.

D.7.4 Verify both DH pumps operating and both LPI MOVs open (MOV-1400 and MOV-1401).

D.8 Once a 50°F margin to saturation is attained.....

**D.9 Monitor BWST level; when BWST level has fallen to 6-foot indicated level or when the corresponding BWST lo-lo-level alarm is received, transfer suction to RB sump by verifying RB sump suction valves inside containment MOV-1414 and MOV-1415 open, opening RB sump suction valves outside containment MOV-1405 and MOV-1406 (a slight upward perturbation should be noted on pump flows indicating suction transfer) then close both BWST outlets MOV-1407 and MOV-1408 (refer to Plant Procedure 23 for RCS temperature control methods). Close NaOH tank outlets MOV-1616 and MOV-1617. MANUAL OVERRIDE PUSHBUTTONS MUST BE DEPRESSED FOR ALL VALVE MANIPULATIONS IF ES ACTUATION HAS OCCURRED.

Figure 4-3 (continued). Excerpt from the procedures for responding to a small LOCA. The critical steps are indicated by a double asterisk.

Given the above assumptions and following a detailed reading of the procedures, everything seems to be in order for a straightforward use of the theories and models in the Handbook, with one exception: the performance of these tasks occurs about an hour after the onset of the small LOCA. The Handbook chapter on stress states that there will be three operators in the control room at this time. However, some of the actions required by this procedure take place outside the control room. Because of the response time involved in donning the protective clothing required for these tasks, it is assumed here that only two qualified operators will be in the control room. Of course, during an incident of this type several people will probably be present in the control room. However, the shift supervisor is still in charge of operations, and personnel working for him are likely to follow his instructions and line of thought. Therefore, it is conservatively assumed that the presence of several people would be no more beneficial than the presence of only three licensed operators.

4.5.4 TALK-THROUGH

4.5.4.1 Discussion

In a talk-through of a set of procedures for which safety-critical events have been identified, the human-reliability analyst questions someone familiar with the performance of that procedure on specific points of the procedure until the analyst is so familiar with the tasks that he could perform them himself or at least understand fully the performance of an operator. The talk-through can be performed on sets of written or oral plant procedures,

standard shop practice, or training methods. It could take place at a simulator instead of at the plant itself, but the human-reliability analyst must take great care in noting which of the characteristics of the simulator are unlike those of the plant.

During the talk-through, the analyst must determine the performance-shaping factors that influence behavior, such as the location and the physical and operating characteristics of specific controls, the type and location of alarms and annunciated indicators, control-room manning and task allocation, time requirements, and limits for alarm indications and responses. He must also "translate" the written procedures into English as he speaks it; that is, he must determine the meaning of the specific instruction resulting from each command given in the set of procedures in the language of that particular plant. The analyst must specify in language he can understand the exact interpretation the operators will make from the sometimes vague wording of plant procedures. At times, these interpretations are based on the operator's knowledge of system operation rather than on a standardized plant definition of the term in question. When this is the case, the analyst must ascertain whether all the operators define that term in the same way.

In performing a talk-through, the human-reliability analyst conducts an interview with a plant employee who is familiar with the performance of the procedure in question. (In the case of a new plant, the person most familiar with the development of the procedures should be interviewed.) To obtain more familiarity with the performance characteristics of the procedure, the analyst should ask general questions about the performance-shaping factors acting at the time of performance and specific questions about the factors affecting the performance of the critical steps.

A talk-through can be performed as part of the control-room survey. In this case, the operator and the human-reliability analyst actually follow the path taken by the operators in performing the procedure. When the procedures call for the manipulation of a specific control or for the monitoring of a specific set of displays, the operator and the analyst approach them at the control panels, and the operator points out the controls and displays in question. The procedure is followed in sequence, and the analyst could generate a link analysis at this time. (Link analysis is discussed in Chapter 3 of the Handbook.)

Careful notes recording the outcome of the talk-through must be taken. Much of the information from these activities will be entered directly into the task-analysis tables (Section 4.5.5) for later use.

4.5.4.2 Example

In the talk-through of the procedures in Figure 4-3, some general information was gathered that relates to the performance of all the steps in the procedure. They are listed below.

1. The plant is following an emergency procedure. (Note for later reference: There will be some level of stress for the operators.)

2. The "Subsequent Activities" section of the procedures will be performed approximately 1 to 1.5 hours after the start of the accident.

3. At least three licensed operators will be available to deal with the situation. One of them will probably be the shift supervisor.

4. At this plant, "verify" means to check and, if necessary, to correct the status of a given item of equipment. For example, if the operator must verify that a valve is open and, on checking its status, finds it closed, he must open it manually.

5. The asterisked note at the beginning of the section indicates that the performance of the procedures in Section D is to be reverified (double-checked) after the procedures have been completed. This constitutes a recovery factor and, as such, will not be included in the HRA event tree at this time.

6. The "caution" in Figure 4-3 stems from actions taken during the incident at Three Mile Island Unit 2. Because of the special implications of performing them incorrectly, these actions will be considered separately.

7. Steps D.2, D.4, D.9, and D.7.4 are performed in the control room. They will be diagrammed separately from steps D.7.1, D.7.2, and D.7.3, which take place outside the control room.

Specifics relating to the performance of individual steps will now be given in the order of the steps.

Step D.2. The pressures of the reactor-coolant system (RCS) are found on a chart recorder; RCS temperatures can be read from digital indicators; both are on a front control board. A copy of the pressure-temperature curve is taped to the side of the computer terminal, adjacent to these other indicators. To manipulate the pressure and temperature values, the heater switches found on the same front control board will be used.

Step D.4. There are four switches for four motor-operated valves (MOVs) for high-pressure injection on the vertical ESF panels. A sketch of the layout of the controls is shown in Figure 4-4. Cooldown is initiated by following another procedure. The operator says that this other procedure is so well known that he cannot think of any situation in which it would actually be necessary to refer to it.

Step D.7.1. Valve MU-13 is a manual valve in the stairwell outside the main unit pump room. This stairwell is two levels down from the control room.

Step D.7.2. The layout of these valves is shown in Figure 4-5, with the channels they represent. One channel should always be completely open so that the operator should only have to open one low-pressure-injection (LPI) discharge valve, two makeup-pump-suction crossover valves, and two makeup-pump-discharge crossover valves. The operators view this entire series of tasks as one unit task: in their interpretation, all these steps are

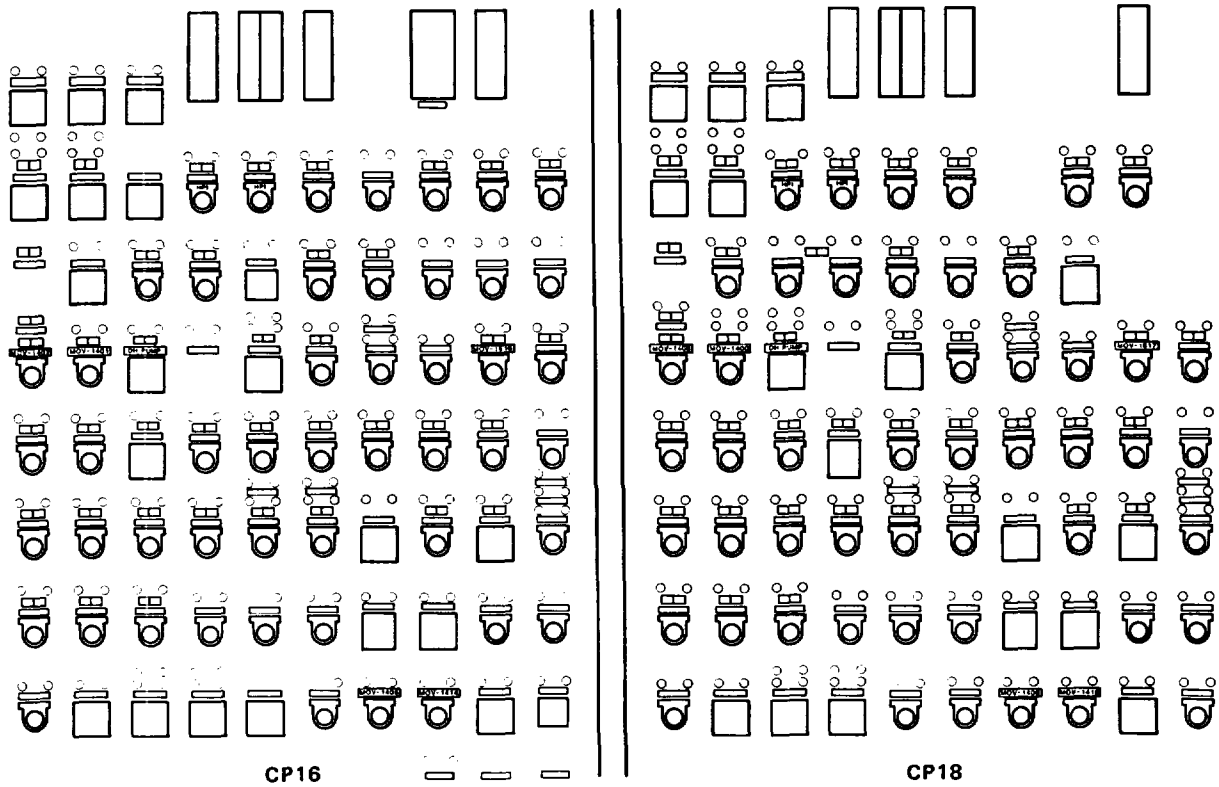


Figure 4-4. Layout of controls on the ESF panels.

performed to satisfy a major system function. These valves are located one level below the makeup-pump room.

Step D.7.3. Valves ABS-13 and ABS-14 are large, locally operated valves located outside the decay-heat (DH) rooms, one level below the decay-heat pump rooms. They are large valves situated under the grating outside the watertight doors. There are no other valves under the grating. The ventilation room is two levels above the control room. The switches for CV-7621, 22, 37, and 38 are on the wall there, in the midst of dozens of other similar switches. They are grouped near each other and near other switches that control equipment in the same physical area of the plant, but there are no location cues on the wall to indicate where this grouping can be found among other groups.

Step D.7.4. Indicators for the decay-heat pumps and for the LPI MOVs are on the vertical ESF panels in the control room. (See Figure 4-4 for the layout of the panels.)

Step D.9. The level indicator is on a panel adjacent to the vertical ESF panels in the control room. The low-low-level alarm sounds when the 6-foot level is reached. During a small LOCA, this should happen no sooner than 1.5 hours after the start of the event. All the MOVs are on the ESF panels.

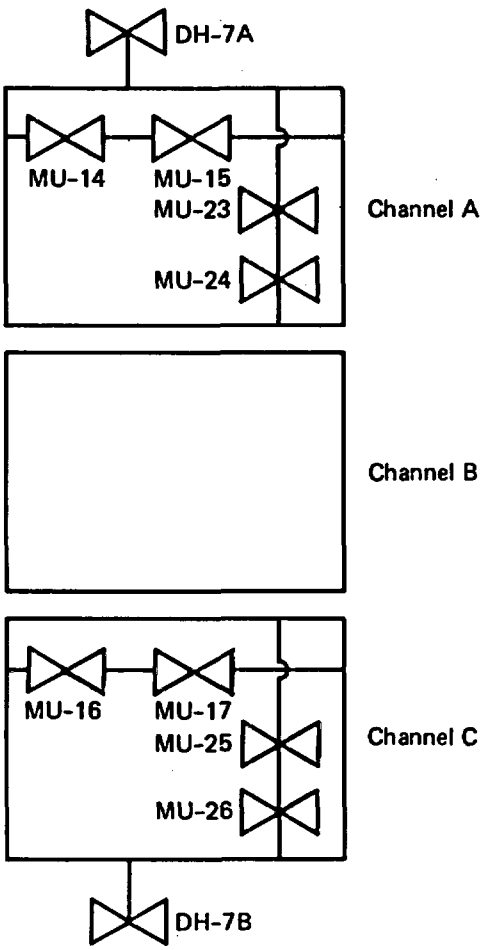


Figure 4-5. Layout of valves in DH pump rooms.

4.5.5 TASK ANALYSIS

4.5.5.1 Discussion

At this point, the procedure should be formally broken into tasks or smaller units of behavior; that is, for each step in the procedure, individual units of operator performance must be identified, along with other information germane to the performance. These individual units of performance constitute elements of behavior for which potential errors can be identified. In other words, a large task consisting of a set of steps should be broken down to allow the identification of errors associated with each step. All of this information must then be entered into a task-analysis table.

The format of this table is not specified, but the table must contain all the information necessary for later parts of the analysis. In most cases, the necessary information will consist of such items as the piece of equipment on which an action is performed, the action required of the operator, the limits

of his performance, the locations of the controls and displays, and explanatory notes. If different tasks are to be performed by different operators, the allocation of tasks to personnel can be indicated in the task-analysis table, or separate task-analysis tables can be made for each operator. The example in this section takes the latter approach.

The level of detail in a task analysis and the amount of information recorded should reflect the level of detail (qualitative or quantitative) of the risk assessment and are obviously determined judgmentally. The guiding rule for this determination is that one should be able at a later date (perhaps when the results of the human-reliability analysis are compared with those of another analysis) to recapitulate the rationale for the human-error probabilities that were used in the analysis.

Once the task steps have been broken down, potential errors must be identified for each step. The analyst must decide whether, for any given step, he should consider an error of omission or the various errors of commission (selection, reversal, sequence, etc.) that are likely for that step. This decision must be made based on the relevant performance-shaping factors and the task analysis. The steps should be listed chronologically.* Considering the characteristics of the actual performance situation, the human-reliability analyst must determine and record which types of errors the operator is likely to make and which he is not. For example, if an operator is directed by a set of written procedures to manipulate a valve and that valve is fairly well isolated on the panel, differs in shape from other valves on the same panel, and is very well labeled, the analyst may decide that errors of selection are not to be considered in this case. He should also have determined that, in following the written procedures, the operator might make an error of omission.

Extreme care should be exercised in deciding which errors, if any, are to be completely discounted. In comparison with tasks in other industries, most of the tasks performed in nuclear power plants have very low human-error probabilities, on the order of 10^{-3}. Although one error in a thousand opportunities seems quite low, a human-error probability of 10^{-3} may contribute substantially to the frequency of system failure. Rather than discounting a "questionable" error that he thinks may be unlikely, the human-reliability analyst should consider it and perform a sensitivity analysis to ascertain its impact on the probability of system success (Section 4.5.12). If the impact is found to be negligible, an appropriate indication can be made in the fault-tree block for the error.

---

*In some cases, it may be discovered that the order of the steps in the procedure is not necessarily the one followed by the operators. The task analysis and the resulting HRA event tree can easily reflect any performance sequence. However, the order of the steps in the procedure is usually assumed to be the most likely order of task performance. Recordkeeping is simplified by following the same task sequence from procedures to task analysis to HRA event trees.

Once he has identified the errors likely to be made in each unit of performance, the analyst must look for other factors that may affect performance. The entire performance scenario must be considered in this search. The analyst is looking for elements that are usually outside the scope of the procedures followed by the operator. For example, if something is to be done at the discretion of the shift supervisor, the supervisor's remembering to order the task will determine whether the task is performed by the operator. These extraneous factors that affect the probability of human error usually involve some sort of failure in the plant's administrative-control system. The quality of the plant's personnel-communication system and the potential for the disruption of communications during a particular performance sequence will also have to be examined in these cases.

Events other than human actions that affect subsequent performance must also be taken into account. If an operator's cue to initiate a task involves some signal from the equipment or an order from a supervisor, the probability of that signal's being generated or that order's being given must be considered. Many times, these equipment-failure probabilities are not provided by the system analysts or are not considered in the analysis on the basis of assumptions provided by the system analysts. The human-reliability analyst should not assume that the supervisor's order will always be given when it should be unless direct evidence supports such a conclusion.

The task analysis is usually designed and performed to agree with the level, dictated by the system analysts, at which the human-reliability analysis is incorporated into the system analysis. However, the level of incorporation--system event trees, a high (subsystem) level of the system fault trees, a low (component unavailability) level of the system fault trees, or any other level--affects only the format of the HRA results. It has no effect on the actual performance of the human-reliability analysis: all tasks are to be analyzed in the contexts of their performances. It is also of little consequence to the human-reliability analyst whether the information about task performances is considered in part or as a whole in another section of the PRA. The results of his analysis can be parceled for inclusion at the component level in the system fault trees or taken as a whole for inclusion at the subsystem level. The format used in the example can accommodate either.

4.5.5.2 Example

The task analysis for the procedures in Figure 4-3 has been done in two consecutive steps: (1) the tasks performed by the operators in the control room and (2) the tasks performed by an auxiliary operator outside the control room.

The table format used for this example is shown in Figures 4-6 and 4-7. The format used for the task analysis is relatively unimportant; it can be modified to reflect the type and the amount of information needed in later phases of the risk assessment. The step number from the written procedures is included for easy reference to the procedures should any questions arise. The actual items of equipment to be manipulated, read, or otherwise dealt with are listed in the "equipment" column. The "action" column contains

the commands given to the operator; they are usually the action verbs contained in the procedure. In the "indication" column, the analyst notes the cues (usually from visual displays) that inform the operator whether the action has been performed correctly and any restrictions on the operator's actions. In the sample task analyses of Figures 4-6 and 4-7, many of the indications are so obvious (e.g., turn switch to ON position) that no entry has been made. The physical positions of the equipment items are given in the "location" column. The "notes" column contains any information the human-reliability analyst believes will be useful in later parts of the analysis. In Figures 4-6 and 4-7, these columns indicate whether the equipment items of interest in the control room are on the ESF panel and whether locally operated valves are isolated or part of a group. The "errors" column lists the errors deemed likely for each task. They are discussed in detail for each step, beginning with those in Figure 4-6.

In Figure 4-6, dashed lines are drawn between sets of actions that apply to specific plant functions. They help the system analysts to keep track of which portion of the HRA event tree should be excerpted for insertion at the subsystem level of the system fault trees. In this case, step D.2 involves the operator's diagnosis of plant status. This step should be excerpted for inclusion with all others since its correct performance affects the probability of correct performance on the rest of the steps. Once this diagnosis has been made correctly, the operator will move to effect cooldown after verifying that saturation is adequate per step D.4. Step D.7.3 involves isolating the decay-heat pump rooms. Step D.7.4 calls for the operator's verifying the initiation of the decay-heat-removal function. Then, from the water level indicated for the borated-water storage tank (BWST), he must diagnose the need for switching to recirculation. This involves the first part of step D.9 (monitoring the BWST level) and must be excerpted along with any of the other errors from step D.9 (effecting recirculation) for inclusion in the system analysis of the recirculation system.

Step D.2. Monitoring and maintaining RCS pressure and temperature within the curve is considered to be a unit task of three steps: (1) reading the pressure chart, (2) reading the temperature from the digital indicator, and (3) manipulating the heater switches to keep the above values within the acceptable range on the pressure-temperature curve. As such, the probability of an error of omission applies to the entire task: only by forgetting to perform the task itself will the operator forget to perform any element of it. The possible commission errors are those made in reading the pressure from the chart recorder, the temperature from the digital readout, and the curve, which is in the form of a graph. The feedback from manipulating the heater switches incorrectly is almost immediate, and therefore the probability of making a reversal error in their operation is not considered. The pressure chart, the digital indicator, and the heater switches are located on one of the front control boards; a graph of the pressure-temperature curve hangs off the CRT console immediately adjacent. This unit task is performed several times per shift under normal and emergency operating conditions. The heater switches are functionally grouped and well labeled. Under these circumstances, errors of selection were not considered. These steps are considered dynamic in that they involve the continuous monitoring of the displays and the operation of the heater switches.

Step	Equipment	Action	Indication	Location	Notes	Errors	HRA event tree
D.2	RCS pressure	Monitor		CB4		1. Omission (all)	1
						2. Reading	2
	RCS temperature	Monitor		CB4		Reading	3
	heater switches	Maintain pressure and temperature	Within curve on chart	CB4		Reading	4
D.4	4 HPI MOVs	Override and throttle		CP16, CP18	ESF	1. Omission (all)	5
						2. Selection (1)	6
		Initiate cooldown	Procedure 12			Omission	7
D.7.3	CV-7621,22,37,38 (room-purge dampers)	Secure	Close switches	Ventilation room		1. Omission (all)	8
						2. Selection (each)	9,10,11,12
D.7.4	Decay-heat pumps	Verify on	Indicator lamps	CP16, CP18	ESF	1. Omission (for MOVs too)	13
						2. Selection	14
						3. Interpretation	15
	MOV-1400, 1401	Verify open	Indicator lamps	CP16, CP18	ESF	1. Selection	16
						2. Interpretation	17
D.9	Borated-water storage tank	Monitor level	>6 feet	CP14		1. Omission	18
						2. Reading	19
	MOV-1414, 1415	Verify open	Indicator lamps	CP16, CP18	ESF	1. Selection	20
						2. Interpretation	21
	MOV-1405, 1406	Open	MOV switches	CP16, CP18	ESF	1. Selection	22
						2. Reversal	23
	MOV-1407, 1408	Close	MOV switches	CP16, CP18	ESF	1. Selection	24
						2. Reversal	25
	MOV-1616, 1617	Close	MOV switches	CP16, CP18	ESF	1. Selection	26
						2. Reversal	27

Figure 4-6. Task-analysis table for actions by operators assigned to the control room. The column labeled "HRA event tree" does not usually appear in a task analysis; it has been included for the reader's convenience. The numbers in this column refer to the error event numbers in the HRA event trees starting with Figure 4-9.

Step	Equipment	Action	Indication	Location	Notes	Errors	HRA event tree
D.7.1	MU-13	Verify closed	Position	Stairwell outside makeup-pump room	Only valve	Omission	2
D.7.2	DH-7A, 7B	Open	Position	Outside decay-heat pump rooms		Omission (for all D.7.2)	3
	MU-14, 15, 16, and 17	Verify open	Position	Decay-heat pump rooms			
	MU-23, 24, 25, and 26	Verify open	Position	Decay-heat pump rooms			
D.7.3	ABS-13, 14	Close	Position	Outside decay-heat pump rooms	Only valve	Omission (for all D.7.3 here)	4
	Watertight doors	Close	Locks in place	Decay-heat pump rooms			

Figure 4-7. Task-analysis table for actions by auxiliary operator outside the control room. The column labeled "HRA event tree"does not usually appear in a task analysis; it has been included for the reader's convenience. The numbers in this column refer to the error event numbers in the HRA event trees starting with Figure 4-10.

Step D.4. Because their manipulations are called out in the same procedural step and because of their close proximity (see Figure 4-4), the operator views the throttling of the four HPI MOVs as a unit action. Therefore, the probability of an error of omission applies to them all. Because on the actual panel they are delineated with colored tape, a selection error for the group is very unlikely. However, as Figure 4-4 shows, a similar switch is next to the last HPI MOV control in the group. A selection error for that control is likely: instead of MOVs 1, 2, 3, and 4, the operator may throttle MOVs 2, 3, and 4 and the other control. The operators have stated that, in initiating cooldown, they probably would not refer to the other set of procedures. For this reason, an error of omission is assigned to the entire task of performing that other procedure.

Step D.7.3. We have assumed that at this time three licensed operators are available to deal with the accident. One of them is performing the activities shown in Figure 4-7. Of the two operators remaining in the control room, one will have to go two levels above the control room to secure (close the switches) the purge dampers for the decay-heat pump rooms. If he performs this task, he will manipulate four MOV switches. (An error of omission is assigned to the manipulation of all four switches because they are all in the same procedural step.) Because of the poor layout of the ventilation room (no cues are provided as to the location of functional groups), selection errors for each of the four switches are assigned.

Step D.7.4. Verifying that the decay-heat pumps are on and verifying that the LPI MOVs are open are called out in the same procedural step. The equipment items are all located on the ESF panel. An error of omission is assigned for forgetting the task entirely. For the decay-heat pumps, the wrong items of equipment could be chosen or the indications on the correct items could be interpreted incorrectly. For the LPI MOVs, the wrong switches could be selected, or their indications could be interpreted incorrectly. Two errors of commission have been assigned to each item.

Step D.9. Monitoring the level of the borated-water storage tank, a dynamic task, cues the operator to perform the rest of this step. If he fails to monitor or if he monitors incorrectly, the other activities in this step will not be performed. An error of omission is assigned to the monitoring task only. A reading error is also assigned to the monitoring task. For the manipulation of the valves, errors of selection and interpretation or reversal are possible.

The errors assigned for the operations outlined in Figure 4-7 were determined in a slightly different manner. First, consider the fact that the auxiliary operator performs these actions in response to an order from the senior control-room operator. If the senior operator fails to order these tasks, they will not be performed. In developing the HRA event tree for this set of tasks (Section 4.5.6), this probable error will have to be considered. Regarding the rest of these tasks, the auxiliary operator must perform them on three different levels of the plant. He views his job at each level as a unit task; therefore, errors of omission apply to each of these unit tasks. If he remembers to stop at a given level, it is assumed that the operator will attempt all the tasks required at that level. Errors of commission are discussed below.

Step D.7.1. Manual valve MU-13 is the only valve located in the stairwell outside the makeup-pump room. No selection error is possible. It is not deemed likely that the operator will make a reversal error on a manual valve in this situation.

Step D.7.2. Valves DH-7A and 7B are outside the decay-heat pump rooms, one on each end of the hall. They are very large valves, and the only other valves in that area are too small to be confused with them. Of all the valves inside the decay-heat pump rooms, these are the ones that are located high on the walls of the rooms; the only other valves in the rooms are on piping lines that run along the floor. In none of these cases are errors of selection deemed likely.

Step D.7.3. Valves ABS-13 and 14 are located under the grating outside the watertight doors. They are the only valves there; likewise, there is only one set of watertight doors at this location. Again, selection errors are not considered likely.

4.5.6 DEVELOPMENT OF HRA EVENT TREES

4.5.6.1 Discussion

In making a probabilistic statement as to the likelihood of human-error events, each error defined as likely in the task analysis is entered as the right limb in a binary branch of the HRA event tree. Chronologically, in the order of their potential occurrence, these binary branches form the limbs of the HRA event tree, with the first potential error starting from the highest point on the tree at the top of the page. An example of an HRA event tree is shown in Figure 4-8.

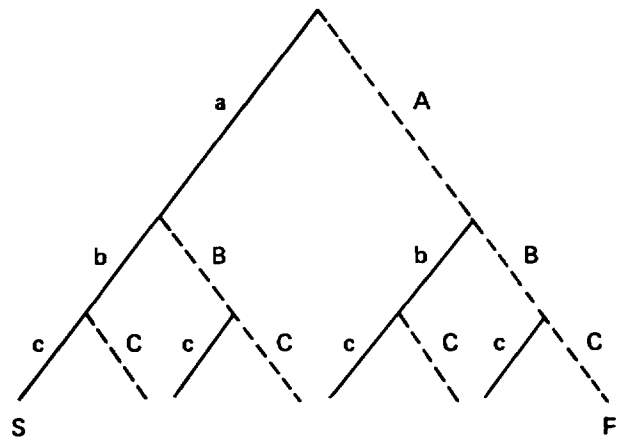


Figure 4-8. An example of HRA event-tree diagramming. Here A, B, and C are the first, second, and third tasks that are performed. Solid lines represent success; broken lines, error.

Any given task appears as a two-limb branch, with each left limb representing the probability of success and each right limb representing the probability of failure. (In a later phase of the human-reliability analysis, the human-error probabilities from the Handbook will be entered into the tree. See Section 4.5.7.) Once a task is diagrammed as having been completed successfully (or unsuccessfully), another task is considered; the binary branch describing the probability of the success (or the failure) of the second event extends from the left (or the right) limb of the first branch. Thus, every limb following the initial branching depicts a conditional probability. The initial branching also represents a conditional probability in that the probabilities for that branch are based on the existence of a given situation. However, it is defined as the starting point for the analysis, not as a conditional probability, since the analysis does not investigate the probabilities of occurrence of the circumstances of the basic situation. (As described in Chapter 5 of the Handbook, the conditional probabilities are understood in the labeling scheme shown in Figure 4-8; for example, a limb labeled b actually means b|a.)

Each limb of the HRA event tree is described or labeled, usually in a form of shorthand. Capital letters in quotation marks ("A") represent certain tasks themselves. Capital letters (A) represent failure or the probability of failure on given tasks. Lowercase letters (a) represent success or the probability of success on certain tasks. The same convention applies to Greek letters, which represent non-human-error events, such as equipment failures. The letters S and F are exceptions to this rule, in that they represent system success and failure, respectively. In actual practice, the limbs are sometimes labeled with a short description of the error itself. This eliminates the need for a legend at the bottom of the page that defines the alphabetic code for each event. The labeling format that is used is unimportant: the critical task in developing HRA event trees is the definition of the events themselves and their translation onto the trees. (Examples of labeling formats are shown in Figures 4-9 and 4-10.)

All the limbs of an HRA event tree are heavy solid lines in the diagram. For illustration only, the limbs representing failure in Figure 4-8 are shown as broken lines. (See Chapter 5 of the Handbook for a more complete discussion of the basics of HRA-event-tree diagramming.)

In a probabilistic risk assessment, the analyst is usually interested in determining the probability of error on a single task or the probability that, for a set of tasks, none or all will be performed incorrectly. For the first case, no HRA event tree need be developed unless performance on that task is affected by other factors whose probabilities should be diagrammed. A description of the task and knowledge of the performance-shaping factors are sufficient for entering Chapter 20 of the Handbook to determine the probability of a single human error.

For the second case, in which we want to know the probability of all tasks being performed without error, a complete-success path through the HRA event tree is followed (as discussed in Chapter 7 of the Handbook). Once an error has been made on any task, a criterion for system failure has been met. Given such a failure, no further analysis along that limb is necessary at

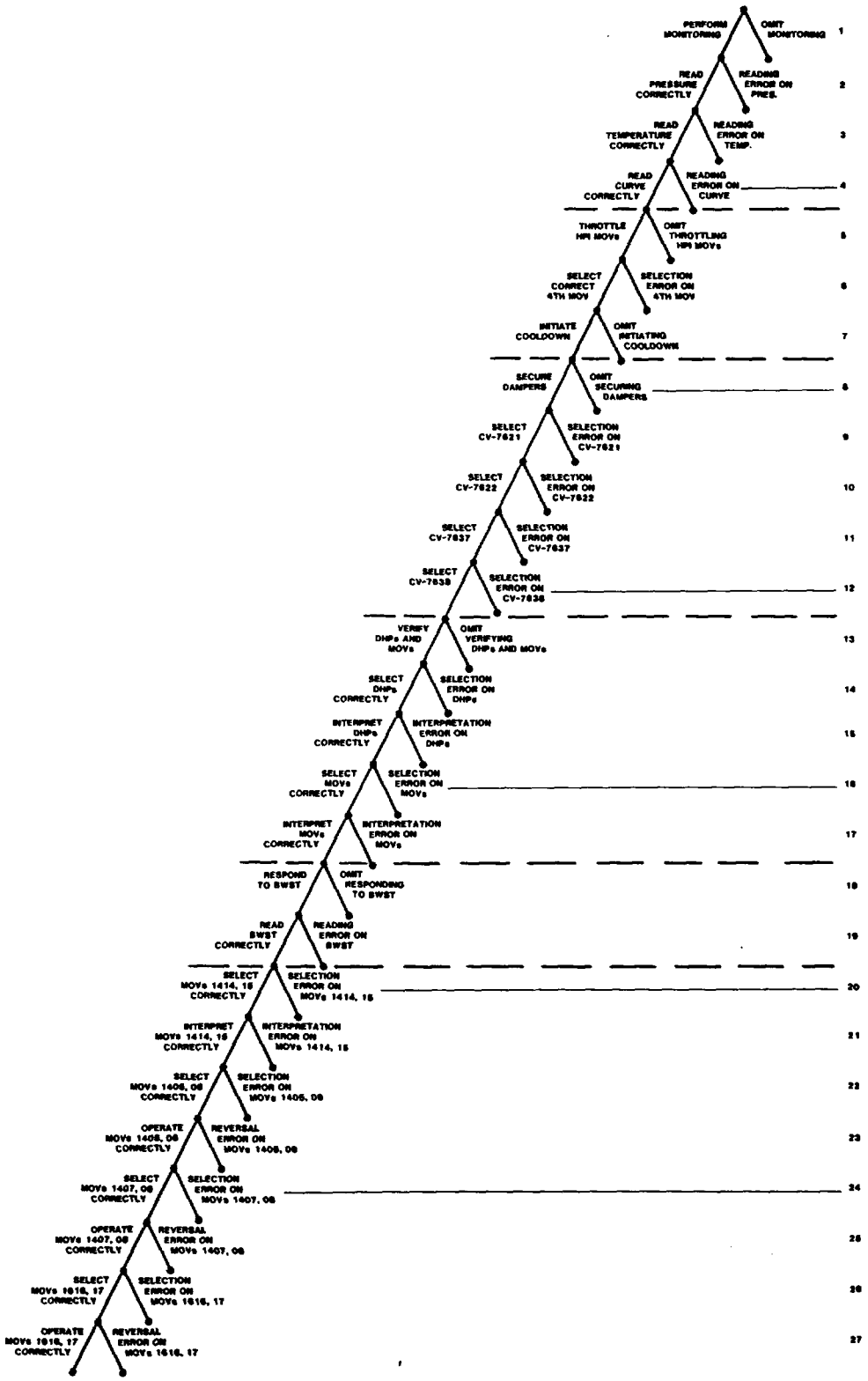
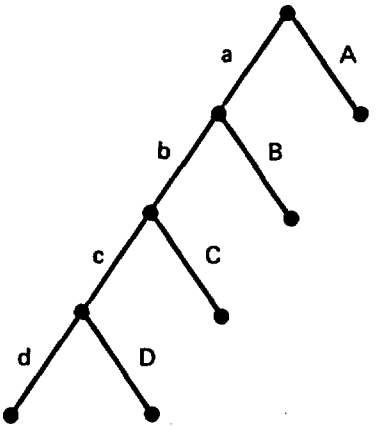


Figure 4-9. HRA event tree for actions by operators assigned to the control room.



Event

A = Control-room operator omits ordering the following tasks

B = Operator omits verifying the position of MU-13

C = Operator omits verifying/opening the DH valves

D = Operator omits isolating the DH pump rooms

Figure 4-10. HRA event tree for actions performed outside the control room.

this point. In effect, the probabilities of event success that follow a failure and still end in a system-success probability constitute recovery factors and should be analyzed later, if at all. Thus, as shown in Figures 4-9 and 4-10, there are HRA event trees that are developed along the complete-success path only. This does not mean that we think this is the only possible combination of events; it means only that, in the initial analysis, we go no further once a system-failure criterion has been met.

The development of the HRA event tree is the most critical part of the quantification of human-error probabilities. If the task analysis has listed the possible human-error events in the order of their potential occurrence, the transfer of this information onto the HRA event tree is much easier. Each potential error and success is represented as a binary branch on the HRA event tree, with subsequent errors and successes following directly from the immediately preceding ones. Care should be taken not to omit the errors that are not included in the task-analysis table but might affect the probabilities listed in the table. For example, administrative-control errors that affect a task's being performed may not appear in the task-analysis table but must be included in the HRA event tree.

4.5.6.2 Example

The HRA event trees shown in Figures 4-9 and 4-10 represent the task analyses shown in Figures 4-6 and 4-7, respectively. Figure 4-9 (HRA event tree for actions by operators assigned to the control room) uses a labeling format that incorporates a short description of each event for its corresponding limb. Such a format is very convenient for analyses in which large numbers of events are diagrammed; referring back and forth to a descriptive legend would be inconvenient. The lines in Figure 4-9 are placed according to those found in the corresponding task-analysis table (Figure 4-6). Again, they are included to aid the system analyst in extracting information from the HRA event tree for inclusion in the system analysis. Figure 4-10 (HRA event tree for actions performed outside the control room) demonstrates that a format consisting of alphabetic labels and a descriptive legend can be used very effectively when a small number of events are involved. The legend format has the advantage of allowing a more complete description of the error events than does the short-label format. As already stated, however, the actual labeling format is of little importance as long as it is helpful to the analyst. Combinations of these two styles can be used, or entirely new formats can be developed by the analyst.

Both of the HRA event trees shown here reflect the technique described above and in Chapters 4 and 5 of the Handbook. The possible errors listed in the respective task-analysis tables have been put directly onto the right limbs of the branches. Only the complete-success paths are shown, as previously explained. The first branch of Figure 4-10 represents the administrative control error identified in the discussion of that set of tasks. In the HRA event tree itself, no distinction is made between the error events that appeared in the task-analysis table and those that were identified during other parts of the analysis.

4.5.7 ASSIGNMENT OF NOMINAL HUMAN-ERROR PROBABILITIES

4.5.7.1 Discussion

When the human errors have been identified, defined, and diagrammed, the analyst must estimate the probability of occurrence for each error. Since the analyst should be familiar with the theories, models, and limitations presented in the Handbook, he will be able to use Chapter 20 of that document for most of these estimates.

First, the task itself must be categorized. The analyst determines whether he is dealing with an operator manipulating valves, checking another's work, using a written procedure, or attempting some other type of task. Errors are then considered on the basis of their being of the omission or the commission type. In the tables in Chapter 20 of the Handbook, human-error probabilities (HEPs) are grouped by the type of error (omission or commission) that may occur in the performance of a certain type of task.

The analyst should become familiar with the organization of the HEPs in Chapter 20 of the Handbook. Some of the tabular data are duplicates of data presented in the subject chapters of the Handbook; others are condensations

of data found in several chapters. An analyst who becomes familiar with the organization of Chapter 20 before trying to use it as a source document will save a considerable amount of time. Furthermore, he will be able to establish beforehand the cases in which he will need to estimate HEPs directly from the task analysis because no such task is described in Chapter 20.

A description of each error identified for every task in the task analysis should be looked up in Chapter 20; that is, the description that most closely approximates the situation under consideration should be identified. In some cases, the description in Chapter 20 will detail a scenario that differs slightly from the one in the analysis. If the differences in specifics are not great, the analyst may decide that they are too minor to affect materially the use of the HEP as is. In other cases, the actual situation and the one described in Chapter 20 may reflect tasks that are basically the same but are performed under different circumstances. The HEP must then be modified to reflect the conditions of actual performance. Usually, this is done during the assessment of the performance-shaping factors acting on the task (Section 4.5.8).

If an HEP entered into the HRA event tree was not obtained from the Handbook, its source should be recorded, along with the assumptions made in its derivation. If Chapter 20 is the source of the HEP, the table number and item number should be recorded. If an HEP from the Handbook was used as a reference point for the derivation of an estimated HEP, its specific source and the reasoning behind its modification should be noted. For easy reference, this information can be added to the task-analysis tables in new columns. This documentation is necessary for many reasons. Other analysts may want to check the similarity of their solutions to other problems. Given that the estimates of many of the HEPs in the Handbook are numerically identical, these other analysts must have some method for tracing the original analysis. The assumptions should be recorded to prevent the analyst's needing to reinvestigate a situation should he need to refer to that analysis again. Also, in the course of performing a series of analyses on a single plant, some sections of an analysis may be used several times. The analyst must, however, be able to demonstrate that the situations are indeed identical before reproducing part of one analysis without modification in another.

In the HRA event tree of Figure 4-11 and in subsequent discussions and figures, results are shown to several decimal places merely to illustrate the arithmetic. In practice, final answers are subjected to judicious rounding.

As mentioned in Section 4.1.3, one of the limitations of the HEPs tabled in the Handbook is that nearly all of them apply to rule-based human actions. For cognitive errors related to the evaluation of display indications, the following interim guideline that should be used as a supplement to the 1980 issue of the Handbook is suggested: A generic estimate of .1 (.01 to .5) per operator should be used for the failure to evaluate an accident properly unless there is plant-specific information to the contrary--unless there is evidence that such errors are not likely to be characterized by an HEP of .1. (In applying this rule, appropriate estimates of the levels of dependence must be made to account for the presence of more than one operator in the control room.) It will be a matter of judgment as to whether modification of the generic HEP of .1 is necessary. For some kinds of abnormal conditions, there are

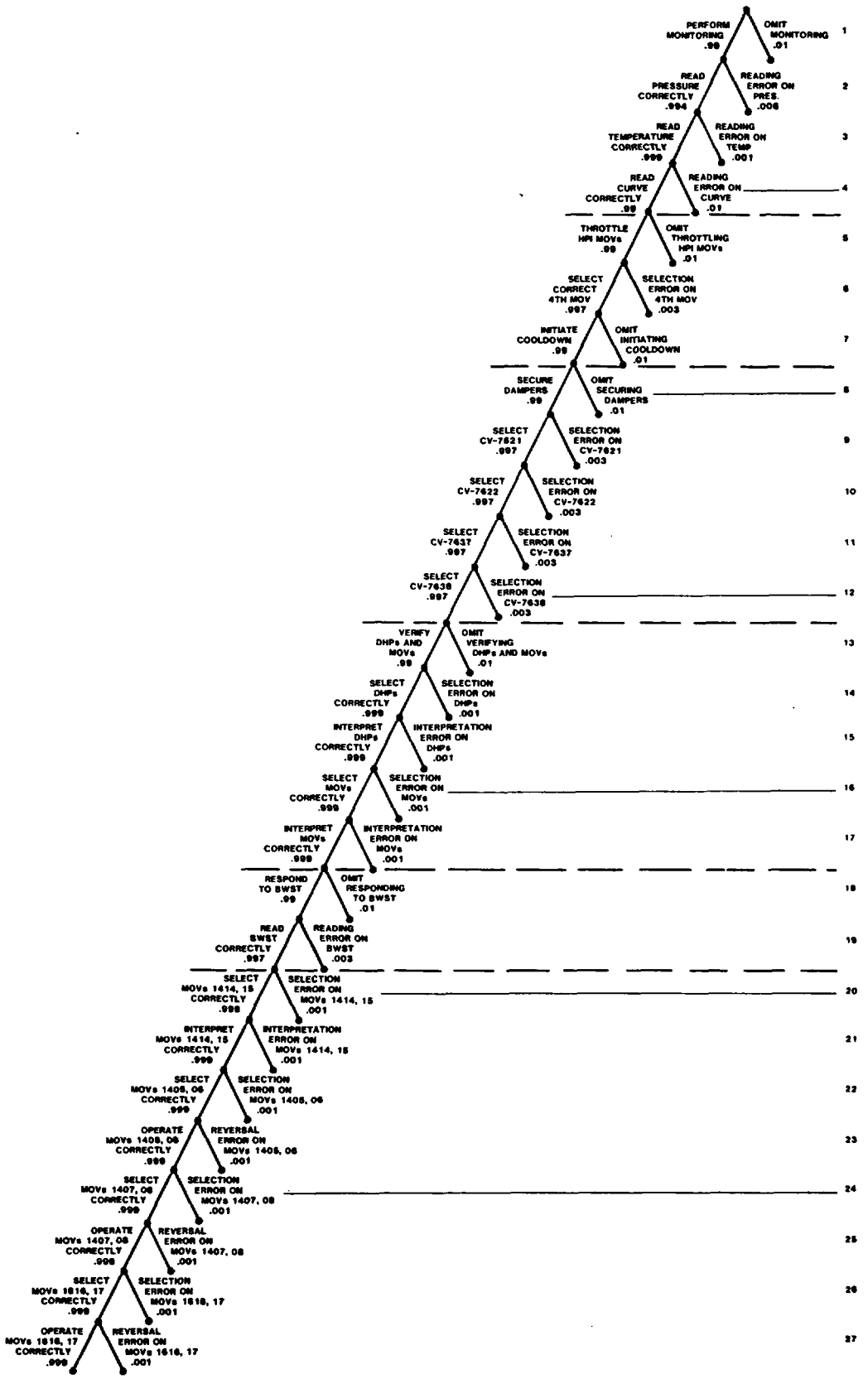


Figure 4–11. HRA event tree for actions by operators assigned to the control room, with estimates of nominal human-error probabilities.

plant-specific operating rules that, if rehearsed properly, will effectively eliminate any initial indecision on the part of the operator when an accident occurs.* In such a case, the main effort of the human-reliability analyst will be to estimate the effectiveness of the provisions for in-plant rehearsal of these operating rules. This type of treatment reflects the state of the art in human-reliability analysis and points to the need for studies of the type mentioned earlier in Section 4.1.3. (See also Section 4.9, "Alternative Methods," for discussions of other approaches to estimating the likelihood of such errors in the cognitive process.)

4.5.7.2 Example

In studying this example, it is necessary to keep in mind the situational characteristics that affect the performance of the tasks in question: the actions of operators who are following a set of written procedures. Any errors are made in the context of using those procedures. Recovery factors are not to be considered at this time. Even though there will be three licensed operators in the control room, this first analysis considers only the actions of one operator.

In the first part of this example, each error and the source of its estimated HEP are discussed in detail. Later in the example, only the source HEPs are given for errors that have already been discussed. Figures 4-11 and 4-12 are the HRA event trees diagrammed in Figures 4-9 and 4-10, but they include the HEP estimates for each error. As shown, this can be done by adding the HEP as part of the label for each limb or by including the HEPs in the legend for the HRA event tree. Again, the method employed for displaying the HEPs on the HRA event tree is unimportant.

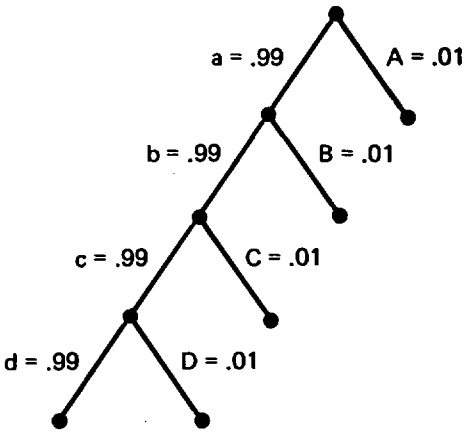
The first error† on the HRA event tree is the operator's failure to perform the monitoring of RCS pressure and temperature. This is the first part of step D.2. If the operator fails to do this part of step D.2, it is presumed that he will fail to carry out the remainder of the step. The failure to maintain RCS temperature and pressure was designated a system failure by the system analysts. Since we are dealing with the operator's following a set of written procedures, we use an estimate of the error from Table 20-20 in the Handbook.‡ This table presents estimates of errors of omission made by operators using written procedures. In other words, these estimates reflect the probability, under the conditions stated, of an

---

*For an example, see the case study described on pages 21-11ff in the Handbook.

†References to error numbers correspond to the numbered events in all related HRA event trees and to like-numbered entries in the task analysis.

‡All cited table and item numbers are from the October 1980 draft of the Handbook.



Event	HEP	Source
A = Control-room operator omits ordering the following tasks	.01 (.005 to .05)	Table 20-22, item 1 (p. 20-31)
B = Operator omits verifying the position of MU-13	.01 (.005 to .05)	Table 20-18, item 3 (p. 20-28)
C = Operator omits verifying/opening the DH valves	.01 (.005 to .05)	Table 20-18, item 3 (p. 20-28)
D = Operator omits isolating the DH pump rooms	.01 (.005 to .05)	Table 20-18, item 3 (p. 20-28)

Figure 4-12. HRA event tree for actions performed outside the control room, with estimates of nominal human-error probabilities.

operator's omitting any one item from a set of written procedures. Since the procedures in this example are emergency procedures that do not require any checkoff of steps by the operator, we use the section of Table 20-20 that deals with procedures having no checkoff provision. Looking at the procedures in Figure 4-3, we see that more than 10 steps must be performed by the operator. This analysis deals with fewer than 10 procedural steps, but the steps must be considered in the context of their performance. The fact that only a few steps are analyzed has no effect on the operator as he follows the set of procedures. Given that this error occurs in using a long list of written procedures that does not require a checkoff, its estimated HEP is .01 (.005 to .05), as given in item 5 of Table 20-20. At this point in the analysis, the nominal value of the HEP is entered into the HRA event tree.

The second error shown in Figure 4-11 is the operator's error in reading the indicator for RCS pressure. This indicator is a chart recorder. Reading errors are errors of commission and are grouped in Chapter 20 according to the type of information that is displayed and to the type of indicator that makes up the display. In this instance, the operator is reading a numerical value from the chart recorder. Table 20-5 presents estimated HEPs for errors made in reading quantitative information from different types of display.

For the chart recorder in question, item 3 from that table is used, .006 (.002 to .02).

The third error also involves reading an exact value from a display. In this case the display is a digital readout; therefore, item 2 from Table 20-5 is used, .001 (.0005 to .005).

The fourth error is also a reading error, this time involving the pressure-temperature curve. Since the curve is presented as a graph, the HEP for errors made in reading quantitative information from a graph is used, item 5 from Table 20-5, .01 (.005 to .05).

Another error of omission appears as the fifth error limb on the HRA event tree in Figure 4-11: the operator's not throttling the HPI MOVs. For errors of omission, the nature of the task does not affect the probability of the error. Therefore, the same HEP that was used for the first error, .01 (.005 to .05), is used again here.

A switch-selection error for the fourth of the HPI MOVs was identified as likely in the task analysis. It is the sixth of the errors on the HRA event tree. Figure 4-4, which shows the layout of the control panels containing the switches for the HPI MOVs, demonstrates that the HPI MOV switches are in similar positions on control panels CP16 and CP18. Surrounding them are several similar switches, one of which (to the immediate right of the switches for HPI MOVs on CP18) is the switch most likely to be the target of the selection error. An estimate of this error of commission is found by looking in the tables in Chapter 20 that deal with errors made in the manipulation of valves. Table 20-14 contains HEPs for errors of commission in changing or restoring valves. Since item 7 most closely approximates the situation described here, the HEP of .003 (.001 to .01) is used as the estimate for this error.

The seventh error involves an omission on the part of the operator to initiate cooldown by following another set of written procedures. As far as we are concerned here, this is a case of his omitting a single step of this procedure, so .01 (.005 to .05) is used again. It is also used for the eighth error, that of omitting to secure the purge dampers for the decay-heat pump rooms.

The 9th, 10th, 11th, and 12th errors are selection errors involving the manipulation of the switches for four MOVs. The switches are probably close to each other on a wall of the ventilation room, but we have no specific information about the ease or difficulty of locating the group. Since it is not known whether the layout and the labeling of the switches in the ventilation room help or hinder the operator in his search for the controls, we take the conservative position of assuming them to be among similar-appearing items. We use the same HEP as that used for the selection error associated with the fourth HPI MOV (error 6), .003 (.001 to .01), for each of these MOVs.

The 13th error is one of omitting a procedural step. The HEP of .01 (.005 to .05), discussed earlier, was used. If this procedural step is performed (is not omitted), errors of selection for both types of components

mentioned (the decay-heat-removal pumps and the LPI MOVs) are possible. These selection errors appear as the 14th and the 16th errors on the HRA event tree. We know from Figure 4-4 that both of these sets of controls are part of groups that have been arranged functionally on the control panels. They are very well delineated and can be identified more easily than can most of the switches in the control room. Since there is no entry in Table 20-14 (commission errors in changing or restoring valves) that accurately reflects this situation, an HEP from Table 20-13 is used. This table consists of HEPs for commission errors in manipulating manual controls (e.g., the hand switch for an MOV). Item 2 in this table involves a selection error in choosing a control from a functionally grouped set of controls; its HEP is .001 (.0005 to .005). (Note: On page 20-19 of the Handbook, please insert the words "locally operated" before the word "valves" in the second sentence. It is intended that the estimated HEPs in this table apply to switches of all kinds, including the control-room switches used to operate MOVs.)

Errors of interpretation are also possible for the decay-heat pumps and the LPI MOVs. Given that the operator has located the correct switches, there is a possibility that he might fail to notice their being in an incorrect state. In effect, this constitutes a reading error, one made in "reading" (or checking) the state of an indicator lamp. No quantitative information is involved, so Table 20-7, which deals with commission errors in checkreading displays, is used. The last item on that page describes an error of interpretation made on an indicator lamp, so .001 (.0005 to .005) is used. The 15th and 17th errors on the HRA event tree represent these interpretation errors.

The HRA event tree's 18th error is defined as the operator's omitting to respond to the level of the borated-water storage tank. The same omission HEP used previously, .01 (.005 to .05), is repeated here. Given no such omission error, a reading error (19 on the event tree) could be made on the BWST meter. Going back to Table 20-5 for commission errors made in reading quantitative information, the HEP to use in considering an analog meter is .003 (.001 to .01), the first term in the table.

Errors 20, 22, 24, and 26 involve selecting the wrong set of MOV switches from sets of functionally grouped switches. As above, this HEP is from item 2 of Table 20-13, .001 (.0005 to .005).

The 21st error (interpretation) is made while checking the status of an indicator lamp. An HEP of .001 (.0005 to .005) (as cited for the 15th error above) is assigned.

The 23rd, 25th, and 27th errors represent reversals made by the operator: instead of opening valves, he closes them, or vice versa. Since errors of commission for valve-switch manipulations are involved, Table 20-13 is used. Item 7 most closely describes this error; hence, the HEP of .001 (.0001 to .01) is used.

For the HRA event tree in Figure 4-12, we are analyzing actions performed outside the control room. The first error diagrammed is one of administrative

control and did not show up in the task analysis: the control-room operator omits ordering another operator to perform this set of tasks. Since the ordering of the tasks is his responsibility, this constitutes a failure to carry out plant policy. An HEP of .01 (.005 to .05) from Table 20-22, item 1, is used.

The second, third, and fourth errors shown in Figure 4-12 are errors of omission by the operator who actually performs the tasks. These tasks call for the manipulation of valves located on levels of the plant under the control room. We assumed that the operator will not be working from a set of written procedures (he will not take a copy of the procedures with him) but from an oral instruction by the control-room operator. The model accounting for errors of omission made in following a set of oral instructions will be followed. The data for this model are found in Table 20-18. It was stated in the discussion of the talk-through (Section 4.5.4) that the operator sees these as three distinct unit tasks, one to be performed on each of the three levels he must visit. We therefore assume that he must recall three tasks and use item 3 in the table, which shows an HEP of .01 (.005 to .05) for each of the tasks.

4.5.8 ESTIMATING THE RELATIVE EFFECTS OF PERFORMANCE-SHAPING FACTORS

4.5.8.1 Discussion

A primary consideration in conducting a human-reliability analysis is the variability of human performance. This variability is exhibited by any given individual in the performance of tasks over time (from day to day, from week to week, etc.). Variability also results from the performances of different personnel (from man to man, shift to shift, or from plant to plant). Variability is caused by performance-shaping factors (PSFs) acting within the individual or on the environment in which the task is performed. Because of this variability, the reliability of human performance usually is not predicted solely as a point estimate but is determined to lie within a range of uncertainty. A point value HEP for the PRA can be estimated by considering the effects of relevant PSFs for the task in question. The estimates provided so far in this chapter apply to nonstressful, normal working conditions. Modifications of these basic estimates can be made on the basis of guidelines provided in the Handbook.

The nominal HEPs are to be used when the scenario outlined in the Handbook reflects the situation being analyzed. If the plant situation is worse in terms of the PSFs or the response requirements than the one described in the Handbook, the HEP for that task should be higher than the nominal value. That is, if the analyst judges that the situation under study is more likely to result in error than the one outlined in the Handbook, he should use an HEP that is closer to the upper bound than the nominal is. Likewise, if a plant's situation is judged to be less likely to result in a human error, the analyst should use an HEP that is closer to the lower bound than the nominal is. However, in a safety analysis, one should generally avoid the optimism that results from using a lower HEP.

In judging these effects, the analyst should first consider the error events individually. For each error probability, a judgment must be made as to whether the nominal HEP should be used. The analyst should examine the performance situation for the factors that might affect each event. For errors of omission, for example, the analyst should search for cues or reminders that would make forgetting any item less likely or for poorly written procedures that would make forgetting an item more likely. For errors of commission, it is necessary to identify the elements of the performance situation that might affect the actions themselves or the operator as he performs them. For example, if the face of a display is such that reading it is unusually difficult, an HEP higher than the nominal value for reading errors for such a display should be assigned.

Next, the analyst should consider the influence of PSFs that have a global effect--those that affect the probability of error for all or most of the events in the analysis. Some models presented in the Handbook reflect the influences of these overriding PSFs. The most commonly encountered ones deal with stress and the operator's level of experience.

The data in the Handbook reflect by their organization the effects of some PSFs. For example, for errors of omission in using a written procedure, the distinction based on the availability of a checkoff provision is really based on the quality of the procedure as a PSF. Whether an available checklist is used properly is an example of the PSF of administrative control. Reading errors for displays are related to the difficulty of the reading task. In these cases, the effects (to some extent) of the PSFs have been already determined for the analyst.

4.5.8.2 Example

For evaluating the effects of PSFs on the individual error events, in each case the scenario described in the Handbook is appropriate for the imaginary plant of these examples, and therefore no modification of the nominal HEPs is necessary.

Now we must consider the effects of overriding PSFs--those that will affect all of the HEPs. It was stated in the original assumptions that the operators are experienced. Since they are following an emergency procedure, we will consider them to be under a moderately high level of stress. We see from Table 20-23 that the HEPs for experienced personnel operating under a moderately high level of stress should be doubled for discrete tasks and multiplied by 5 for dynamic tasks. Discrete tasks are defined as the tasks that require essentially one well-defined action by the operator. Dynamic tasks are those requiring a series of connected (continuous) subtasks; an example is monitoring an indicator over a period of time.

Figure 4-13 shows the HRA event tree for control-room actions with the nominal HEPs of Figure 4-11 modified to reflect the effects of a moderately high stress level. The only dynamic tasks in Figure 4-13 are those calling for monitoring activities: the monitoring of the RCS temperature and pressure indicators (tasks 2 and 3) and the interpolation of these values onto the

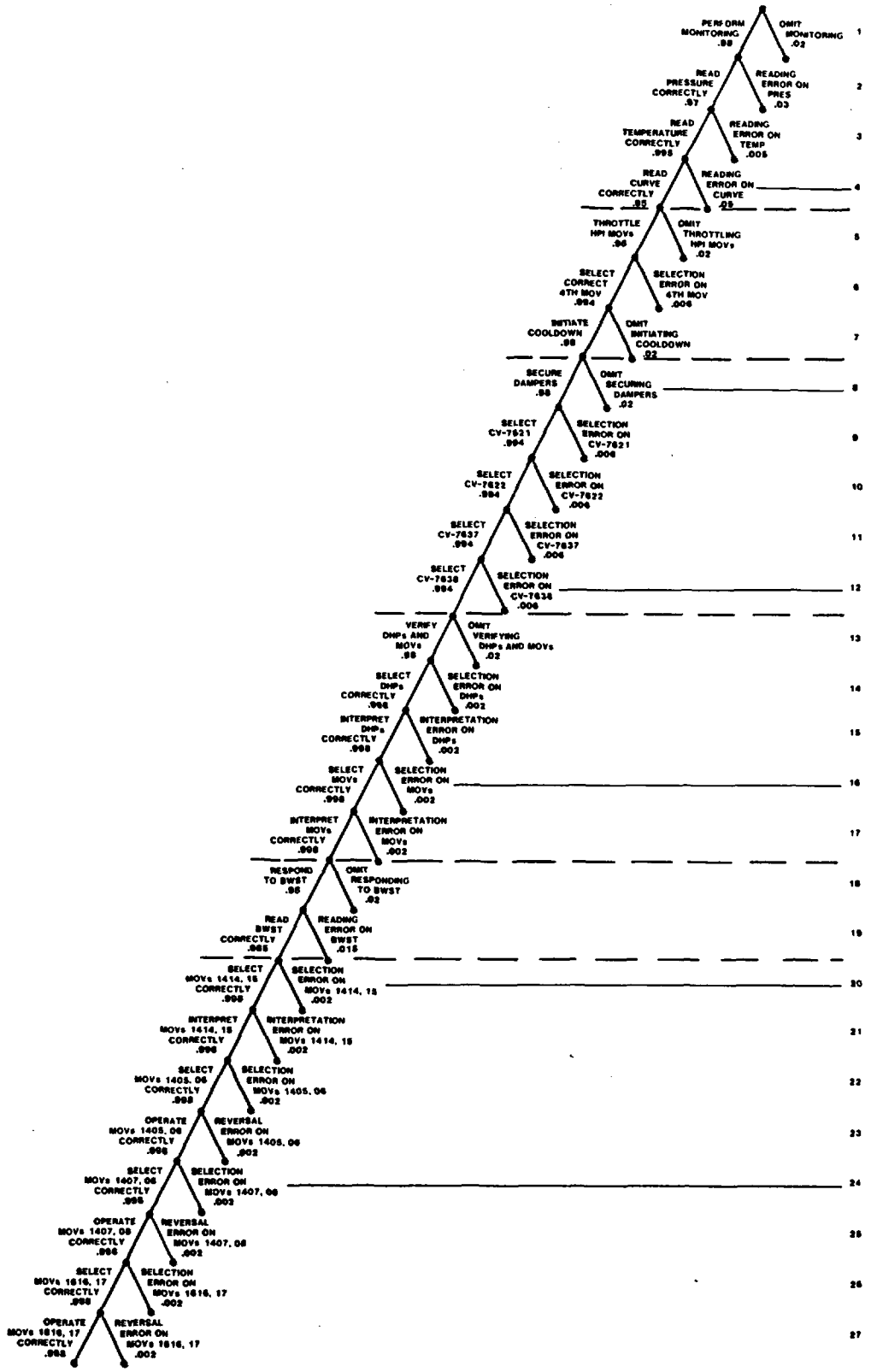
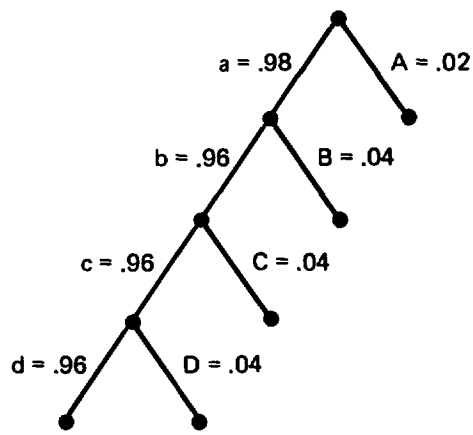


Figure 4-13. HRA event tree for actions performed by operators assigned to the control room, with human-error probabilities modified to reflect performance-shaping factors.

cooldown curve (task 4) and the monitoring of the BWST level (task 19). The nominal HEPs for these tasks have been multiplied by 5; those for the other events in this figure have been doubled.

Another overriding PSF that must be considered, this time for the tasks performed outside the control room, is the effect of the operator's having to wear protective clothing. If protective clothing is necessary, we assume that the operator is highly motivated to complete the task quickly because of the heat in the working environment, his isolation, and the general discomfort caused by the protective clothing. These factors combine to increase the HEPs for tasks performed by operators wearing such clothing. This is discussed on pages 3-8 and 17-7 of the Handbook. On the latter page, it is stated that the HEPs for such tasks should be doubled.

Figure 4-14 shows the events taking place outside the control room, with their HEPs modified to reflect these PSFs. The first error (failure of administrative control) takes place in the control room. The HEPs for this and for the other events have been doubled to reflect the effects of the moderately high stress level. The HEPs for the three tasks that actually take place outside the control room have been doubled again to reflect the effects of the operator's wearing protective clothing.



Event	HEP	Source
A = Control-room operator omits ordering the following tasks	.02 (.01 to .1)	Table 20-22, item 1 (p. 20-31)
B = Operator omits verifying the position of MU-13	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)
C = Operator omits verifying/opening the DH valves	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)
D = Operator omits isolating the DH pump rooms	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)

Figure 4-14. HRA event tree for actions performed outside the control room, with human-error probabilities modified to reflect PSFs. The HEP for event A has been modified to reflect the effects of moderately high stress and dependence; the HEPs for events B, C, and D have been modified to reflect the effects of moderately high stress and protective clothing.

4.5.9 ASSESSMENT OF DEPENDENCE

4.5.9.1 Discussion

It has been stated earlier that, except for the first branch of an HRA event tree, all branches represent conditional probabilities of success and failure. Dependence between events directly affects these conditional probabilities. Some cases of dependence will be spotted during the talk-through, which is a good time to make note of equipment similarities that contribute to the level of dependence between actions performed on like items.

Dependence can occur between two performances with respect to errors of omission, errors of commission, or both. If dependence is assessed because two actions are called for in the same procedural step, dependence is likely to affect HEPs for errors of omission. If components are to be manipulated at different times in a given procedure, the dependence is likely to affect the HEPs for errors of commission, especially for selection errors. Common-cause dependence is likely to affect the HEPs for all types of errors. In effect, the overriding PSFs discussed in the preceding section are sources of common-cause dependence in that they result in modifications to all HEPs.

Guidelines for assigning the level of dependence are found in the dependence chapter of the Handbook. There are no cut-and-dried rules for this kind of assessment, but it must be made only after a carefully detailed study of the performance situation since it is highly situation-specific. The dependence level should be assessed for every task performed in every procedure targeted for human-reliability analysis. This is necessary because dependence may exist between one task considered during the analysis and one that is not. Given the performance context of each analysis, the effects of such dependence must still be quantified.

A decision as to whether complete dependence or complete independence applies to a given case can be made relatively easily. That is, it should be obvious that one action is the causal factor for another or that two actions are totally unrelated. Distinctions between the three intermediate levels of dependence are more difficult to make. First, we must decide whether there is any dependence at all--whether the actions are completely independent. If dependence does exist, we must decide whether complete dependence is appropriate and, if so, under what circumstances it applies. If we decide that the dependence is greater than zero but less than complete, an intermediate level must be assigned. This judgment can be based on the relation of the actual situation to zero and complete dependence. If we decide that the dependence is much closer to zero than to complete dependence, a low level of dependence is assigned. If, on the other hand, we decide that the situation exhibits a degree of dependence that is very close, but not equal, to complete dependence, a high level of dependence is assigned. If we cannot make a definitive statement to the effect that either of the above is true, moderate level of dependence is to be assigned.

Another method of assigning an intermediate level of dependence is to make a precise estimate as to the percentage of time the effects of zero or complete dependence will be seen. That estimate is used to assign the intermediate dependence level that most closely approximates it. For example, if we make a judgment (perhaps on the basis of a frequency count from actual

data or from our knowledge of the work situation) that task B will be performed correctly half of the time, given that task A has already been performed correctly, we have assigned a conditional probability of b|a = .5.

It should be remembered that the dependence model in the Handbook deals only with the effects and the quantification of positive dependence. If negative dependence is found to be appropriate to a situation, its effects will have to be determined directly rather than by using the dependence model. Furthermore, dependence is not necessarily symmetrical. The level of dependence may not be the same for the success and the failure paths of an HRA event tree.

The model presents some point estimates that can be used in lieu of the exact equations to determine the conditional probabilities of dependent events. These point estimates should be used only when the basic human-error probability (BHEP) is less than or equal to .01. In other cases, the equations should be used.

4.5.9.2 Example

In the sample problem, several cases of dependence have already been accounted for. For example, in the case of the four HPI MOV switches, their physical similarity, their positions in the procedure, and their location in relatively identical positions on the control panel led to our assumption that, for errors of omission, they are completely dependent. In considering dependence for the selection errors that could be made on these MOV switches, the same factors plus the layout of the rest of this control board led us to decide that the first three are completely dependent for selection errors (none are considered likely), and the fourth is susceptible to such an error. The nature of the tasks performed outside the control room and the operator's perception of them (from interviews with plant operators we determined that the operator typically views each set of tasks performed on a plant level as a single unit task) led to our considering them to be completely dependent with respect to errors of omission.

The presence of more than one operator in a given location constitutes a recovery factor. If we determine the effects of having more than one operator in the control room during the performance of this procedure, we are in fact quantifying a recovery factor for the procedure. However, since we will show that there is some level of dependence among the operators in the control room, we will quantify these effects now as an illustration of dependence.

According to Chapter 17 of the Handbook, one can assume that, after 20 minutes into an incident, three operators are present in the control room, with a moderate to high level of dependence between the two senior operators present and a high to complete level of dependence between the most junior operator and each of the two others. We have modified these assumptions to reflect the actual situation.

Since this procedure calls for the performance of several tasks outside the control room and since these tasks require the wearing of protective

clothing, we assume that one of the three operators will leave the control room during the entire procedure to prepare for and then perform these tasks. We assume that this will be the most junior operator in the control room since the other two are more capable of handling the incident from the control room. Responding to the nature of the control-room tasks, we assumed high dependence between the operators there. This assumption is based on the fact that, at this time in the incident, one of the operators will be involved mainly in directing the actions of the junior operator as he changes the positions of locally operated valves. Telephone communication between the two will call for most of this operator's concentration as he describes the necessary operations. The other control-room operator will be involved with monitoring the displays and performing the manipulations necessary at the ESF panels. High dependence is assumed because we judge that the operator on the telephone will, for the most part, rely on the operator at the ESF panels to perform those tasks correctly. Nevertheless, we judge that despite his primary task of coordinating the junior operator's tasks by telephone, this operator will catch errors made by the other control-room operator about half the time.

Figure 4-15 shows the HRA event tree of the actions performed by the control-room operators, with the HEPs (already modified to reflect the effects of performance-shaping factors) modified to reflect the effects of dependence. The probabilities of error for both the available operators have been collapsed onto a single limb for each type of error. The numbers in parentheses (shown for illustration only) are the conditional HEPs for the second operator's making the same error as the first. The other numbers are the products of these conditional HEPs and the basic HEPs of the first operators, and thus they represent the probability of both operators committing each error. The actions taking place in the ventilation room do not demonstrate any dependence between operators since we assume that one operator will be performing them. The only event in Figure 4-16 that is affected by dependence is the first. If the senior control-room operator forgets to order those tasks, the other senior operator or the junior operator himself may remind him of the necessity to do this.

4.5.10 DETERMINATION OF SUCCESS AND FAILURE PROBABILITIES

4.5.10.1 Discussion

Once the human-error events have been identified and quantified individually, their contribution to the probabilities of system success and failure must be determined. All paths in an HRA event tree should be defined as resulting in system success or failure in terms of their possible system consequences, not in terms of the specific human errors leading to these consequences. The system analysts will have identified the human-system interfaces to be analyzed in the human-reliability analysis, but errors made in operating at these interfaces may not significantly degrade system reliability or safety. For example, an error made in manipulating a system-critical component may not result in system failure as defined by the system analysts. The human-reliability analyst must point out potential human errors for a given set of tasks and then must quantify the probability of these errors; he does not,

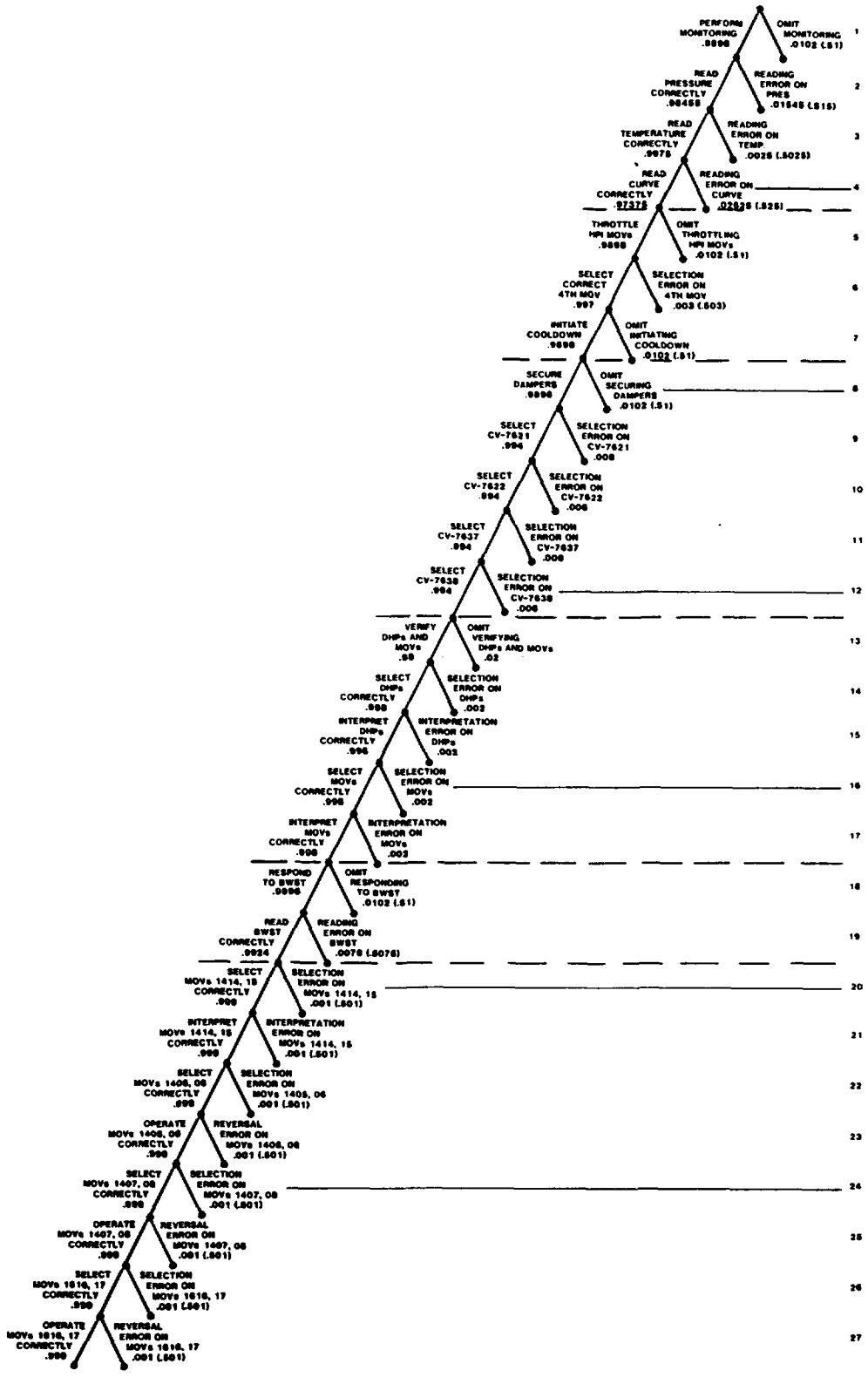
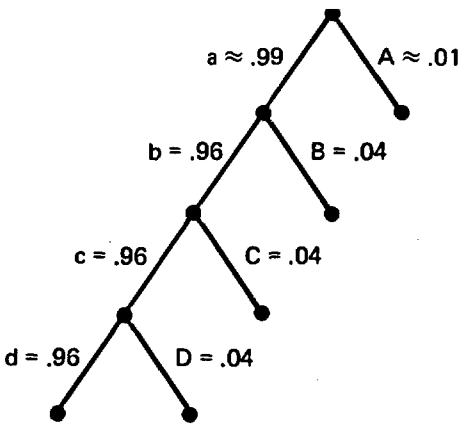


Figure 4–15. HRA event tree for actions by operators assigned to the control room, with human-error probabilities modified to reflect dependence. (Refer to page 4–47 for an explanation of the numbers in parentheses.)



Event	HEP	Source
A = Control-room operator omits ordering the following tasks	.01 (.005 to .05)	Table 20-22, item 1 (p. 20-31)
B = Operator omits verifying the position of MU-13	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)
C = Operator omits verifying/opening the DH valves	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)
D = Operator omits isolating the DH pump rooms	.04 (.02 to .2)	Table 20-18, item 3 (p. 20-28)

Figure 4-16. HRA event tree for actions performed outside the control room, with human-error probabilities modified to reflect dependence. The HEP for event A has been modified to reflect the effects of moderately high stress and dependence; the HEPs for events B, C, and D have been modified to reflect the effects of moderately high stress and protective clothing.

however, decide whether a given sequence through the HRA event tree will contribute to system success or failure.

At this point in the human-reliability analysis, the system analyst should examine the HRA event tree for discrepancies between his understanding of the system and the human-reliability analyst's representation of it. He should consider the implications of each path through the HRA event tree, and then he should label each end point of the tree as a system success or failure. These end points should be quantified as probabilistic statements; the statements will be combined to formulate total system success and failure probabilities. This examination of the HRA event tree by the system analysts could be performed during the early stages of the human-reliability analysis or during the initial screening of the system. It is done here for illustrative purposes.

4.5.10.2 Example

After deciding which errors contribute to system failure probabilities, the system analyst made the following adjustments for Figure 4-15 (the final analysis to this point of the actions performed by the control-room operator): he defined the paths ending in error events 1, 2, 3, 4, 7, 18, 19, 22, and 23 as system failure and those ending in error events 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 20, 21, 24, 25, 26, and 27 as system success. Since the implications of the accident at Three Mile Island Unit 2 have great potential impact on error events 5 and 6, these error events were removed from the analysis at this point, to be considered separately.

For the HRA event tree of Figure 4-16, a similar decision was made by the system analyst. He decided that all of the paths terminating in a human error constituted contributions to system failure.

Once the paths that result in system failure have been determined, total system success and failure probabilities can be quantified in either of two ways. The first method is the simpler, requiring no redrawing of the HRA event trees. In it, the end points of the limbs on the existing HRA event tree are simply labeled as success or failure. All of the terminal success probabilities are summed to reach the total system success probability. The failure probabilities are obtained by the same method or by subtracting the total system success probability from 1.

The second method is more complex and requires that the HRA event tree be redrawn. When error on a human task does not contribute to system failure, both limbs representing this task on the HRA event tree contribute to the probability of system success. Algebraically, a probability of 1 is being multiplied by the system success probability since the results of paths going through both limbs are combined into the system success probability. In effect, that error has no influence on system failure. Therefore, we need not even consider it since we are concerned with estimating the probability of system failure in a risk assessment. The branches that represent events whose outcomes do not contribute to total system failure probabilities can be deleted from the HRA event tree altogether. The tree should be redrawn, diagramming only the events that have some effect on the probability of system failure. Figure 4-17 shows how the HRA event tree for actions performed by the control-room operators is changed when this second method for quantifying total system success and failure probabilities is used.

4.5.11 DETERMINING THE EFFECTS OF RECOVERY FACTORS

4.5.11.1 Discussion

Complete analyses are performed for the dominant sequences that show up in the computer modeling of the fault trees. To save time and effort in the human-reliability analysis, the effects of recovery factors are not considered until it is determined that a given analysis is part of a potentially dominant sequence. The probability of system failure due to human error will certainly be higher when recovery factors are ignored than when they are included. If the situation being analyzed does not appear as a potentially dominant sequence

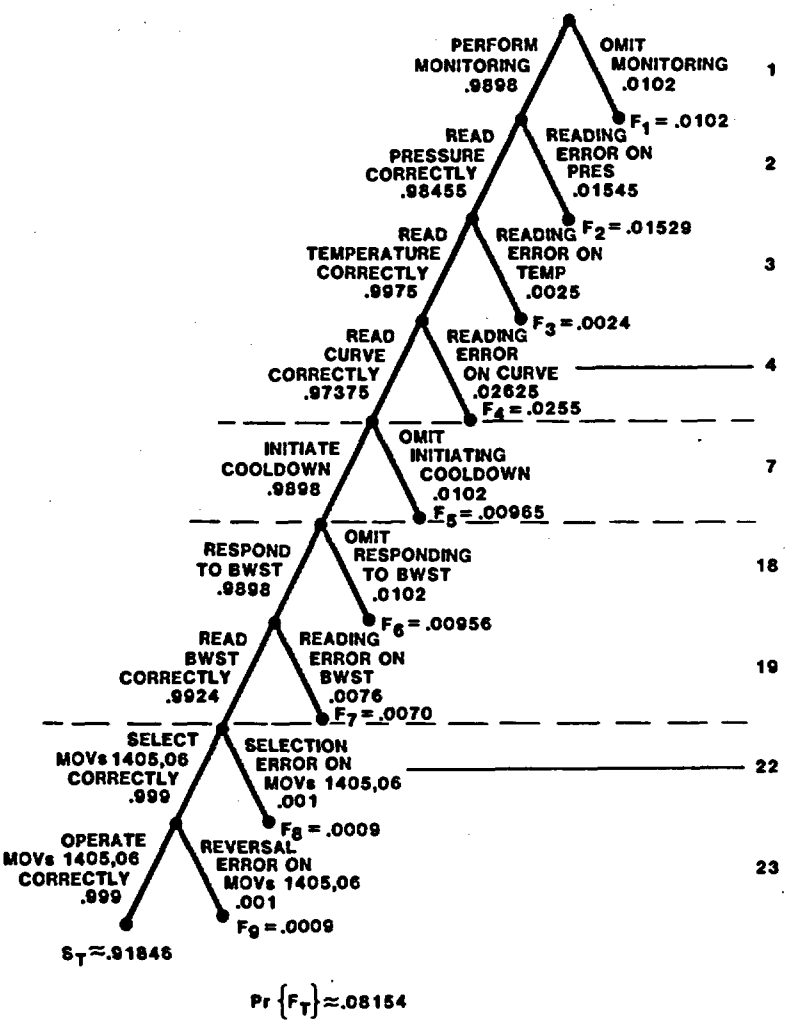


Figure 4-17. HRA event tree for actions by operators assigned to the control room, modified by second method for quantifying system success and failure probabilities.

when this inflated system failure probability is used, there is no need to analyze it further. In fault-tree terms, the frequency of an accident sequence can only be decreased by considering recovery factors.

To decrease the actual number of human-reliability analyses that must be performed for each plant, it is recommended that recovery factors not be included in the preliminary analyses. Once potentially dominant sequences have been identified, recovery factors for each can be added to see whether a complete representation of the system as it operates will eliminate the potential dominance. The incorporation of recovery factors can be done in stages, the purpose being to decrease the amount of time required for each analysis. If there are five recovery factors for a given scenario, the human-reliability analyst may choose to model only two of them at first. If the inclusion of these results in that sequence's ceasing to be potentially dominant, no more work need be done at this time. If this scenario still shows up as one of the system's potentially dominant sequences, the other three recovery factors should be analyzed.

Some recovery factors are highly situation-specific, while others can be applied generically. Alerting cues for recovery actions for any given incident will always depend on the specifics of response requirements for that incident. However, when analyzing recovery factors operating after maintenance activities it will sometimes be possible to generate HRA generic event trees that can be applied without modification to every such case for that plant. This is possible because, in many plants, a single procedure dictates the steps to be followed in restoring components after maintenance. In either case, the recovery factor can take the form of a point value (an HEP) or of a separate HRA event tree. The point value or the total success probability of the recovery HRA event tree should be inserted onto the associated error limb of the main HRA event tree. The probability of error for that limb is then multiplied by the success probability of the recovery HRA event tree and by the probabilities of the other events in that path to obtain the probability of recovery from the error. The end point of the original system failure path for that error is multiplied by the failure probability for the recovery factor to obtain the probability of an unrecovered error.

4.5.11.2 Example

As mentioned earlier, human redundancy as a recovery factor has already been analyzed for this problem to demonstrate the quantification of the effects of dependence. We can now consider situations in which the operator could catch his own errors or in which another operator working at a later date could catch his errors. An example would be an inspection process like the walk-around (see Chapter 8 of the Handbook). Since this problem deals with responding to an emergency, however, it is not appropriate to use the walk-around as a recovery factor. It is also possible for the operator to catch his own errors when the situation provides some additional alerting cue either to the action that should be taken or to the error itself.

In this problem and from the procedures in Figure 4-3, we see that the operator should respond to the BWST level's falling to 6 feet. His response is cued from two sources: if he is following the written procedures correctly, he will be monitoring the meter indicator of the BWST level; if he is not using the written procedures, there is still a possibility that the low-low-level alarm (annunciator) will remind him that he needs to perform the follow-up actions. We will treat the alarm as an additional alerting cue and analyze its effect as a recovery factor. From Chapter 20 of the Handbook, we need to find an estimate of an HEP for response to an annunciator. Table 20-4 lists HEPs for failing to respond to one of any number of annunciating indicators. We have no exact information on this, but assume that at this time into the incident 10 annunciators are alarming. The probability of the operator's failing to respond to any one of these 10 is .05 (.005 to .5). Figure 4-18 shows the diagramming for this recovery factor. Note that its inclusion in the analysis increased the unrounded probability of total system success from .91846 to .92746. If this is an adequate increase (if the sequence does not prove to be potentially dominant when the success probability is .92746), no more recovery factors need be analyzed.

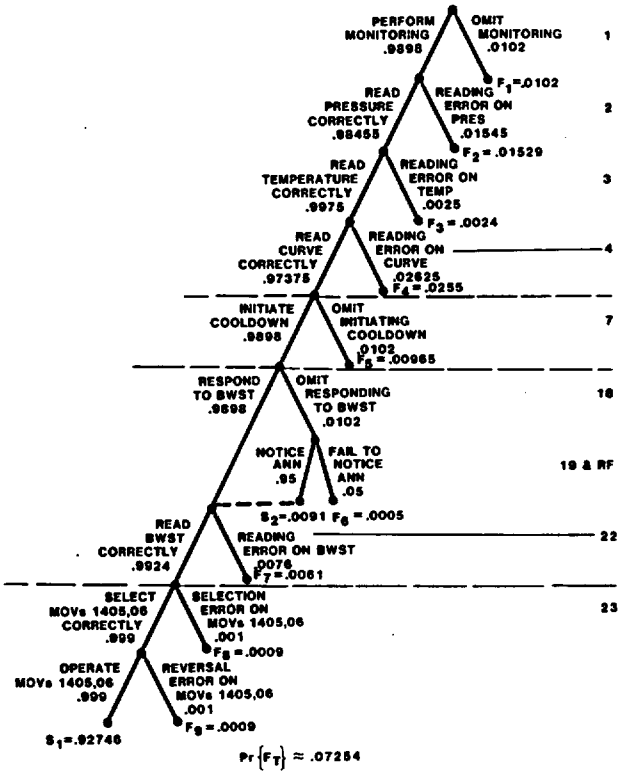


Figure 4-18. HRA event tree for actions by operators assigned to the control room, including one recovery factor.

4.5.12 SENSITIVITY ANALYSIS

4.5.12.1 Discussion

At times during the course of a human-reliability analysis, the analyst will want to determine the effects of manipulating the values of one or more of the elements analyzed. He may do this because he has some reservations about the assumptions he made, because the data he used are very uncertain (e.g., estimates of diagnosis errors by control-room personnel), or because he has not been able to obtain detailed information about some set of performance-shaping factors he judges are important determiners of the reliability of a task he has to analyze. Changing the assumptions of the analysis or changing the values of certain parameters may affect the probabilities of system success and failure. It may be of interest to manipulate these values to determine the effects of changes in design or procedures before such changes are made.

If the probabilities of some errors in an analysis stand out with respect to those of others, the analyst may want to see what effect lower probabilities for these errors would have on total system success and failure probabilities. The HEPs can be decreased by the action of recovery factors (see Section 4.5.11) or by changing the characteristics of the task to reflect a situation in which an error is less likely. These changes can be

accomplished by improving man-system interfaces, by increasing feedback adequacy, or by upgrading the quality of associated procedural steps. The new, lower HEPs can be entered onto the HRA event tree, and the resulting differences in total system success and failure probabilities evaluated. Sensitivity analyses are extremely useful in tradeoff analyses of proposed design changes and in pinpointing areas of potential system improvement.

In performing best- and worst-case analyses for a PRA, a bounding analysis can be executed, as described in detail in the appendix to NUREG/CR-2254 (Bell and Swain, 1981). For this exercise, two sets of HEPs are used and the results of the two analyses compared. The upper and lower bounds of the nominal HEPs for a given situation can be used, or two sets of assumptions and PSFs relating to the situation can be defined. The results of these two analyses can be evaluated by entering them onto the appropriate fault tree to see how sensitive some part of the PRA is to the two sets of HEPs. For PRA, the criterion for evaluating the sets of results should be risk significance. If there is very little difference in outcome, the analyst may decide to select the more conservative set for inclusion in the final PRA, at least as a temporary measure. If the difference in outcome is considerable, he should take steps to obtain better data.

4.5.12.2 Example

In this problem, the two most important errors, in terms of their probabilities, are errors 2 and 4, reading errors on the RCS pressure chart recorder and the graph of the pressure-temperature curve. Suppose we want to find out, as a design tradeoff comparison, whether changing either or both of these tasks to result in lower task HEPs is worthwhile in terms of system success probability. The simplest change involves changing the nature of the displays themselves to make reading errors less likely. For RCS pressure, the display could be a digital meter instead of a chart recorder. From Table 20-5 in the Handbook, we see that this would change the basic HEP for that task from .006 (.002 to .02) to .001 (.0005 to .005). This new HEP of .001 must be modified to .005 (.0025 to .025) to reflect the effects of stress and then modified again to reflect the effects of dependence, becoming .0025 (.001 to .01). Using the .0025 instead of the .01545 for this HEP results in a total system success probability of .9396 as opposed to .927.

If we make the same sort of adjustment for error 4, we might redesign the graph so that it is comparatively easy to read. If we now use the lower bound of the HEP in Table 20-5, item 5, instead of the nominal value, we have .005 (.002 to .02). This becomes .025 when modified for stress and .0128125 when modified for human redundancy. Modifying only this graph results in a total system success probability of .9402.

For a larger increase in the total system success probability, we could analyze the effects of both changes. An HRA event tree with these new values is shown in Figure 4-19. The total system success probability becomes .95262. Whether the new estimate of the probability of system success is large enough to warrant the incorporation of both changes is, of course, a management decision.

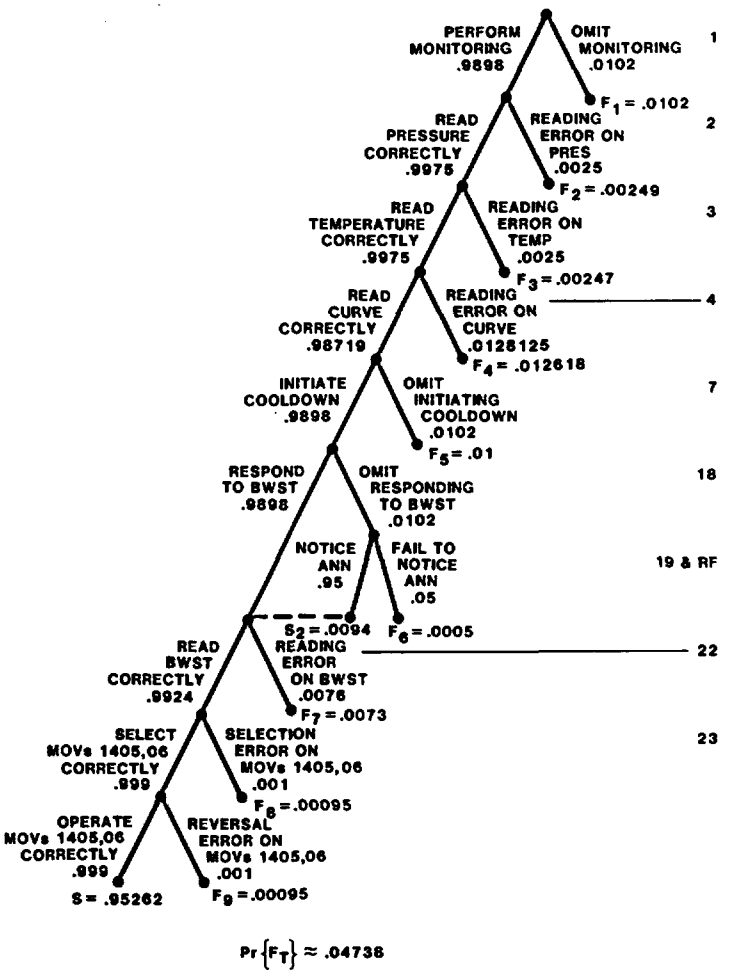


Figure 4-19. HRA event tree for actions by operators assigned to the control room, with tasks 2 and 4 modified.

4.5.13 SUPPLYING INFORMATION TO SYSTEM ANALYSTS

4.5.13.1 Discussion

All of the information used in performing the human-reliability analysis, especially the assumptions made and the modified HRA event trees, should be presented to the system analysts. The human-reliability analyst should then go over his analysis with them to ensure that there are no misunderstandings--no unresolved conflicts between the two concepts of the operating system. The system analyst should be familiar enough with the basic principles of HRA event-tree diagramming that he can use the HRA event tree itself to obtain the necessary inputs for his analyses. He should be able to use the total system success and failure probabilities or an HEP for a single item of equipment or for a single error for a given piece of equipment. These values can be entered directly into the human-error blocks of the system fault trees. The sources of the HEPs may be of interest to the system analysts, but are not strictly necessary. Section 4.6 discusses the method for formatting this information so that it is usable.

Any dependence found by the human-reliability analyst should be specifically indicated to the system analysts, especially in the case of dependence between different items of equipment. When dependence exists because of two operators performing the same task, combined HEPs representing the performances of both are entered into the human-error block of the fault tree--no change in the system fault-tree model is necessary. When dependence exists between performances on different items of equipment, the fault trees must be modified to reflect this common-mode failure. Identifying where and between which system elements the dependence exists will enable the system analyst to modify his models accordingly.

4.5.13.2 Example

If the system analyst needs an HEP for the entire procedure outlined in Figure 4-19, he should use the total system success probability, .962. If he needs a value for all possible human errors made in operating MOVs 1405 and 1406, he must consider all three of those diagrammed: the error of omission for the entire step (18), the selection error (22), and the reversal error (23). In effect, the combination of these errors represents a small HRA event tree. The system analyst must use the product of the success probabilities for each error event, .988, as the probability of success on those components. If the system analyst were only interested in the likelihood of an error of omission when dealing with MOVs 1405 and 1406, he would use the HEP for that specific error, .0102.

The human-reliability analyst should point out to the system analyst that MOVs 1405 and 1406 are completely dependent for all errors considered in the analysis. They (as a single item of equipment) are also dependent on the monitoring task (18): an equipment failure of the BWST meter would result in an error on MOVs 1405 and 1406.

4.6 METHODS OF DOCUMENTATION

The results of the human-reliability analysis go directly into the system analyses as probability statements. The only HRA data that are used in the rest of the risk assessment are the HEPs for given error events or for total system success and failure probabilities, and the information on dependence (where and what kind). The most important part of any final HRA report is the cataloging of the HEPs by item (of equipment) or by procedure, depending on the level of detail in the system fault trees and the system event trees, and the pinpointing of existing dependence. Other information included in the final report is not necessary as an input to the analysis itself, but is instead necessary as a reference on the performance of any particular human-reliability analysis.

Other human-reliability analysts must be able to trace through the analyses and to understand them fully. To obtain the necessary information, they must have access to the material on which the analysis was based. The

analyst should therefore provide in the final HRA report a set of the written procedures analyzed or his written version of the "standard operating procedure," along with the assumptions made in defining the situation under which the procedure would be performed. These assumptions will have been made during the visit to the plant and during the talk-through of the procedures with plant personnel. A copy of the final HRA event tree resulting from the analysis should be included. The basic HEP for each limb of the tree and its source as well as the source for any modifications (performance-shaping factors, dependence) should be included. This information can be added to the table of the task analysis; this is a clear, concise method for presenting a definition of the error events found in the HRA event tree. If recovery factors were considered or a sensitivity analysis was performed, the outcomes of these should be included.

In short, the final report should include all information necessary for the system analyst to check his assumptions about the performance situation against the human-reliability analyst's. It should also include sufficient information so that another human-reliability analyst could analyze the same scenario and arrive at a similar result.

4.7 DISPLAY OF FINAL RESULTS

As mentioned in Section 4.6, the most efficient method for displaying the results of a human-reliability analysis is to use the task-analysis format shown in Figures 4-6 and 4-7. These tables can be expanded to include the other information necessary for a complete documentation, as shown in Figures 4-20 and 4-21 for the example that was worked in this chapter. With these tables and copies of the HRA event trees, the system analysts should be able to take information in any form or at any level needed for input into the fault trees. The expanded task-analysis tables, HRA event trees, list of assumptions, and copy of the procedure should provide sufficient documentation for a human-reliability analysis.

This type of complete documentation of a human-reliability analysis is important for PRAs to be performed at various times in the life of a plant. As the plant equipment, manning, or operations change over time, the PRAs reflecting the different assumptions become points of comparison for the effects of these changes.

4.8 UNCERTAINTY AND VARIABILITY IN HUMAN-RELIABILITY ANALYSIS

Each estimate of a human-error probability for the performance of a task or activity is associated with some degree of uncertainty. Therefore, each such estimate is bounded by some range of values that is judged to have a high probability of encompassing the actual value of any given performance. This section discusses various sources of this uncertainty and

Step	Equipment	Action	Indication	Location	Notes	Errors	HRA event tree	HEP	T,I[a]	Final[b]
D.2	RCS pressure	Monitor		CB4		1. Omission (all)	1	.01	20, 5	.0102
						2. Reading	2	.006	5, 3	.01545
	RCS temperature	Monitor		CB4		Reading	3	.001	5, 2	.0025
	heater switches	Maintain pressure and temperature	Within curve on chart	CB4		Reading	4	.01	5, 5	.02625
D.4	4 HPI MOVs	Override and throttle		CP16, CP18	ESF	1. Omission (all)	5	.01	20, 5	.0102
						2. Selection (1)	6	.003	14, 7	.003
		Initiate cooldown	Procedure 12			Omission	7	.01	20, 5	.0102
D.7.3	CV-7621,22,37,38 (room-purge dampers)	Secure	Close switches	Ventilation room		1. Omission (all)	8	.01	20, 5	.0102
						2. Selection (each)	9,10,11,12			
D.7.4	DH pumps	Verify on	Indicator lamps	CP16, CP18	ESF	1. Omission (for MOVs too)	13	.01	20, 5	.02
						2. Selection	14	.001	13, 2	.002
						3. Interpretation	15	.001	7, 9	.002
	MOV-1400, 1401	Verify open	Indicator lamps	CP16, CP18	ESF	1. Selection	16	.001	13, 2	.002
						2. Interpretation				
D.9	Borated-water storage tank	Monitor level	>6 feet	CP14		1. Omission	18	.01	20, 5	.0102
						2. Reading	19	.003	5, 1	.0076
	MOV-1414, 1415	Verify open	Indicator lamps	CP16, CP18	ESF	1. Selection	20	.001	13, 2	.001
						2. Interpretation	21	.001	7, 9	.001
	MOV-1405, 1406	Open	MOV switches	CP16, CP18	ESF	1. Selection	22	.001	13, 2	.001
						2. Reversal	23	.001	13, 7	.001
	MOV-1407, 1408	Close	Switches	CP16, CP18	ESF	1. Selection	24	.001	13, 2	.001
						2. Reversal	25	.001	13, 7	.001
	MOV-1616, 1617	Close	Switches	CP16, CP18	ESF	1. Selection	26	.001	13, 2	.001
						2. Reversal				

[a]These numbers refer to table and item numbers in Chapter 20 of the Handbook.

[b]The nominal HEPs have been modified to reflect the effects of a moderately high stress level and (in some cases) high dependence between two operators.

Figure 4–20. Display of final results in a task-analysis table for actions by operators assigned to the control room. The column labeled "HRA event tree" does not usually appear in a task analysis; it has been included for the reader's convenience. The numbers in this column refer to the error event numbers appearing in HRA event trees starting with Figure 4–9.

Step	Equipment	Action	Indication	Location	Notes	Errors	HRA event tree	HEP	T,I[a]	Final[b]
D.7.1	MU-13	Verify closed	Position	Stairwell outside makeup pump room	Only valve	Omission	2	.01	18, 3	.04
D.7.2	DH-7A, 7B	Open	Position	Outside DH pump rooms		Omission (for all D.7.2)	3	.01	18, 3	.04
	MU-14, 15, 16, and 17	Verify open	Position	DH pump rooms						
	MU-23, 24, 25, and 26	Verify open	Position	DH pump rooms						
D.7.3	ABS-13, 14	Close	Position	Outside DH pump rooms	Only valve	Omission (for all D.7.3 here)	4	.01	18, 3	.04
	Watertight doors	Close	Locks in place	DH pump rooms						

[a]These numbers refer to table and item numbers in Chapter 20 of the Handbook.
[b]The nominal HEPs have been modified to reflect the effects of a moderately high stress level and (in some cases) high dependence between two operators.

Figure 4-21. Display of final results in a task-analysis table for operations by an auxiliary operator outside the control room. The column labeled "HRA event tree" does not usually appear in a task analysis; it has been included for the reader's convenience. The numbers in this column refer to the error event numbers appearing in HRA event trees starting with Figure 4-10.

describes some methods for assigning uncertainties in a human-reliability analysis. (A detailed discussion of measures of uncertainty and their propagation is found in Chapter 12.)

4.8.1 SOURCES OF UNCERTAINTY

There are five major sources of uncertainty in estimating the probabilities of human errors in the operation of nuclear power plants:

1. The dearth of data on human performance in nuclear power plants.

2. The inexactness of models of human performance that purport to describe how people act in various situations and conditions.

3. The identification of all relevant performance-shaping factors and their interactions and effects.

4. The skill and knowledge of the human-reliability analyst.

5. The variability in the performance of a given individual and among the performances of different individuals.

The first source, the shortage of human-performance data specific for nuclear power plants, is the most critical. Historically, such data have not been collected on a scale large enough to establish a data base for operations in nuclear power plants. There are, however, some data sources that have been used for human-reliability analysis. The licensee event reports include descriptions of incidents involving human error, but no information on human-error rates or probabilities is given. Furthermore, the determination of what constitutes human error in these reports is frequently questionable.

Although programs to collect data useful for human-reliability analysis are under way, there is at present no single source of data collected from the measurement of human performance in nuclear power plants. Therefore, most estimates of human-error probabilities must involve extrapolation from other sources of information. These sources include (1) the collective judgment of experts (i.e., people with expertise on the performance of the tasks being evaluated) who may directly or indirectly assess error probabilities, (2) the human-performance models and the associated derived data from sources like the Handbook, and (3) data gathered on operationally similar tasks. For example, the actions involved in closing a valve, as specified in a set of procedures, often will be very similar whether the actions are performed in a chemical processing plant or in a nuclear power plant. Such data from similar tasks can be extrapolated or modified to account for dissimilarities in the situations. This extrapolation is subject to error itself, but represents the best approximation available. Many of the estimated human-error probabilities in the Handbook represent this type of extrapolation.

In those cases for which data from operationally similar situations or even derived data are not available, various methods for the use of expert

judgment can be applied. These methods, however, vary greatly in their consistency and validity (Stillwell et al., 1982). (The NRC is sponsoring programs at Sandia and Brookhaven National Laboratories to develop recommended methods and procedures for given nuclear-power-plant applications.) The use of expert judgment as a substitute for actuarial data represents an extreme in the extrapolation process.

The second source of uncertainty is the modeling of human performance. The state of the art of human-reliability analysis is such that the modeling of human behavior can qualitatively account for its variability and for discrepancies in response situations, but there are definite limitations in quantifying such models. There are many models of human performance, but few can be used to estimate the probability of correct or incorrect human performance in applied situations. Furthermore, all models, even those that can be applied to a human-reliability analysis (e.g., the models in the Handbook) are themselves abstractions of real-world circumstances. As such, they only partially represent the situations they simulate. In some cases, experimental data have provided strong support for the general form of the models (e.g., the usual curvilinear form of the performance-under-stress curve), but in others the forms are still speculative (although based on sound psychological concepts).

The third source of uncertainty, the identification of the performance-shaping factors associated with a task, also involves some abstraction and is subject to some interpretation on the part of the analyst. This is probably the biggest source of error in extrapolating data from other sources to the nuclear power plant. Unless the tasks required in both situations are analyzed in sufficient detail, data from other sources may be misapplied to the tasks performed in a nuclear power plant. For example, a valve-restoration task in a chemical processing plant may be superficially similar to an equivalent task in a nuclear power plant, but the HEP from the chemical plant may be based on errors made by people using well-designed checklists, whereas the valve-restoration procedures carried out in the nuclear power plant may be performed from memory only. Using the HEP from the chemical plant to estimate the HEP for the nuclear power plant would obviously result in a gross underestimation of the true HEP.

The above difficulties will be exacerbated if there is little interaction between the human-reliability analyst and other members of the PRA team. Unless the human-reliability analyst is a real working member of the team, his identification of relevant performance-shaping factors and his estimates of the effects of these factors in the human-reliability analysis may ignore important influences of certain plant-specific factors. His estimates of nominal HEP values may be too low or too high. In such cases, the assignment of large uncertainty bounds will not compensate for his lack of knowledge.

The analyst himself is the fourth source of uncertainty; that is, the PRA team may include an HRA analyst who is not fully qualified. He may not be able to perform the necessary extrapolations or to use the human-performance models correctly. The less the PRA team knows about the operations and human activities in a given plant, and the less the team (or at

least the designated person) knows about the underlying psychology, physiology, and sociology of human behavior in general, the less accurate their estimates of human-error probabilities will be. That is obviously a form of uncertainty, but the untutored analyst may not recognize it as such. An independent, qualified observer, however, would want to increase the uncertainty bounds around the estimates made by less qualified analysts. It must be reiterated, however, that merely increasing the uncertainty bounds will not compensate for large errors in estimating the nominal values of the HEPs around which the bounds are placed.

Finally, in the prediction of human behavior, there is an uncertainty that results from the inherent variability of human performance due to individual differences, both within and between the people whose performances are being assessed in the human-reliability analysis. Even if one had a large amount of excellent-quality human-performance data collected for years on all nuclear-power-plants tasks, this variability would contribute to the uncertainty in a human-reliability analysis. A human-reliability analysis does not attempt to estimate the performance of one known person; instead, the analyst's estimates have to account for the fact that any given task may be performed by any one of many individuals, each of whom may vary somewhat in his reliability from day to day or even within a day.

The amount of uncertainty resulting from intra- and inter-individual differences is judged to be considerably less than that resulting from the combination of all the other sources of uncertainty. Some data on individual differences in a wide variety of industrial tasks were collected by Wechsler (1952). These data indicate that for routine and very well defined tasks the ratio of the performance scores of skilled performers near the top of a distribution for some measure of ability to the scores of performers near the bottom of the distribution is about 3:1. In these measures, the upper and lower one-tenth of 1 percent of the distribution was ignored, and thus the 3:1 range ratio includes about 99.9 percent of the scores. In the Handbook, a more conservative range ratio of 4:1 was assigned for individual differences per se, excluding the upper and lower 5 percent of the distribution of HEPs on routine tasks performed by skilled personnel. Thus, it is presumed that the 4:1 range ratio includes the middle 90 percent of the HEPs due to individual differences alone.

In the Reactor Safety Study (USNRC, 1975), to account for the variability in modeling human performance in general and the occurrence of a given error in particular, the Handbook's 4:1 range ratio was increased to 10:1 for most tasks and to 100:1 for tasks whose nature could not be well defined and for tasks performed under conditions that were ill defined or judged to be highly stressful. The Handbook has adopted and refined this concept of larger uncertainty bounds for "more uncertain task behavior." For routine tasks the typical range ratio is 10:1. For tasks involving interpretation or decision-making, a 20:1 ratio is not uncommon (in the revised draft in press), and a high 25:1 range ratio is used for performance under high stress. Each range reflects the uncertainty due to human variability, the lack of representative data, the imprecision of the modeling process, and the identification of relevant performance-shaping factors, but excludes the uncertainty attributable to analysts untrained in HRA techniques.

For applications of the Handbook HEPs and uncertainty bounds to human-reliability analysis, it is assumed, as noted earlier in this chapter, that the PRA team has the necessary expertise not only in HRA techniques but also in the other areas relevant to probabilistic risk assessments.

To summarize, the most significant contributors to uncertainty in the human-reliability analysis of nuclear-power-plant operations can be ranked by importance. Assuming the necessary analytical skills, the lack of data from actual human performance in nuclear power plants is the most important contributor. Naturally, if we had sufficient data on human-error probabilities for each task being analyzed, it would not be necessary to model each task. The second most important contributor to uncertainty is the inexactness of the models. No abstraction can fully define or account for all the variables in response situations as complex as those found in a nuclear power plant. Furthermore, it is unrealistic to suppose that each model will be applied consistently across all analyses. This lack of consistency is related to the difficulties in performing the necessary analyses of human inputs, mediating processes, and responses so that the relevant performance-shaping factors can be identified and assessed correctly (the third most important contributor to uncertainty). The fourth most substantial contributor to uncertainty is the variability of human performance. The uncertainty bounds associated with the estimates of human-error probability are almost certainly very conservative in accounting for the range of possible human performance on the various tasks modeled by various human-reliability analysts.

4.8.2 METHODS FOR HANDLING UNCERTAINTIES IN A HUMAN-RELIABILITY ANALYSIS

A human-reliability analysis consists of combining, in some fashion, HEPs for many different tasks or activities. For some PRA purposes, the use of uncertainty bounds may not be necessary. Instead, it may be sufficient to use single-point estimates as illustrated earlier in this chapter. When it is necessary to assign uncertainty bounds, there are two general approaches that have been used. The first is to propagate uncertainty bounds throughout the HRA portions of the PRA, using the methods discussed in Chapter 12. The second approach is to proceed with the usual propagation of point estimates through the HRA portion and then to assign uncertainty bounds about the final point estimate (i.e., the total human-error term for each portion of the human-reliability analysis). These methods can result in uncertainty bounds that are quite different, and it is up to the PRA team to select and justify the method it employs.

With regard to the first approach, the propagation of uncertainty bounds for each HEP, a commonly accepted method is that of using a Monte Carlo procedure to sample values from the distribution of each error probability in the analysis. Generally, in applying a Monte Carlo procedure, random sampling from each distribution in the analysis is used. In actual fact this procedure will not reflect the true response situation in that a dependence over tasks could exist. If an operator's skill level is fairly constant with respect to those of other operators for any of the tasks he

undertakes, his error probabilities are likely to fall close to the same relative position on each of the distributions being analyzed. Therefore, if the same operator performs each of the tasks being analyzed, there is very little likelihood that his performance will correspond to a set of randomly sampled HEP. To avoid this problem, one could set up a sampling procedure to reflect the above or other sources of dependence.

An alternative is the discrete probability distribution (DPD) method, also discussed in Chapter 12, in which the distribution of each HEP is graphed as a discrete histogram. In essence this method represents each continuous distribution with some finite number of points. To evaluate the uncertainty associated with combinations of human actions and other events, histographs representing the distributions of each can be combined to derive an uncertainty distribution associated with the combined failure probabilities of interest. The above-stated cautions about sources of dependence also apply to the DPD method.

If the robustness of a Monte Carlo or a DPD procedure is deemed unnecessary or inappropriate in view of the lack of actual data on human-error distributions in the performance of nuclear-power-plant tasks, the second approach to the treatment of uncertainties can be used. This approach avoids the necessity of propagating uncertainty bounds through the HRA portion of the PRA. Instead, uncertainty bounds are assigned to the total human-error probability obtained from each HRA portion of the PRA. For example, one would assign uncertainty bounds to the total error probability obtained from an HRA event tree like the one shown in Figure 4-18. In the remainder of this discussion on uncertainties, the HRA-event-tree method from the Technique for Human Error Rate Prediction is used to explain some methods used in this second approach to the treatment of uncertainties. However, the discussion pertains to any other HRA method as well.

In discussing the second approach, it is useful to define some terms. An HEP and uncertainty bounds are given in the form of

$$\text{HEP}\left(\frac{1}{k_1} \times \text{HEP},\ k_2 \times \text{HEP}\right)$$

where the first term in parentheses is the lower bound and the second term in parentheses is the upper bound. For example, as in the tables from the Handbook, if the estimates are

$$.005\ (.001 \text{ to } .05)$$

then

$$\text{HEP} = .005, \quad k_1 = 5, \quad k_2 = 10$$

If $k_1 = k_2$, the bounds are said to be symmetrical and the "error factor" is used to denote both k values. The uncertainty range (UR) for asymmetrical uncertainty bounds is $UR = k_1 k_2$, and for symmetrical bounds it is the square of the error factor.

Discussed briefly below are three methods, or approximations, that involve the usual propagation of point estimates through the HRA event tree, with the assignment of uncertainty bounds about the final point estimate (i.e., the total failure term for the tree). The output--that is, the final failure term and the associated uncertainty bounds--is then entered into the appropriate places in the system event or fault trees. What the point estimate represents (for instance, whether it is the mean or the median of some distributions) depends on the analyst's interpretation and understanding. However, if point estimates are taken from the Handbook, the usual practice is to consider them as medians of a lognormal distribution.

The simplest of the three methods is to assign some arbitrary set of uncertainty bounds to the total failure probability obtained from the HRA event tree. In some PRAs, once this total failure probability was determined as a point estimate, uncertainty bounds of a factor of 10 on each side of the point estimate were assigned. It is important to note that this error factor of 10 is considerably larger than the typical error factors for the individual HEPs that were used to calculate the total failure probability. For a lengthy and interactive HRA event tree, especially one that represents the performance of more than one person, some analysts might judge that an error factor of 10 is not sufficiently conservative.

Another method for assigning uncertainty bounds to the total failure term of an HRA event tree is to take the largest error factor (the square root of the uncertainty range about an HEP) found for any HEP in the tree and to apply it as the error factor for that total failure term. This method should be employed only where the distribution of the uncertainty bounds about the total failure probability is to be symmetrical.

The third method, a variant of the second, does not require symmetrical uncertainty bounds. The largest uncertainty range about an HEP is used as the uncertainty range for the resulting probability of total failure in the human-reliability analysis.

In following either the second or the third method, we say that the uncertainty associated with the entire analysis is no greater than that associated with the most uncertain element of the analysis. In some cases, this assumption may not be sufficiently conservative.

Some of these methods have been documented, as they were used in PRAs that have already been completed. In view of the different viewpoints as to how uncertainties should be propagated in a PRA, no recommendation can be made here as to the best method for assigning uncertainty bounds in the human-reliability analysis per se. Furthermore, because most uncertainty bounds for individual HEPs are not determined from data collected in nuclear power plants, the method employed may not be very critical in a PRA so long as the uncertainty bounds for terms entered into the system analysis are not unrealistically narrow. It is apparent that a sensitivity analysis can be very useful to ascertain the impact on the system analysis of assuming different uncertainty bounds for the human-error terms to be incorporated into the system event or fault trees.

4.9 ALTERNATIVE METHODS OF HUMAN-RELIABILITY ANALYSIS

While other methods for estimating the human-error contribution to system reliability have been developed and documented, it is important that the reader keep in mind the state of the art of human-reliability analysis in considering them for use in a probabilistic risk assessment. Several of the newer methods were developed specifically for use in PRAs, while others are the result of modifications made to models of human performance that were initially developed for quite different purposes. Some human-performance models can be used to estimate the likelihood of human errors, but many of them may not be useful for a PRA in that they cannot be applied to all situations modeled in a risk assessment. Some models that have been documented are very limited in scope; they model human performance at a level so detailed that it cannot be realistically observed and thus cannot be verified. Other models deal with human performance in contexts that are largely covered by other portions of the PRA. For example, human errors made in conducting maintenance operations (rather than in restoring equipment after such operations) will usually be detected in the equipment-failure rates. The inclusion of such errors in the system models constitutes a double accounting: the impact of human errors made in maintaining equipment will be incorporated into the system fault trees twice. Some of the alternative methods simply represent restatements or reorganizations of the material in the Handbook or other sources and should be used if their presentation formats fit in better with the overall scheme of a particular PRA. Extreme care should be taken in employing these or any HRA methods since the potential for error in using them is high given the context of the PRA.

4.9.1 HUMAN-RELIABILITY ANALYSIS IN THE OCONEE PRA

In the human-reliability analysis performed for the Oconee PRA, human errors were classified into two types, latent and dynamic (Dougherty, 1981). Latent errors are made by maintainers or operators who fail to restore components or systems to their proper states after testing, maintenance, or calibration. These errors result in component or system unavailabilities and occur before a transient (during which, it is assumed, the component or system would be required). Dynamic errors are made by operators during the course of an accident. The circumstances under which any error is made are usually of less interest than are the system effects of that error. In other words, whether a valve is unavailable because of an error in restoration after testing or because an operator locked it while responding to a transient is irrelevant in terms of the system effects, which are that the valve is unavailable. The causes of the unavailability are important to the estimation of the probability of the underlying error, but not to the estimation of the system effects of the error itself. The distinction between latent and dynamic errors is, however, supported by the different classes of recovery factors that apply to each case. Also, this classification fits in well with the scheme of the Oconee study for incorporating the results of the human-reliability analysis into the entire PRA, as discussed below.

In the Oconee PRA, estimates of human errors were incorporated at three levels (Dougherty, 1982):

1. Above the system level (in the system event trees or in the logic connecting the system fault trees to the system event trees).

2. At the system level of the system fault trees.

3. At the component level of the system fault trees.

At the first level, the Oconee PRA took into account the effects of several factors that have the potential for affecting the probability of human error in responding to a transient. These include the operator's perception of the severity of the situation, the timing of the accident sequence, the amount and the quality of direct indications of plant status in the control room, the success options available to the operator, and the training and/or procedures available to the operator that would support his successful completion of the proper response to the transient.

The general criteria for estimating the probabilities of human errors and the effects on these probabilities of the above-mentioned factors were obtained from the Handbook (NUREG/CR-1278) an the subjective judgment of the HRA team for the Oconee study. A Delphi method was used to solicit estimates of the basic human-error probabilities and the relevant factors. The group sampled included members of the HRA team and former plant operators. The HRA team was interested in obtaining order-of-magnitude best estimates of human-error probabilities.

The human errors that were included in the first level of incorporation were grouped according to four general types (Dougherty, 1982):

1. Situations where the actions of the operator represent an immediate redundancy to system performance.

2. Situations where the operator acts to find alternative success paths.

3. High-stress situations where the operator has little time to succeed or must leave the control room to succeed.

4. Low-stress situations where the operator has long times to succeed but must make significant repairs to plant systems.

At the second level of incorporation, the system level, the estimates of human-error probabilities were input at the top of the system fault trees. At this level, human errors that could affect the availability of an entire system were considered. For example, if an operator misdiagnoses an accident, he can disable an entire system required to respond correctly to the accident. The probabilities of these misdiagnoses were determined by using a "confusion matrix" developed for the Oconee study. This matrix is the result of interviews with PWR operators who estimated the likelihood that different initiators would be mistaken for each other. The time available to the operator for making a diagnosis--that is, the interval between

the initiation of the accident and the time at which system reliability would be degraded--was taken into account in estimating these errors. Errors in calibrating safety systems that could result in out-of-tolerance system performance were also included at this level.

At the third level of incorporation, the component level, three types of errors were identified: errors made in restoring items of equipment after testing, maintenance, or calibration; violations of technical specifications in concurrently performing maintenance or testing on parallel systems, thus rendering them unavailable; and procedure-based errors in which the operator, in trying to respond successfully to an accident or a transient, causes the unavailability of some component. The probability of concurrent maintenance was judged by the Oconee HRA team to be negligible because the plant has a very good administrative-control system. These errors were not included in the analysis. Neither was the last type of error defined at this third level of incorporation--the errors made by the operator in attempting to follow the correct set of procedures in responding to an accident--included at this point in the analysis. The Oconee HRA team judged that several different operator errors at this point would result in the same system effects, and these errors were therefore grouped with others for inclusion at a higher level in the system models.

4.9.2 THE OPERATOR-ACTION TREE

The operator-action tree (OAT) has been used in the PRA for the Susquehanna nuclear plant. In general, it involves a higher-level human-reliability analysis than that described in the Handbook because the OAT format provides for the incorporation of the HRA results at the system-event-tree level and because, in modeling the response to a transient, it emphasizes the importance of units of team performance over those of the individual. (This level of incorporation of the human-reliability analysis into the PRA can conceivably be accomplished with the results of a Handbook human-reliability analysis, but the Handbook method is not specifically designed for this level of incorporation.)

The OAT method uses a horizontal event-tree format to model the probability of occurrence of the initiating event and the following human behaviors: monitoring indicators, interpreting the problem correctly, and taking timely correct action (Wreathall, 1981). Monitoring indicators involves the operators' taking notice of any displays that give information as to the type of event that has occurred. Interpreting the problem correctly calls for the operators' correctly assessing the state of the reactor from the available displays. This ability is very strongly influenced by the amount and the type of training the operators have received and by their familiarity with that particular event. Taking timely correct action depends almost entirely on the operators' correct interpretation of the event. It involves their correcting errors made in preparing the plant for the proper automatic response and taking appropriate steps to mitigate the effects of the event. (It is possible that this step could be performed correctly (at least for a time) when an incorrect interpretation was made. This might happen if the operators mistook for the true initiating event an event with similar response requirements. It is assumed that correct

response while reacting to an incorrect model of plant status would not be possible for the entire course of the accident sequence.)

Data for the monitoring activities, for taking correct action, and for taking recovery action can be obtained from the Handbook or from a similar source of human-performance data. Data for the correct interpretation of plant status can be derived from the OAT time-reliability curve (Wreathall, 1982).

Since the time available for making a correct diagnosis and correctly responding is the major variable affecting performance, it is the factor used to characterize the operators' response behavior. The time-reliability curve plots the probability of failure against the time available for the operator to make a correct diagnosis. The available time is defined as the interval between the initiation of the accident and the time at which response activities would come too late to avoid undesirable system consequences. The curve ignores the first few minutes after a transient as involving behavior that is too uncertain to model. It deals with team behavior; that is, it plots the probability of the entire control-room team's failing to diagnose the event correctly. This allows implicit consideration of the types of team interaction considered in some of the Handbook's models, such as the dependence model.

The data points for the time-reliability curve are obtained from the expertise of the analysis team. The members of the analysis team use their familiarity with the specific plant being analyzed and their knowledge of the principles of human behavior to estimate the probability of the operating team's performance in diagnosing transients correctly. In the Susquehanna study, the analysis team included persons with expertise in engineering psychology, systems engineering, and nuclear plant operations.

To account for the uncertainty in the data-gathering process and for the variability of human performance, the time-reliability curve is characterized by an uncertainty range consisting of an order-of-magnitude spread on either side of the best-estimate predictions. This uncertainty range is not meant to imply statistical confidence limits, but only to reflect the predicted middle 80 percent of the actual performance distribution for the operating team. This uncertainty range is also used to accommodate the effects of "reluctance" factors, which are similar in effect to the performance-shaping factors described in the Handbook. For example, if an operator is required by the plant condition to take an action he would normally avoid because of his training, he is less likely to perceive the requirement for this action in comparison with an action that is in agreement with his training. In this case, the probability of a failure in diagnosis at any given point in time on the OAT time-reliability curve would be increased by some factor, usually 2 to 5.

In incorporating the results of the analysis into the system fault trees, the OAT method accounts for dependence among events by assigning dependent events the same fault designator. Thus, when unrelated components are affected by behaviorally related activities, these activities are linked by giving them the same label in the fault tree. That fault-tree event will appear as the developed set of potential human errors. In this way, the dependence can be included in the fault tree for any component.

4.9.3 ACCIDENT INITIATION AND PROGRESSION ANALYSIS

In the accident initiation and progression analysis (AIPA) performed for a high-temperature gas-cooled reactor (HTGR), an operator-response model was developed to "provide a consistent basis for evaluating both the time and likelihood of a proper operator response for the accident sequence under consideration" (Fleming et al., 1978). The model is essentially an input/output model for the operators of the HTGR, with the inputs being any incoming information presented to the operators, such as alarms or other signals, and the outputs being the set of possible operator responses.

These possible operator responses were grouped into two categories: mitigating activities and nonmitigating activities. In general, mitigating activities involve an operator's responding to abnormal plant conditions by reducing power or initiating plant shutdown. Nonmitigating activities involve an operator's responding to abnormal plant conditions by taking inappropriate action or by taking no action, either of which would degrade system reliability (Raabe et al., 1977). Human-factors methods were developed during the AIPA study to treat both the beneficial and the detrimental actions of operators and maintenance crews (Hannaman, 1981).

The characteristics of an HTGR are such that extremely rapid responses on the part of the operators are rarely, if ever, required. Under most abnormal plant conditions, the operators are allowed sufficient time to make and reevaluate decisions about the nature of the occurrence, which makes it likely that they will take at least some corrective action. Because of this, in the first phase of the study, the effect of the operators' taking inappropriate or uncorrected action was modeled as taking no action to simplify the analysis. In the second phase, inappropriate actions or errors of commission were incorporated on a case-by-case basis.

The AIPA approach to modeling the impact of human errors consisted of several activities. Event trees and fault trees were used to define the explicit human interactions that could change the course of a given accident sequence and to define the time allowed for corrective action in that sequence. A time-dependent operator response model was developed that related the time available for correct or corrective action in an accident sequence to the probability of successful operator action. A time-dependent repair model was developed to account for the likelihood of recovery actions for a sequence, with these recovery actions being highly dependent on the system-failure modes. Data on human-error contributions were collected for each event and included in the fault or event trees both as common-mode fractions and as random system or component failure rates (Hannaman, 1981; Fleming et al., 1979).

In operating, testing, and maintaining equipment, human errors that cause component or system failures are treated explicitly in the system fault-tree analyses and implicitly in the method used to model the reliability characteristics of dependent failures in redundant systems (Fleming et al., 1978). The implicit treatment arises from the use of failure-rate and dependent-failure experience data that include contributions from human errors (Hannaman and Kelley, 1978).

The bases for the operator model are as follows:

1. Initially there is a probability of zero that the operator will respond instantaneously.

2. As time increases, the probability that an operator will take corrective actions increases.

3. If the operator discovers that his initial actions are insufficient for plant recovery, he will take further action until a stable condition is reached.

These factors indicate an increasing probability of operator success in time. The probability of success in this model increases until a time t_{max} is reached. The parameter t_{max} is the time available for operator action, determined from computer models that simulate the physical behavior of the system for the postulated accident and the transient response of key components. In a particular accident, the time available for operator action is determined by the transient thermal and structural response of the reactor core, vessel, structures, and containment. Usually a limiting component temperature or pressure defines the time available for operator action.

The likelihood that the operator will be able to take action to mitigate the consequences of an initiating event increases as the time available for such action increases. The time available to take such action is the time until the point at which such action will no longer significantly change the consequences of the event. The time within which 63 percent of trained operators will take successful action is the mean time to operator response (MTOR), the expected response time for an average, adequately trained operator. Data on the MTOR can be "obtained from measurement of operator response, estimates of knowledgeable experts, or development of a functional relationship for the most important variables contributing to the response time in the reactor control room environment" (Fleming et al., 1975). In the AIPA study, expert judgment was used to estimate MTOR, which was assumed to have a lognormal distribution. Confidence limits on the MTOR were determined by computing the standard deviation or by plotting the estimates and determining the variability graphically. To account for the effects of stress on operator performance, the estimates of MTOR were increased by 10 to 20 percent, in effect reducing the probability of correct operator action for a given time under stressful conditions.

The AIPA operator-response model is intended for HTGR conditions. For other situations, the probability distributions on time, MTOR, and their functional relationships should be investigated before applying this model (i.e., for short or long t_{max} other models may be useful).

The steps taken in applying the operator-response model were as follows (Fleming et al., 1975):

1. Determine the need for operator action in a branch-point fault tree.

2. Identify the operator's situation.

   a. Identify instrumentation that is operating, failed, etc., which may be dependent on the particular branch conditions.

   b. Identify the expected or trained-operator response, which may come from technical specifications or planned operator procedures (training).

3. Obtain data and analyze operator response.

   a. Utilize data sources (i.e., the Reactor Safety Study, abnormal occurrence reports, or expert opinion).

   b. Adjust data to include stress factors.

   c. Use the data range to determine uncertainty in the MTOR.

   d. Consider the interrelation of multiple operator actions within the same fault tree, which may require the use of a common-mode beta factor.

   e. Determine an upper limit (P_s), which is generally in the range of .99 to .9999.

4. Treat the resulting probability (P_{of}) and uncertainties as equipment-failure blocks in the fault-tree diagram (which may include the use of the sample computer code to determine the overall fault-tree uncertainty).

5. Use the time factor to help determine the range of consequences resulting from the two branches.

Although the consideration of human factors in the AIPA study was balanced between beneficial and detrimental actions in line with the objective of making realistic risk estimates, certain elements of the treatment may be viewed as conservative and still others as optimistic. Among the former are the use of maintenance data to quantify the timing of operator actions during accident situations and the omission from consideration of (1) human ingenuity to terminate the accident and (2) the mobilization of experts and technicians to supervise long-term external actions to mitigate the accident consequences. The most important class of actions whose omission can lead to underestimates of accident risk appears to be errors of commission that either initiate accidents or compound their consequences and those that cause the failure of multiple, otherwise independent, systems.

4.9.4 CONCLUSIONS

The methods outlined above have been applied in actual PRAs. There are, in fact, several other methods and models of human-reliability analysis in existence, but most of them have seen limited application or no application in PRAs as yet. The state of the art of human-reliability analysis is

changing rapidly at present. New methods are being developed, and older models are being revised and updated to accommodate the type of information needed for a PRA. The users of this guide are urged to investigate recent developments in human-reliability analysis that are or will shortly be available in the public literature. Limitations to these models should be observed carefully, and professionals with experience in human-performance techniques should be responsible for their use.

Of especial interest in current months are examples of "cognitive models," developed to provide estimates of errors made in diagnosing particular accident signatures and in deciding on corrective action. These are highly speculative and should be investigated with caution before application in a PRA. However, for such errors screening models are available, and they can be used more readily because of the extremely wide uncertainty bounds associated with them.

4.10 ASSURANCE OF TECHNICAL QUALITY

To ensure that the quality of any given human-reliability analysis is maintained and that the quality of the several analyses is constant, a program plan for the performance of these analyses should be developed. This plan should be developed by the director of the human-reliability analysis in conjunction with the PRA team leader.

To meet internal quality standards (those relating to any given human-reliability analysis), the plan should provide for scheduling the various stages of the analysis, integrating it into the entire PRA, and monitoring its progress. To this end, dates, places, personnel, and expected results should be identified. Working from the block diagram in Figure 4-2, for example, tables or charts should be set up itemizing each task; the elements necessary for its completion (including personnel); its relation to and/or interfaces with other PRA groups; the date, time, and place of its expected performance; the expected results; and the method of its documentation.

To meet external quality standards (those relating to human-reliability analyses performed for several plants), the plan should provide for cross-plant comparisons. This implies that the team leader for a new PRA should be familiar with the HRA program plan implemented in earlier PRAs, using this information to ensure that the control and documentation of the ongoing analysis are complete.

REFERENCES

Bell, B. J., and A. D. Swain, 1981. A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants, NUREG/CR-2254, draft USNRC report for interim use and comments.

Dougherty, E. M., 1981. "The Human Element in a Probabilistic Risk Assessment," in Proceedings of the Myrtle Beach Workshop on Human Factors and Nuclear Safety, August 1981.

Dougherty, E. M., 1982. "Treating Human Interactions in Risk Assessment," in Proceedings of the ANS Topical Conference on PRA, April 1982, American Nuclear Society, Inc., La Grange Park, Ill.

Embrey, D. E., 1976. Human Reliability in Complex Systems: An Overview, NCSR.R10, National Centre of Systems Reliability, United Kingdom Atomic Energy Authority, Warrington, England.

Embrey, D. E., 1981. "The Use of Quantified Expert Judgment in the Assessment of Human Reliability in Nuclear Power Plant Operation," in Proceedings of the Human Factors Society 25th Annual Meeting, Human Factors Society, Santa Monica, Calif.

Fleming, K. N., et al., 1975. HTGR Accident Initiation and Progression Analysis Status Report, Vol. II, "AIPA Risk Assessment Methodology," U.S. Energy Research and Development Administration, Washington, D.C.

Fleming, K. N., et al., 1978. HTGR Accident Initiation and Progression Analysis Status Report: Phase II Risk Assessment, U.S. Department of Energy, Washington, D.C.

Fleming, K. N., F. A. Silady, and G. W. Hannaman, 1979. "Treatment of Operator Actions in the HTGR Risk Assessment Study," Transactions of the American Nuclear Society, Vol. 33

Hannaman, B., 1981. "Human Factor Considerations in the Accident Initiation and Progression Analysis," in Proceedings of the Myrtle Beach Workshop on Human Factors and Nuclear Safety, August 1981.

Hannaman, G. W., and A. P. Kelley, 1978. "Synthesis of Experience Data for Risk Assessment and Design Improvement of Gas-Cooled Reactors," in Proceedings of the ANS Topical Meeting on Probabilistic Safety, Los Angeles, May 8-10, 1978, American Nuclear Society, Inc., La Grange Park, Ill.

Meister, D., 1971. Comparative Analysis of Human Reliability Models, L0074-107, Bunker-Ramo Electronics Systems Division, Westlake Village, Calif.

Pew, R. W., S. Baron, C. E. Feehrer, and D. C. Miller, 1977. Critical Review and Analysis of Performance Models Applicable to Man-Machine Systems Evaluation, AFOSR-TR-77-0520, U.S. Air Force Office of Scientific Research, Bolling Air Force Base, Washington, D.C.

Raabe, P. H., et al., 1977. HTGR Accident Initiation and Progression Analysis Status Report, Vol. VIII, "Responses to Comments on AIPA Status Report," U.S. Energy Research and Development Administration, Washington, D.C.

Stillwell, W. G., D. A. Seaver, and J. P. Schwartz, 1982. Expert Estimation of Human Error Probabilities in Nuclear Power Plant Operations: A Review of Probability Assessment and Scaling, USNRC Report NUREG/CR-2255 (in press).

Swain, A. D., and H. E. Guttmann, 1980. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, draft USNRC report for interim use and comment.

U.S. Department of Defense, 1981. Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, MIL STD-1472C, Washington, D.C.

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

USNRC (U.S. Nuclear Regulatory Commission), 1981a. Evaluation Criteria for Detailed Control Room Design Review, NUREG-0801.

USNRC (U.S. Nuclear Regulatory Commission), 1981b. Guidelines for Control Room Reviews, NUREG-0700, draft USNRC report for interim use and comment.

Wechsler, D., 1952. Range of Human Capacities, Williams & Wilkins, Baltimore, Md.

Wreathall, J., 1981. "Operator Reliability Model," in Proceedings of the Myrtle Beach Workshop on Human Factors and Nuclear Safety, August 1981.

Wreathall, J., 1982. Operator Action Trees--An Approach to Quantifying Operator Error Probability During Accident Sequences, NUS-4159, NUS Corporation, Gaithersburg, Md.

Chapter 5

Data-Base Development

5.1 INTRODUCTION

Two types of events identified during accident-sequence definition and system modeling must be quantified for the event and fault trees in order to estimate frequencies of occurrence for accident sequences: (1) initiating events (see Section 3.4.2) and (2) component failures, or primary events (see Section 3.5.3.1). This chapter describes how this quantification is performed.*

The quantification of initiating and primary events involves two separate activities. First the reliability model for each event must be established, and then the parameters of the model must be estimated. The quantification also involves various types of data analysis (e.g., a statistical analysis of raw information), the use of generic and specific data, and, in some cases, the collection and use of subjective data. The necessary data include component-failure rates, repair times, test frequencies and test downtimes, common-cause probabilities, and uncertainty characterizations. Also involved is the quantification of human errors, a subject not covered here because it is discussed in Chapter 4.

The objective of the task described in this chapter is to estimate the frequencies of the initiating events and the probability of the primary events identified in accident-sequence definition and system modeling (Chapter 3) and thus to develop a data base for accident-sequence quantification (Chapter 6). It is important to note that the output of this task must be consistent with the general approach chosen and the tools to be used in accident-sequence quantification. Before this task is performed, a decision will have been made as to whether the PRA will use a classical or a Bayesian framework for treating uncertainties. This decision will affect the way data are evaluated. In addition, the tools used in sequence quantification will also affect the data analysis, in that the data must be in a form compatible with the tools. For example, the data analysis may yield probability distributions for reliability models that cannot be exactly represented by any defined distribution (e.g., a gamma or a lognormal distribution), and yet the quantification tools require that all inputs be described by one of a set of predefined distributions. It will be the data analyst's job to make the data output fit this quantification requirement, by finding the "best" distribution to fit the actual result, and then to record any uncertainty (Chapter 12) that is thus introduced in the analysis. Hence, the task described in this chapter is closely linked with the tasks of Chapters 3, 6, and 12.

---

*The numerical quantities obtained by the procedures of this chapter are in a very strict sense estimates; that is, these quantities should be considered judgments of the values for the numerical quantities of interest.

5.2 OVERVIEW

The development of a data base for accident-sequence quantification is a multistep process involving the collection of data, the analysis of data, and the evaluation of appropriate reliability models. It produces tables that specify the quantity to be used for each event in the fault and event trees.

While the task of data-base development may seem to lie between the tasks of accident-sequence development and quantification (Chapters 3 and 6), it is most likely to be accomplished largely in parallel with accident-sequence development.

The steps that need to be addressed in developing a data base are outlined below, in the order the tasks would be accomplished. As in many engineering analyses, the order may be modified as the work progresses, or iteration may be required. It is also possible that time constraints, budget constraints, or study goals may allow, or even require, some steps to be shortened or bypassed. For example, instead of collecting and analyzing raw data, it may be sufficient to use data from a previous PRA study. This could save considerable time and cost, but it may diminish confidence in the results. Figure 5-1 indicates the flow of the steps outlined below.

Selection and Use of Event Models. The data analyst must select several types of models for event quantification: failure models, maintenance models, test models, and initiating-event models. The factors to be considered in these decisions are discussed in Section 5.3.

Data Gathering. Early in the PRA project, the gathering of all information that may be pertinent to events usually included in PRA studies should begin. At this point the development of accident sequences will not have been completed, and hence this early information gathering must rely on previous experience. The information should include published data reports, data from other PRA studies, and available information about the specific plant that is being analyzed. This task is described in Section 5.4.

Estimation of Model Parameters. After the models have been selected, their parameters must be evaluated. Two approaches to parameter estimation, the Bayesian approach and the classical approach, are described in Section 5.5.

Evaluation of Dependent Failures. It is generally recognized that dependent failures may make significant contributions to system unreliability. Section 5.6 addresses various methods available for estimating these contributions.

Uncertainties in Data. A major concern in a probabilistic risk assessment is the issue of uncertainty in the various evaluations. Section 5.7 discusses the factors in data-base development that contribute to uncertainty.

Documentation. The results and the process of data-base development must be documented. Guidelines for documenting the data base in a clear and consistent manner are presented in Section 5.8.

Assurance of Technical Quality. It is very important that the resultant data base be as accurate and as consistent as possible. Procedures for ensuring that the data base is of the best possible quality are presented in Section 5.9.

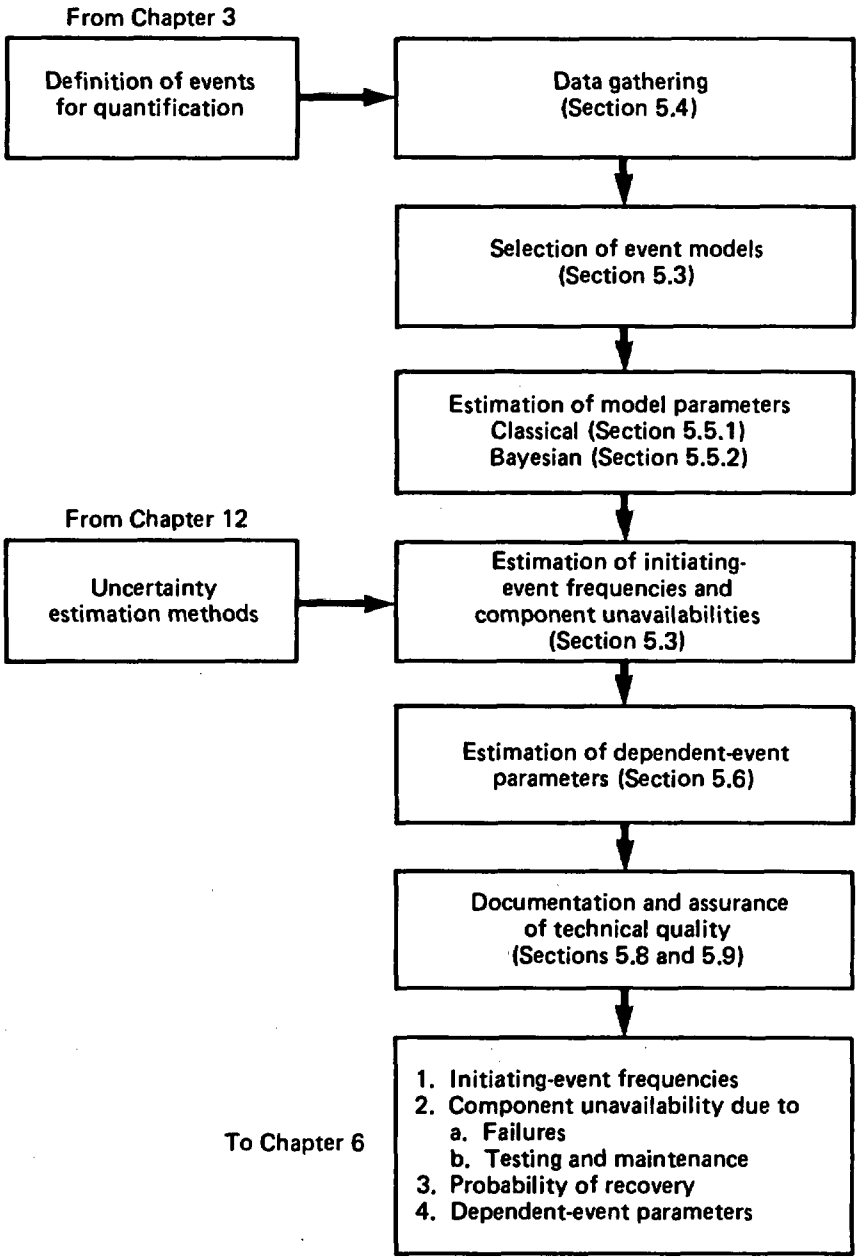


Figure 5-1. Inputs, outputs, and steps in data-base development.

5.3 EVENT MODELS AND THEIR USE

The primary events in the fault trees and event trees can be analyzed with four types of models: component-failure models, test-contribution models, maintenance-contribution models, and initiating-event models. The first three of these models provide estimates of the probability that a plant element cannot accomplish its design function because it has failed, is being tested, or is being maintained. The model for initiating events provides the estimated frequency of the specific event of interest.

5.3.1 COMPONENT-FAILURE MODELS

Component-failure models can be divided into two general types: time-related models and demand models. This section defines both types of models and explains their application.

5.3.1.1 Time-Related Models

5.3.1.1.1 Definition

Reliability as a function of time can be modeled by a number of probability distributions, the more common models being the exponential, the Weibull, the gamma, and the lognormal. Each represents a different type of failure process.

The exponential gives the distribution of time between independent events occurring at a constant rate. The Weibull gives the distribution of time between independent events occurring at a rate that varies in time. The gamma gives the distribution of time required for exactly k independent events to occur, assuming a constant rate of occurrence. An exponential distribution is a gamma with $k = 1$. The lognormal implies that the logarithms of lifetimes are normally distributed. There are also other models that provide for time-dependent failure rates, an example being the inverse Gaussian (Chhikara and Folks, 1977).

In most PRA studies, the exponential is the most commonly used time-to-failure distribution. It is used basically for two reasons: (1) many reliability studies have found the exponential justifiable on empirical grounds and (2) both the theory and the required calculations are simple. It is important to note that, even though the time to failure is not exponential over the entire life of the component, the in-use portion may be exponential. This assumes replacement by a component that is also in its exponential-behavior time period.

The validity of the assumptions underlying the choice of the exponential distribution can be examined by several methods. These methods are not discussed here because most PRAs have not found it necessary to justify their choices of reliability models. Should there be a need to examine the time-to-occurrence distribution, the graphical methods described by Hahn and

Shapiro (1967) and the analytical methods described by Mann et al. (1974) can be used.

In this chapter the exponential distribution will be used to model the time to component failure. The equation for the exponential distribution is

$$U(t) = 1 - e^{-\lambda t} \qquad (5\text{-}1)$$

which represents the cumulative probability that the event has occurred by time t. The parameter λ is the failure rate and is expressed in units of failures per unit time.

5.3.1.1.2 Use of Time-Related Models

Failure in Time: Standby

Many components in a nuclear plant are in a standby mode; that is, they are not used until needed or tested. Often such components are assumed to fail in time while in this standby mode.

Standby components are usually subjected to periodic testing, which occurs, for example, once a month or perhaps once a year. The time between tests is the length of time the component is exposed to failure without detection, and hence the term "fault-exposure time." This time is often designated by τ. The fault-exposure time τ is usually determined from plant procedures, but some caution should be used when examining a system for test intervals. As an example, consider the system in Figure 5-2. This system is tested in various pieces; that is, the logic is tested once a month, as are the spray pumps.

The sensors are calibrated once a year and are tested once a year through the logic. However, the entire system is never tested end to end. This results, in this example, in a specific contact never being tested during the life of the plant. Figure 5-3 focuses on this situation.

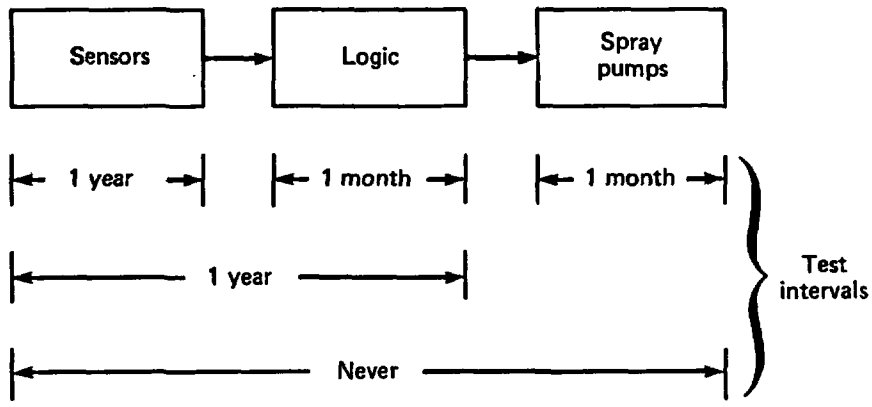


Figure 5-2. Test intervals for sample system.

The logic testing verifies that the coil is energized when the test contact closes and the light is illuminated. However, the contact for pump start is not tested. The analyst then must decide on a value of τ for this contact that is not directly tested during the life of the plant. Indeed, it may be deemed appropriate to assign a τ of 40 years. However, in this case a 40-year value for τ is inappropriate, because the contact is part of a relay that is tested in part and has an associated mean time to failure; thus, the relay will be periodically replaced and the untested contact will be renewed. It is therefore suggested that the τ for the untested element be the reciprocal of the mean time to failure of the tested elements in the relay combined through an OR operation.

In the present example, assume that the coil has a mean time to failure of 20 years and the tested contact has a mean time to failure of 5 years. These can be combined by adding the failure rate, defined to be the reciprocal of the mean time to failure, and then inverting the result; that is, $\tau = \left[(1/20) + (1/5)\right]^{-1} = 4$ years. Thus, it would be appropriate to use $\tau = 4$ years for the contact that is not directly tested.

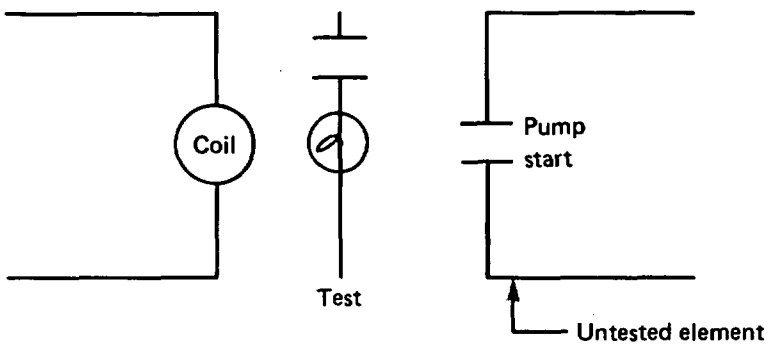


Figure 5-3. Interface schematic.

After determining an appropriate τ for each component that is modeled to fail in time during standby, it is necessary to define the unavailability due to each component's random-failure distribution in time. The expression for the availability of a component that fails in time over a period τ is given by the cumulative distribution function of the time-to-failure distribution for that component. For example, if a component is found to have an exponential failure density function (i.e., $f(t) = \lambda e^{-\lambda t}$), then the unavailability is given by

$$U(t) = 1 - e^{-\lambda t}$$

However, the demand on the safety systems and components occurs randomly in time. Thus, it is necessary to evaluate the unavailability function during the fault-exposure time τ. If it is assumed that the demand can occur with equal likelihood at any point in the τ interval, as it usually does, the

unavailability that should be used is the frequency-weighted unavailability* over the time period τ. Thus,

$$\bar{U} = \frac{1}{\tau} \int_0^{\tau} U(t)\, dt$$

or, for the exponential considered above,

$$U = \frac{1}{\tau} \int_0^{\tau} (1 - e^{-\lambda t})\, dt$$

$$= 1 + \frac{1}{\lambda\tau} (e^{-\lambda\tau} - 1)$$

$$= \frac{\lambda\tau}{2!} - \frac{(\lambda\tau)^2}{3!} + \frac{(\lambda\tau)^3}{4!} - \cdots$$

$$\approx \frac{\lambda\tau}{2}$$

Note that the often-used approximation for the frequency-weighted component unavailability assumes that (1) the failure density function is exponential and (2) higher-order terms of the exponential are negligible.

Failure in Time: Annunciated

For some components, failure is detected immediately (e.g., an annunciated failure). The probability that such a component is not available if needed is related to the frequency of failure and the average time needed to return the component to service. This unavailability is given by

$$U = \frac{\lambda T}{1 + \lambda T}$$

where λ is the failure rate and T is the average total time to respond to the failure, repair the component, and return it to service. Note that if λT is much smaller than unity, the unavailability may be approximated:

$$U \approx \lambda T$$

Failure in Time After Successful Start

It is often necessary to evaluate the probability of a component's starting successfully but failing in time before completing its mission.

---

*The term "frequency-weighted unavailability" is used here to distinguish between this quantity and a similar quantity, average (un)availability. See a reliability text, such as that by Barlow and Proschan (1975), for the definition and use of the term "average availability."

The mission time is here designated τ^*. The probability that a component fails before τ^* is given by the cumulative distribution function. For the exponential case,

$$R(\tau^*) = 1 - e^{-\lambda\tau^*}$$

$$\approx \lambda\tau^*$$

It should not be assumed that the failure rate λ in this case is the same as the failure rate in standby. Indeed, in estimating the rate for failures occurring after a successful start, the analyst must take into account any adverse environment as well as recognize differences between the rates of standby and operation failures.

Often, failure to start on demand and failure to run for some time τ^* are both included in the tree. It must be noted that failure to run is dependent on a successful start; that is, the probability of failure to run for τ^* hours must be modified by the probability of successful start. There are two possible approaches to modeling this combination in the fault trees: (1) as dependent events or (2) as one event.

If failure to start and failure to continue running after starting are separate events, they should be modeled as mutually exclusive events (see Figure 5-4).

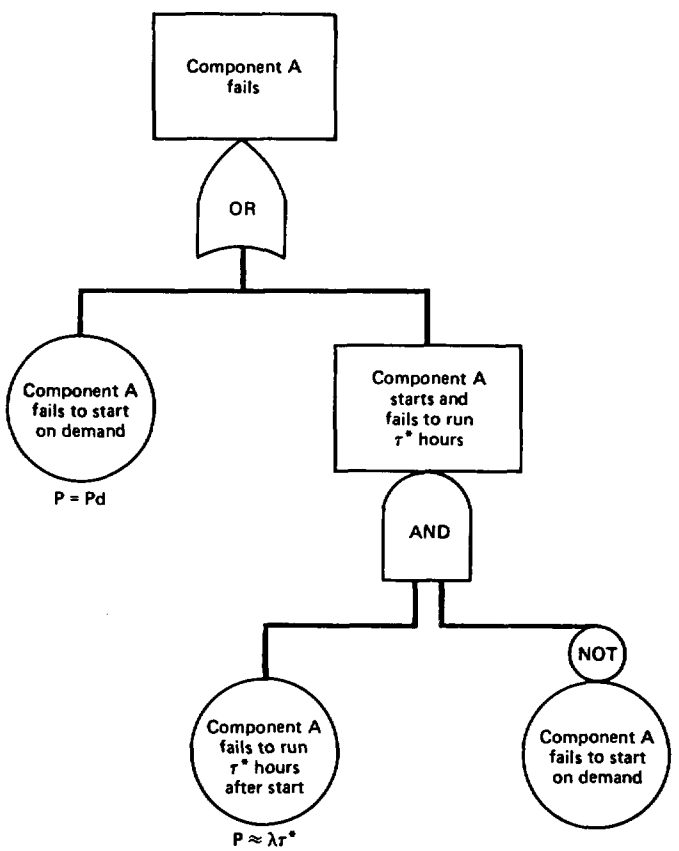


Figure 5-4. Modeling of mutually exclusive events.

If both modes are treated as one event, then

$$P_E = P_F + (1 - P_F)\ \lambda\tau^*$$

That is, the model accounts for the probability of failure to start on demand plus the probability of a successful start and failure to run for τ^* hours.

Recovery

It is possible that some events can be reversed in time to prevent core damage. There are data that provide recovery times for the loss of offsite power and emergency power. For accident sequences that are initiated by a loss of offsite power and the subsequent failure of all emergency diesels, recovery within a specified time can prevent core damage.

Such events can be broken into two parts: (1) frequency of loss or failure and (2) probability of recovery by time t, given loss or failure. This process is illustrated by the example given below, using point estimates. The data used in this example should not be taken for an actual assessment, though the results should be comparable with those of an actual assessment.

Example: Total Loss of AC Power (Station Blackout)

Loss of Offsite Power. The distribution for the duration of an offsite-power loss is given below. The data were collected from 46 sites where 45 losses occurred in 313.03 site-years, the rate of loss being .144 per site-year.

Duration (hours)	Percentage of events
<2	70
2 to 4	3
4 to 8	15
>8	12

Diesel Failure. Data from 36 plants were used to estimate the failure of diesel generators to start. If a configuration of three diesels is assumed and one diesel is needed for an adequate supply of power, the relevant probabilities for failure to start are as follows:

P(diesel 1 fails to start) = .0261

P(diesel 2 fails to start|diesel 1 has failed) = .234

P(diesel 3 fails to start|diesels 1 and 2 have failed) = .552

P(all three diesels fail to start) = .00337

The repair-time probabilities are

P(diesel not repaired within 2 hours) = .66

P(diesel not repaired within 4 hours) = .47

P(diesel not repaired within 8 hours) = .23

Probability of Station Blackout Given Duration. First we define the following:

D = duration of station blackout

L = duration of loss of station power

G = duration of diesel unavailability

S = event station blackout occurs in a year

Then for some period of time t,

$$P(D > t|S) = P(L > t \text{ AND } G > t|S)$$

$$= P(L > t|S)\ P(G > t|S) \quad \text{(assuming independence)}$$

If F_D is the failure of all diesels on demand and F_L is the loss of offsite power in a year, then assuming independence between diesel and offsite-power failures,

$$P(S) = P(F_D)\ P(F_L)$$

the probabilities being

$$P(F_L) = .144$$

$$P(F_D) = .0034$$

and

$$P(S) = 4.9 \times 10^{-4}\ yr^{-1}$$

Then

$$P(S \text{ and } D > t) = P(D > t|S)\ P(S)$$

For t = 2 hours:

$$P(S \text{ and } D > t) = (.30)\ (.66)\ (4.9 \times 10^{-4})$$

$$= 9.7 \times 10^{-5}\ yr^{-1}$$

For t = 4 hours:

$$P(S \text{ and } D > t) = (.27)\ (.47)\ (4.9 \times 10^{-4})$$

$$= 6.2 \times 10^{-5}\ yr^{-1}$$

For t = 8 hours:

$$P(S \text{ and } D > t) = (.12)\ (.23)\ (4.9 \times 10^{-4})$$

$$= 1.3 \times 10^{-5}\ yr^{-1}$$

5.3.1.2 Demand Model

Another type of model for describing component failures is the demand model. It is used to describe the failure of a component at the time of a demand for its use. The number of failures in n trials is described by the binomial distribution, and the demand model is appropriate for components that are in a dormant state until the moment of need, when they are switched on. The underlying assumption is that at each demand the probability of failure is independent of whether or not a failure occurred at any previous demand. The demand model is one that will be carried through this chapter and has been commonly used in PRAs.

The equation for the binomial distribution is as follows:

$$Pr(X \leq r) = \sum_{x=0}^{r} \binom{n}{x} p^x (1 - p)^{n-x} \qquad (5\text{-}2)$$

It gives the probability of r or fewer failures in n independent trials, given the probability of failure in a single trial is p. The parameter needed in this model is p, the probability of failure at each demand.

5.3.1.3 Demand Model vs. Time-to-Failure Model

Several very important factors should be taken into account when using the demand model. If the event being considered really could occur before the demand, then using the demand model "lumps" the failure rate into the instantaneous time of the demand. Thus, for different demand rates the probability of failure would actually be different, and if the demand model is used, a reasonable estimate is obtained only if the demand rates are similar. A component that behaves exactly as the demand model will have the same probability of failure on demand whether the demand occurs once per hour or once per decade.

The relationship between a failure-on-demand model and a failure-in-time model (assuming a constant failure rate) can easily be seen mathematically. The following assumptions are typical of this situation:

1. Component failures can be detected only at tests that occur every τ hours.

2. Components found failed are immediately repaired or replaced; components found operable are returned to service in working condition.

The data from such a situation yield x failures in N tests. The probability of failure on demand is P = x/N. Note that the results from successive tests are independent and that the exponential distribution allows a component to be considered as good as new after the test. Thus the number of tests failed has a binomial distribution with parameters N and $1 - e^{-\lambda\tau}$. The maximum-likelihood estimate (MLE) of $1 - e^{-\lambda\tau}$ is x/N, and thus the MLE of λ is

$$\hat{\lambda} = -\frac{1}{\tau} \ln(1 - P)$$

For small P, $\hat{\lambda} \approx P/T$, which is the usual estimate for $\hat{\lambda}$. However, this approximation is nonconservative. For example, if half the tests are failed,

$$\hat{\lambda} = \frac{\ln 2}{\tau} = \frac{0.69}{\tau}$$

where the approximation yields

$$\hat{\lambda} \approx 0.5/\tau$$

If it is necessary to obtain a new probability of failure on demand, P_1, for a new test period τ_1, the above relationships must be considered. The new demand probability is

$$\hat{P}_1 = 1 - \exp(-\hat{\lambda}\tau_1)$$

$$= 1 - \exp\left[-\frac{\tau_1}{\tau} \ln(1 - P)\right]$$

$$= 1 - (1 - P)^{\tau_1/\tau}$$

For example, if $P = 1 \times 10^{-2}$, τ = 720 hours (1 month), and τ_1 is 1 year, then $\tau_1/\tau = 12$, and

$$\hat{P} = 1 - \left[1 - (1 \times 10^{-2})\right]^{12} = 1.14 \times 10^{-1}$$

5.3.2 TEST CONTRIBUTIONS TO COMPONENT UNAVAILABILITY

Some test activities render a component or group of components unavailable to the system should a demand occur. Such an activity should appear on the appropriate tree as a separate event.

The probability that a component will be in testing when a demand occurs is simply the frequency of the test multiplied by the average

duration of the test, normalized by the time between the start of tests. For example,

$$P_T = \frac{(1 \text{ test/month})(L_T \text{ hr})}{730 \text{ hr/month}}$$

Here L_T is the average length of a test that occurs once every month.

The model often used in PRAs for the time to complete a test is the lognormal distribution. Although this assumption has not been extensively tested, several studies have found the lognormal distribution to provide a reasonable fit (Lapides, 1975; USNRC, 1975, Appendix III; McClymont and McLagan, 1982).

The equation for the lognormal distribution is

$$C(t) = \frac{1}{\sigma\sqrt{(2\pi)}} \int_{-\infty}^{\ln t} \exp\left[-\frac{(y-\mu)^2}{2\sigma_2}\right] dy \quad \sigma^2 \qquad (5\text{-}3)$$

This equation represents the cumulative probability that the event has been completed by time t. The parameters σ and μ can be expressed in other terms:

$$\mu = \ln M$$

$$\sigma = \frac{\ln(EF)}{1.64}$$

where the parameter M is the median time to completion and the error factor EF is the quantity that, when multiplied by the median, gives the time of completion that is equal to or longer than 95 percent of all times to complete the event.

Sections 5.5.1 and 5.5.2 show how to estimate the parameters of a lognormal time-to-completion distribution as either distributions or point estimates with confidence limits. Methods for propagating these uncertainty measures can be found in Chapter 12. These methods can be used to estimate the distribution or point estimate with confidence limits for P_T from the parameter distributions or point estimates and confidence limits. The quantity P_T is then the input required for the accident-sequence quantification discussed in Chapter 6.

5.3.3 MAINTENANCE CONTRIBUTIONS TO COMPONENT UNAVAILABILITY

A maintenance act is considered to be any unscheduled activity that causes a component or system to be taken out of service. It may be expected that repair takes place, but this repair may vary from the very simple to the very complex.

The evaluation of the maintenance contribution is similar to that of testing, except that maintenance acts occur randomly in time, whereas for

tests the time is fixed. The Reactor Safety Study (USNRC, 1975, Appendix III), for example, found that the time of maintenance for all components could be modeled by a lognormal distribution with 5th and 95th percentile points of 1 and 12 months, respectively. In most cases, it may be expected that the frequency of maintenance will exceed the frequency of failure for a component in the fault tree because the number of component failures requiring maintenance far exceeds the number of failures that completely negate a component's ability to function in its safety role. A good example is a motor-operated valve that must open to successfully perform its safety role. Failure to open occurs less frequently than valve-stem leaks, which require the valve to be taken out of service for repacking, but do not directly negate the safety role of the valve.

The probability that a component is in maintenance when a demand occurs is shown below as

$$P_M = \frac{f_M L_M}{1 + f_M L_M}$$

In this expression, f_M is the average frequency of required maintenance and L_M is the average length of the maintenance.

The lognormal distribution (see Equation 5-3) can be used for the time to complete maintenance, while the frequency of occurrence may be lognormal or exponential. Sections 5.5.1 and 5.5.2 show how to estimate the parameters of both the lognormal and the exponential distributions as either distributions or point estimates with confidence limits. Chapter 12 gives the methods for propagating the distribution or point estimate with confidence-limit parameters to the event P_M, which will then be a distribution or a point estimate with confidence limits. The quantity P_M, then, is the required input for accident-sequence quantification (Chapter 6).

5.3.4 INITIATING-EVENT MODELS

Initiating events are the occurrences that initiate an accident sequence. The desired measure for such events is frequency. A plant may experience tens of these events per year or only one in 10,000 years.

Initiating events are assumed to occur randomly in time, and they are usually assumed to occur at a constant rate. However, data on events that occur more frequently indicate that the rate of occurrence may be higher during the plant's first years than during subsequent years. There are insufficient data to predict whether or not the frequency of these initiators might increase in later life.

For purposes of this chapter it is assumed that the model for initiating events will be based on a constant rate of occurrence (the Poisson model).

It should be noted that in most PRAs initiating events are treated as single events. However, the initiating event can be quantified by

combining several events. This combination can be accomplished through a fault tree, an event tree, or a similar tool. While this may not affect the underlying event modeling and data analysis, it may require quantification tools that differ from those used to evaluate system/sequence frequency-weighted unavailability via fault trees, event trees, etc. That is, it may be necessary to quantify the synthesized initiating event as a frequency, rather than a probability.

5.4 DATA GATHERING

Before collecting and analyzing data, it is important to know what kind of data are needed. In a PRA the events of interest are modeled as events that occur randomly. In general, they occur either randomly in time or randomly at each challenge. Thus, for each classification of events, data will be either x events in time T or x events in n trials (or demands). In addition, if it is necessary to test the component-reliability models, the actual time history of the failures is needed. More specifically, if the failure of motor-operated valves to open when needed is a class of events to be evaluated, it will be necessary to search data sources to determine the number of occurrences for this event, either the number of demands or the time over which these events occurred, and when each failure to open occurred. It will also be useful to examine other data bases for information about the event of interest.

In general, for events involving components in safety systems, the quantity of interest is the probability that the component cannot perform its intended function when the initiating event occurs.

Thus, the objective of the data-gathering task is to obtain the raw information needed for estimating the event-model parameters identified in the preceding section: (1) the number of failures in time or the number of demands for reliability models; (2) the frequency and duration of tests for systems or components; (3) the frequency and duration of maintenance on components; and (4) the frequency of initiating events. The data may also be used to test the applicability of the event model; in this case, it is necessary to have the time of each failure. The sources of data may include plant records, existing data reports, and previous PRAs. This section describes various sources of available data and their attributes; it then discusses the process of data collection. It is strongly recommended that representative existing data sources be closely examined to establish clearly the type of data needed before beginning the collection of plant data.

5.4.1 EXISTING DATA SOURCES

As the data analyst proceeds to determine the appropriate reliability data, he finds a spectrum of available resources. In some cases a clearly appropriate source is available. In other instances, however, there are few sources of data whose content and format allow unambiguous selection. The

data analyst must decide on the appropriateness of the data he examines. The data source does not always specify what failure modes or mode is represented; whether, for example, the pump driver is included in all pump failures; what environment is applicable; or what the total population is. Often, additional research may be needed to discover the information not available in the reported data. Discussed below are the following sources that may be useful in building a data base for a PRA:

1. A report (EPRI, 1982a) on anticipated transients without scram.

2. A report (EPRI, 1982b) on the loss of offsite power at nuclear power plants.

3. A report (McClymont and McLagan, 1982) on diesel-generator reliability at nuclear power plants.

4. Data summaries of the licensee event reports submitted to the Nuclear Regulatory Commission.

5. The Reactor Safety Study (USNRC, 1975).

6. An IEEE data manual on electronic, electrical, and sensing components.

7. The Nuclear Plant Reliability Data System.

8. The National Electric Reliability Council.

A substantial number of other sources are summarized in Appendix C.

ATWS: A Reappraisal, Part III, "Frequency of Anticipated Transients," EPRI NP-2330. Published in 1982 by the Electric Power Research Institute (EPRI), this report contains information on the type and frequency of initiating events that lead to reactor scram. The information was gathered from about 60 percent of the nuclear power plants in the United States. Initiating events like pipe breaks are not included. The data are presented as incidents that resulted in a reactor scram and are sorted into categories. Since data analysis is minimal, the user must extract the information as needed and perform the necessary analysis.

Loss of Off-Site Power at Nuclear Power Plants: Data and Analysis, EPRI NP-2301. This 1982 report presents data on the frequency of loss and subsequent recovery of offsite power at nuclear power plants. The data were collected from the sites of 47 plants. Results are presented as events per site and by National Electric Reliability Council region. Data analysis includes point estimates for frequency with confidence limits, assuming a constant rate of occurrence. Recovery time is analyzed with a lognormal distribution for the time to recover. All raw data are reported to allow the user to perform his own analysis. This document is the most comprehensive source of data on the loss of offsite power for PRA usage.

Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis, EPRI NP-2433 (McClymont and McLagan, 1982). This report presents data related to the reliability of emergency diesel generators.

The sources include plant records, utility records, and licensee event reports submitted to the Nuclear Regulatory Commission. The data include both raw information and estimates of event-model parameters. The report details failure to start, failure to continue running, and repair times.

Data Summaries of Licensee Event Reports at U.S. Nuclear Power Plants. Published by the Nuclear Regulatory Commission, these data summaries are available as six separate reports:

1. Diesel Generators (NUREG/CR-1362; EG&G-EA-5092).

2. Pumps (NUREG/CR-1205; EG&G-EA-5044).

3. Valves (NUREG/CR-1363; EG&G-EA-5125).

4. Selected Instrumentation and Control Components (NUREG/CR-1740; EG&G-EA-5388).

5. Primary Containment Penetrations (NUREG/CR-1730; EG&G-EA-5188).

6. Control Rods and Drive Mechanisms (NUREG/CR-1331; EG&G-EA-5079).

They describe the results of analyses of component failures reported to the Nuclear Regulatory Commission in licensee event reports. Component failures are reported for individual plants, by reactor vendor, by failure mode, and for all plants considered together. Included are failure rates, failures on demand, and some information on repair times. The estimates of event-model parameters, however, are based on estimates of population, demands, and exposure time. Hence, the statistical analysis includes estimated information together with actual plant data.

Reactor Safety Study, WASH-1400, Nuclear Regulatory Commission, 1975. Appendix III of this report, "Failure Data," contains the failure data used in the study, including raw data from 1972, notes on test time, notes on maintenance time and frequency, the results of a human-reliability analysis, aircraft-crash probabilities, estimates of the frequency of initiating events, and some information on common-cause failures. From the assembled information, this appendix also defines the "assessed range" for each failure rate. The authors state, however, that "this data may not be sufficiently detailed, general, or accurate enough for use in other quantitative reliability models or in applications involving greater specificity."

IEEE Project 500 Data Manual, Institute of Electrical and Electronics Engineers, Inc. This document contains data for electronic, electrical, and sensing components. The reported values are mainly synthesized from the opinions of some 200 experts. Each expert has submitted a low, a recommended, and a high value for the failure rate under normal conditions and a maximum value that would be applicable under all conditions (including abnormal ones). The pooling of estimates was done by geometric averaging, a method judged to be a better representation of expert estimates, which are often given as negative powers of 10. While some estimates include hard

data, the reader is not made aware of which estimates are based only on opinion, on hard data, or a combination of both.

Nuclear Plant Reliability Data System (NPRDS), Southwest Research Institute. The NPRDS collects failure data on safety-related systems and components. At present, 61 plants are reporting data. The data are compiled and disseminated in periodic reports to the participants of the program and other potential users. In addition, special searches of the data base may be requested by the participants and others, or the users can access the data through their computer terminals. Typical information that NPRDS provides includes the following:

1. The plant operating mode (i.e., operating, standby, and shutdown).
2. The calculated in-service hours of the system.
3. Outage times.
4. Number of failures per million in-service hours.
5. Number of applicable tests.
6. Number of actuations for standby equipment.
7. Component failure modes and effects.

The main disadvantage is the dependence of the NPRDS on regular participant reporting. If no report is received from a participant in a reporting period, it is assumed that no failures have occurred. In the near future, data from plants with irregular reporting will be filtered from the data base to avoid this disadvantage.

National Electric Reliability Council (NERC). On January 1, 1979, the Edison Electric Institute (EEI) transferred to NERC the responsibility for operating its equipment-availability data system--the prime utility-industry source for the collection, processing, analysis, and reporting of information on power-plant outages and overall performance. The Unit Year Summary computer program produces a report for each individual unit, including statistics for the latest year and cumulative statistics for the life of the unit. In addition, the Equipment Availability Task Force produces annually a report on equipment availability for a 10-year period. Finally, the EEI has established a procedure for processing special requests for the analysis of reliability data.

5.4.2 COMPONENT-DATA COLLECTION FROM NUCLEAR POWER PLANTS

At present, no nuclear plant keeps records of component reliability for the specific purpose of using them as data for risk assessments. The PRAs that have been conducted to date have had to depend on other sources for plant-specific data. These sources include many plant records and procedures that may be available to the PRA analysts. The usefulness of a particular source depends on the reliability models chosen to represent components in system fault trees. On the other hand, the availability (or the absence) of various data sources may affect the choice of models by a system analyst. Table 5-1 lists the most common parameters used to represent components, the data required to derive estimates of the parameters, and the potential sources of such data at plants. How these sources can be used to extract needed information is briefly explained below.

Table 5-1. Sources of plant data

Parameter	Data requirements	Potential sources
1. Probability of failure on demand	a. Number of failures	Periodic test reports, maintenance reports, control-room log
	b. Number of demands	Periodic test reports, periodic test procedures, operating procedures, control-room log
2. Standby failure rate[a]	a. Number of failures	See 1a above
	b. Time in standby	Control-room log
3. Operating failure rate[a]	a. Number of failures	See 1a above
	b. Time in operation	Control-room log, periodic test reports, periodic test procedures
4. Repair-time distribution parameters	Repair times	Maintenance reports, control-room log
5. Unavailability due to maintenance and testing	Frequency and length of test and maintenance	Maintenance reports, control-room log, periodic test procedures
6. Recovery	Length of time to recover	Maintenance reports, control-room log
7. Human errors[b]	a. Number of errors b. Opportunities	Maintenance reports, control-room log, periodic test procedures, operating procedures

[a]See Section 5.3.1.1.

[b]While this chapter does not deal with the evaluation of human errors, it is likely that a search for plant-specific data would find human-error data to supplement the analysis methods described in Chapter 4.

5.4.2.1 Periodic Test Reports and Procedures

Periodic test reports and procedures are a potential source of data on failures, demands, and operating time for components that are tested periodically. Test reports for key components or systems typically contain a description of the test procedure and a checklist to be filled out by the

tester as the steps are performed. For example, in an operating test of an emergency diesel generator, the procedure may call for starting the diesel and running it for an hour. The record of a specific test would report whether or not the diesel started and whether it ran successfully for the entire hour. Another example is a test of emergency system performance, in which the procedure calls for the tester to give an emergency signal that should open certain flow paths by moving some motor-operated valves and starting one or more pumps. The position of the valves and the operation of the pump are then verified, giving records of whether the valves and pumps responded successfully to the demands. As shown by these examples, records of periodic tests provide a self-contained tally of demands on some components, as well as the failure (and success) of the component given these demands.

When failures are reported in periodic tests, however, the failure mode should be examined carefully, if possible, before the failure is included in a failure-parameter estimate to be used in system fault trees. In the diesel-generator example, the report may note that the result of the test was unsatisfactory because the diesel tripped on a signal of low oil pressure, high oil temperature, or the like. Since many of these trips are disabled by a LOCA signal, such an event should not be counted in deriving a failure-parameter estimate for a fault tree that is part of a LOCA sequence, even though the test report indicated an unsatisfactory performance by the diesel generator. If, on the other hand, the diesel would have failed if the trip was bypassed, it must be counted as a failure. Similarly, a test report on diesel-generator operability may log an unsatisfactory result due to an air-compressor failure. Such a failure would cause a diesel-generator failure to start only if it occurred in conjunction with a leak in the diesel air tank. In this instance, the test report indicates a failure even though no actual demand was placed on the diesel.

If the records of actual periodic tests are not readily available, the test procedures can be used to estimate the number of testing demands or the operating time during tests for a component over a period of time. To do this, the number of demands or the operating time of a single test can be multiplied by the frequency of the test and the pertinent calendar time. Of course, this approach is valid only if the tests are conducted at the prescribed frequency. Some tests may in fact be conducted at more frequent intervals than those stated in the procedures. Plant personnel should be interviewed to determine what adjustments are necessary.

If this approach is used, a count of failures must be obtained from different sources (e.g., maintenance reports). Since these sources may not indicate clearly which failures occurred during the periodic tests considered, the failure-parameter estimates derived by this approach are probably conservative. In order to correctly match failures with demands or operating time for a component, the number of demands or the duration of operating time occurring outside periodic tests must be obtained. Such information is usually much more difficult to extract from typically available data sources.

5.4.2.2 Maintenance Reports

Reports of maintenance on components are potential sources of data on failures, repair times after failure, and other unavailability due to maintenance. These reports typically include the following:

1. A plant identification number for the component undergoing maintenance and a description of the component.

2. A description of the reason for maintenance.

3. A description of the work performed.

4. An indication of the time required for the work or the duration of the component's unavailability.

The report may indicate that maintenance was needed because the component failed to operate adequately or was completely inoperable. Such an event may then be added to the count of component failures. The maintenance report often gives information about the failure mode and mechanism as well as the amount of time spent on repair after the failure was discovered. Such information must be interpreted carefully, because the actual repair time may cover only a fraction of the time the component was unavailable between the detection of the failure and the completion of repairs. In addition, the repair time is often given in terms of man-hours, which means that the actual time spent on repair could be shorter, depending on the size of the work crew; the use of recorded man-hours would therefore lead to a conservative estimate of repair time. The complete out-of-service time for the component can, however, be derived, because the maintenance record often states the date on which the failure was discovered and the date on which the component was made available after repair.

Maintenance reports that record preventive maintenance can be used to estimate the contributions of these actions to component unavailability. Again, the report may show that a component was taken out of service on a certain date and restored some time later, giving a sample of the duration of maintenance. The frequency of these events can be derived from the number of preventive-maintenance reports in the calendar time considered.

Unfortunately, not all maintenance reports present all of the information listed above. Often, the descriptions of a component's unavailability or the work performed are unclear (or missing altogether), requiring guesswork as to whether an unfailed component was made unavailable by maintenance or whether the maintenance was the result of component failure. An additional problem that has already been mentioned is the difficulty in matching up the failures recorded in maintenance reports with the demands or operating times reported in other documents.

5.4.2.3 Operating Procedures

Operating procedures can be used to estimate the number of demands on certain components in addition to demands occurring during periodic tests.

This estimate is obtained by multiplying the number of demands imposed on a component during a procedure by the number of times the procedure was carried out during the calendar time of interest. Unfortunately, the latter number is not always easily obtained. For procedures followed during plant startup or shutdown, the number of times the procedure was performed should be readily obtainable, but for procedures followed during operation, this information will be available only from the control-room log.

5.4.2.4 Control-Room Log

Many of the gaps in a component-reliability data base compiled from test and maintenance records can be filled by examining the control-room log, which is a chronological record of important events at the plant. For example, the log has records of demands made (e.g., pumps and diesel generators) at times other than periodic tests. It notes the starting and stopping times for these components, thus supplying operating-time data. The log also notes the initiation of various operating procedures, thus adding to the information about demand. Furthermore, it records periods when certain components and systems are out of service, and in this the log is often more accurate than the maintenance reports.

There is, however, a problem with using the control-room log as a source of component data: all events in the log are listed chronologically, without being separated by system, type of event, or any other category. The analyst must therefore search through many irrelevant entries to find those needed for the data base. The additional accuracy that is supplied to the estimates of component-failure parameters by data from the log may not be worth the effort needed to search through several years of the plant history recorded in the log.

5.5 ESTIMATION OF MODEL PARAMETERS

After model selection, the parameters of the models can be estimated. Two methods of estimation are described in this chapter and are complemented by the relevant methods in Chapters 6 and 12: (1) classical methods and (2) Bayesian methods.

A Bayesian analysis allows the augmentation of available data by quantified personal opinion. The analyst quantifies his belief about the parameters (unknown constants) in the model, exclusive of the information in the data, by a probability distribution; that is, he not only models the occurrence of accidents probabilistically but also develops a probability model for his beliefs about such occurrences. The data analyst should be aware that this may be difficult to do, and it will be even more difficult to convince the community at large to adopt his degree of belief as their own.

In a classical analysis, knowledge and expertise also play a role, but less formally, in general serving only as aids in choosing probability models and relevant data. For example, data obtained under normal operating conditions may or may not be applicable to accident conditions. An understanding of the situation is needed to resolve this question. Once such questions are resolved, a classical analysis lets the data "speak for themselves." The users of a classical analysis must be aware that limited data can lead to imprecise estimates. Though the introduction of a quantified degree of belief can improve the apparent precision of risk estimates, it may be useful and informative to do both a Bayesian and a classical analysis, thus allowing the reader of a PRA to separate the data and the belief components of the results.

5.5.1 CLASSICAL ESTIMATION

5.5.1.1 Point Estimation

Reliability and availability models involve a variety of parameters, such as component-failure rates and expected repair times, that need to be estimated in order to estimate the probability of specific accident sequences. Choosing a point estimate can involve a variety of considerations, depending on the information available. If data are available and it is desired to obtain estimates that are strictly functions of the data, then, for the models commonly used in risk analysis, point estimators are well established. The point estimators generally used for the binomial, Poisson, and lognormal models, and appropriate data, are given below.

Binomial Distribution. The data, parameter, and estimate for binomial models are as follows:

Data: f failures in n demands. The number of demands is known; the outcomes, success or failure, are statistically independent; and the failure probability is constant across these demands.

Parameter: p, the probability of failure on demand (dimensionless).

Estimate:

$$p^* = f/n$$

Poisson Distribution. For Poisson models, the data, parameter, and estimate are the following:

Data: f failures (or occurrences of an initiating event) in T time units. The quantity T is known; failures occur independently and at a constant rate in time and across different items, which may be combined to obtain the data.

Parameter: λ, the failure rate (number of failures per unit time).

Estimate:

$$\lambda^* = f/T$$

Lognormal Distribution. The data, parameters, and estimates for lognormal models are as follows:

Data: n independent positive observations, $X_1, X_2, \ldots, X_n$, such as repair times, whose logarithms are modeled as being normally distributed.

Parameters: μ, the expected value of $t = \log_e(X)$ and σ^2, the variance of t.

Estimates:

$$\mu^* = \sum_{i=1}^{n} \frac{t_i}{n} = \bar{t} \quad \text{for the sample mean}$$

$$\sigma^{2*} = \frac{\sum(t_i - \bar{t})^2}{n - 1} = s_t^2 \quad \text{for the sample variance}$$

All the estimates given here are unbiased, which means that, on the average, they equal the parameter being estimated. Moreover, all but σ^{2*} are maximum-likelihood estimators. Additional details pertaining to these estimates are available in a text by Mann et al. (1974), which also provides statistical estimators for other models, such as the Weibull and gamma distributions, and other situations, such as a fixed number of failures/random operating-time estimates of the failure rate λ.

Classical point estimates are attempts to identify single parameter values indicated by the data. As such, they are data summaries, and information is necessarily lost in the summarization. The loss is serious in the case of point estimation because the amount of data going into the estimates is lost. For example, one failure in 10,000 hours yields the same point estimate of a failure rate as do ten failures in 100,000 hours, but clearly more information is present in the latter case. If this information is ignored or not communicated, an incomplete analysis results. Two classical methods by which the amount of information pertaining to parameters of interest can be conveyed are standard errors and statistical confidence intervals.

5.5.1.2 Standard Errors

If the data-yielding process described above is repeated, the parameter estimates will vary; that is, in another n demands or T time units, the number of failures will vary (in a manner described by the probability models used to analyze those data). Furthermore, the n repair times collected in the future would differ from those observed at present. The variance over such repetitions of the estimators described above provides a measure of the information contained in the point estimates obtained. The larger the variance, the less reliable the point estimate. In general, the variance of an estimator is not known, but it can be estimated in these cases. The square

root of the estimated variance of an estimator is termed the "standard error of the estimate." For the parameters considered in the preceding section, the standard errors (s.e.) are as follows:

Binomial:

$$\text{s.e. } (p^*) = \left[\frac{p^*(1 - p^*)}{n}\right]^{1/2}$$

Poisson:

$$\text{s.e. } (\lambda^*) = \left(\frac{\lambda^*}{T}\right)^{1/2}$$

Lognormal:

$$\text{s.e. } (\mu^*) = \frac{\sigma^*}{n^{1/2}}$$

$$\text{s.e. } (\sigma^{2*}) = \sigma^{2*}\left(\frac{2}{n - 1}\right)^{1/2}$$

(The information contained in an estimated variance is usually conveyed by reporting the degrees of freedom, n - 1 in the case considered here, rather than a standard error.)

One way in which standard errors are used is to obtain approximate classical confidence limits on the parameter of interest. For example, the point estimate plus or minus twice its standard error provides a crude 95-percent confidence interval on the parameter. Thus, a large standard error, relative to the point estimate, indicates that the data do not provide a very clear indication of the parameter. If only a point estimate is given, this information about the data is lost, and an unwarranted and misleading aura of precision may result. Without standard errors, any comparison of point estimates, say for the purpose of ranking accident sequences, may be misleading.

5.5.1.3 Interval Estimation

A given set of data, say f failures in T hours, can occur in sampling from a variety of Poisson distributions. That is, many other values of λ besides $\lambda^* = f/T$ can give rise to this particular outcome. Some values of λ, however, are more consonant with the data than others. This realization is the basis for classical confidence intervals, whose purpose is to identify ranges of parameter values that are consonant with the data to some specified extent. For example, suppose an upper 95-percent limit on λ is found to be $\lambda_{95} = 10^{-4}$ failures per hour. This means that, for λ values greater than 10^{-4}, the observed data are in the extreme 5 percent of possible outcomes; such λ values are not very consistent with the data. Values

of λ less than 10^{-4} are less unconsonant with the data. Both upper and lower confidence limits, at any specified confidence level, can be obtained, and the interval between these limits is termed a "classical confidence interval." Classical confidence intervals have the property that, in repeated sampling, the probability that the confidence interval will contain the parameter of interest is at least at the specified confidence level.

As indicated above, approximate confidence intervals on a parameter can be obtained from a point estimate and its standard error. For the three distributions considered here, though, exact confidence limits or better approximations can be readily obtained.

Binomial Distribution

The upper $100(1 - \alpha)\%$ confidence limit on p is obtained by solving

$$\alpha = \sum_{x=0}^{f} \binom{n}{x} p^x (1 - p)^{n-x}$$

for p. The lower $100(1 - \alpha)\%$ confidence limit on p is obtained by solving

$$\alpha = \sum_{x=f}^{n} \binom{n}{x} p^x (1 - p)^{n-x}$$

for p. Tables, slide rules, and computer programs are available for solving these equations (Green and Bourne, 1972; Hald, 1952). A useful approximation for small f, large n is

$$P_U(1 - \alpha) = \frac{\chi^2(2f + 2; 1 - \alpha)}{2n}$$

$$P_L(1 - \alpha) = \frac{\chi^2(2f; \alpha)}{2n}$$

where $P_U(1 - \alpha)$ and $P_L(1 - \alpha)$ are the upper and the lower $100(1 - \alpha)\%$ confidence limits, respectively, and $\chi^2(m, \gamma)$ denotes the 100 γ-percentile of the chi-squared distribution with m degrees of freedom. The interval between $P_L(\alpha)$ and $P_U(\alpha)$ constitutes a $100(1 - 2\alpha)\%$ confidence interval.

Poisson Distribution

The upper and the lower $100(1 - \alpha)\%$ confidence limits on λ are obtained by solving the following equations:

$$\lambda_U(1 - \alpha) = \frac{\chi^2(2f + 2; 1 - \alpha)}{2T}$$

$$\lambda_L(1 - \alpha) = \frac{\chi^2(2f; \alpha)}{2T}$$

Note that, mathematically, confidence limits on a failure rate λ are similar to those on a failure probability p, with time units replacing the number of demands.

Lognormal Distribution

The upper and the lower $100(1 - \alpha)\%$ confidence limits on μ are obtained from

$$\bar{t} \pm t(n - 1, 1 - \alpha)(\sigma^*/n^{1/2})$$

where $t(f,\gamma)$ denotes the γ-percentile of the Student's t distribution with f degrees of freedom.

For the upper and the lower $100(1 - \alpha)\%$ confidence limits on σ^2, the following equations are used:

$$\sigma_U^2(1 - \alpha) = \frac{(n - 1)\ \sigma^{2*}}{\chi^2(n - 1, \alpha)}$$

$$\sigma_L^2(1 - \alpha) = \frac{(n - 1)\ \sigma^{2*}}{\chi^2(n - 1, 1 - \alpha)}$$

As already discussed, classical confidence intervals supplement point estimates as a summary of the data-based information about the parameters of a probability model. They also serve to provide guidance on the parameter ranges that should be covered in a sensitivity analysis (see Chapter 12). That is, if one is interested in the change in an accident-sequence probability that results from a change in a component parameter, confidence intervals provide a plausible range over which the component parameter should be varied.

Occasionally, in probabilistic risk assessments classical confidence limits are misinterpreted as percentiles on a probability distribution of the parameter. Because confidence limits are derived under the assumption that these parameters are constants, not random variables, such an interpretation is unwarranted, except perhaps as a Bayesian degree-of-belief distribution, given a uniform prior distribution. One reason confidence limits are given a distributional interpretation is to provide input to probabilistic uncertainty analyses (Chapter 12). One could view such an analysis as a mathematical device for obtaining approximate classical confidence limits on an accident-sequence probability, given data pertaining to the parameters in the accident model, but better methods are available (Chapters 6 and 12). One particular treatment of confidence limits that should be avoided is the fitting of distributions to classical confidence limits on failure rates or probabilities.

An example of the application of classical techniques is included in Section 5.5.2.5, where the result can be compared with Bayesian treatments of the same data.

5.5.2 BAYESIAN ESTIMATION

The Bayesian approach is similar to the classical approach in that it yields "best" point estimates and interval estimates, the intervals representing ranges in which, we are confident, the parameter really lies. It differs in both practical and philosophical aspects, though. The practical distinction is in the incorporation of belief and information beyond that contained in the observed data; the philosophical distinction lies in assigning a distribution that describes the analyst's belief about the values of the parameter. This is the so-called prior distribution.

The prior distribution may reflect a purely subjective notion of probability, as in the case of a Bayesian degree-of-belief distribution, or any physically caused random variability in the parameter, or some combination of both. Physically caused random variations in a parameter like a failure rate may stem from plant and/or system effects, operational differences, maintenance effects, environmental differences, and the like. The distribution that describes this physically caused random variation in the parameter is sometimes referred to as the "population variability" distribution (Apostolakis et al., 1980) and can be represented by a Bayesian prior distribution. However, such random variation in the parameter can also be modeled by classical methods, using compound distributions in which the population-variability distribution becomes the mixing distribution. On the other hand, if the prior distribution embodies subjective probability notions regarding the analyst's degree of belief about the parameter, the Bayesian method is the appropriate framework for making parameter estimates. A comparative discussion of both interpretations of the notion of probability, the subjective and the relative-frequency notions, is given by Parry and Winter (1981).

Whether the analyst does or does not have objective relative-frequency data, he will often have other information based on engineering designs, related experience in similar situations, or the subjective judgment of experienced personnel. These more or less subjective factors will also be incorporated into the prior distribution--that is, into the description of his prior knowledge (or opinions) about the parameter.

The Bayesian method takes its name from the use of Bayes' theorem and the philosophical approach embodied in the 18th-century work of the Rev. Thomas Bayes (modern reproduction, 1958). Bayes' theorem (see Section 5.5.2.1.1) is used to update the prior distribution with directly relevant data. Here the term "generic data" will be used to refer to parameter-related information that is nonspecific to any particular plant or application, being an aggregation over more than one use condition. A prior distribution is often based on such generic data sources (Apostolakis et al., 1980). A PRA for a particular plant, of course, requires not generic data but rather estimates that are specific to the plant or application. Bayes' theorem then updates the prior distribution with plant-specific evidence and has the effect of "specializing" the prior to the specific plant. The updated, or specialized, prior is called the "posterior distribution" because it can be derived only after the plant-specific evidence is incorporated. The prior reflects the analyst's degree of belief about the parameter before such evidence; the posterior represents the

degree of belief after incorporating the evidence. Plant-specific estimates are then obtained from the posterior distribution as described in Sections 5.5.2.3 and 5.5.2.4.

5.5.2.1 Essential Elements of the Bayesian Approach

This section considers the essential elements of the Bayesian approach to data reduction. It presents a brief discussion of Bayes' theorem, the basic notions of Bayesian point and interval estimation, and a step-by-step outline of the procedures for obtaining Bayesian estimates.

The main benefit in using the Bayesian approach to data reduction is that it provides a formal way of explicitly organizing and introducing into the analysis assumptions about prior knowledge. This knowledge may be based on past generic industry-wide data and experience, engineering judgment, expert opinion, and so forth, with varying degrees of subjectivity. The parameter estimates will then reflect this knowledge. A noteworthy feature of the nuclear industry is that such prior information is often available to the extent that it may contribute more to knowledge about the parameter than does the more directly applicable (but sparse) plant-specific information.

5.5.2.1.1 Bayes' Theorem

The fundamental tool for use in updating the generic prior distribution to obtain plant- or application-specific parameter estimates is Bayes' theorem. If the parameter of interest is a failure rate λ (number of failures per unit time), Bayes' theorem states that

$$f(\lambda|E) = \frac{f(\lambda)\ L(E|\lambda)}{\int_0^\infty f(\lambda)\ L(E|\lambda)\ d\lambda} \qquad (5\text{-}4)$$

where $f(\lambda|E)$ is the posterior distribution, the probability density function of λ, conditional on the specific evidence E; $f(\lambda)$ is the prior distribution, the probability density function of λ based on generic information but incorporating no specific evidence E; and $L(E|\lambda)$ is the likelihood function, the probability distribution of the specific evidence E for a given value of λ.

If the parameter of interest is the probability of failure on demand, p, rather than a failure rate λ per unit time, then λ is simply replaced by p in Equation 5-4. However, the likelihood function will differ for the different cases, as shown in Sections 5.5.2.3.1 and 5.5.2.4.

In certain special cases, the integral on the right-hand side of Equation 5-4 can be done analytically to give a closed-form expression for the posterior distribution. The term "conjugate prior" is used to describe the prior-distribution form that conveniently simplifies the integration. For example, if the likelihood function is the Poisson distribution (see

Section 5.5.2.4), then the gamma family represents the conjugate prior: the posterior distribution will be expressible in closed form as another gamma distribution. Section 5.5.2.2.3 will discuss this in more detail. In general, a closed-form integration will not be possible, and numerical techniques must be used; alternatively, the continuous prior distribution can be approximated by a discrete approximation and the integral replaced by a sum. An example of the latter approach has been given by Apostolakis et al. (1980).

Numerical integration or a discrete approximation is often needed when the generic data include a precise description of a prior distribution, so that the analyst lacks the flexibility to choose a mathematically tractable form for it. For example, if a lognormal prior distribution is specified for λ and the likelihood is the Poisson distribution, then the posterior distribution cannot be obtained analytically in closed form. On the other hand, if we have incomplete information, this choice can be made from the conjugate family of distribution (see Section 5.5.2.2.3), which yields the mathematical convenience and resultant simplicity of a closed-form expression for the posterior distribution. Sensitivity studies can then be used to examine the effects of this choice.

The discrete form of Bayes' theorem is

$$f(\lambda|E) = \frac{f(\lambda_i)\ L(E|\lambda_i)}{\sum_{i=1}^{m} f(\lambda_i)\ L(E|\lambda_i)} \qquad (5\text{-}5)$$

where λ_i $(i = 1,2,\ldots,m)$ is a discrete set of failure-rate values. The prior and posterior distributions are approximated by the discrete functions $f(\lambda_i)$ and $f(\lambda_i|E)$, respectively.

The discrete form of Bayes' theorem is mathematically convenient and is sometimes used as an approximation to the continuous form given by Equation 5-4 when the denominator in Equation 5-4 cannot be evaluated in closed form. In such cases, the range of the parameter is carved into a set of intervals and the probability content of each interval is then associated with a single point inside the interval.

There are two important issues that should be raised in conjunction with the discrete-prior approach. First, it sometimes happens that the use of a discretized approximation to a continuous prior does not produce a meaningful well-spread posterior distribution (see Apostolakis et al., 1980, Examples 2 and 3). In such cases, the prior distribution must be finely spread in the appropriate region after the initial posterior distribution has been obtained. Thus, the method may require more than one iteration to produce a meaningful posterior, and such recursive procedures may be unacceptable. Second, if continuous priors of a specified form (e.g., a lognormal distribution) are discretized, the results may be interpreted as a crude approximation to the integration in Equation 5-4. A better approximation is to use Equation 5-4 in conjunction with an appropriate numerical integration method, such as the Gauss quadrature, thus maintaining in effect a continuous prior distribution. This is the approach used by Ahmed et al. (1981).

The denominator of either Equation 5-4 or Equation 5-5 can be thought of simply as a normalizing factor that makes the posterior distribution integrate or sum to unity. Thus, Bayes' theorem can be stated verbally as simply saying that the posterior distribution is proportional to the product of the prior distribution and the likelihood function.

5.5.2.1.2 Bayesian Point and Interval Estimation

The prior distribution summarizes the uncertainty in a parameter as reflected by prior judgment and/or the generic data sources on which the prior is based. Similarly, the posterior distribution summarizes the uncertainties in the plant-specific value of the parameter as reflected by the combined influence of both the prior distribution and the likelihood function. In either case, it is frequently desired to obtain either a point or an interval estimate of the underlying parameter.

A Bayesian point estimate is a single value that, in some precisely defined sense, best estimates or represents the unknown parameter. Two commonly used point estimates are the mean and the median (50th percentile) of the prior or the posterior distribution. The mean of a distribution is the Bayesian estimate that minimizes the average squared error of estimation (averaged over the entire population of interest), while the median is the one that minimizes the average absolute error. Thus, either the mean or the median of the prior distribution can be used as a point estimate of the unknown generic parameter; likewise, the mean or the median of the posterior distribution can be used as a point estimate of the unknown plant- or application-specific parameter. The properties of the two estimators are discussed by Martz and Waller (1982). The mean or the median would be found by conventional statistical procedures: using the prior distribution, the mean of a failure rate λ is given by

$$\mu_\lambda = \int_0^\infty \lambda f(\lambda)\, d\lambda$$

while the median is the solution to

$$F(\lambda) = \int_0^\lambda f(t)\, dt = .5$$

$F(\lambda)$ denoting the cumulative distribution function. Using the posterior distribution, the prior $f(\lambda)$ would be replaced by the posterior $f(\lambda|E)$ in Equations 5-6 and 5-7.

Now consider the problem of obtaining an interval estimate for λ, using either the prior or the posterior distribution, depending on whether one is concerned with a generic or a specific failure rate. Suppose we want a probability of $(1 - \gamma)$ that the interval estimate really includes the unknown failure rate. (For example, $\gamma = .05$ for .95 probability.) We can

obtain a 100(1 - γ)% two-sided Bayes probability interval estimate of λ by solving the two equations

$$\int_0^{\lambda_L} f(\lambda)\, d\lambda = \frac{\gamma}{2} \tag{5-8}$$

and

$$\int_{\lambda_U}^{\infty} f(\lambda)\, d\lambda = \frac{\gamma}{2} \tag{5-9}$$

for the lower end point λ_L and the upper end point λ_U. It follows immediately that $P(\lambda_L < \lambda < \lambda_U) = 1 - \gamma$. Such an interval is often called a "Bayesian confidence interval"; we avoid that term here because it is not a confidence interval in the classical sense. The coefficient (1 - γ) is the subjectively defined probability that the interval estimate (λ_L, λ_U) contains λ.

For a Bayesian interval estimate of an unknown plant-specific failure rate, the posterior distribution $f(\lambda|E)$ would replace the prior distribution $f(\lambda)$ in Equations 5-8 and 5-9. The interval estimate (λ_L, λ_U) would then be such that $P(\lambda_L < \lambda < \lambda_U\ E) = 1 - \gamma$.

Analogous results hold when the parameter of interest is a failure-on-demand probability p rather than a failure rate λ.

5.5.2.1.3 Step-by-Step Procedure for Bayesian Estimation

The PRA analyst goes through several steps in Bayesian data reduction. For estimating a parameter like a component-failure rate or a failure-on-demand probability, the steps are as follows:

1. Identify the sources and forms of generic information to be used in selecting an appropriate prior distribution for the parameter (see Section 5.5.2.2.1).

2. Select a prior-distribution family if none has been specified as part of the generic information (see Sections 5.5.2.2.2 and 5.5.2.2.3).

3. Choose a particular prior distribution by reducing and/or combining the generic data from step 1 (see Sections 5.5.2.2.4 through 5.5.2.2.8).

4. Plot the prior and summarize it by determining its mean, variance, and selected summary percentiles.

5. If generic estimates are required, determine them from the prior as in Section 5.5.2.1.2.

6. If plant- or application-specific estimates are required, then--

   a. Obtain data representing operating experience with the specific component.

   b. Identify an appropriate form for the likelihood function (see Sections 5.5.2.3.1 and 5.5.2.4.1).

   c. Use Bayes' theorem to get the posterior distribution (see Section 5.4.2.1.1).

   d. Plot the posterior distribution on the same page with the prior and summarize the posterior in the same manner as in step 4.

   e. Compare the prior and the posterior distributions to see the effect of the specific data.

   f. Obtain the desired estimates from the posterior distribution.

7. Investigate the sensitivity of the results to the prior distribution.

5.5.2.2 Determining Prior Distributions

A fundamental part of any Bayesian estimation procedure is the selection and fitting of a prior distribution. This section considers "generic" data that can be used to determine a prior distribution, including sample sources of such data, and then discusses some methods for reducing or combining such data in fitting a prior. Subsequently, several classes of priors that have been found useful in reactor applications will be introduced. Particular emphasis is given to the class of noninformative prior distributions, useful when there are few or no prior generic data. Lognormal, gamma, and beta prior distributions are presented for possible use when prior generic data are available.

5.5.2.2.1 Sources of Data for Use in Bayesian Estimation

Three types of information about the reliability parameter of interest are often available: (1) engineering knowledge about the design, construction, and performance of the component; (2) the past performance of similar components in similar environments; and (3) the past performance of the specific component in question. The first two types constitute the "generic" information (or data) and may include varying degrees of subjective judgment. The third type, constituted of objective data, is the "plant- or application-specific" information (or data).

Generic Data

Generic data may be available in many forms. The analyst may have raw (unreduced) failure data or reduced failure-rate data in the form of point or interval estimates, percentiles, and so forth.

Two sources of failure-rate data that have been previously used (Apostolakis et al., 1980) in nuclear plant PRAs are the Reactor Safety Study (RSS) and the IEEE Std-500 Data Manual. The RSS data have been updated in a recent report (Murphy, 1980) that summarizes the generic (and some specific) component-failure-rate data that are currently available for nuclear plant PRAs. The use of both of these sources is described by Apostolakis et al. (1980).

Another method of using raw generic data for determining a prior distribution is described by Kaplan (1981a); it uses Bayes' theorem to determine the prior distribution.

Plant- or Application-Specific Data

There are several sources of plant- or application-specific data that can be used via Bayes' theorem to determine posterior distributions suitable for application-specific estimates. Reliability data bases like the Nuclear Plant Reliability Data System (NPRDS), the In-Plant Reliability Data System (IPRDS), and the NRC licensee event reports (LERs), all of which report on component populations and failure events, are good sources of plant-specific data. Such data are also often available in summary form in secondary reports derived from these basic sources.

5.5.2.2.2 Noninformative Prior Distributions

"Noninformative" prior distributions are a class of priors that loosely minimize the relative importance of the prior (compared with the data) in generating a posterior estimate. There are many ways of precisely quantifying this basic notion and hence a variety of classes of noninformative priors and corresponding methods for their attainment in practice. The notion adopted here for the noninformative prior is that of Martz and Waller (1982), in which, roughly speaking, a prior is said to be noninformative if the plant-specific data serve only to change the location of the corresponding likelihood and not its shape. This and other notions have also been discussed by Jeffreys (1961), and a summary of the relevant literature on this subject has been presented by Parry and Winter (1981).

Noninformative priors are useful when little or no generic prior information is available; they should not be used when there is such information, because they deliberately downgrade its role in the estimation process. Frequently, Bayesian estimates from noninformative priors are identical with, or very close to, the classical estimates, a fact illustrating the versatility of the Bayesian method. However, interval estimates generated by their use are probability intervals, not classical confidence intervals. Section 5.5.2.3.2 presents the noninformative prior

for failure-on-demand probabilities, and Section 5.5.2.4.2 does so for failure rates. Since noninformative priors contain no generic information, it may be preferable to avoid their use when even minimal generic prior data are available.

5.5.2.2.3 Natural Conjugate Prior Distributions

Natural conjugate prior distributions have the property that, for a given likelihood function, the posterior and prior distributions are members of the same family of distributions. In such cases, the posterior distribution has a closed-form analytical representation (at least to the extent that the prior does), and accordingly the expressions for computing the Bayesian point and interval estimates can usually be represented in terms of well-defined probabilities. This will be seen in Sections 5.5.2.3.3 and 5.5.2.4.3. The parameters of such priors are often especially easy to interpret, playing the role of prior failure data entirely analogous to the specific data used in the likelihood function. This will also be illustrated in Sections 5.5.2.3.3 and 5.5.2.4.3. Such families of priors are often rich enough and flexible enough to permit the analyst to model reasonably a wide range of prior data that may be encountered (Martz and Waller, 1982). Finally, there are well-developed methods for fitting natural conjugate priors to generic prior data. Some of these will be discussed in Sections 5.5.2.2.6 and 5.5.2.2.7.

For these reasons, natural conjugate priors have found application in nuclear plant PRAs (see, for example, Apostolakis and Mosleh, 1979). Their use is recommended (see, for example, Ahmed et al., 1981) whenever the exact form of the prior has not been specified as part of the generic prior data, but the data are sufficient to determine a reasonable member of the natural conjugate family. If incomplete information exists on the prior, as often happens, the analyst will have the flexibility to select the form of the distribution, and the conjugate prior is often the natural selection. However, a sensitivity analysis should be performed to confirm this choice.

5.5.2.2.4 Using Generic Data Sources

The generic prior data must be reduced to a form that permits the selection of a specific prior distribution from a suitable family. For example, if a lognormal family has been selected, the two lognormal parameters must be determined from the generic data. If there are multiple sets of generic prior data, these must likewise be reduced to a common consensus prior.

A Single Source

For convenience consider the case of failure-rate (per unit time) estimation. If a two-parameter prior distribution is to be fitted, such as a lognormal or a gamma distribution, the generic data must contain at least two independent pieces of information. For example, the generic data may consist of upper and lower limits on the failure rate. Each of these limits

is then equated to its theoretical counterpart derived from the prior family considered. Since each theoretical expression will be a function of the two prior parameters, the two equations can be solved simultaneously for the values of the two parameters.

Example 1. Given that a diesel generator starts successfully, its subsequent hourly failure rate is given in the Reactor Safety Study as a lognormal distribution with 5th percentile $\lambda_L = 3 \times 10^{-4}$ and 95th percentile $\lambda_U = 3 \times 10^{-2}$. For the lognormal distribution we have the pair of equations given by

$$\Phi\left[\frac{\ln(3 \times 10^{-4}) - \xi}{\sigma}\right] = 0.05$$

and

$$\Phi\left[\frac{\ln(3 \times 10^{-2}) - \xi}{\sigma}\right] = 0.95$$

where ξ and σ are parameters of the lognormal family (Section 5.5.2.4.4) and $\Phi(\cdot)$ is the standard normal cumulative distribution function. Since $\Phi(-1.645) = 0.05$ and $\Phi(1.645) = 0.95$, we have

$$\ln(3 \times 10^{-4}) - \xi = -1.645\sigma$$

and

$$\ln(3 \times 10^{-2}) - \xi = 1.645\sigma$$

from which $\xi = -5.81$ and $\sigma = 1.40$. Thus, the fitted lognormal prior based on the RSS data becomes

$$f(\lambda) = \frac{1}{1.40\lambda\sqrt{(2\pi)}} \exp\left[-\frac{1}{2(1.40)^2}(\ln\lambda + 5.81)^2\right] \quad (0 < \lambda < \infty)$$

An alternative technique is considered in Section 5.5.2.2.8.

Similar techniques can be used for generic data like means or medians. However, if only a "best" point estimate is given (as in some of the IEEE Std-500 cases), there will usually be a need for some additional specification by the analyst. First, he must decide whether to use the mean, median, or mode of the distribution as the suitable central value representing the "best" estimate. Second, the analyst may have to introduce a second parameter value in order to define a distribution without ambiguity. For example, suppose one is to fit a gamma prior for a failure rate when the only available datum is the mean of the generic rate. Since the mean does not uniquely determine a gamma distribution, the variance could also be introduced and treated as an unspecified parameter.

Often the prior data from a single generic source are inconsistent in the sense that no common prior distribution can be fitted to the data.

There is no universally accepted method of rectifying such inconsistencies, but any of several approaches could be taken. One would be to take the set of all priors implied by the generic data and define some "most conservative" criterion to select a single prior from the set. Another would be to consider the entire set of priors as representing multiple sources of generic data and employ the procedures suggested in the discussion that follows.

Combining Multiple Sources

Often, multiple sources of generic prior data must be reduced to a single prior distribution that satisfactorily reflects and incorporates the views of each source. The multiple sources might be generic data from two or more studies (e.g., the RSS or IEEE Std-500) that report on the same generic component; they may consist of the opinions of several experts about the same component; or, as noted above, the multiple "sources" may consist of the set of unrectified priors obtained from a single inconsistent source.

Three procedures are suggested for forming a consensus prior distribution, although several methods are described in the literature (see for example, Eisenberg and Gale, 1959; Brown and Helmer, 1964; Winkler, 1968; Stone, 1961; Winkler and Cummings, 1972; De Groot, 1974; and Morris, 1974, 1977). For convenience, consider a failure-rate estimation as before. If each source provides both a point and an interval estimate, the first method is to pool (combine) the estimates by means of simple geometric averaging techniques:

$$\hat{\lambda} = \left(\prod_{i=1}^{n} \hat{\lambda}_i \right)^{1/n} \qquad (5\text{-}10)$$

This is equivalent in effect to forming the usual arithmetic average of failure rates described by their logarithms. This estimate implicitly assumes that the underlying sources are statistically independent and of equal importance. If the sources are unequal in their contribution to the consensus prior, a weighted geometric mean could be used with weights chosen to reflect the importance of each source.

Martz and Bryson (1982) have developed a classical statistical model for combining multiple sources of data. The resultant maximum-likelihood consensus point estimator is a weighted geometric mean of the individual estimates in which the weights are simple functions of the uncertainty bounds supplied by each data source. A corresponding consensus confidence-interval estimator is also provided. The maximum-likelihood point estimator of Martz and Bryson (1982) reduces to Equation 5-10 under two conditions: if each data source reports the exact same range of uncertainty, and if there is no location bias in the individual estimates.

The above pooling method was used to synthesize the opinions of some 200 experts in developing the IEEE Std-500 data base. Martz and Waller (1978) examined the effectiveness of this approach in a simulation and concluded that the method produced good point estimates; however, the combined interval estimates generally tended to be too narrow and thus had less than the desired assurance.

The second method yields a consensus prior that is generally more diffuse (spread out) than that obtained by the method just described. This method, discussed by Winkler (1968) and Stone (1961), is often referred to as the "mixture method." It involves fitting a suitable prior to each generic source and then combining the individual prior distributions by forming a mixture,

$$f(\lambda) = \sum_{i=1}^{n} w_i f_i(\lambda) \qquad (5\text{-}11)$$

The coefficients w_i are positive weights that sum to 1. Winkler (1968) suggests several methods for determining the weights. In the absence of any reason for preferring one source over another, the selection $w_i = n^{-1}$ is an obvious possibility. An interesting feature of this method is that it may yield a non-unimodal prior distribution. If such a mixture is used as a prior distribution, the corresponding posterior distribution from Equation 5-4 will also be a mixture of the individual (component) posterior distributions, namely,

$$f(\lambda|E) = \sum_{i=1}^{n} w_i f_i(\lambda\ E) \qquad (5\text{-}12)$$

where the new (updated) weights are

$$w_i' = \frac{w_i \int_0^\infty f_i(\lambda)\ L(E|\lambda)\ d\lambda}{\sum_{i=1}^{n} w_i \int_0^\infty f_i(\lambda)\ L(E|\lambda)\ d\lambda} \qquad (i = 1,2,\ldots,n) \qquad (5\text{-}13)$$

Since this method generally yields a more diffuse consensus prior than does geometric averaging, it provides more-conservative interval estimates. For this reason it is often preferred. However, it should be pointed out that the mixture method is computationally more difficult; numerical methods are frequently required for determining such quantities as the prior moments and percentiles.

A third method has been described by Kaplan (1981b) and earlier by Guttman (1970). This method, called a "two-stage" Bayesian procedure by Kaplan, uses a Bayesian procedure for forming the prior (stage 1) before combining the prior with the likelihood function (stage 2).

To describe the two-stage method, assume that the problem to be solved is to estimate the failure rate of machine S and express the degree of confidence in this failure rate given the following relevant information:

E_1: engineering knowledge of the design and construction of the machine

E_2: past performance of similar machines in similar applications

E_3: past performance of the specific machine in question

The information E_3 is of the format

$$E_3 = \langle h_s, T_s \rangle$$

that is, a doublet stating that machine S has failed h_s times in T_s years. This information is used in Bayes' theorem:

$$f(\lambda|E_1,E_2,E_3) = \frac{f(\lambda|E_1,E_2)L(E_3|\lambda_1,E_1,E_2)}{\int_0^\infty f(\lambda|E_1,E_2)L(E_3|\lambda_1,E_1,E_2)}$$

where $f(\lambda|E_1,E_2,E_3)$ is the posterior probability distribution for λ_S. This distribution expresses the final state of knowledge about λ_S in light of all the evidence E_1,E_2, and E_3. On the right, $f(\lambda|E_1,E_2)$ is the "prior" distribution representing the state of knowledge without information E_3 but including E_1 and E_2.

This use of Bayes' theorem to incorporate the specific evidence E_3 is a conventional application of Bayes' theorem and is the second stage of the two-stage approach. The first stage of the two-stage approach is aimed at determining the prior $f(\lambda|E_1,E_2)$, from the information E_2, which is of the form

$$E_2 = \{\langle h_1,T_1\rangle, \langle h_2,T_2\rangle,\ldots,\langle h_M,T_M\rangle\}$$

E_2 then is the set of doublets giving the operating experience of a set of M components deemed similar to that being analyzed.

To use E_2, this set of M components is thought of as a sample from an infinite population Q of similar components. Considering the whole of Q, there is a frequency distribution $\Phi(\lambda)$, where λ is the failure rate of a member of Q, such that $\Phi(\lambda)\,d\lambda$ is the fraction of the population with failure rates in the interval $d\lambda$. Kaplan denotes $\Phi(\lambda)$ as the "population variability curve" for the population Q.

If the population variability curve was known, it could be used as a prior, that is,

$$f(\lambda|E_1,E_2) = \Phi(\lambda)$$

Since $\Phi(\lambda)$ is now known, it is necessary to express what is known or can be inferred about $\Phi(\lambda)$ from the evidence E_2. For this purpose, consider the function $\Phi(\lambda)$ as being imbedded in a space of functions $\Phi(\lambda)$. Then a probability distribution, call it $f(\Phi|E_1,E_2)$ over this space F of functions exists, expressing knowledge of where, in F, Φ is located. For this purpose, Kaplan writes the "first-stage" application of Bayes' theorem in the form

$$f(\Phi|E_1,E_2) = \frac{f(\Phi|E_1)L(E_2|\Phi,E_1)}{\int_0^\infty f(\Phi|E_1)L(E_2|\Phi,E_1)}$$

Thus $f(\Phi|E_1,E_2)$ is the state of knowledge about Φ "posterior" to having the information E_3.

Once $f(\Phi|E_1,E_2)$ is known, then the desired prior $f(\lambda|E_1,E_2)$ to the second stage of the process is calculated from

$$f(\lambda|E_1,E_2) = \int_F f(\Phi|E_1,E_2)\, d\Phi$$

Kaplan (1981b) uses discretization techniques to find the population-variability curve. This can be illustrated by choosing a two-parameter family of lognormal* curves as follows:

$$\Phi_{ij}(\lambda) = \frac{1}{\sqrt{(2\pi)}\ \lambda\sigma_j} \exp\left\{-\frac{[\ln(\lambda/\mu_i)]^2}{2(\sigma_j)^2}\right\}$$

where the two parameters μ_i, σ_j range over a discrete "grid." Thus,

$$p(\Phi_{ij}|E_1,E_2) = \frac{p(\Phi_{ij}|E_1)\ p(E_2|\Phi_{ij},E_1)}{\sum_{i=1}^{I}\sum_{j=1}^{J} p(\Phi_{ij}|E_1)\ p(E_2|\Phi_{ij},E_1)}$$

and

$$p(E_2|\Phi_{ij},E_1) = \prod_{m=1}^{M}\left[\int_0^\infty \Phi_{ij}(\lambda)\ \frac{(\lambda T)_m^{K_m}}{K_m!} \exp(-\lambda T_m)\, d\lambda\right]$$

where M is the number of components with data K_m failures in T_m hours.

The prior $p(\Phi_{ij}|E_1)$ is the information that describes the grid of the parameters μ_i and σ_j. This is determined from experience, or it could be a noninformative prior.

A further simplification can be made by finding a "best estimate" for Φ, or the mean value for the distribution $p(\Phi_{ij}|E_1,E_2)$; that is,

$$\bar{\Phi}(\lambda) = \sum_{ij} \Phi_{ij}(\lambda)\ p(\Phi_{ij}|E_1,E_2)$$

This could then become the final prior for combining with the likelihood function from E_3.

---

*The choice of this family of lognormal curves should be regarded as illustrative. Any desired family of curves could be used, subject only to the requirement that somewhere in the family there would be at least one good approximation to the true variability curve Φ.

5.5.2.2.5 Using Expert Opinion

Expert opinion is often used for a prior probability distribution when other information is inadequate. If neither physical nor theoretical models are available and relative frequency is unavailable as well, subjective assessment is the only alternative for obtaining a probability. The practical feasibility of this alternative is supported not only by theoretical foundations that show judgments about uncertain events can be expressed as probabilities but also by practical assessment procedures. Holloway (1979) reviews the basis for these procedures and gives examples for several assessment approaches. The following summary of assessment procedures draws on his book. After this summary, well-known cautions and guidelines for interpreting and reviewing expert opinions are presented to highlight the care and caveats that must accompany the quantitative assessment.

However, the user of this guide should be cautioned against the indiscrete use of the methods described in this section. These techniques and results are not necessarily applicable to PRAs, which often treat extremely small probabilities of various events. More research is needed to determine the direct applicability of these methods and findings to PRAs. The user should be aware that the subjective estimates frequently used in PRAs can have large biases and errors.

Assessment Lotteries

An assessment lottery is a physical example of a random process. The uncertainty represented by the lottery must be easily recognized by the expert and have definite, objective probabilities. Such a lottery is the reference scale that measures an expert's degree of belief about the uncertain event. The operational definition for subjective probability, then, is the fraction of this reference uncertainty scale that makes an expert just indifferent between the assessment lottery and the feeling of uncertainty toward the event being assessed.

One example of assessment lotteries is an urn containing balls of different colors, some fraction being one color and the rest the other color. Drawing a ball at random from the urn is supposed to provide a visualization of an objective probability. Spetzler and Stael von Holstein (1975) developed and clinically tested another procedure that uses the spinning of a reference wheel as the assessment lottery. Their experience has shown that these probability wheels provide a strong visual image of an uncertain process.

Assessment Procedures

Two approaches to subjective probability assessment are in practical use, either the direct approach or the indirect approach. With the direct approach, the expert is asked to declare the probability number associated with the feeling of uncertainty for the occurrence of an event. With the indirect approach, an expert is asked to choose between a reference assessment lottery and the uncertain feeling (the degree of belief) in an opinion or judgment. Until an expert has shown an ability both to form a knowledgeable opinion and to assess, unaided, a probability for the degree of belief associated with that opinion, the indirect approach is preferred. The

well-known difficulties in obtaining useful subjective probability assessments are summarized below in the section entitled "Validity of Expert Opinion." These difficulties are magnified by inexperienced, unaided direct assessments. The references in that section give some experience comparing the two approaches.

The direct approach has the expert state a number that represents the assessment of the probability. Some studies have shown it possible for people to become better at assessing their own feelings of uncertainty as probabilities (see for example, Stael von Holstein, 1970; Lichtenstein et al. 1977). This improvement in direct assessment comes from specific training and guided practiced discipline rather than by trial and error. A good direct assessment comes from one who is both an experienced expert in what is known about a technical area (as well as how much is not known) and an experienced expert on how to express that judgment with little cognitive bias. This is an uncommon combination of expertise.

Assessment lotteries are used in the indirect approach to disclose the subjective probability. This external reference is used as a scale to measure the internal degree of belief an expert holds toward an opinion. Dividing between the expert and the assessors the responsibility to provide both a well-founded, knowledgeable judgment and an accurate representation of that judgment as a probability allows the use of expert opinion in PRAs. Most technical experts are not practiced, good probability assessors of themselves. Using the indirect approach improves the quality of expert opinion over that obtained by unaided, inexperienced direct assessment. Fischhoff et al. (1981) have shown that people qualified as technical experts are by no means qualified as probability assessors of that expertise.

Assessment Models

The representation used to model the uncertain event, either intuitively or formally, is a significant part of obtaining a good assessment. How the expert thinks about the problem of giving a judgment on the event likelihood should be recorded (see the discussion on "Recording Expert Opinion," page 5-44). It is this representation that fashions the eventual probability that is assessed. If disputes or questions arise in reviewing the quality of the expert opinion, a brief description of the thought model can focus the issue to a particular facet of that judgment.

Often, the expert is better able to provide a judgment by refining the event description into underlying events or factors. This formal assessment model can be subdivided until the expert finds it easy to examine each part, provide an opinion conditioned on each one, and review the formally computed probability of the original event for completeness and accuracy. This aid to assessment relieves an expert from making logical, or procedural, errors in combining the underlying knowledge. Reducing this source of error with the use of assessment models allows the assessor to focus on revealing a more subtle bias in the judgment.

Validity of Expert Opinion

The validity of a subjective assessment comes from two distinct parts: the knowledge content provided by the expert and the procedural process

provided by the assessor. If the expert is playing both of these roles, the distinction blurs, but it is still useful to describe the source of inaccuracies.

The content factor is evaluated from the credentials provided by the expert. Identifying who knows what and how much is a routine task for a professional community. Even for a recognized expert, a peer review can use the assessment model to judge whether or not all the significant factors were included in the expert's opinion. Inaccuracies, disputes, omissions, and limits to knowledge can then be examined to improve the accuracy of the substantive, or content, portion of the probability assessment.

The procedural process is more difficult to evaluate. The judgmental processes used by the expert, the effect the assessor has on expanding or limiting the formation of the expert's opinion, the effect of misunderstandings, and the natural cognitive limits on human information processes are all hidden factors in a practical assessment. Clinical studies, however, have examined these process factors that affect expert opinion. These studies provide a catalog of possible sources of inaccuracy due to bias and the extent of their effect.

It is well known that various biases may accompany the subjectively quantified assessments of an expert. For example, Alpert and Raiffa (unpublished work, 1969) found that experts often overestimate the degree of certainty of their estimates and claim too high a level of assurance. They observed that interval estimates for which 98-percent assurance was claimed tended in reality to have an assurance of about 70 percent (i.e., to include the correct value 70 percent of the time). Alternatively stated, interval estimates are often too narrow for the assurance level that is claimed. Tversky and Kahneman (1974) attribute such bias in part to the phenomenon of "anchoring": the expert tends to focus, or "anchor," on an initial guess and is reluctant to deviate too far from that guess in accounting for possible misjudgment. The results of such studies suggest that the assurance associated with expert-supplied interval estimates should be reduced from that claimed. For example, if a 90-percent interval estimate is solicited, then the interval could perhaps be considered to be an actual 70-percent interval in fitting a prior.

It is also well known that the manner chosen to encode (solicit) the subjective probabilities held by the expert is crucial and may significantly affect the quality of the information (see, for example, Du Charme and Donnell, 1973; Winkler, 1967; and Seaver et al., 1978). Spetzler and Stael von Holstein (1975) describe and recommend a structured-interview procedure and suggest a number of techniques for reducing biases in the quantification of judgment.

Holloway (1979) finds two findings from these studies encouraging. First, persons who are procedural experts in obtaining probability distributions are able, by using a variety of assessment techniques, to elicit consistent, well-founded judgments from substantive experts. Second, the substantive experts who are knowledgeable about the event being assessed are able to learn quickly about the significant procedural factors of probability assessment.

Recording Expert Opinion

The procedure used for assessing expert opinion and the assessment model used by the expert to construct the judgment should be described in a record of the expert opinion.

A subjective probability is an evaluation. The important procedural and substantive factors in that evaluation should be recorded, like any other engineering analysis, to permit a peer review to determine the quality of that result.

This record does not have a standard format; however, with time and experience, one may evolve. Nevertheless, the probability number can be meaningless without a description of how it was obtained and what its principal foundations were.

5.5.2.2.6 Beta Prior Distributions

The beta family of prior distributions is the conjugate family when failure-on-demand probabilities are estimated with a binomial likelihood function (Section 5.5.2.3). To fit a beta prior, values of the two prior beta parameters must be selected.

Martz and Waller (1982) present a table-lookup procedure, along with two sets of tables, that can be directly used to determine the beta-parameter values. Two situations are considered: (1) when the prior mean and 5th percentile of the prior distribution of failure-on-demand probabilities are specified and (2) when the prior mean and 95th percentile are specified. The procedure then yields directly the two beta parameters, as described by Martz and Waller with examples.

Mosleh and Apostolakis (1982) also describe a procedure for determining the beta-parameter values corresponding to various combinations of 5th, 50th, and 95th percentiles as well as the mean. Their procedure is to approximate the beta distribution as a gamma distribution and use corresponding techniques for determining the gamma parameters. Ahmed et al. (1981) have developed a computer code, called BURD, that finds the beta-parameter values corresponding to specified 5th and 95th percentile values.

5.5.2.2.7 Gamma Prior Distributions

The gamma family of prior distributions is the conjugate family when failure rates are estimated with a Poisson likelihood function (Section 5.5.2.4). The gamma family is a two-parameter family, and both parameter values must be identified by specifying some two conditions.

Martz and Waller (1982) present a simple procedure for determining the values of both parameters when two percentiles are given, corresponding to tail areas of 0.5, 1, 2.5, 5, 10, 25, 50, 75, 90, 95, 97.5, 99, or 99.5

percent. Mosleh and Apostolakis (1982) also present a procedure for determining the two gamma-parameter values for specified pairs of values--the (5th, 95th), (5th, 50th), (50th, 95th), (mean, 5th), or (mean, 95th). Ahmed et al. (1981) describe the use of the BURD code to determine the gamma-parameter values for specified 5th and 95th percentile values.

5.5.2.2.8 Lognormal Prior Distributions

The lognormal distribution is frequently used as a prior distribution for failure rates, especially when the failure rates typically encountered are so low (say, 10^{-6} per demand or per unit time) as to make a logarithmic transformation attractive. Apostolakis et al. (1980) make use of lognormal priors, as did the Reactor Safety Study. We consider here a simple procedure for determining the lognormal parameters ξ and σ (see Section 5.5.2.4).

Suppose that two symmetrically located percentiles are specified for the lognormal, denoted by λ_γ and $\lambda_{1-\gamma}$, where $0 < \gamma < 0.5$. Thus,

$$P(\lambda < \lambda_\gamma) = P(\lambda > \lambda_{1-\gamma}) = \gamma$$

The geometric mean of the percentiles is defined as

$$M = (\lambda_\gamma \lambda_{1-\gamma})^{1/2}$$

and a generalized error factor is

$$EF = (\lambda_{1-\gamma}/\lambda_\gamma)^{1/2}$$

Then the desired parameter values are

$$\xi = \ln M \quad \text{and} \quad \sigma = \ln EF/z_{1-\gamma} \tag{5-14}$$

where $z_{1-\gamma}$ is the $100(1 - \gamma)$th percentile of a standard normal distribution. In this case the mean, the variance, the mode, and the median of the fitted lognormal distribution can be found from the parameters as follows:

Mean: $\exp(\xi + \sigma^2/2)$

Mode: $\exp(\xi - \sigma^2)$

Median: $\exp(\xi) = M$

Variance: $[\exp(2\xi + \sigma^2)][\exp(\sigma^2) - 1]$

It is further observed that M is the median of the lognormal distribution and that the two percentiles are $\lambda_{1-\gamma} = (EF)(M)$ and $\lambda_{\gamma} = M/(EF)$, in accord with the notion of an error factor.

Example 2. On reconsidering Example 1, where $\lambda_{0.05} = 3 \times 10^{-4}$ and $\lambda_{0.095} = 3 \times 10^{-2}$, we find immediately that $M = 3 \times 10^{-3}$ and $EF = 10$. These are then substituted into Equation 5-14 to obtain $\xi = -5.81$ and $\sigma = 1.40$, for the latter making use of the fact that $z_{0.95} = 1.645$. Equations 5-15 give for the mean, mode, median, and variance the values 8×10^{-3}, 4×10^{-4}, 3×10^{-3}, and 4×10^{-4}, respectively.

Apostolakis et al. (1980) present a similar method for fitting a lognormal prior when, in addition to the two symmetric percentiles λ_{γ} and $\lambda_{1-\gamma}$, the median is also specified. Their method requires resolution of the evident inconsistency when the geometric mean of the upper and lower percentiles is not equal to the specified median.

5.5.2.3 Estimating Failure-on-Demand Probabilities

5.5.2.3.1 Binomial Likelihood Function

The binomial distribution is the distribution of the number of failures, r, out of n independent demands, on each of which the component has a constant failure-on-demand probability p. Given this statistical framework, the likelihood in Equation 5-4 is the binomial distribution, given by

$$L(E|p) = \frac{n!}{r!\ (n - r)!}\ p^{r}(1 - p)^{n-r} \qquad (5\text{-}16)$$

for $r = 0,1,2,\ldots,n$ and the parameter p between 0 and 1. If the parameter p is small (as usually happens in a PRA) and n is sufficiently large, then Equation 5-16 will usually be most conveniently approximated by the Poisson distribution, to be discussed in a slightly different context in Section 5.5.2.4:

$$L(E|p) = (np)^{r} \exp(-np)/r! \qquad (5\text{-}17)$$

where, because the number of demands is so large in comparison with the number of failures, r is treated as being able to assume any nonnegative integral value. The large values of r thus contribute negligibly to the probability distribution.

In the Bayesian approach, the parameter p is regarded as a random variable with a specified prior distribution. Returning now to the general binomial context, we consider three methods of generating a prior: (1) a noninformative prior; (2) a natural conjugate beta prior; and (3) a lognormal prior. The next three sections consider three priors, presenting in the interests of conciseness only the major results and formulas required to compute appropriate moments and estimates. Details can be found in the text by Martz and Waller (1982).

5.5.2.3.2 Noninformative Prior Distribution

One prior density is calculated from

$$[p(1 - p)]^{-0.5}/\pi \quad (0 \leq p \leq 1)$$

The prior mean, median, and variance are as follows:

Prior mean: 0.5

Prior median: 0.5

Prior variance: 0.125

and the prior 100(1 - γ)% symmetric probability interval is obtained from

$$\frac{0.5}{0.5 + 0.5F_{1-\gamma/2}(1,1)}; \frac{0.5F_{1-\gamma/2}(1,1)}{0.5 + 0.5F_{1-\gamma/2}(1,1)}$$

where $F_{1-\gamma}(a,b)$ is the 100(1 - γ)th percentile of an F-distribution with a and b degrees of freedom.

The posterior density, after r failures in n demands, is obtained from

$$\frac{\Gamma(n + 1)}{\Gamma(r + 0.5)\ \Gamma(n - r + 0.5)} p^{r-0.5}(1 - p)^{n-r-0.5} \quad (0 \leq p \leq 1)$$

and the formulas for calculating the posterior mean, median, and density are as follows:

Posterior mean: $(r + 0.5)/(n + 1)$

Posterior median: $$\frac{r + 0.5}{r + 0.5 + (n - r + 0.5)\ F_{0.5}(2n - 2r + 1,\ 2r + 1)}$$

Posterior variance: $$\frac{(r + 0.5)(n - r + 0.5)}{[(n + 1)^2\ (n + 2)]}$$

and the posterior 100(1 - γ)% symmetric probability interval is obtained from

$$\frac{r + 0.5}{r + 0.5 + (n - r + 0.5)\ F_{1-\gamma/2}(2n - 2r + 1,\ 2r + 1)};$$

$$\frac{(r + 0.5)\ F_{1-\gamma/2}(2r + 1,\ 2n - 2r + 1)}{n - r + 0.5 + (r + 0.5)\ F_{1-\gamma/2}(2r + 1,\ 2n - 2r + 1)}$$

5.5.2.3.3 Beta Prior Distribution

For the beta prior distribution, the prior density is obtained from

$$\frac{\Gamma(n_0)}{\Gamma(r_0)\,\Gamma(n_0 - r_0)}\, p^{r\hat{0}-1}(1 - p)^{n\hat{0}-r\hat{0}-1} \qquad (0 \leq p \leq 1)$$

where the positive values n_0 and r_0 are parameters of the beta distribution but may be interpreted as the numbers of demands and failures, respectively, in the prior data. The prior mean, median, and variance are calculated as follows:

Prior mean: r_0/n_0

Prior median: $$\frac{r_0}{r_0 + (n_0 - r_0)\, F_{0.5}(2n_0 - 2r_0,\ 2r_0)}$$

Prior variance: $$\frac{r_0(n_0 - r_0)}{n_0^2(n_0 + 1)}$$

and the formula for the prior $100(1 - \gamma)\%$ symmetric probability interval is

$$\frac{r_0}{r_0 + (n_0 - r_0)\, F_{1-\gamma/2}(2n_0 - 2r_0,\ 2r_0)};$$

$$\frac{r_0\, F_{1-\gamma/2}(2r_0,\ 2n_0 - 2r_0)}{n_0 - (r_0 + r_0)\, F_{1-\gamma/2}(2r_0,\ 2n_0 - 2r_0)}$$

The posterior density is given by

$$\frac{\Gamma(n + n_0)}{\Gamma(r + r_0)\,\Gamma(n - r + n_0 - r_0)}\, p^{r+r\hat{0}-1}(1 - p)^{n-r+n\hat{0}-r\hat{0}-1} \qquad (0 \leq p \leq 1)$$

and the other formulas are as follows:

Posterior mean:

$$(r + r_0)/(n + n_0)$$

Posterior median:

$$\frac{r + r_0}{r + r_0 + (n - r + n_0 - r_0)\, F_{0.5}(2n - 2r + 2n_0 - 2r_0,\ 2r_0 + 2r_0)}$$

Posterior variance:

$$\frac{(r + r_0)\,(n - r + n_0 - r_0)}{(n + n_0)^2\,(n + n_0 + 1)}$$

Posterior $100(1 - \gamma)\%$ symmetric probability interval:

$$\frac{r + r_0}{r + r_0 + (n - r + n_0 - r_0)\,F_{1-\gamma/2}(2n - 2r + 2n_0 - 2r_0,\ 2r + 2r_0)};$$

$$\frac{(r + r_0)\,F_{1-\gamma/2}(2r + 2r_0,\ 2n - 2r + 2n_0 - 2r_0)}{n - r + n_0 - r_0 + (r + r_0)\,F_{1-\gamma/2}(2r + 2r_0,\ 2n - 2r + 2n_0 - 2r_0)}$$

5.5.2.3.4 Lognormal Prior Distribution

The lognormal distribution is often used as a prior distribution on p, but its parameters must be so chosen that the probability density outside the actual range of p--that is, above the value p = 1--is sufficiently small to be ignored or effectively truncated. Apostolakis and Kaplan (1981) discuss the effect of such a truncation. As noted earlier, the lognormal was used as a prior in the Reactor Safety Study (USNRC, 1975) and in Apostolakis et al. (1980) as well as in other PRAs.

The prior density is obtained from the formula

$$\frac{1}{\sigma p\,\sqrt{(2\pi)}}\,\exp\left[-\frac{1}{2\sigma}\,(\ln p - \xi)^2\right] \quad (p > 0)$$

The prior moments, etc., are given in Section 5.5.2.2.8, and the prior $100(1 - \gamma)\%$ symmetric probability interval is calculated by using the following:

$$\left[\exp(\xi - z_{1-\gamma/2}\sigma);\ \exp(\xi + z_{1-\gamma/2}\sigma)\right]$$

The posterior distribution cannot be obtained in closed form. However, the approximation given in Equation 5-5 can be used to approximate the posterior distribution where $f(p_i)$ denotes the area under the lognormal prior over an interval represented by $p = p_i$ and $L(E\ p_i)$ denotes either Equation 5-16 or 5-17 evaluated at $p = p_i$ for the selected set of discrete values p_i $(i = 1,2,\ldots,m)$.

5.5.2.4 Estimating Constant Failure Rates

5.5.2.4.1 Poisson Likelihood Function

A common assumption in reliability models is that failure times are independent, with a common exponential (constant failure rate) distribution. It follows that the distribution of the number of failures r in a fixed total operating time T has a Poisson distribution. In this case the likelihood function that is defined in Equation 5-4 is the Poisson density given by the following:

$$L(E|\lambda) = (\lambda T)^r \exp(-\lambda T)/r! \quad (r = 0,1,2,\ldots)$$

where λ denotes the constant failure rate.

We consider three cases: (1) one noninformative prior distribution; (2) a natural conjugate gamma prior distribution; and (3) a lognormal prior distribution on λ.

5.5.2.4.2 Noninformative Prior Distribution

The various formulas for the noninformative prior distribution are as follows:

Prior density: $\lambda^{-0.5}$ (an improper distribution) $(\lambda > 0)$

Posterior density: $\dfrac{T^{r+0.5}}{\Gamma(r+0.5)} \lambda^{r-0.5} \exp(-\lambda T)$ $(\lambda > 0)$

Posterior mean: $(2r + 1)/(2T)$

Posterior median: $\chi^2_{0.5}(2r + 1)/(2T)$

where $\chi^2_{1-\gamma}(n)$ is the $100(1 - \gamma)$th percentile of a chi-square distribution with n degrees of freedom.

Posterior variance: $(2r + 1)/(2T^2)$

Posterior $100(1 - \gamma)\%$ symmetric probability interval:

$$\left[\chi^2_{\gamma/2}(2r + 1)/(2T);\ \chi^2_{1-\gamma/2}(2r + 1)/(2T)\right]$$

5.5.2.4.3 Gamma Prior Distribution

The prior density is obtained from

$$\frac{\beta_0^{\alpha_0}}{\Gamma(\alpha_0)} \lambda^{\alpha_0-1} \exp(-\beta_0\lambda) \quad (\lambda > 0)$$

where the positive shape parameter α_0 can be interpreted as the prior number of failures in β_0 prior total operating time. (β_0, also positive, is the scale parameter.)

The other formulas are as follows:

Prior mean: α_0/β_0

Prior median: $\chi^2_{0.5}(2\alpha_0)/(2\beta_0)$

Prior variance: α_0/β_0^2

Prior $100(1 - \gamma)\%$ symmetric probability interval:

$$[\chi^2_{\gamma/2}(2\alpha_0)/(2\beta_0);\ \chi^2_{1-\gamma/2}(2\alpha_0)/(2\beta_0)]$$

Posterior density:

$$\frac{(\beta_0 + T)^{\alpha_0+r}}{\Gamma(\alpha_0 + r)} \lambda^{\alpha_0+r-1} \exp[-(\beta_0 + T)\lambda] \quad (\lambda > 0)$$

Posterior mean: $(\alpha_0 + r)/(\beta_0 + T)$

Posterior median: $\chi^2_{0.5}(2\alpha_0 + 2r)/(2\beta_0 + 2T)$

Posterior variance: $(\alpha_0 + r)/(\beta_0 + T)^2$

Posterior $100(1 - \gamma)\%$ symmetric probability interval:

$$[\chi^2_{\gamma/2}(2\alpha_0 + 2r)/(2\beta_0 + 2T);\ \chi^2_{1-\gamma/2}(2\alpha_0 + 2r)/(2\beta_0 + 2T)]$$

5.5.2.4.4 Lognormal Prior Distribution

The prior density is obtained from

$$\frac{1}{\sigma\lambda\sqrt{(2\pi)}} \exp[-(\ln \lambda - \xi)^2/2\sigma)^2] \quad (\lambda > 0)$$

The prior moments, etc., are given in Section 5.5.2.2.8, and the prior $100(1 - \gamma)\%$ symmetric probability interval is calculated as follows:

$$\exp(\xi - z_{1-\gamma/2}\sigma);\ \exp(\xi + z_{1-\gamma/2}\sigma)$$

The posterior distribution cannot be obtained in closed form. However, the discrete approximation in Equation 5-5 can be used to approximate the posterior distribution, or numerical integration can be used in conjunction with Equation 5-4. There $f(\lambda_i)$ denotes the area under the lognormal prior in the vicinity of λ_i and $L(E|\lambda_i)$ denotes the likelihood (density function) above evaluated at the chosen discrete set of values λ_i $(i = 1,2,\ldots,m)$.

5.5.2.5 Example: Failure of Diesel Generators To Start

Presented below is an example from Apostolakis et al. (1980). The frequency with which diesel generators fail to start (measured in terms of the failure rate per demand) was assumed in the Reactor Safety Study to have alognormal distribution with 5th and 95th percentiles of 10^{-2} and 10^{-1}, respectively. Thus, using the procedure outlined in Section 5.5.2.2.8, we find that $\xi = 3.45$ and $\sigma = 0.70$ are the two lognormal parameter values. The prior mean, mode, median, and variance are then found to be 0.04, 1.9×10^{-2}, 3.2×10^{-2}, and 1×10^{-3}, respectively.

Suppose now that the evidence E from a certain plant consists of $r = 5$ failures in $n = 227$ test demands (see Section 5.5.2.3). Table 5-2 shows the discretized lognormal prior and calculations required to compute the corresponding posterior distribution by means of Equation 5-5; values smaller than 10^{-4} have been treated as equal to zero.

Figure 5-5 shows a plot of the discretized prior and posterior distributions and gives a graphic illustration of the change in the generic prior brought about by the influence of the plant-specific evidence. The posterior mean and variance are computed to be 0.025 and 8.2×10^{-5}, respectively. The effects of the plant-specific evidence are, first, to shift the distribution of the failure-to-start probability toward lower values and, second, to reduce the dispersion.

Another alternative Bayesian procedure is to approximate the binomial likelihood with a Poisson distribution (see Section 5.5.2.3.1) and to assign a conjugate gamma prior distribution to the corresponding failure rate. Taking the 5th and 95th percentiles to be 10^{-2} and 10^{-1}, respectively, and using the procedure of Martz and Waller (1982) (see Section 5.5.2.2.7) yields a gamma prior distribution with the shape parameter $\alpha_0 = 2.4$ and

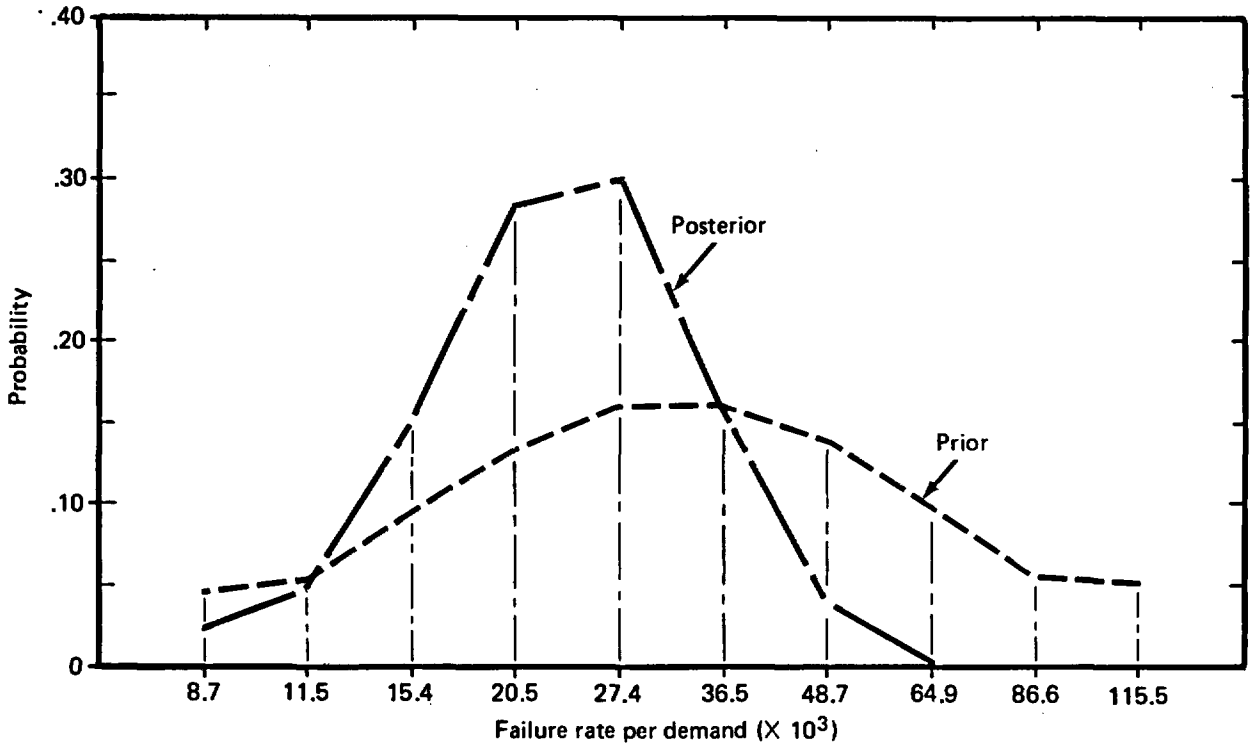


Figure 5-5. Prior and posterior histograms for diesel-generator failure to start. From Apostolakis et al. (1980).

the scale parameter $\beta_0 = 52.68$. Using the results in Section 5.5.2.4.3, the posterior distribution is another gamma distribution with the shape parameter 7.4 and the scale parameter 279.68. The corresponding posterior mean and variance are computed to be 0.026 and 9.5×10^{-5}, respectively. The posterior 5th, 50th, and 95th percentiles are also easily computed to be 0.013, 0.038, and 0.045, respectively.

Consider now the estimation of the probability of diesel-generator failure to start by the classical methods of Section 5.5.1. The data, f/n = 5/227, lead to a maximum-likelihood estimate of $p^* = .022$, which has a standard error of .0097. Note that the square of this standard error is 9.5×10^{-5}, which is slightly larger than the Apostolakis posterior variance. The difference in precision reflects the effect of the selected prior distribution.

Table 5-3 gives lower and upper classical confidence limits on the failure-to-start probability for a variety of confidence levels. It presents both the exact solutions to the expressions given in Section 5.5.1.3 and the chi-squared approximations. Both sets of confidence limits are shown to four decimals only to illustrate the close agreement between the exact and the approximate bounds for these data.

Because of the discretizing that is used, it is difficult to compare the Bayesian results in Table 5-2 with the classical results in Table 5-3. Qualitatively, however, both analyses suggest strongly that the failure probability of interest is between .01 and .05. As one method of

comparison, note that data of 7.5 failures in 300 demands would yield a maximum-likelihood estimate and a squared standard error essentially equal to Apostolakis' posterior mean and variance; thus, his prior effectively contributed additional data of 2.5/73 to his results.

In general, all three analyses of these data agree quite closely, even though the interpretation is quite different. The main reason for this agreement is the rather large quantity of plant-specific data, which results in a likelihood that dominates the prior distribution in the Bayesian analysis.

Table 5-2. Estimation of diesel-generator failure to start by the Bayesian method[a]

Failure rate (failure to start)	Prior probability	Likelihood	(Prior) x (likelihood)	Posterior probability
.0087	.0500	.0343	.0017	.0206
.0115	.0587	.0750	.0044	.0529
.0154	.0967	.1320	.0128	.1535
.0205	.1350	.1734	.0234	.2815
.0274	.1596	.1544	.0246	.2963
.0365	.1596	.0820	.0131	.1572
.0487	.1350	.0218	.0029	.0353
.0649	.0967	.0023	.0002	.0027
.0866	.0587	.0001	.0000	.0000
.1155	.0500	.0000	.0000	.0000
Sum	1.0000		.0831	1.0000

[a]From Apostolakis et al. (1980).

Table 5-3. Classical confidence limits on the probability of diesel-generator failure to start (Five failures in 227 attempts)

Confidence level (%)	Exact solution		Chi-squared approximation	
	Lower	Upper	Lower	Upper
50	.0205	.0249	.0206	.0249
75	.0149	.0325	.0148	.0327
90	.0108	.0405	.0107	.0407
95	.0087	.0458	.0087	.0463
97.5	.0072	.0507	.0072	.0513
99	.0057	.0567	.0056	.0577

5.6 EVALUATION OF DEPENDENT FAILURES

To support the analysis of dependent failures, which are discussed in detail in Section 3.7, appropriate data must be gathered. In gathering these data, it is necessary to establish what events will be classified as dependent and whether the beta-factor method or the binomial failure-rate (BFR) model will be used. An alternative approach is to use the various data reports by Atwood. These reports (Atwood, 1980a, 1982a,b; Atwood and Steverson, 1982a,b) include point estimates and confidence levels for the BFR model for a number of components at nuclear plants. Furthermore, the binomial failure rates can be used to estimate a beta factor, if desired. In addition, a computer code, BFR (Atwood and Suitt, 1982) is available to assist in the evaluation of data.

5.6.1 CLASSIFICATION OF EVENTS

A number of definitions have been used for the classification of events as dependent failures. Indeed, EPRI began a program in 1982 to refine the definition of such failures and thereby establish clearly which events involve dependences. The definition used here is consistent with Atwood's reports, but the data analyst may find it necessary to revise this definition for a particular study. For example, the analyst may wish to treat all multiple failures as if they were attributable to common causes, regardless of the mechanisms that caused the failure.

For this discussion, then, events that are simultaneous because of some external shock to the events are dependent. Two events occurring in the same time frame without such a shock are not considered to be dependent.

The data reports mentioned above (Atwood, 1982a,b; Atwood and Steverson, 1982a,b) give several examples of the classification of events, and these documents should be examined before the classification of specific data is begun.

5.6.2 CALCULATION OF PARAMETERS

The method presented here for the calculation of dependent-event parameters is that of Atwood and Steverson. Again, their documents should be consulted for additional detail and examples.

The quantities of interest are the following:

p	probability that a specific component fails, given that a shock occurs
m	number of components simultaneously susceptible to a shock
λ	failure rate for an individual component, not counting failures due to a common-cause shock

μ	rate of common-cause shocks
$\lambda_+ = \mu(1 - q^m)$	rate of shocks that cause at least one component failure--that is, rate of "visible" shocks (here $q = 1 - p$)
$r_1 = \lambda + \mu p$	rate at which a specific component fails, either because of individual failure or because of a common-cause shock
$r_k = \mu p^k$, $k \geq 2$	rate at which a specific set of k components fails simultaneously (because of a common-cause shock)
r_k/r_1	probability, given that a certain component has failed, that specific k components will also fail at the same time.

The quantities $r_1, r_2, \ldots$ are the relevant rates for fault-tree analysis. If a cut set of a fault tree involves k pumps, $k \geq 1$, then the relevant rate is r_k. The beta factor for any cut set can be estimated from the ratio r_k/r_1, where there are k elements in the cut set.*

The data set for any dependence must then be broken down such that the analyst is comfortable with including all the events as a single kind of shock. While this seems undesirable, the alternative requires obtaining multiple parameters for each shock from a data set that is probably small. Uncertainty methods should be used to allow for the variability in the parameters.

Basically, it is necessary to estimate the parameters p, λ, and μ. The analyst should refer to a report by Atwood (1980b) to estimate these parameters. The other parameters can be evaluated from p, λ, and μ.

5.7 UNCERTAINTIES

The data-development process, as presented herein, includes both classical and Bayesian viewpoints of uncertainty in parameter estimation. While these techniques treat, to some extent, the uncertainty that is related to the amount of data and the variability due to differences between data sources, there are other uncertainties that are not treated at all. This section briefly describes the potential sources of uncertainty and methods of judging their effects. In addition, Chapter 12 should be consulted for an overview of the treatment of uncertainty.

---

*Note that in Section 3.7 the beta factor is defined somewhat differently. For $k = 2$, these definitions are identical. When $k > 2$, the beta factor defined in Section 3.7 is a compromise among the various quantities r_k/r_1.

5.7.1 SOURCES OF UNCERTAINTY

Before discussing sources of uncertainty, it is important to remember what one may be uncertain about. This chapter has so far presented methods for estimating the following:

1. The failure rate of components.

2. The probability that components (or systems) fail on demand.

3. The probability that components (or systems) are unavailable because of testing or maintenance.

This estimation process involves the use of various models and estimates of the parameters in these models. Thus, there may be uncertainty in the models and/or the parameters.

Since the analyst first chooses a model for the data items, there is obviously some uncertainty in that selection, as no physical occurrence exactly fits a mathematical model. Next, there is uncertainty in the parameter of that model, even given that the model is correct. The sources for parameter uncertainty include (1) the amount of data, (2) the diversity of data sources, and (3) the accuracy of data sources.

5.7.2 PROCEDURES FOR TREATING MODELING UNCERTAINTIES

The first source of uncertainty mentioned above is that of model choice. The best way to determine the effect of this choice is to try another model--that is, perform a sensitivity assessment. The difference in the point estimate and confidence interval can then be reported. It is not expected that this will be an important contribution to uncertainty, and hence these extra evaluations need be done only for dominant events where the model does not seem to fit well.

5.7.3 PROCEDURES FOR TREATING PARAMETER UNCERTAINTIES

Uncertainty in the data parameters is already treated explicitly in the data process for certain sources by including uncertainty due to the amount of data. In addition, the data process can include differences between sources of data--that is, variability of an event's rate (or probability) of occurrence from one facility to another. In addition, the data process can be used to incorporate inaccuracies in the data sources. Of course, judgment is likely to enter into the process at this point. For example, in using data from licensee event reports, the number of demands is often estimated. Instead of treating this estimate as constant, the Bayesian approach could treat it as a random variate, while the classical approach could treat this value as a point estimate with error bounds.

5.8 DOCUMENTATION OF THE DATA BASE

An important aspect of developing the data for accident-sequence evaluation is to document the various steps of the process. This includes not only the final numbers but also the various assumptions and sources of information. The reader should be able to trace each data item from the fault tree or event tree back to the source, with each assumption and calculation apparent.

Documentation should include the output of the data process (i.e., the numbers used in quantification) and the general data base used in the PRA. These two types of documentation are discussed below.

5.8.1 DOCUMENTATION OF THE GENERAL DATA BASE

The general data base for the PRA includes all work from the source of data through the numerical results for the general types of events evaluated.

5.8.2 DOCUMENTATION OF DATA APPLIED TO EACH MODEL

The basic inputs to the task of accident-sequence quantification, and the outputs of the data process, are the numerical representations of each event. Forms like those shown in Figures 5-6 and 5-7 should be used to tie the specific events to the general data base.

Figure 5-6 is an example of a data table for hardware events. The first two columns, event name and description, come from the fault tree or the event tree. They give the alphanumeric code for an event and a brief description. The third column, the failure rate or probability of failure on demand, gives the data from the general data base for the type of event modeled. Note that the type of distribution and the parameters are included. The fault exposure time or mission time applies to events that occur as a function of time (either failure in time after a successful start or failure in time during standby). This time, then, is the length of time the component must survive to ensure success or the time between tests.

An example of tabular format for documenting test or maintenance acts is shown in Figure 5-7. The first column gives the event name as it appears in the fault tree or event tree. The second column is a brief description of the event. The third and fourth columns list the model used for act frequency and the model for the duration of the act. Note that these values could be average values, distributions, or point estimates with error factors. The fifth column contains a list of all the components included in the one act. For a test, this is often several components. This list helps to indicate the level in the tree where the act is modeled. Also included is a column for indicating the source of the information used to develop the act models.

BASIC EVENTS: HARDWARE						
Event name	Description	Failure rate or failure-on-demand probability	Fault exposure time or mission time (τ)	Data source	Quantification model	Comments
EVLV12	Valve fails to open	Lognormal 1×10^{-3} per demand Error factor = 3	NA	Reactor Safety Study	Distribution: lognormal 1×10^{-3} (3) mean: 1.3×10^{-3}	
EPM12F	Pump fails to start	Lognormal 1×10^{-3} per demand Error factor = 3	NA	Reactor Safety Study	Distribution: lognormal 1×10^{-3} (3) mean: 1.3×10^{-3}	
EPM12D	Pump discontinues running after start	Lognormal 3×10^{-5} per hour Error factor = 10	24 hr	Reactor Safety Study	Distribution: lognormal 7.2×10^{-4} (10) mean: 1.9×10^{-3}	
ECL12D	Clutch fails during mission	Lognormal 1×10^{-6} per hour Error factor = 20	24 hr	Reactor Safety Study	Distribution: lognormal 2.4×10^{-5} (20) mean: 1.3×10^{-4}	

Figure 5-6. Example of data table for hardware.

BASIC EVENTS: TEST AND MAINTENANCE ACTS							
Event name	Description	Frequency-of-act model	Duration-of-act model	Components in act block	Data source	Quantification model	Comments
EHPIMA	Maintenance of HPI leg A	1/3 month	Lognormal 4 hr Error factor = 1.5	Manual valve 11, MOV-12, pump	Plant data	Distribution: lognormal 1.8×10^{-3} (1.5) Point estimate: 1.9×10^{-3}	

Figure 5-7. Example of data table for test or maintenance acts.

The most important column in the tables is the quantification model. This column is the output of the data section and the input to sequence quantification. It includes the distribution and mean (or point estimate and interval estimates) for each specific event. Note that for time-dependent events it is a function of τ and the failure rate (see Section 5.5).

5.9 ASSURANCE OF TECHNICAL QUALITY

The term "assurance of technical quality," as used here, refers only to the quality of the data base that results from the procedures given in this chapter. Many factors affect the quality of the data base, including the overall programming, planning, and scheduling, as well as budget limitations; such items are discussed in Chapter 2, Section 2.3.3. The objective of this section is to address the items that will enhance the data quality within the program constraints.

The most beneficial activities to maximize quality are reviews and checks. As each data quantity is produced, it should be checked against other data bases. Major discrepancies should be justified. Other staff members should review the event quantifications for their models and cross-compare with others with the same type of events. Finally, the team leader should review the data, using his experience to look for unusual results. Of course, outside peer review is an important part of the review process, though feedback for revision via this path usually takes longer than does feedback within the study.

Documentation is the key to the quality of the data base. The data analyst should keep a notebook to document his decisions and assumptions. This notebook will make final documentation easier and make the data traceable from event results back to the source. It is also important to carefully document computer runs so that, if necessary, the runs producing particular results can be found. Often a keypunch error can result in an incorrect result.

REFERENCES

Ahmed, S., D. R. Metcalf, R. E. Clark, and J. A. Jacobsen, 1981. BURD--A Computer Program for Bayesian Updating of Reliability Data, NPGD-TM-582, Babcock & Wilcox, Lynchburg, Va.

Apostolakis, G., and S. Kaplan, 1981. "Pitfalls in Risk Calculations," Reliability Engineering, Vol. 2, pp. 135-145.

Apostolakis, G., S. Kaplan, B. J. Garrick, and R. J. Duphily, 1980. "Data Specialization for Plant-Specific Risk Studies," Nuclear Engineering and Design, Vol. 56, pp. 321-329.

Apostolakis, G., and A. Mosleh, 1979. "Expert Opinion and Statistical Evidence: An Application to Reactor Core Melt Frequency," Nuclear Science and Engineering, Vol. 70, pp. 135-149.

Atwood, C. L., 1980a. Common Cause and Individual Failure and Fault Rates for Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, draft, EGG-EA-5289, EG&G Idaho, Inc., Idaho Falls, Idaho.

Atwood, C. L., 1980b. Estimators for the Binomial Failure Rate Common Cause Model, USNRC Report NUREG/CR-1401.

Atwood, C. L., 1982a. Common Cause Fault Rates for Pumps: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, January 1972-September 1980, USNRC Report NUREG/CR-2098.

Atwood, C. L., 1982b. Common Cause Fault Rates for Instrumentation and Control Assemblies: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1978, USNRC Report NUREG/CR-2771.

Atwood, C. L., and J. A. Steverson, 1982a. Common Cause Fault Rates for Diesel Generators: Estimates Based on Licensee Event Reports at U.S. Nuclear Power Plants, 1976-1978, USNRC Report NUREG/CR-2099.

Atwood C. L., and J. A. Steverson, 1982b. Common Cause Fault Rates for Valves: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1980, USNRC Report NUREG/CR-2770.

Atwood, C. L., and W. J. Suitt, 1982. User's Guide to BFR, A Computer Code Based on the Binomial Failure Rate Common Cause Model, USNRC Report NUREG/CR-2729.

Barlow, R. E., and F. Proschan, 1975. Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc., New York.

Bayes, T., 1958. "Essay Toward Solving a Problem in the Doctrine of Chances" (reprinted), Biometrika, Vol. 45, pp. 293-315.

Brown, B., and O. Helmer, 1964. Improving the Reliability of Estimates Obtained from a Consensus of Experts, P-2986, the Rand Corporation, Santa Monica, Calif.

Chhikara, R. S., and J. L. Folks, 1977. "The Inverse Gaussian Distribution as a Lifetime Model," Technometrics, Vol. 19, pp. 461-468.

De Groot, M. H., 1974. "Reaching a Consensus," Journal of the American Statistical Association, Vol. 69, pp. 118-121.

Du Charme, W. M., and M. L. Donnell, 1973. "Intrasubject Comparison of Four Response Modes for 'Subjective Probability' Assessment," Organizational Behavior and Human Performance, Vol. 10, pp. 108-117.

Eisenberg, E., and D. Gale, 1959. "Consensus of Subjective Probabilities: the Pari-Mutuel Method," Annals of Mathematical Statistics, Vol. 30, pp. 165-168.

Fischhoff, B., P. Slovic, and S. Lichtenstein, 1981. "Lay Foibles and Expert Fables in Judgments About Risks," in R. O'Riordan and R. K. Turner (eds.), Progress in Resource Management and Environmental Planning, Vol. 3, John Wiley & Sons, Chichester, England.

Green, A. E., and A. J. Bourne, 1972. Reliability Technology, Wiley-Interscience, New York.

Guttman, I., 1970. "Tolerance Regions: Classical and Bayesian," Griffin Statistical Monographs, Griffin, London, England.

Hahn, G. J., and S. S. Shapiro, 1967. Statistical Models in Engineering, John Wiley & Sons, Inc., New York, Chapter 8.

Hald, A., 1952. Statistical Theory with Engineering Applications, John Wiley & Sons, Inc., New York.

Holloway, C. A., 1979. Decision Making Under Uncertainty: Models and Choices, Prentice Hall, Englewood Cliffs, N.J.

Jeffreys, H., 1961. Theory of Probability, 3rd ed., Clarendon Press, Oxford, England.

Kaplan, S., 1981a. "On a Two-Stage Bayesian Procedure for Determining Failure Rates from Experiential Data," IEEE Transactions on Power Apparatus and Systems (preprint).

Kaplan, S., 1981b. "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations--Applications to Seismic Risk Assessment," Risk Analysis, Vol. 1, No. 3.

Lapides, M. E., and E. L. Zebroski, 1975. Use of Nuclear Plant Operating Experience To Guide Productivity Improvement Programs, EPRI SR-26-R, Electric Power Research Institute, Palo Alto, Calif.

Lichtenstein, S., B. Fischhoff, and L. D. Phillips, 1977. "Calibration of Probabilities: The State of the Art," in H. Jungermann and G. DeZeeuw (eds.), Decision Making and Chance in Human Affairs, D. Reidel, Amsterdam, the Netherlands.

Mann, N. R., R. E. Shafer, N. D. Singpurwalla, 1974. Methods for Statistical Analysis of Reliability and Life Data, John Wiley & Sons, Inc., New York.

Martz, H. F., and M. Bryson, 1982. "On Combining Data for Estimating the Frequency of Low-Probability Events with Application to Sodium Valve Failure Rates," to be published in Nuclear Science and Engineering.

Martz, H. F., and R. Waller, 1978. An Exploratory Comparison of Methods for Combining Failure-Rate Data from Different Data Sources, LA-7556-MS, Los Alamos National Laboratory, Los Alamos, N.M.

Martz, H. F., and R. Waller, 1982. Bayesian Reliability Analysis, John Wiley & Sons, New York.

McClymont, A., and G. McLagan, 1982. Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis, EPRI NP-2433, Electric Power Research Institute, Palo Alto, Calif.

Mosleh, A., and G. Apostolakis, 1982. "Some Properties of Distributions Useful in the Study of Rare Events," to be published in IEEE Transactions on Reliability.

Morris, P. A., 1974. "Decision Analysis Expert Use," Management Science, Vol. 20, pp. 1233-1241.

Morris, P. A., 1977. "Combining Expert Judgment: A Bayesian Approach," Management Science, Vol. 23, pp. 671-693.

Murphy, J., 1980. Component Failure Rates for Nuclear Plant Safety System Reliability Analysis, draft report, U.S. Nuclear Regulatory Commission, Washington, D.C.

Parry, T. W., and P. W. Winter, 1981. "Characterization and Evaluation of Uncertainty in Probabilistic Risk Analysis," Nuclear Safety, Vol. 22, pp. 28-42.

Seaver, D. A., D. V. Winterfeldt, and W. Edwards, 1978. "Eliciting Subjective Probability Distributions on Continuous Variables," Journal of Organizational Behavior and Human Performance, Vol. 21, pp. 379-391.

Spetzler, C. S., and C. A. S. Stael von Holstein, 1975. "Probability Encoding in Decision Analysis," Management Science, Vol. 22, pp. 340-358.

Stael von Holstein, C. A. S., 1970. Assessment and Evaluation of Subjective Probability Distributions, the Economic Research Institute, Stockholm School of Economics, Stockholm, Sweden.

Stone, M., 1961. "The Opinion Pool," Annals of Mathematical Statistics, Vol. 32, pp. 1339-1342.

Tversky, A., and D. Kahneman, 1974. "Judgment Under Uncertainty: Heuristics and Biases," Science, Vol. 185, pp. 1124-1131.

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

Winkler, R. L., 1967. "The Assessment of Prior Distributions in Bayesian Analysis," Journal of the American Statistical Association, Vol. 62, pp. 776-800.

Winkler, R. L., 1968. "The Consensus of Subjective Probability Distributions," Management Science, Vol. 15, pp. B61-B75.

Winkler, R. L., and L. L. Cummings, 1972. "On the Choice of a Consensus Distribution in Bayesian Analysis," Organizational Behavior and Human Performance, Vol. 7, pp. 63-76.

Chapter 6

Accident-Sequence Quantification

6.1 OVERVIEW

6.1.1 INTRODUCTION

This chapter describes the process of quantifying accident sequences, which, as described in Section 3.4, are developed by an event-tree procedure that considers both initiating events and the success or failure of the relevant systems (or functions) in succession. The quantification may address each individual sequence or each of several groups of sequences, called "plant-damage bins" (PDBs), formed by combining sequences with certain similarities. Depending on the purpose and the intended use of the study, it may be desirable to estimate the uncertainty in the analysis that results from uncertainties in estimating the frequencies of initiating events and the probabilities of primary events. As defined in Chapter 3, primary events include basic events, undeveloped events, developed events, and external events. Both primary and secondary failures may be modeled by primary events.

The quantification task uses combinations of primary-event probabilities and the Boolean expressions developed in Chapter 3 to calculate a sequence frequency. Two approaches to this task are outlined. One approach is fault-tree linking, which determines the minimal cut sets for an accident sequence or a plant-damage bin. The minimal cut sets of an accident sequence are subsequently quantified to produce an estimated frequency for an accident sequence or a plant-damage bin. The other approach, which uses event trees with boundary conditions, quantifies system models under various conditions and multiplies system-failure probabilities by initiating-event frequencies to estimate an accident-sequence frequency.

Each accident sequence contains an initiating event and the subsequent failure of one or more safety systems. The system failures can represent combinations of faults undetected before the initiating event, failures of components or the operator to act on demand, failures of components to operate throughout a specified interval, or component unavailabilities due to testing or maintenance. In each case the component is functionally ineffective and unable or unavailable to carry out its mission. The probability of any of these faults is termed "failure probability." Thus, as used here, "failure probability" incorporates failure to start and/or failure to operate. The primary-event types and models for their treatment, including means or other distribution parameters, are described in Chapters 4 and 5. If the accident-sequence frequency is to be expressed as a point value, point-value estimates for primary events will be required. Possible point-value estimates include the mean, median, maximum-likelihood, and engineering estimates. Whichever point-value estimate is selected, the basis and the rationale for its selection should be given.

The results of the accident-sequence quantification task may or may not be the last task of the PRA study. In a level 1 PRA (see Chapter 2), where the objective is the quantification of core-melt sequences, the final product is the estimated frequency of the accident sequences, and there may be no need to distinguish these sequences in more detail than by the occurrence of core melt. In the more general case, in which containment failure, radionuclide release, or offsite consequences are to be analyzed (level 2 or 3 PRA), the results of the accident-sequence quantification are used as input to the containment analysis described in Chapter 7. In this case, the containment analyst will provide guidance as to which sequences are to be aggregated into the various plant-damage bins.

Besides the results generated for use in the risk assessment, the fault trees, event trees, and logic models can provide great insight into design and operation. They can be used to obtain both quantitative and qualitative information about systems. Quantitative techniques are available for using fault-tree models to derive reliability parameters (Henley and Kumanoto, 1981) and importance measures (Barlow and Proschan, 1975; Lambert and Gilman, 1977) for systems and components appearing in the accident-sequence models. Qualitatively, the models have a number of uses, from determining the minimal cut sets for a system to using variable transformations to analyze common-cause events (Worrell and Stack, 1981).

The remainder of this overview section discusses general approaches to accident-sequence quantification. Section 6.2 identifies the inputs to event-tree quantification: initiating events, component-failure values, dependent failures, and system fault trees. Section 6.3 covers the steps in accident-sequence quantification; it also discusses the treatment of multiple sequences, which can be combined into plant-damage bins, and presents the logic for reducing the quantification effort through screening and truncating. Section 6.4 describes methods for treating uncertainties and tracing their propagation through the accident sequences. Section 6.5 discusses some modeling considerations for accident-sequence quantification.

Section 6.6 discusses the computer codes that can be used for event- and fault-tree quantification or searches to identify potential dependent failures. Finally, Sections 6.7 and 6.8 summarize requirements for documentation and the assurance of technical quality, respectively.

6.1.2 APPROACHES TO ACCIDENT-SEQUENCE QUANTIFICATION

This section describes ways of evaluating the frequency of accident sequences from the initiating event, fault-tree models of the systems, and event-tree descriptions of the system failures making up that sequence. The fault trees are the logic models for combining faults (primary events) within a system or sequence; they are a set of Boolean expressions that can be reduced to minimal cut sets via Boolean algebra. These minimal cut sets represent the smallest sets of primary events that must exist simultaneously for the system failure (or sequence) to occur. A probability expression for the top event of the system failure or sequence can be determined from the minimal cut sets and used to quantify the probability of the top event.

Chapter 3 describes how the fault trees are developed to obtain Boolean expressions for each sequence. Additional information regarding fault-tree development and reduction as well as Boolean algebra can be found in the Fault Tree Handbook (Vesely et al., 1981a) and Applied Boolean Algebra (Hahn, 1966). In the discussion that follows, it is assumed the reader is familiar with these concepts.

At least two distinct approaches have so far been used to quantify the frequencies of accident sequences. One consists of combining system and component failures that are not necessarily independent; the other consists of combining event-tree tops that are all independent. The first approach automatically takes into account intersystem dependences within a sequence; the second method involves two steps--the quantification of each independent top event and the multiplication of the probabilities of those top events to get a sequence frequency. The quantification method chosen should correspond to the method used to create event- and fault-tree models.

Fault-Tree Linking

This approach combines (links) the fault trees for the event-tree tops (system headings) with an AND gate to form a new top event that is the accident sequence. Furthermore, if accident sequences with the same initiating event are combined in the same plant-damage bin, an OR gate may be used to combine the accident-sequence fault trees into a single model. Since initiating events are assumed to be mutually exclusive, the estimated frequencies for sequences with different initiating events can be summed to produce an estimated frequency of the plant-damage bin. The assumptions and ramifications of ORing the sequences in a bin are discussed in Section 6.3. A fault-tree-reduction code is then used to find the minimal cut sets of this new top event. Any dependences in the way of shared components or support systems are thus automatically accounted for in the Boolean reduction process, provided that unique identifiers have been assigned to these components across the respective fault trees. With this process the quantification takes place on the overall sequence cut sets as opposed to the individual systems or subsystems.

Event Trees with Boundary Conditions

In this approach, dependences like those between a support system and two or more front-line systems are explicitly displayed in the event tree. A front-line system is a system that directly performs a safety function, an example being the high-pressure injection system. A support system is a system that is needed for a front-line system to perform its safety function; an example is the ac electric power system. Each system is quantified for every set of boundary conditions that have a unique effect on system-failure probability, where the boundary conditions are a given set of component and system states that affect the system being quantified. The quantification involves the calculation of conditional probabilities since specific component and system states are assumed. Events are combined within the event tree by multiplication to obtain estimated frequencies or approximate frequency distributions for each sequence. The estimated sequence frequencies within each plant-damage bin are then summed to obtain a total estimated frequency for each bin.

6.2 INPUTS TO ACCIDENT-SEQUENCE QUANTIFICATION

The plant logic model consists of the event trees and fault trees developed in Chapter 3. It is composed of various primary events, which may be initiating events, component failures, unavailabilities due to testing or maintenance, recovery failures, dependent failures (beta factors), human errors, or external events. All primary-event values are expressed as probabilities except for the values of initiating events, which are frequencies, and the values of external events, which can be frequencies or probabilities. Table 6-1 lists the sources for primary-event values in this document. Solution of the plant logic model yields combinations of initiating events and system failures that are evaluated to yield accident-sequence frequencies.

Table 6-1. Sources of primary-event values

Primary event	Source (section)
Initiating event	5.3.4
Component failure	
Failure on demand	5.3.1.1.2
Failure in time (standby)	5.3.1.1.2
Failure in time (annunciated)	5.3.1.1.2
Failure in time after successful start	5.3.1.1.2
Test unavailability	5.3.2
Maintenance unavailability	5.3.3
Recovery (i.e., nonrecovery)	5.4
Dependent failures (beta factors)	5.4
Human errors	4
External events	10

Figure 6-1 shows the important elements in the quantification procedure. This particular diagram illustrates the steps in the fault-tree-linking approach. When event trees with boundary conditions are used, the steps are somewhat different, as will be described in Section 6.3; however, the inputs, as indicated within the broken lines, are similar.

Before quantification begins, the logic models are defined and developed as described in Chapter 3. Consistent event trees and the fault-tree models required by their top events (headings) are developed by the systems analyst(s). These logic models go hand in hand regardless of whether fault-tree linking or event trees with boundary conditions are used in quantification. The fault-tree logic models identify the primary events in sufficient detail for the data analyst to interpret them and provide models and the associated parameters for their quantification, including undependabilities and frequencies, and their distribution parameters if uncertainty is to be propagated.

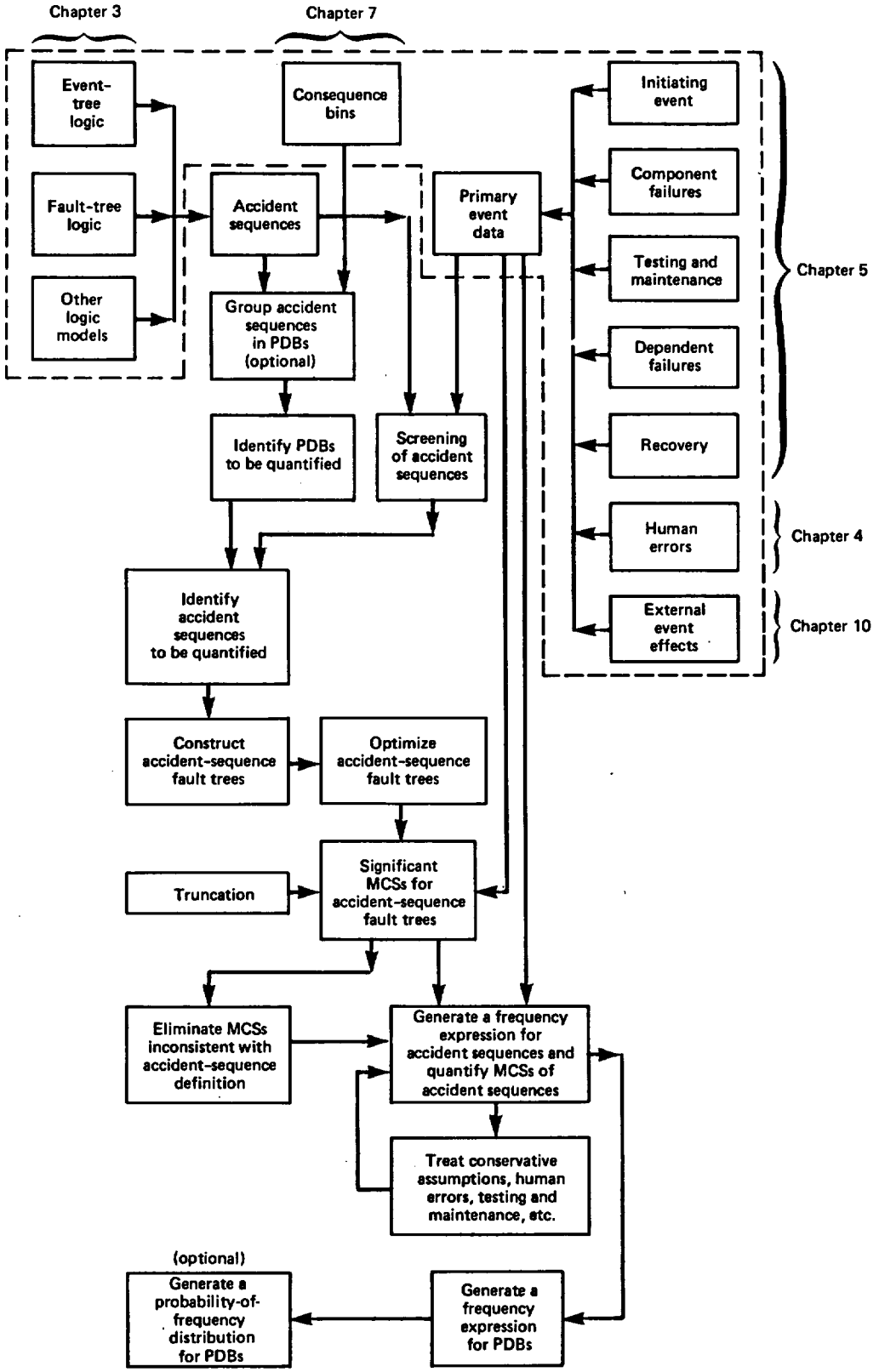


Figure 6–1. Inputs and steps for quantification.

The data base (models and parameters) for hardware failures and for test and maintenance activities is provided in Chapter 5, while that for human errors either in maintenance or during post-accident recovery procedures is provided in Chapter 4. The analysis of external hazards is conducted as described in Chapter 10, if that option is part of the study scope.

The event trees for each initiating event define the accident sequences to be evaluated, including the definition of the set of system faults that are included in each. The fault-tree models indicate the primary-event faults and fault combinations that cause these system faults to occur.

The consequences of accident sequences are then evaluated by the process described in Chapter 7. This process may or may not group the accident sequences into plant-damage bins. However, because of the similarities among certain accident sequences and the amount of work involved in their analysis, the accident sequences are usually so grouped. For our purposes a PDB can contain one accident sequence (in which case the PDB and the accident sequence are synonymous) or many accident sequences if the results of the containment analysis so specify. Basically, the binning process provides some ability to combine and reduce the total number of sequences in quantification, but binning is not a requirement for quantification.

6.3 QUANTIFICATION OF ACCIDENT SEQUENCES

6.3.1 GENERAL PROCEDURE

Accident-sequence analysis begins with the identification of the accident sequences to be analyzed, usually followed by a grouping of accident sequences into plant-damage bins, as defined by the consequence analysis. Sequences that cause similar physical responses in the plant are grouped into the same bin. The selection criteria for a PDB can be as coarse as "core melt" or "no core melt" or so fine as to require a unique bin for each accident sequence. The accident sequences in each bin may then be screened to eliminate those that will not contribute significantly to the total frequency of the bin.

Once the accident sequences to be quantified have been screened, a probability expression for each sequence is created from the solution of the plant logic model and then used to combine the estimated values for initiating and primary events. The two methods described in this section (i.e., fault-tree linking and event trees with boundary conditions) differ in this part of the process. In fault-tree linking, the accident sequence is represented by a fault tree whose top event is an AND gate with inputs representing the top gates of the system fault trees for each system depicted in the accident sequence. System dependences are explicitly treated in the fault-tree logic. The resultant sequence fault tree can then be analyzed by a number of available fault-tree-reduction techniques. The result of this step is a set of accident-sequence minimal cut sets (discussed in Chapter 3)

whose frequency estimates dominate the frequency of the accident sequence. The cut sets are then used to develop a probability expression for determining the sequence or bin frequency. This frequency can be characterized as a distribution or as an estimate.

If the analyst elects to use the other quantification method--event trees with boundary conditions--each branch of the event tree is evaluated, with the appropriate boundary conditions reflecting the various states of the support systems appearing in the path of the accident sequence. Thus these support dependences are treated within the event tree. Once all branch-point probabilities have been quantified, the accident-sequence frequency is obtained by simply multiplying the probabilities of the branch points in the accident sequence. If uncertainty calculations are to be made, the uncertainty for each branch point is derived and propagated through the accident sequence.

Both fault-tree linking and the use of event trees with boundary conditions result in point estimates for accident sequences or plant-damage bins. Section 3.7, "Analysis of Dependent Failures," explains the basic premise of both approaches and the fact that both methods, when rigorously applied, will result in equivalent solutions. However, since both methods apply some approximations and assumptions in practice, the final results for any given solution may vary if the assumptions used are not carefully examined. Fault-tree linking and event trees with boundary conditions are described below in Sections 6.3.2 and 6.3.3, respectively.

6.3.2 FAULT-TREE-LINKING METHOD

This approach involves constructing accident-sequence fault trees, solving these fault trees for dominant cut sets, generating a probability expression from the accident-sequence dominant cut sets, and combining the probability expressions for each accident sequence into an expression for the entire plant-damage bin.

6.3.2.1 Identification of Accident Sequences To Be Quantified

The first step is the identification of the accident sequences to be quantified. Of some help in this is the concept of plant-damage bins (PDBs), which are generated during the consequence analysis when accident sequences use the same mapping to release categories. When a PDB contains more than one sequence, the probabilities of the accident sequences can be summed to yield a PDB frequency that is mapped with the release categories. However, if the mutual exclusivity of the accident sequences has been lost (i.e., success states were not modeled in the accident logic), a conservative result may be obtained when the algebraic sum is used. This potential problem can be reduced by using a logical OR to combine accident sequences that are not mutually exclusive, thereby eliminating cut sets or sequences that subsume others within the PDB.

Valuable information can be gained by examining the release-category mapping for each PDB. This information can be used to establish the relative effects of each PDB on the analysis results and determine which ones will have the greatest effect on the results of the consequence analysis. This will allow the analyst to ensure that low-probability/high-consequence sequences will not be left out of the analysis. Some analysts choose sequences without regard to the PDBs, whereas others rely on the PDBs for guidance in choosing sequences for quantification. If accident sequences are chosen without regard to PDBs, a small-probability cutoff is used to eliminate sequences from consideration. If that cutoff results in the elimination of all sequences from the more-severe PDBs, the truncation value is lowered until sequences in the most-severe PDBs appear. Care must be taken to ensure that all significant contributions to bin frequency are taken into account, including the contributions of large numbers of low-frequency sequences.

If PDBs are used to group sequences, a number of approaches for eliminating accident sequences are available. If the frequency of a particular PDB can be shown to be less than the frequency of other, more-severe, PDBs, the entire PDB and its sequences can be eliminated.

Within a particular PDB chosen for quantification, some sequences can be discarded for any one of several reasons. Boolean reduction, at the system level, can eliminate several sequences in a PDB. It may be possible to estimate the frequency of some of the sequences and to eliminate those that do not significantly contribute to the PDB frequency. Finally, sequences within a PDB that are identical except for their initiating events can be modeled as one sequence, with a single initiating-event frequency representing the combined frequencies of the initiating events.

Boolean manipulation of the accident sequences in a PDB can generate a subset of sequences that can replace the original set of sequences. For example, given accident sequences TABC and $T\bar{A}BC$, where A, B, and C are system fault trees identical for both sequences, the Boolean properties of consensus and subsuming terms allow us to perform the following:

$$TABC + T\bar{A}BC = TBC$$

thereby replacing two more complex sequences with one simple sequence. A practical amount of sequence reduction at the sequence level can decrease the number of sequences that must be analyzed.

Some systems represented in the accident sequences are sufficiently similar to systems analyzed elsewhere that a reasonable failure-probability estimate can be used. In some cases, it may be possible to estimate the probability of a sequence, keeping in mind the potential systems interactions. If an accident sequence has a very low probability estimate, in comparison with the other sequences in its PDB, it can be eliminated from further analysis.

6.3.2.2 Construction of Accident-Sequence Fault Trees

The accident-sequence fault tree has an AND gate as its top gate. The inputs to the top gate are as follows:

1. The initiating event.

2. The system fault trees for the system failures depicted in the accident sequence. The minimal cut sets of the Boolean intersection of the system fault trees will be called the "system-failure minimal cut sets."

3. The dual fault trees for the system successes depicted in the accident sequence. (A dual fault tree is a success tree--the complement of the normal fault tree.)

Inclusion of the dual fault trees used to model system successes will eliminate system-failure minimal cut sets, which cause the failure of a system defined to be in a state of success. This will prevent system-failure cut sets from appearing in multiple accident sequences. The inclusion of these dual fault trees can greatly complicate the analysis and may not be required to obtain the desired result. The elimination of accident-sequence cut sets violating system-success states defined in accident sequences is discussed later in this section.

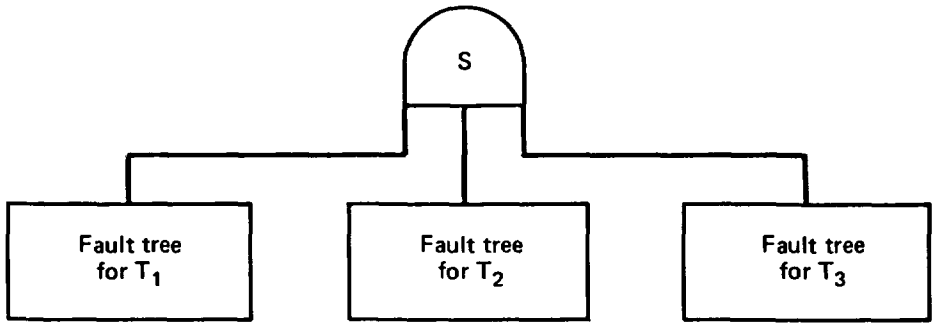
In fault-tree linking, there is a potential for the problem of the so-called circular-logic loop. When a number of fault trees are linked together, certain types of dependences can result in a situation where the failure of system A causes the failure of system B and the failure of system B causes the failure of system A. Any attempt to combine the two fault trees for these systems will meet with difficulties unless one branch of the circular logic is artificially cut off. Such problems would be revealed by the fault-tree processing code. Should this situation arise, it should be brought to the attention of the fault-tree modeler(s), who should modify the logic in one of the fault-tree logic models accordingly.

6.3.2.3 Optimization of Fault Trees

The number of events in the system fault trees can be substantially reduced by defining an equivalent system fault tree in which independent subtrees (modules) are replaced by developed events. The independent subtrees must be independent with respect to all of the systems represented in the accident sequence, including the initiating-event fault tree.

The concept of independent subtrees is relative to the top event of the fault tree being evaluated. In a particular event-tree sequence, such as $S = T_1 * T_2 * T_3$, a subtree of T_1 may be independent in fault tree T_1 but may contain events that also appear in T_2. This implies that the subtree is not independent with respect to the event-tree sequence S. The subtrees

that are independent with respect to S are found by identifying the independent subtrees of the following accident-sequence fault tree:



However, if this approach is taken for each event-tree sequence, then the independent subtrees will have to be identified for each event-tree sequence. A more efficient approach is to identify the independent subtrees relative to the intersection of all system failures represented in the event tree. Then the independent subtrees will be independent for any sequence of system failures and system successes. Some of the advantages of this approach are the following:

1. Once the independent subtrees have been identified, they can be used for any event-tree sequence.

2. Quantification and evaluation of the independent subtrees need to be done only once and will apply to all event-tree sequences.

3. The fault-tree analyst who wishes to verify that the reduced fault trees are equivalent to the original fault trees needs to become familiar with only one set of independent subtrees that applies to all event-tree sequences.

The concept of independent subtrees is very powerful, and their use is almost always beneficial. The fault-tree analyst can frequently create independent subtrees while coding his tree for computer analysis, although care should be taken to ensure that only events appearing as a group are included in the module. Because of the relative simplicity of the independent subtrees, a number of more-sophisticated analysis techniques, such as an analysis of time-dependent failures, can be performed on the independent subtree and the results included in the accident-sequence fault tree as a primary event with an associated probability.

6.3.2.4 Determination of Significant Minimal Cut Sets for an Accident Sequence

The accident-sequence minimal cut sets can represent the solution to a very large fault tree because the accident-sequence fault tree is formed by combining, under an AND gate, several system fault trees. Consequently, there may be millions or even billions of minimal cut sets for a particular

accident sequence. In order to minimize the number of minimal cut sets at this stage of the analysis, the dual fault trees representing system successes are typically not included at this time. (Although their inclusion would eliminate some system-failure minimal cut sets, it greatly increases the size and complexity of the fault-tree model being analyzed.) To reduce the number of minimal cut sets, a truncation value can be used to eliminate cut sets that make a negligible contribution to the total sequence probability. Note that truncation eliminates minimal cut sets that do belong to the set of the minimal cut sets for the accident sequence, whereas not including system-success states may leave in, for the time being, sets of primary events that appear to be the minimal cut sets of the accident sequence but, in fact, are not.

The truncation process eliminates minimal cut sets from the set of minimal cut sets for the accident sequence and thus is nonconservative. If a suitably low truncation value is used, the effect on the total accident-sequence probability is slight. Since this process is nonconservative, care must be taken to ensure that an appropriate truncation value is used. The truncation value should be constant or increasing throughout the solution process. The effect of the truncation value used should be bounded and shown to be insignificant. If at any time after truncation the point estimate of a primary event is increased, the truncation is not valid, and the process must be repeated with the new value.

In truncation the primary events are treated as if they are statistically independent and any dependences have been incorporated into the primary-event probabilities. A problem that may lead to a nonconservative result can arise when the cut set includes components whose failure probability was derived from pooled information under the assumption that they are identical. When the primary-event probabilities for those components are multiplied together, the result may be smaller than the result obtained by a cut-set evaluation that uses a single distribution or confidence bound to represent both components. If the uncertainty in the point estimate is relatively small, the error thus introduced is not significant. However, this error can become important when uncertainties are large. Unfortunately, at present there is no automated approach to this problem, and therefore analysts should use care to minimize this effect.

If the remaining cut sets are processed in any manner that serves to increase their likelihood (i.e., the addition of beta factors or common-cause human-error events), the truncation process is invalid, because some of the truncated cut sets could be increased in value above the truncation point. When truncation is used, all primary-event commonalities must be explicitly represented in the fault tree.

The cut sets that survive the truncation must then be examined to eliminate those that are inconsistent with the accident-sequence definition. The cut sets are inspected and modified to remove overly conservative assumptions about primary-event data. The minimal cut sets can be inconsistent with the accident-sequence definition for the following reasons:

1. The cut set may violate the system-success states in the sequence.

2. Cut sets may contain mutually exclusive primary events.

These minimal cut sets can be eliminated either manually or through the use of fault-tree models and computer codes.

The system-success states appearing in the accident-sequence fault tree can be accounted for by directly inspecting the minimal cut sets when there are few significant minimal cut sets. Unfortunately, a large number of significant minimal cut sets may prohibit direct inspection. It is then necessary to use a computer code, which can be done by either of two methods: list matching or the dual-fault-tree approach.

The list-matching approach is based on the fact that, if a minimal cut set for the system-failure portion of an accident sequence will also imply the failure of a system required to be in a success state, this minimal cut set should be deleted. List matching is performed by matching the failure cut sets of the accident sequence with the fault tree for system success. Any sequence-failure minimal cut set that is an implicant of a minimal cut set for a system success can be eliminated.

The dual-fault-tree approach involves obtaining the set of minimal cut sets of the dual fault tree and forming the Boolean conjunction of this set with the set of minimal cut sets for the accident-sequence failures. This process eliminates any terms that are products of an event and its complement because $P * \bar{P} = \phi$. To get a result of the same form as that obtained with list matching, the complemented events are deleted, and the resulting cut sets are simplified and reduced. Care must be taken to ensure that primary-event definitions are consistent for the system fault trees and dual fault trees.

When multiple failure modes of components appear in the system fault trees (e.g., switch A fails open and switch A fails closed) without modeling the mutually exclusive nature of these events, it is possible for minimal cut sets to contain mutually exclusive primary events. Such minimal cut sets should be eliminated, either through direct inspection or by using a computer code and a transformation of variables to explicitly model the mutually exclusive failure modes. Applying the identity $P * \bar{P} = \phi$ will accomplish this. These techniques have been used in modeling operational procedures such as technical specifications and plant management policy.

If conservative assumptions have been made about component recovery from failure or conservative probability estimates have been used in screening cut sets, it may be desirable to treat these conservatisms in a more realistic manner. Two methods are used to this end:

1. Some accident-sequence cut sets may contain events where repair or recovery may occur before the time the component is required to perform its function. This stems from a desire to simplify the system models or the fact that recovery from equipment failures can be dependent on other failures that have occurred. When the system analyst has determined that credit for a recovery act can be taken, that recovery act can be appended to the cut set as a primary event with an associated probability, thereby reducing the probability of the cut set.

2. If a conservative probability estimate has been used in the cut-set-screening process, more realistic estimates may be used if such data are available.

If conservatism in the screening process has been excessive, then a relaxation of the conservatisms may lower cut-set probabilities drastically. This may necessitate additional fault-tree quantification since cut sets previously excluded in the truncation process may become relatively significant.

6.3.2.5 Quantification of Accident-Sequence Cut Sets

The quantification of accident-sequence cut sets begins with the generation of a probability expression for the sequence minimal cut sets. This expression is then used to quantify the accident sequence by using the estimated values for primary-event probabilities and estimated initiating-event frequencies to yield a best-estimate value for the frequency of the event sequence. The probability expression is also used as the basis for the uncertainty analysis described in Section 6.4.

A number of techniques are available to generate probability expressions for the minimal-cut-set representation of accident sequences (Barlow and Proschan, 1975). They range from generating an upper bound by means of the sum-of-products rare-event approximation (often adequate in nuclear plant risk analysis because of the small numerical magnitude of the core-melt risk frequencies), using bounding techniques that generate both upper and lower bounds, or generating the exact probability expression for the top event. Where the sum-of-products method yields an overconservative expression for the accident-sequence frequency (e.g., system-success probabilities and the failure probabilities of less reliable individual systems would have cut sets that do not fit the rare-event approximation), one of the bounding techniques or an approximation of the exact expression can be used.

When an approximation other than the sum of products is used, it is usually done by eliminating cut-set intersections that do not contribute to the final result probabilistically. The approximation can be conservative or nonconservative, but the effects on the final result must be shown.

Generation of the probability expressions can be extremely difficult: most computer codes that generate an exact probability expression are generally unable to handle more than a few hundred minimal cut sets because of the required computer time and storage. However, a new method (Corynan, 1982) may significantly increase this number.

Two techniques are used to generate, for accident sequences, Boolean expressions that can be more efficiently quantified: the creation of independent subtrees (modularization) and the creation of mutually exclusive sets of cut sets. These techniques are described below.

The use of independent subtrees, or modules, allows the analyst to replace a portion of the fault tree with a single event. A probability expression for the independent subtree is then generated, and a probability

for the single event is created. This process combines a number of cut sets and greatly reduces the work of constructing the probability expression. Care must be taken, however, to ensure that an independent subtree is truly independent with respect to all logic within an accident sequence. The probabilities (e.g., unavailabilities) calculated for the independent subtree may also be time dependent for nonrepairable failures (see the discussion of nonrepairable failures in Chapter 5).

If a plant-damage bin containing multiple accident sequences is to be quantified, the probability expressions for the accident sequences within the bin must be combined. If the sequences have retained their mutual exclusivity, the probability expressions can simply be summed. However, the fault-tree-linking method usually does not yield mutually exclusive accident-sequence cut sets. The sequence-probability expressions can be summed to yield a conservative result in this case. If more exact results are desired, advantage can be taken of the fact that initiating events are generally treated as mutually exclusive. The PDB cut sets can be put into mutually exclusive groups by sorting the accident-sequence cut sets by initiating event. These groups are mutually exclusive, and their probability expressions can be summed to yield an expression for the entire PDB. Care must be taken to ensure that the combined initiating events are identically defined.

Once a probability expression for a plant-damage bin has been developed, the frequency for the bin can be obtained by replacing the variables in the probability expression with their best estimates and evaluating the equations. If a distribution for the frequency of the bin is desired, the uncertainty analysis described in Section 6.4 can be used to propagate primary-event distributions to obtain a probability-of-frequency distribution.

6.3.2.6 Evaluation of Common-Cause Events and Dependences

Fault-tree linking provides a structure that can be used to perform the common-cause analysis described in Section 3.7. The dependent-failure approach and the qualitative common-cause search can be applied to the fault tree directly or to the minimal cut sets of the accident-sequence fault tree. The approach taken depends primarily on the number of minimal cut sets generated by the accident-sequence fault tree since the solution and enumeration of large numbers of cut sets are impractical.

If the dependent-failure approach is to be used for quantifying common-cause events, there are at least two distinct methods for applying it. Typically with small fault-tree models generating hundreds of cut sets, the beta-factor method can be applied on a cut-set basis. This approach requires that all the minimal cut sets for the fault tree be generated (i.e., no probability truncation) and that each cut set be individually examined to determine whether a dependent-failure probability should be applied to increase the cut-set frequency or probability. Since all the cut sets must be generated and examined, there is a limitation on the total number of cut sets that can be analyzed. While it may prove to be impractical to apply dependent-failure probabilities to all the cut sets of the accident

sequence, it may be possible to apply them to the cut sets of independent subtrees within the accident-sequence fault tree, since the independent subtrees are quantified individually and replaced by primary events within the accident-sequence fault tree. If the fault tree has been modularized, care must be taken that dependences between modules are calculated and included.

For accident-sequence fault trees that generate too many minimal cut sets for using dependent-failure probabilities on an individual basis, Section 3.7 describes a method for introducing dependent-failure probabilities as primary events in the system fault trees. This method uses solutions at intermediate gates of the accident-sequence fault tree to analyze portions of systems and derive dependent-failure probabilities from those solutions. The accident-sequence fault tree is then modified to include new primary events representing the dependent-failure probabilities, at the appropriate places. The modified fault trees are then solved in a normal typical fashion (including truncation) to yield a result with dependent-failure probabilities included.

Similarly, qualitative searches can be made for common-cause events on the accident-sequence cut sets (Burdick et al., 1976; Rooney and Fussell, 1978; Worrell and Stack, 1981). As already discussed, if any cut sets were eliminated during the fault-tree solution, the common-cause analysis is not complete, and the results of common-cause searches may not include all significant common-cause events. One way around this problem is to break the accident-sequence fault tree into subtrees for which all the cut sets can be obtained. The cut sets for each subtree are then searched for common-cause modes within that subtree and the results are propagated to the top of the accident-sequence fault tree (Wagner et al., 1977). In this manner all the cut sets can be analyzed.

Another approach to the common-cause search is to use a transformation-of-variables technique to change the fault tree to a form reflecting the effects of common-cause events; it has been described by Rasmuson et al. (1979), Putney (1981), and Worrell and Stack (1981). Once the fault tree has been transformed, it can be solved to yield minimal cut sets containing one or more common-cause events, combinations of common-cause events, or cut sets containing common-cause events. Combining multiple common-cause events and combining common-cause events with random-failure events have been shown to be important in Fire Related Accident Sequences at CRBRP (Science Applications, Inc., 1978).

6.3.3 EVENT TREES WITH BOUNDARY CONDITIONS

When the method of event trees with boundary conditions is used, algebraic expressions are (usually) implicitly developed for each PDB by a stepwise process. This development process is implicit because, unlike in the fault-tree-linking method, no single Boolean expression at the component level is defined for each bin--it is merely implied. However, after an optional initial screening for dominant sequences, either method can be used to combine distributions in an identical way. The key differences between the methods lie in how the dominant sequences are defined and how the frequency for each plant-damage bin is arrived at. The main steps in this

approach are outlined below, followed by a discussion of means to limit event-tree size.

As described in Section 3.7.3.3, the method of event trees with boundary conditions uses more detailed event trees and therefore simpler fault trees than does the fault-tree-linking approach. In particular, the support systems found to be important are included explicitly as top events in the event trees. In this approach, then, "systems" or "top events" are narrowly defined. Thus, important dependences between top events are shown explicitly in the event tree rather than being contained in the fault trees underlying the top events. In this approach, separate fault trees or system models are, in effect, also written for each branch point of the event tree. These fault trees then explicitly recognize the states of the systems or top events upstream on the path leading to that branch point.* When such a fault tree is quantified, it yields the split fractions--that is, the frequencies of the events that make up the sequence--for that specific branch point. To be more specific, it yields the split fraction for that top event conditional upon the path through the event tree by which that top event is reached.

Consider as a simple example the event tree in Figure 6-2.

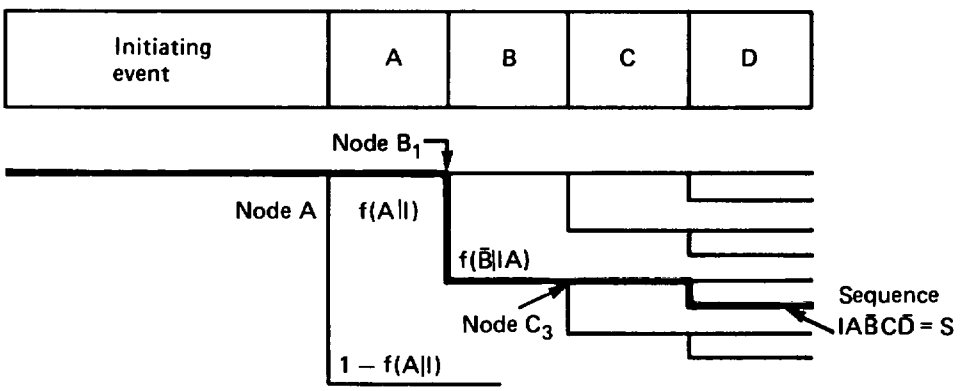


Figure 6-2. Sample event tree.

Each path through this event tree (i.e., each accident sequence) is characterized by the particular initiating event (or entry state to the tree) and by the failed and partially failed systems in the path. Consider, for example, the path

$$S = IA\bar{B}C\bar{D}$$

This sequence, consisting of initiating event I followed by the success of systems A and C and the failure of subsystems B and D, is represented by the

*This recognition can also be thought of as boundary conditions on the system fault tree--hence the term "event trees with boundary conditions."

darkened line in the diagram and is designated by a bar over the symbol in the name of the sequence.

The likelihood of a sequence is quantified by reference to a "thought experiment" in which the reactor in question is imagined to be operated for many, many billions or trillions of years. We then ask ourselves, "In this experiment, how frequently, in times per operating year, does this accident sequence occur?" This frequency is referred to as the "sequence frequency," or, if the sequence is represented by a path in an event tree, it could be called the "path frequency."

Since we have not, in fact, done this experiment, we cannot, of course, say what this sequence frequency is with complete certainty. However, we can logically infer some things about this frequency from the frequencies of the "elemental" events that make up the sequence (i.e., the split fractions).

These elemental frequencies are themselves known only within a certain degree of accuracy, which can be expressed by giving a probability curve for each elemental frequency. These elemental probability curves can then be combined or "propagated" appropriately to develop probability curves for the frequencies of the accident sequences, if desired.

In the thought experiment, let $\phi(I)$ be the frequency per plant-year with which the initiating event I occurs. This is then the frequency of the left end, or "trunk," of the tree in Figure 6-2. It is then split up into the frequencies of the various branches. Thus, now consider all the instances in our thought experiment when event I occurred and let $f(A|I)$ be the fraction of those instances in which system A succeeded (i.e., was available). Then $f(A|I)$ is the fraction of those sequences entering node A that emerge through the upper branch at the right of node A.

In our thought experiment, then, $\phi(I)\ f(A|I)$ is the number of sequences, per plant-year, that enter node B_1. Out of all those sequences, let $f(\bar{B}|IA)$ be the fraction that emerges from B_1 along the lower branch. The term $f(\bar{B}|IA)$ is then the split fraction at node B_1.

Proceeding in this way, we can finally express the frequency of sequence S, in our thought experiment, in terms of $\phi(I)$ and the split fractions along the path. Thus,

$$\phi(S) = \phi(I)|\, f(A|I)\ f(\bar{B}|IA)\ f(C|IA\bar{B})\ f(\bar{D}|IA\bar{B}C)$$

where

$\phi(S)$ = the frequency of accident sequence S

$\phi(I)$ = the frequency of initiating event I

$f(A|I)$ = the frequency of success for system A, given that I has happened (i.e., the split fraction at node A)

$f(\bar{B}|IA)$ = the frequency of failure for system B, given that I has happened and A has succeeded (the split fraction at node B_1)

$f(C|IA\bar{B})$ = the frequency of success for system C, given that I has happened, A has succeeded, and B has failed

$f(\bar{D}|IA\bar{B}C)$ = the frequency of failure for system D, given I, A, $\bar{B}$, and C

From this equation, therefore, we can calculate the frequency of sequence S from $\phi(I)$, which comes directly from data analysis (see Chapter 5), and from the split fractions that come from system fault trees.

Note that these fault trees must be specialized to each branch point. Thus, for example, suppose A and B were support systems. Then $f(C|IA\bar{B})$, the split fraction at node C_3, must be calculated from the system model for system C with the recognition (or "boundary condition") that support system A is working and support system B is not.*

The next section elaborates on the development of event trees and the computation of the split fractions. After that, we generalize the example of Figure 6-2 and discuss the calculation of PDB frequencies.

6.3.3.1 Event-Tree Development and the Determination of Split Fractions

The first step is to develop event trees displaying all the significant intersystem dependences between the front-line systems whose performance is pertinent for the initiating event of interest. These result from common support systems and any other dependences (human error, environmental) judged to be important. The event trees include these support-system operability states as well as those of the front-line systems. Section 3.7.3 illustrates the event-tree development. Note that the pertinent dependences between support systems are to be identified and displayed in the event tree. In addition, multiple branches (reflecting partial success) rather than just binary (success or fail) branches are used where this more appropriately describes the support-system states and facilitates the quantification of the front-line system. For example, for the electric power heading of the event tree with, say, two buses supplying the safety systems, four branches would be included in the event tree to describe the availability of electric power. These branches would represent "both buses working," "bus 1 working and bus 2 failed," "bus 1 failed and bus 2 working," and "both buses failed."

When the event trees have been completed, the split fractions in the event trees are determined from logic models for the system or top event under the conditions represented by the particular branch point or node in question. The system logic models are usually in the form of fault trees, but they can be reliability block diagrams, GO models, subevent trees, FMEA models, or any other kind of model, all of these forms, if properly done, being logically equivalent.

---

*This can often be conveniently accomplished as suggested in Section 3.7.3.3 by writing a single fault tree for system C in which the states of systems A and B are regarded as "house events." It is not necessary to do this, however.

Simple fault trees are then written to relate the state of the top-event system to the states of its components. From the minimal cut sets of these trees, we can obtain the necessary condition for system failure in terms of sets of component failures. That is, the system does not fail unless at least one cut set of components fails.

The question then devolves upon what could cause the failure of one of these cut sets. The answers to this question are recorded and systematized through the use of a cause table (see Figure 6-3 for an abbreviated example). In this table, all possible causes ("candidate" causes) are listed in the left column. Each cause is then evaluated as part of the system analysis. The components that would fail from this cause are listed in column 3. If those components constitute a cut set, thus failing the system, this is noted in column 4. If a particular cause does result in system failure, the frequency* of that failure is recorded in column 2. (More specifically, what is recorded here is the fraction of times in our thought experiment that the system fails at the branch point in question as a result of this particular cause.)

The sum of the entries in column 2 (i.e., the sum of all frequencies of system-failure causes) is the split fraction for system failure at the branch point in question. The bottom of the cause table can be used to accommodate the contribution from "other" causes (i.e., from all causes not otherwise called out in the table). If such entries are used, the analyst should be careful to list all contributors to "other causes."

If the system should fail as a result of a particular cause, we then ask whether that same cause might also result in some other system failing or in an initiating event. If so, then it is a potential "common" cause and needs to be called out for special treatment in the analysis. Columns 5 and 6 in the cause table are used to call attention to such situations. Because split fractions are simply multiplied together, the identification of dependent failures in the cause table and subsequently in the event tree is critical and should be given a great deal of attention.

6.3.3.2 Computation of PDB Frequencies

Event trees are not limited as in Figure 6-2 to nodes with two branches. Therefore, to generalize the notation, let f_{nb} denote the split fraction at node n that goes with branch b. With these quantities established for each branch point, one can calculate the frequency of each accident-sequence path as

$$\phi(S) = \phi(I) f_{1b,1} f_{2b,2} \cdots f_{nb,n} \cdots \qquad (6\text{-}1)$$

$$= \phi(I)\, f(S)$$

where b_n is the branch chosen by the path at node n.

*These, along with the $\phi(I)$, are examples of elemental frequencies.

Cause	Failure frequency	Effect			
		Components	System	Other systems	Initiating events
Coincident hardware failures	4.5×10^{-6}	Mainly pumps	Fails	No effect	No effect
Testing	1.0×10^{-10}	Pumps	No effect	No effect	No effect
Maintenance and hardware failure	2.0×10^{-4}	Pumps or MV-8700A, B	Fails	No effect	No effect
Human error and hardware failure	8.2×10^{-9}	MOV-8809A, B closed failure on other side	Fails	No effect	No effect
Other	4.6×10^{-5}	Valves or pumps	Fails	No effect	No effect
Total	3.0×10^{-4}				

Dominant contributor = maintenance combined with hardware failure.

Figure 6-3. Example of format for a cause table for double failures (buses available).

The term f(S) on the right-hand side, the product of split fractions along a given path, thus has the meaning of "conditional frequency"; that is, for all the times initiating event I occurs, f(S) is the fraction of times in which accident sequence S results. In this way one can compute the conditional frequency for each path in the tree. These numbers thus characterize the tree itself, without reference to the frequency of the incoming entry state. Each sequence or path culminates in an exit state (i.e., a particular state of operability-functionability with respect to front-line systems).

Now let us focus attention on a particular exit state, say y_j, and let S_{ih} denote a particular accident sequence going from entry state i to exit state y_j. By summing over all such sequences, we obtain

$$m_{ij} = \sum_h f(S_{ih}) \tag{6-2}$$

The quantity m_{ij} is thus the conditional frequency of occurrence of exit state y_j given that initiating event i has occurred. That is, out of all the times entry state i occurs, m_{ij} is the fraction of times that exit state j occurs.

If we now let $\phi(I_i)$ be the frequency of initiating event i, then

$$\phi(I_i)m \tag{6-3}$$

is the frequency of occurrence of exit state y_j as a result of initiating event I_i. Moreover,

$$\sum_i \phi(I_i)m_{ij} \tag{6-4}$$

is the frequency of occurrence of exit state y_j as a result of all initiating events.

Equation 6-2 can now be recognized in essence as a matrix multiply operation. Thus, if we assemble the m_{ij} into a plant matrix M and the $\phi(I_i)$ into an initiating-event row vector ϕ^I, then

$$\phi^Y = \phi^I M \tag{6-5}$$

where ϕ^Y is a row vector containing the frequencies $\phi(Y_j)$ of the various plant-damage states Y_j.

The process of Equations 6-1 through 6-5 is carried through by first using point estimates (essentially mean values) of all the frequencies and split fractions to obtain point estimates for the frequencies $\phi(Y_j)$. These point estimates can then be used to eliminate from the uncertainty analysis those sequences whose point estimates do not contribute to the point estimate of the result. When point estimates are used, the analyst should ensure that the failure-rate dependences among systems containing components assumed to be identical will not cause a nondominant sequence to become a

contributor to the PDB frequency. To determine probability distributions for the $\phi(Y_j)$, we "propagate" the uncertainties in the elemental cause and initiating frequencies through the cause table and through Equations 6-1 through 6-5. In this operation, as in all probabilistic operations, attention must be paid to dependences between probability distributions. Also, as in all arithmetic, minor quantities in the calculation need not be treated with high accuracy; they can be approximated, upper bounded, or rounded off as appropriate, but such shortcuts should be well documented. Such shortcuts are especially useful in the computation of probability curves to avoid unnecessary computational labor.

6.3.4 APPROACHES TO REDUCING EVENT-TREE COMPLEXITY AND PROCESSING EFFORT

In order to keep the event trees manageable in size and the analysis practical, the analyst will need to make some assumptions and approximations that permit the omission of certain dependences from the event tree. In addition, some iteration is to be expected between logic-model development and quantification; that is, to some extent the event tree may have to be modified as quantification proceeds. Techniques available to assist the analyst include screening, bounding, and the use of impact vectors.

6.3.4.1 Bounding

To simplify the event trees and the quantification task, a conservative assumption can be used, perhaps by not taking full credit for the provided redundancy. For example, in the case of two highly reliable actuation signals, each of which initiates both of two safeguards systems, it may be useful to assign and restrict one signal to each system, thus eliminating the need to explicitly include actuation as a common support system.

A second example would be the assumption that all valve motor control centers connected to a vital electric-power bus are in effect a part of that bus. Such an assumption would be made to avoid the necessity of multiple additional electric-power states when the elements of a distribution system could potentially be common to valves in two front-line systems. This particular example is related to the discretization of support states considered in the event tree.

If no dominant impact results from making conservative assumptions, as often happens, the assumption can be accepted. However, should such an assumption artificially yield a dominant impact, it may be necessary to reexamine and refine the event-tree model to reduce the impact.

6.3.4.2 Screening

A study or an analysis can be made to examine the necessity of including a support system. If it can be shown that the support system is

extremely reliable, it may be possible to leave it out because it will have a negligible impact. The basis for such an assumption should obviously be documented.

6.3.4.3 Use of Impact Vectors

This technique, illustrated by an example in Section 3.7.3.3, can be a powerful logical approach. The support-system event tree is developed separately from that for the front-line systems. Then the impact of each support-system state (success/failure combination) on the front-line systems is developed in the form of an "impact vector" that describes the front-line systems that fail as a result of support-subsystem failures. The sequences can be collapsed down to the unique impacts that serve as the boundary conditions for evaluating the front-line systems. This variant of the event tree-boundary condition approach uses the quantification of the intermediate support-system states. Since both frequencies and damage-level information are available, it is possible to determine the risk-dominant support-system states before quantifying the front-line trees. Support-system states not significant to risk can be "pruned" at this step.

6.3.5 COMMENTS ON DIFFERENCES IN SEQUENCE-QUANTIFICATION APPROACHES

Two approaches to accident-sequence quantification--fault-tree linking and event trees with boundary conditions--have been described. Both make use of event trees in conjunction with fault trees. Both approaches require some assumptions and approximations to be practical--for example, the truncation of cut sets or the elimination of some dependences by making use of approximations. In the fault-tree-linking technique, the event trees have been constructed at a high level in terms of the function or system success or failure definition: it is necessary to display only the front-line functions or systems. The dependences on support systems and subsystems are accommodated entirely within the fault trees. The resultant linked fault trees are thus large and complex. When the fault trees and event trees are large, the existence of automated and efficient computer reduction techniques makes analysis by this approach possible in spite of the many cut sets that can be generated for quantification.

In the other quantification method, which uses event trees with boundary conditions, the more elaborate event trees are broken down to explicitly display the significant dependences. The resultant fault trees (or reliability block diagrams) for the event-tree top events are thus simpler and independent, and can be analyzed by hand without resorting to computer-assisted fault-tree reduction. Heavy reliance is placed on the analyst to identify and separate the dependences in the event-tree modeling. Considerable care must therefore be taken to ensure that the significant dependences in a sequence have either been identified and included as top events in the event tree or are otherwise accounted for in generating the split fractions along an accident-sequence path.

It should be noted that the use of event trees with boundary conditions generally yields many more sequences because of its evaluation for the various mutually exclusive support-system states. Several such sequences would combine to result in the same front-line-system configuration as that identified in fault-tree linking.

Overall, the basic conceptual difference between the methods is where in the process quantification (conversion from symbolic representation to numerical results) takes place: stepwise throughout the process (for event trees with boundary conditions) or as a single step near the end (for fault-tree linking). Both methods can be successfully employed and have been used in major studies performed to date. An advantage of stepwise quantification is a reduction in the need to carry through algebraic terms, so that quantification can be performed manually. An advantage of quantification as the last step is that the symbolic representation allows computer searches for dependences as the last step before quantification and the presentation of results in terms of cut sets for dominant accident sequences.

6.4 TREATMENT OF UNCERTAINTY

The probability or frequency estimates that are obtained by analyzing fault trees or event trees are generally associated with considerable uncertainty. The uncertainty comes from the following principal sources:

1. The specified models are incorrect. Basic assumptions about the accident sequences, system-failure modes, and the application of the quantification formulas may not be correct.

2. Important failure modes have been overlooked (completeness problem). The scope of the risk assessment may preclude the analysis of all initiating events, the analyst may not have all the required information, or the quantification process may have truncated large numbers of low-probability events that sum to a significant probability.

3. The values of the input parameters are not exactly known. Data limitations or uncertainties in component-failure rates require the use of probability distributions or interval estimates to model frequencies for initiating events and probabilities for system failures.

Although it may be possible to quantify the contribution to total uncertainty made by each of these sources, in practice it is very difficult to develop credible quantitative measures for all the sources of uncertainty in the analysis. It is usually more practical to perform additional analyses to ensure that the modeling is correct than to try estimating a particular quantitative uncertainty. This section discusses these uncertainty sources and describes a method for evaluating their contribution to total uncertainty in the analysis.

6.4.1 SOURCES OF UNCERTAINTY

Table 6-2 lists the uncertainties that can affect the estimates of accident-sequence frequencies as well as the sections of this guide that discuss these uncertainties. The major sources of uncertainty that are directly related to accident-sequence quantification are truncation schemes that eliminate accident sequences or accident-sequence cut sets that are determined to be insignificant. The errors they produce are nonconservative. Another source of error in quantification is the rare-event approximation used to develop a probability expression for the accident sequences; it produces conservative errors. Accident-sequence quantification provides the opportunity for assessing the effect of uncertainties in the input data on the calculated frequencies of accident sequences.

Table 6-2. Contributors to uncertainty in estimates of accident-sequence frequency

Uncertainty type	Source of uncertainty	PRA Procedures Guide section
Model uncertainties	Event- and fault-tree models do not correctly account for time-dependent component failures, component dependences, etc.	3.9
	Failure modes improperly defined	3.9
	Component-failure models may not be correct (i.e., exponential failure model)	5.7
	Approximations are used to sum large numbers of cut sets (i.e., rare-event approximation)	6.4.1
	Human errors	4
	External events	10.4, 11.2, 11.3, 11.4
Completeness	Event- and fault-tree models do not contain important failure modes	3.9
	Data base may not include all pertinent failures or experience	5.7
	Large numbers of low-probability accident sequences and cut sets may have been eliminated through truncation	6.4.1
Input-parameter uncertainty	Mission time for the operation of various systems may not be known exactly	3.9
	There are uncertainties in the frequencies of initiating events, component-failure rates, and test and maintenance parameters	5.7, 6.4.1

6.4.2 SOME PROCEDURES FOR UNCERTAINTY AND SENSITIVITY ANALYSIS

The uncertainty introduced through Boolean manipulations, truncations, and screenings should be small in comparison with that in the accident-sequence logic models and the data base. However, significant uncertainty can be introduced through the elimination of large numbers of low-frequency cut sets or accident sequences whose sum contributes significantly to the PDB frequency. In order to quantify this contribution, the cut sets must be generated and quantified. Unfortunately, most truncation schemes used in fault-tree analysis have no capability for estimating this contribution.

One way to estimate the total contribution of many low-frequency events is to use a direct-quantification code like WAM-BAM (see Section 6.6). The direct-quantification codes are very efficient and can use a much lower truncation value because they do not have to perform cut-set manipulations. Moreover, WAM-BAM has the capability to estimate an upper bound on the sum total of the truncated terms. By comparing the direct-quantification result obtained with a lower truncation value against the result of the cut-set solution, the analyst can determine whether a lower truncation value would significantly affect the result. In addition, the WAM-BAM output can be examined to determine the upper bound probability of the terms eliminated during the direct quantification. If the value is small, the use of truncation can be shown to have a small effect on the cut-set solution process.

When trying to evaluate the contribution to system-failure probability from variations in input parameters, the analyst can either perform a probabilistic importance analysis to get a qualitative feel for the effect of input parameters on the results or derive probability distributions or interval estimates for the result.

Probabilistic importance measures are a means of estimating the contribution of a primary event to the accident-sequence frequency. There are three principal types of measure: the Barlow-Proschan (Barlow and Proschan, 1975), the Fussell-Vesely (Fussell, 1975), and the Birnbaum (1969) measures; they have been defined and described by Lambert and Gilman (1977). The Barlow-Proschan and the Fussell-Vesely measures are more closely related to each other than to the Birnbaum measure. The exact nature of the relationships among these and other measures is discussed by Engelbrecht-Wiggans and Strip (1981).

The Barlow-Proschan and the Fussell-Vesely measures compute the probability that a primary event is contributing to the failure of a system and therefore provide information on which primary events, if made more failure-resistant through improved quality or redundancy, will most decrease the probability of a system failure.

The Barlow-Proschan measure of the importance of a primary event i is the probability of the system failing because a minimal cut set containing i fails, with primary event i failing last. By this definition, the most important primary event in a system is the most unlikely primary event in the most likely minimal cut set.

The Fussell-Vesely measure of the importance of a primary event is the probability primary event i is contributing to system failure, given the

system has failed. It is estimated by dividing the sum of the failure probabilities of the minimal cut sets that contain primary event i by the failure probability of the system. The most important primary event in the system according to this definition is the primary event in the most likely group of minimal cut sets. Thus, this definition gives some measure of the probability that the recovery of a primary event will restore the system.

The Birnbaum measure indicates the sensitivity of the overall system-failure probability to the probability of an individual primary event. Thus, it measures the rate of change in system-failure probability to change in primary-event probability. The upgrading function, which is closely related to the Birnbaum measure, can be used in many circumstances to help decide which primary events would contribute most to reducing system-failure probability.

As described by Engelbrecht-Wiggans and Strip (1981), these measures are intimately linked, and their differences are quite subtle. It is therefore difficult to recommend which measures are appropriate in different situations. The choice between the Barlow-Proschan/Fussell-Vesely and the Birnbaum measures is difficult because they measure slightly different aspects of system-failure probability, although frequently the former measures are more appropriate for measuring system improvement. However, Lambert (1975) demonstrates the use of the upgrading function (a variant of the Birnbaum measure) for selecting primary events for change to improve system-failure probability.

Chapter 12 discusses various methods for performing sensitivity studies and for propagating probability distribution and interval estimates based on the simplified equation for the frequency. Section 6.6 discusses the computer codes (e.g., SAMPLE) that can be used in the actual propagation. The manner in which the propagation is performed should be consistent with the data used in the analysis.

A consideration in the propagation of primary-event uncertainty through a top-event probability expression is the method of treating the uncertainty distribution or interval estimates of two primary-event probabilities derived from components assumed to be identical. Their uncertainty parameters are considered to be correlated. In evaluating the probability expression, only one distribution should be used to represent uncertainty for every primary event whose probability is derived from components assumed to be identical. Consider, for example, the probability expression

$$\begin{aligned} P(\text{top}) = {} & P(\text{pump A}) * P(\text{pump B}) \\ & + P(\text{pump A}) * P(\text{control B}) \\ & + P(\text{pump B}) * P(\text{control A}) \\ & + P(\text{control B}) * P(\text{control B}) \end{aligned}$$

If pumps A and B along with controls A and B are assumed to have identical failure rates, the probability expression should be changed to the form

$$P(\text{top}) = [P(\text{pump})]^2 + 2[P(\text{pump})\ P(\text{control})] + [P(\text{control})]^2$$

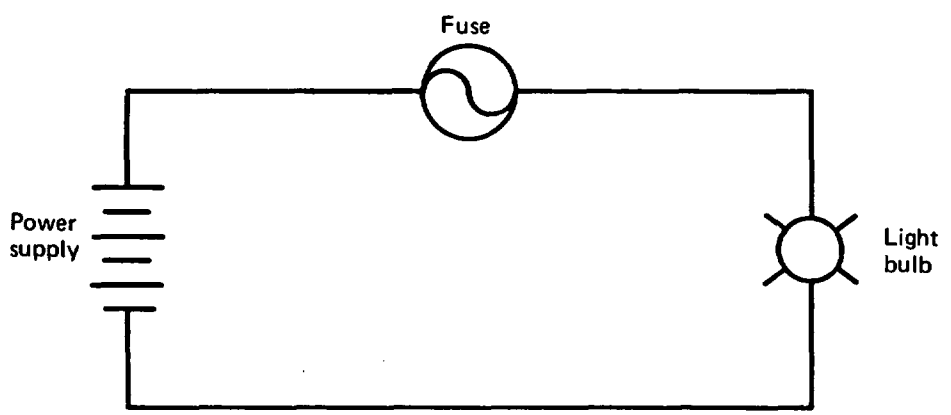
In this way the assumption that the primary events are identical can be correctly evaluated. With independent primary events and distributions, the sums or products of the means of the distributions for the individual primary events will yield the correct mean for the top event. The potential cause for error in assuming that components are identical has been discussed by Apostolakis and Kaplan (1981). In practice, the propagation of uncertainty in primary-event probability may be very difficult to perform by methods other than Monte Carlo for large numbers of independent modules containing similar components.

6.5 SOME MODELING CONSIDERATIONS FOR ACCIDENT SEQUENCES

While performing the general quantitative procedures it is important to note problems that can give erroneous results if the quantification analyst indiscriminately plugs primary-event probabilities into a fault-tree logic model. These problems relate to (1) repair when a secondary fault exists and (2) the potential for simultaneous testing and maintenance. Both cases can be resolved by requantifying a new primary event with a slight modification to the fault tree or pertinent cut set.

6.5.1 QUANTITATIVE ANALYSIS OF FAULT TREES THAT DO NOT REPRESENT REPAIR TREES

Probabilistic risk assessment uses fault trees to model the system failures represented in event trees. In quantifying these fault trees, all methods used in PRA computer programs assume the system fault trees also represent the system repair trees; that is, if component A fails and causes the system to fail, then repairing component A repairs the system. All system fault trees containing secondary failures of components, however, do not represent system repair trees, and the system-failure probabilities calculated by means of these fault trees and standard methods are underestimated. (Secondary failures are causes of malfunction for which the component itself is not accountable.)



Consider, for example, the system shown on the preceding page and the loss of light resulting from fuse-opening failures only. An analysis finds two sources of fuse-opening failures: (1) the fuse opens because of fuse defects ($\lambda_1 = 10^{-6}$ hr^{-1} and $\mu_1 = 10^{-2}$ hr^{-1}) and (2) the power supply surges, causing the fuse to open ($\lambda_2 = 10^{-2}$ hr^{-1} and $\mu_2 = 1$ hr^{-1}). Here the failure rate λ is the probability the component fails in time t to t + dt. The repair rate, μ dt, is the probability a component is repaired in time t to t + dt given the component is failed at time t. Using the standard methods and assuming the time-to-failure and time-to-repair distributions are exponential, the steady-state unavailability of the light from fuse-opening failures only is found to be

$$\bar{A}_{fuse} = \bar{A}_1 + \bar{A}_2 - \bar{A}_1\bar{A}_2$$

$$\approx \frac{\lambda_1}{\mu_1 + \lambda_1} + \frac{\lambda_2}{\mu_2 + \lambda_2}$$

$$= \frac{10^{-6}}{10^{-2} + 10^{-6}} + \frac{10^{-2}}{1 + 10^{-2}}$$

$$= 0.01$$

This calculation assumes that the fuse (and thus the system) is repaired when the power supply is repaired if it caused the failure. Repair in this case, however, requires fixing both the power supply and the fuse. Thus, regardless of the cause of failure, the fuse must be repaired in order for the light to be available. For this example, the steady-state unavailability of the light from fuse-opening failures only is approximately 0.5. (The fuse fails at a rate of approximately 10^{-2} hr^{-1} and is repaired at a rate of approximately 10^{-2} hr^{-1}. The method for determining the repair rate is given on page 6-30.)

The error results from treating the failure logic for the component malfunction (the fuse failing open in this case) as the repair logic when, in fact, it is not. The malfunction occurs because the component is defective or because a secondary cause of failure arises; the malfunction is repaired only when the component and the secondary cause of failure are repaired. In such cases, appropriate measures must be taken to account for this difference in failure and repair logic. One method of eliminating this problem is to include all secondary causes of component failure in a single new secondary-failure primary event for that component. This must be implemented before the minimal cut sets are obtained. The data for this new secondary-failure primary event should reflect the rate at which the component fails from any secondary failure (neglecting those accounted for in the common-cause analysis) and the rate at which it and any secondary-failure causes are repaired. The failure and repair characteristics of the new secondary-failure primary event can be estimated directly from failure and repair data (Chapter 5) or can be synthesized from the failure logic and the failure and repair characteristics of the secondary causes of failure.

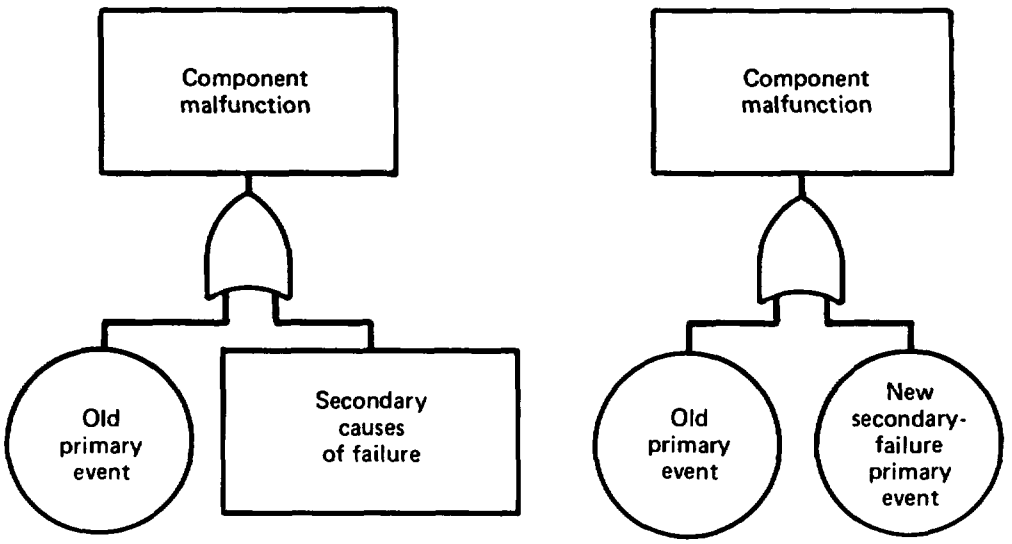


Figure 6-4. Procedure for synthesizing the failure and repair characteristics of a new primary event.

The procedure for synthesizing the failure and repair characteristics of this new primary event is as follows (see Figure 6-4):

1. Identify each primary event in a system fault tree that is affected by secondary failures. This requires examining each primary event in a system fault tree to determine whether it will fail as a result of other primary-event failures in the fault tree. In general, these secondary causes of failure are logically OR'ed with the primary event.

2. Calculate by standard methods a failure rate (λ) and a repair rate (μ) for a fault event that represents the secondary failure. This fault event can then be treated as a new secondary-failure primary event.

3. Calculate for the new secondary-failure primary event an adjusted repair rate that accounts for the repair of the secondary failures and the old primary event. Plant repair policy determines how to calculate the adjusted repair rate for the new secondary-failure primary event. For example, if the old primary event and secondary failures are simultaneously repaired, then the repair rate for the new secondary-failure primary event is given by

$$\mu_{npe} = \min(\mu_{ope}, \mu_{sf})$$

where the subscripts npe, ope, and sf stand for new secondary-failure primary event, old primary event, and secondary failures, respectively. If the old primary event is repaired after the simultaneous repair of secondary failures, then

$$\mu_{npe} = \left(\frac{1}{\mu_{ope}} + \frac{1}{\mu_{sf}}\right)^{-1}$$

Other repair policies may dictate other appropriate methods for calculating the repair rate for the new secondary-failure primary event.

After all the identified primary events have been transformed by this procedure, the system fault tree will represent the system repair tree. The primary events in this system fault tree, however, are not necessarily independent. This dependence among primary events results from common events in the development of secondary causes of component failure for the various malfunctions appearing in the logic model. To ensure correctness, these dependences must be accounted for if they occur.

6.5.2 TEST AND MAINTENANCE

Before quantification, accident-sequence cut sets are screened to eliminate those that are inconsistent with the accident-sequence definition. Thus, cut sets containing two or more test and maintenance primary events considered mutually exclusive because of noncoincident testing schedules or technical specifications are eliminated from the list of accident-sequence cut sets in a plant-damage bin. For the remaining cut sets that contain test and maintenance primary events, these events are assumed to be random and independent. If a cut set contains two or more test and maintenance primary events, however, the probability that these primary events occur simultaneously will often be greater than the value calculated by treating them as random and independent. In this case, the cut-set frequency can significantly increase because of the simultaneous occurrence of these primary events.

Simultaneous testing and maintenance can occur for any of several reasons. Components in separate systems may unknowingly be tested at the same time because of coincident testing schedules. For example, a pump in system A tested every 8000 hours and a pump in system B tested every 6000 hours might be simultaneously tested every 24,000 hours after the first simultaneous test. Human error that results in simultaneous testing and maintenance in violation of technical specifications is another cause. These and any other causes of simultaneous testing and maintenance must be accounted for to avoid underestimating the frequency of an accident sequence.

To illustrate the significance of simultaneous testing and maintenance, suppose a cut set contains two test primary events for two diesel generators. If testing is monthly and requires an hour, then the estimated testing unavailability of each diesel generator is 1.4×10^{-3}, and the unavailability contribution of the pair, assuming random and independent testing, is 1.9×10^{-6}. If, however, the two diesel generators are simultaneously tested once every 10 years in violation of technical specifications, then the simultaneous-testing unavailability of the pair is 1.1×10^{-5}.

The following procedure can be used to account for the effect of simultaneous testing and maintenance:

1. Identify the cut sets in a plant-damage bin that contain two or more test and maintenance primary events.

2. For each of these cut sets, replace the test and maintenance primary events with a single new test and maintenance primary event that represents the unavailability due to simultaneous testing and maintenance.

The probability to be used for the new simultaneous test and maintenance primary event is the fraction of time the replaced test and maintenance primary events occur simultaneously. If the simultaneous testing and maintenance results are in violation of technical specifications, then the probability for this new primary event is given by the product of the probability of violating technical specifications through simultaneous testing and maintenance and the probability of the replaced primary event with the shortest average test and maintenance time. For example, if the probability of violating technical specifications is .01 and the probabilities of three replaced test and maintenance primary events are .001, .0001, and .00001, then the probability for the single new test and maintenance primary event is 10^{-6}.

If the simultaneous testing and maintenance is due to coincident test schedules, then the probability of this new primary event is given by

$$\bar{A}_{npe} = \frac{\min\left(T_{av,i}\right)}{T_{period}} P$$

where $T_{av,i}$ is the average amount of time required to perform testing and maintenance on each replaced primary event i in the cut set, T_{period} is the time between coincident tests, and P is the probability the replaced primary events are tested and maintained at the same time during the test period.

Consider, for example, the coincident test schedules of the two pumps described earlier. If the average test and maintenance time for either pump is 4 hours and testing is to be performed within a 72-hour period, then the probability of the new simultaneous test and maintenance primary event for these two pumps is given by

$$\bar{A}_{npe} = \frac{4}{24,000} \quad \frac{4}{72} = 9.3 \times 10^{6}$$

This assumes random testing of the pumps during the 72-hour period.

6.6 COMPUTER CODES

This section describes a number of computer codes currently available for the qualitative and quantitative evaluation of system or plant logic models. It is difficult to recommend a specific code for use in evaluating plant or system logic models. A great many codes or code packages are available, each code having some particular objective toward aiding or

improving the solution of complex models. This document does not endorse any of the computer codes described here.

Even for a particular function, it is difficult to reach a consensus on a given code because many different factors--such as available computer facilities, staff expertise, and the specific objectives of the analysis--affect the selection of computer assistance. Moreover, not all existing codes are described here--only those which are not proprietary and for which sufficient literature is available; also included are some codes whose owners provided related material and documents.

Some comments can be made, however, on the basis of experience with several of these codes. The code SETS, developed at Sandia National Laboratories, has wide applications in solving fault- and event-tree models as well as in searching for dependent failures. Being relatively sophisticated, it may require a considerable amount of computer time and knowledge of the code if its substantial capabilities are fully exercised. The WAM series, whose development was sponsored by the Electric Power Research Institute, also has broad applications and is readily usable.

The codes described here are divided into five groups by general function. Groups 1 through 4 are summarized in Tables 6-3 through 6-6. Group 1 consists of codes that perform the qualitative evaluation of a fault tree (i.e., codes that compute minimal cut and/or path sets). Group 2 contains codes for quantitative analyses. This group includes codes that require as input the structural information embodied in the cut sets and those that are designed to perform direct numerical evaluations of a system without computing cut sets as a necessary intermediate step. It also contains several codes that have special applications in quantitative analysis. The codes in group 3 have been developed to aid in the identification or analysis of dependent failures. Group 4 consists of codes that can perform uncertainty analyses through the input cut sets, system function, or fault-tree structure (i.e., provide confidence intervals for point estimates). Finally, group 5 contains all codes developed to aid data and other analyses. Because of their diversified functions, the codes in this group are not being presented in tabular form. Besides these five groups of codes, there is a group of codes that are proprietary and therefore not discussed in this guide.

6.6.1 COMPUTER CODES FOR THE QUALITATIVE ANALYSIS OF FAULT TREES

This section deals with codes that compute the minimal cut and/or path sets of a fault tree or perform Boolean reduction for the fault trees. Minimal cut sets give all the unique combinations of primary-events that cause system failure; minimal path sets give the smallest group of primary-event failures that must not occur in order for the system failure not to occur.

Minimal cut sets are used by some codes to evaluate fault trees. In particular, minimal cut sets are used by some codes (e.g., KITT and SUPERPOCUS) to calculate the probability, unavailability, or unreliability of the

top event. Some codes, such as SAMPLE and SPASM, use minimal cut sets for sensitivity or uncertainty analyses. Minimal cut sets are also used in some codes to perform importance calculations (e.g., IMPORTANCE). Finally, in dependent-failure analysis, some codes (e.g., COMCAN) use minimal cut sets for common-cause searching. The minimal cut sets themselves provide much useful information about the design weaknesses of the system. Furthermore, minimal cut sets can be compared with the original tree to identify possible errors in the fault-tree logic.

Two methods of calculating minimal cut sets are used in the codes. One is deterministic; the other is a Monte Carlo approach. The deterministic method uses Boolean-algebra principles to sort through the fault-tree structure, which must first be encoded in a suitable format. Although accurate and rigorous, this method can be slow for large fault trees. However, modern approaches like fault-tree modularization have made its use for large fault trees very feasible. The Monte Carlo approach randomly selects the events in the fault tree and combines them to test whether the fault-tree logic is satisfied. If an event combination is selected that does satisfy the logic, a cut set has been established. This method is less accurate but sometimes faster than the deterministic method. Both methods can be streamlined for more economical use by limiting the size of the fault tree to be examined or by setting a limit on the size of the output minimal cut sets. Further details about the methods for determining minimal cut sets can be obtained from the Fault Tree Handbook (Vesely et al., 1981a).

One disadvantage of the minimal-cut-set codes is that the storage and computer time for processing even medium-size trees can become quite prohibitive. The number of cut sets can increase drastically with a slight increase in the number of gates or primary events. For example, one tree with 299 primary events and 324 gates had more than 67 million cut sets. However, the number of gates and primary events is not the only indicator of the complexity of the tree, whereas the configuration of the gates and primary events is an important contributor to its complexity. Therefore, a fault tree with fewer gates and primary events than another tree can contain more cut sets, simply because it has a different logical or structural configuration. Thus, it is often difficult to predict the storage requirements and running time for a given tree.

Several methods can be used to overcome or at least alleviate the problem of obtaining all the minimal cut sets. The most common is to eliminate, during the processing, cut sets whose order (number of events in the cut set) is larger than a preselected number or whose probability is less than a specified value. In the Reactor Safety Study (USNRC, 1975), for example, only single- and double-event cut sets were retained; the higher-order cut sets were analyzed only for common-cause-failure potentials. Another method of alleviating the problem is to reduce and simplify the fault tree before generating cut sets; for example, the WAMCUT-II method substantially reduces the number of cut sets. Finally, tree modularization is sometimes used as an alternative method of reducing the number of cut sets (e.g., the PL-MOD method).

Presented below are brief descriptions of the qualitative-evaluation codes, including purpose, method, input and output, language and type of

computer, and special features. It should be noted that a number of the qualitative-evaluation codes have limited quantitative capabilities. These capabilities are also discussed. A summary of these codes is presented in Table 6-3.

ALLCUTS

ALLCUTS finds minimal cut sets from fault trees with AND and OR gates (Van Slyke and Griffing, 1975).

ALLCUTS uses a top-down successive Boolean substitution algorithm similar to that of MOCUS. An auxiliary program, BRANCH, can be used to check the input and cross reference the gates and input primary events.

Required input consists of control information and a description of the fault tree, but the code allows the option of entering primary-event probabilities. If these data are input, ALLCUTS can compute the top-event probability. Output from ALLCUTS can be printed. The cut sets are sorted, and up to 1000 minimal cut sets in descending order of probability can be generated and printed. Cut sets within a specified probability range can be obtained and printed.

The limited number of cut sets that ALLCUTS generates restricts its use, especially for large fault trees. ALLCUTS handles up to 175 primary events and 415 gate events. The code is very similar to MOCUS. If requested, ALLCUTS performs a limited search of minimal cut sets to identify common manufacturer, common susceptibility to secondary failure causes, and close proximity of primary events. ALLCUTS is written in Fortran IV for the CDC 7600 computer.

FATRAM

FATRAM is used to find minimal cut sets from fault trees with AND and OR gates (Rasmuson and Marshall, 1978).

The FATRAM algorithm is very similar to that of MOCUS, but it uses less core and less computation time. The reduction in core requirements is achieved by (1) resolving OR gates with gate inputs and AND gates as early as possible, (2) handling replicated primary events, (3) postponing until last the resolution of OR gates with only primary-event inputs, (4) writing out cut sets without expanding in core, and (5) eliminating supersets at very early stages.

Required input consists of control information and a description of the fault tree. Eight-character alphanumeric names can be used for the fault-tree events. The output consists of minimal cut sets up to a level specified by the user.

Most of the characteristics of FATRAM are similar to those of MOCUS. However, because of the improved methodology, larger fault trees can be handled with more efficiency. FATRAM has an input-error-checking procedure and is written in Fortran IV for the CDC Cyber 76 computer.

Table 6-3. Computer codes for qualitative analysis[a]

Code	Input	Limit on number of gates or events	Types of gates	Limit on number or size of cut sets[b]	Method of generating cut sets[a]	Other outputs	Fault-tree truncation	Other features	Type of computer, language, and availability
ALLCUTS	8-character alphanumeric names, control information, primary-event probability, fault-tree description	175 primary events and 425 gates	AND OR	Up to 1000 cut sets can be generated	Top-down successive Boolean substitution	Cut sets in specified probability range, cut set and top-event probability	Minimal cut sets, probability	Fault-tree plotting option	IBM 360/370 CDC 7600 Fortran IV
FATRAM	8-character alphanumeric names, control information, fault-tree description	None	AND OR	None	Top-down successive substitution with gate-coalescing option	Minimal cut sets up to specified order	Minimal cut sets	--	CDC Cyber 76 Fortran IV Available from EG&G Idaho, Inc.
FTAP	8-character alphanumeric names, control information, fault-tree description	None; computer memory is limiting factor	AND OR K-of-N NOT	Minimal cut sets of up to order 10 can be generated	Top-down, bottom-up, and Nelson method (prime implicants)	Minimal cut sets and prime implicants	Minimal cut sets	Independent subtrees automatically found and replaced by module	IBM 360/370 CDC 6600-7600 Fortran IV Available from Operations Research Center, University of California, Berkeley
MOCUS	8-character alphanumeric names, control information, fault-tree description	None	AND OR INHIBIT	Minimal cut sets of up to order 20 can be generated	Top-down successive Boolean substitution	Path sets	Minimal cut sets	Cut sets can be automatically punched on cards or on-line data sets for use by KITT or SUPERPOCUS	IBM 360/370 CDC 7600 Fortran IV Available from Argonne Software Center
PL-MOD	79-character alphanumeric names, control information, fault-tree description, failure data	None; computer memory is limiting factor	AND OR NOT K-of-N	None	Bottom-up modularization and decomposition of fault tree into best modular representation	Probability of top event, time-dependent characteristics of top event, minimal cut sets, uncertainty for top event	Minimal cut sets	Option of not generating minimal cut sets for quantifying fault tree	IBM 360/370 PL/I Available from Argonne Software Center
PREP	8-character alphanumeric names, control information, fault-tree description	2000 primary events and 2000 gates	AND OR INHIBIT	Minimal cut sets of up to order 10 can be generated	Combinatorial testing	--	No	Minimal cut sets can be automatically punched on cards or on-line data sets for use in KITT or SUPERPOCUS	IBM 360/370 CDC 7600 Fortran IV Available from Argonne Software Center
SETS	16-character alphanumeric names, user's program, failure data, fault-tree description	8000 events (gates and primary events together)	AND OR INHIBIT PRIORITY Exclusive or special	None	Top-down Boolean substitution, but user's program can be designed for any other method	Probability of minimal cut sets, prime implicants	Yes, based on both cut-set order and probability	Automatic fault-tree merging and plotting; on-line data sets can be stored on tapes for use in other runs; independent subtrees can be obtained to simplify cut-set generation	CDC 7600 Fortran IV Available from Argonne Software Center
SIFTA	10-character alphanumeric names, control information, failure data, fault-tree description	None; computer memory is limiting factor	AND OR K-of-N	No cut sets generated	Pattern-recognition technique to reduce structure of tree; numerical simulation to calculate probabilities	New structure of tree after reduction; probability of top event	Independent branches of tree with small probability	Handles trees with multiple top events; merging of fault trees possible; fault trees can be plotted	HP-1000 Available from Atomic Energy Control Board, Ottawa, Canada

Table 6-3. Computer codes for qualitative analysis[a] (continued)

Code	Input	Limit on number of gates or events	Types of gates	Limit on number or size of cut sets[b]	Method of generating cut sets[a]	Other outputs	Fault-tree truncation	Other features	Type of computer, language, and availability
TREEL and MICSUP	8-character alphanumeric names, control information, fault-tree description	None; computer memory is limiting factor	AND OR INHIBIT	Minimal cut sets of up to order 10 are generated	Top-down successive Boolean substitution	Path sets	Minimal cut sets	Can determine minimal sets of intermediate gates	CDC 6400 Fortran IV Available from Operations Research Center, University of California, Berkeley
WAMCUT, WAMCUT II	10-character alphanumeric names, control information, failure data, fault-tree description	1500 primary events and 1500 gates	AND OR NOT NOR NAND ANOT ONOT K-of-N	Up to 2000 minimal cut sets of any order can be generated	Bottom-up Boolean substitution; WAMCUT-II finds independent subtrees, replaces them by pseudo-component, then uses top-down Boolean substitution	Probabilities of minimal cut sets and top event; first and second moments of minimal cut sets and top event	Yes, based on both cut-set order and probability	Plot option; can generate minimal cut sets of intermediate gates	CDC 7600, IBM 370 Extended Fortran IV Available from EPRI Code Center

[a]All the codes listed here have routines for checking input errors. These routines are very extensive in the codes FTAP, MOCUS, PREP, SETS, SIFTA, TREEL-MICSUP, and WAMCUT. ALLCUTS uses the auxiliary code BRANCH for checking input errors.

[b]Or prime implicants.

FTAP

FTAP, used to obtain minimal cut and path sets (Willia, 1978), determines minimal cut sets of any order for fault trees with AND, OR, K-of-N, and NOT gates.

The FTAP algorithm is based on one of three methods selected by the user: top-down, bottom-up, and Nelson. The top-down and the bottom-up approaches are basically akin to the methods used in MOCUS and MICSUP, respectively; the Nelson method is a prime-implicant algorithm that is applied to trees containing complement events and uses a combination of top-down and bottom-up techniques. FTAP uses two basic techniques to reduce the number of nonminimal cut sets, thereby increasing the code's efficiency. The first technique, used in the bottom-up and Nelson methods, is modularizing independent portions of the tree; it is somewhat similar to the SETS algorithm. The second technique, used in the top-down and Nelson methods, is called the "dual algorithm." In this algorithm, the product of sums is transferred to the sum of products whose dual is then taken by using a special method. It is claimed that the nonminimal sets appearing during the construction of the dual "will always be less than the number of such sets in [the original product of sums], usually many times less."

The input information required by FTAP consists of control information and a description of the fault tree. Eight-character alphanumeric names are used for the events in the fault tree. The output, which can be printed, includes the list of minimal path and cut sets and, where applicable, the list of prime implicants.

The code is able to generate cut sets of high order with high efficiency. Flexibility in the use of one of the three algorithms provides a tool to more efficiently evaluate large fault trees. FTAP has an extensive error-checking procedure. Written in Fortran IV and assembly language, FTAP can be used with the CDC 6600/7600 and the IBM 360/370 computers.

MOCUS

MOCUS is used to find minimal cut or path sets from fault trees with AND, OR, and INHIBIT gates (Fussell et al., 1974). Written to replace PREP as a minimal-cut-set generator for the KITT codes, it can determine minimal cut sets of up to order 20 (maximum length specified by the user).

The MOCUS algorithm uses successive Boolean substitution, starting from the top event and working down the tree until all gates have been replaced by primary events. If the tree contains no replicated events, the end result of the substitution is minimal cut or path sets; otherwise Boolean identification should be applied to minimize the cut or path sets.

Required input consists of control information and a description of the fault tree. Optional input includes eight-character alphanumeric names for primary events, primary-event failure rates, and primary-event repair times.

MOCUS output can be printed, punched on cards, or written to either a temporary or permanent on-line set. The list of minimal cut sets can be

passed to the quantitative codes SUPERPOCUS or KITT-1 and KITT-2 from the punched cards or from on-line data sets.

The computer time required by MOCUS is approximately a linear function of the order of the cut sets desired. However, large fault trees require a prohibitive amount of time to generate cut sets of high order (say four events or more). Since it does not handle NOT gates and special gates, MOCUS is somewhat limited in use, but it is very efficient in determining low-order cut sets. In addition to the top event, the cut sets of intermediate gates can be obtained. MOCUS is written in Fortran IV for the IBM 360/370 and the CDC 7600 computers. It has an extensive routine for checking input errors and requires no external routine.

PL-MOD

PL-MOD directly obtains modular minimal cut sets of any length for fault trees developed with AND, OR, NOT, and K-of-N gates (Olmos and Wolf, 1977). Modular minimal cut sets make fault-tree quantification very simple.

The PL-MOD algorithm is based on fault-tree decomposition and modularization. A module is a collection of primary events that are independent of the result of the tree and can be replaced by a "supercomponent" (i.e., the module). PL-MOD separates all replicated events from the rest of the tree, modularizes the independent portion of the tree, and then finds Boolean relations between the replicated events and the modules. The Boolean relation is reduced and presented in the disjunctive normal form that is the modular minimal cut set. The code MODCUT is used (Modarres et al., 1980) to expand the modular minimal cut sets to obtain the minimal cut sets. MODCUT determines minimal cut sets of any length (maximum length specified by the user).

Required input is control information and a description of the fault tree; optional input includes up to 79-character alphanumeric names for the primary events and the gates of the fault tree, primary-event failure rates, repair rates, and average test length. The input is free in format. Output from PL-MOD or MODCUT can be printed; it includes the list of modular minimal cut sets and minimal cut sets as well as the probabilities of primary events, modules, and gates.

An option of time-dependent analysis (the PL-MODT code) calculates system unavailability at different times. Fussell-Vesely importance calculations can be performed for all primary events, modules, and modular cut sets, and a Monte Carlo simulation option is available for uncertainty analysis. The Monte Carlo simulation subroutine is similar to SAMPLE, but, because PL-MOD uses modular cut sets for quantification, the calculations are more efficient. Because PL-MOD is written in PL/I language, it has the disadvantage of machine dependence (PL/I is not available in many computer systems) and lack of familiarity with PL/I language among scientific users. However, the use of the code is very simple and straightforward.

PREP

PREP obtains minimal cut or path sets from fault trees with AND, OR, and INHIBIT gates (Vesely and Narum, 1970). It can determine minimal cut sets up to order 10 (maximum length specified by the user).

PREP consists of two parts: TREBIL and MINSET. TREBIL (for "tree build") takes the user's input description of a fault tree and builds a Fortran subroutine of the Boolean equations representing the fault tree. MINSET then uses the TREBIL-produced subroutine to determine cut and/or path sets. MINSET uses combinatorial testing to find the minimal sets. For example, it systematically fails all single primary events, pairs of primary events, groups of three primary events, etc., to find which combinations cause the top event of the fault tree to occur. The time required for the analysis is an exponentially increasing function of the average length of the desired cut sets.

Required input consists of control information and a description of the fault tree. Optional input includes eight-character alphanumeric names for primary events, primary-event failure rates, and primary-event repair times. Most of the PREP input is identical with the input to MOCUS. Output can be printed, punched on cards, or written to either a temporary or a permanent on-line data set. The list of minimal sets can be passed to the quantitative codes SUPERPOCUS, KITT-1, or KITT-2 from the punched cards or from on-line data sets.

The main disadvantage of PREP is that it requires a prohibitive amount of computer time for large-order cut sets (more than, say, three events). Moreover, PREP does not handle NOT gates and special gates, which makes the use of PREP somewhat limited. However, for obtaining cut sets of low order (up to, say, three events), PREP is very efficient. The primary events are assumed to be independent; unlimited replicated events are allowed; cut and path sets of intermediate gates cannot be generated. Written in Fortran IV for the IBM 360/370 and the CDC 7600 computers, PREP has an extensive routine for checking input errors and requires no external routine.

SETS

The SETS (Set Equation Transformation System) code, developed by Sandia National Laboratories, is a general program for the manipulation of Boolean equations to find minimal cut or path sets (Worrell and Stack, 1978). It finds cut sets of any length (the maximum length can be specified by the user) for fault trees with AND, OR, NOT, or special gates (specified by the corresponding Boolean equation).

SETS is run by using a user's program designed by the user. The user's program must be so set up that the fault tree is evaluated efficiently, and it largely determines the evaluation algorithm. In general, two major algorithms are used. The first substitutes the Boolean equation of each for the top to the lowest branches of the tree. The second identifies independent subtrees, replaces them by a module, and then performs a simple substitution of the Boolean equation from top to bottom. By manipulating the user's program, these two algorithms can be applied first to intermediate gates and then to higher-order gates, which causes a bottom-up solution of the tree.

Required input consists of the SETS user's program and a description of the fault tree. Input events (gates and primary events) can have up to 16-character alphanumeric names. The input is free in format, which makes its preparation very simple. The output can be printed or stored on tape or

disk for further use. For example, if cut sets are obtained for an intermediate gate and stored on tape, in another SETS run one can read the equation from this tape to solve the Boolean equation of higher-order gates. The list of minimal sets can be passed to the SEP code (Olman, 1981) for uncertainty or importance analysis. The SEP code gives a powerful quantitative capability to SETS.

SETS has an option of logical merging for fault trees. This is very useful when systems in the event trees (i.e., front-line systems) must be merged with their support systems. Steady-state probability calculations are performed by SETS and make it possible to truncate the Boolean equation by probability or cut-set order. SETS can handle up to 8000 events (gates and primary events), which makes it capable of handling very large fault trees. Its main disadvantage is that an efficient fault-tree evaluation is highly dependent on a right setup of the user's program, which requires extensive knowledge and experience on the part of the user. SETS has been used in several PRA studies conducted in the Interim Reliability Evaluation Program and the Reactor Safety Study Methodology Applications Program. A plot code can be used to plot the fault trees on a Calcomp plotter from the input fault-tree description of the SETS output tape. SETS is written in Fortran IV for the CDC 7600 computer. An extensive routine for input-error checking is available.

SIFTA

SIFTA (Simple Fault Tree Analysis) performs logical restructuring and reduction, and probability calculation on fault trees with AND, OR, and K-of-N gates (Waddington and Wild, 1981).

The algorithm for evaluating fault trees is not based on the traditional generation of cut sets: a pattern-recognition technique restructures the fault tree by using relations between the laws of Boolean algebra and regrouping certain patterns of events. For example, if replicated event C is input to two different OR gates A and B, and A and B are input to AND gate T, then event C can be taken out from A and B and put directly into gate T. Hence, the restructuring makes the replicated event C a regular primary event. Several other more complex patterns are recognized and changed to a new reduced form. The numerical evaluation starts with the direct calculation of independent branches, followed by a calculation of branches made independent through the reduction of common events. If the structure of the tree does not allow full reduction, the residual tree is processed by simulation. Unavailability is simulated by failure in a proportionate number of trial periods of 0.01 year. The simulation terminates after 10 occurrences of the top event.

Input is very simple and free in format. Events in the tree can be input by up to 10-character alphanumeric names. The output can be displayed on the terminal and includes the new structure of the tree and the numerical results.

SIFTA is a code that is simple to use and can handle trees with multiple top events. Merging of fault trees is possible during interactive inputting of the fault tree. There is thorough error checking. Noteworthy is

the ability to untangle loops caused by errors in logic or by the misspelling of event codes. SIFTA can plot the fault tree by first displaying it on the screen of the terminal. The displayed tree can be edited and plotted fully or partially by a multicolor plotter. The SIFTA method, however, is highly dependent on the logical structure of the tree. It would be very difficult for the code to handle large trees (1000 events and up) or trees with a significant number of dependences. SIFTA is written for HP-1000 computers but is being implemented on a CDC computer.

TREEL AND MICSUP

TREEL and MICSUP are used to obtain minimal cut or path sets from fault trees with AND and OR gates (Pande et al., 1975). They find minimal cut sets of up to a specified order (maximum length specified by the user).

The algorithm is similar to that used in MOCUS, except that, working from the top event down, MICSUP (MInimal Cut Set UPward) starts with primary inputs of the lowest-level gate and works upward to the top event. TREEL is a preprocessor that checks the tree for errors and determines in advance the maximum number and order of the cut and path sets.

Required input consists of control information and a description of the fault tree; optional input includes eight-character alphanumeric names for the primary events in the fault tree. The output can be printed. This output includes the list of minimal path and cut sets.

In most of their characteristics, TREEL and MICSUP are similar to MOCUS. However, because of the bottom-up algorithm used in MICSUP, the path and cut sets of intermediate gates can be more easily found. TREEL has an extensive error-checking procedure. TREEL and MICSUP are written in Fortran IV for the CDC 6400 computer.

WAMCUT

WAMCUT is used to obtain minimal cut sets and to quantify the gates and top events of fault trees (Leverenz and Kirch, 1978). It finds cut sets of any length for fault trees with AND, OR, NOT, NOR, NAND, ANOT, ONOT, and K-of-N gates.

WAMCUT consists of two parts: WAM and CUT. WAM is a preprocessor that reads the fault-tree description and checks for logic and syntax errors. CUT is the cut-set finder routine, which takes the restructured input fault tree from WAM and finds the cut sets of each gate, working from the bottom to the top of the tree.

Required input consists of control information and a description of the fault tree; optional input includes 10-character alphanumeric names for primary events and gates, primary-event probabilities, and the number of cut sets to be generated. Output includes a list of cut sets and the probability of each. The cut sets can be saved for use in SPASM for uncertainty analysis.

WAMCUT is very easy to use. It can process large fault trees with up to 1500 gates and 1500 primary events without large expenditures of computer

time. The number of cut sets per gate is limited to 2000. Probability truncation of cut sets makes the code practical for PRA. Written in Extended Fortran IV for the CDC 7600 computer, WAMCUT has been used in several PRA studies.

WAMCUT-II

WAMCUT-II, an advanced version of WAMCUT, is used to obtain minimal cut sets and to quantify the gates and top events of fault trees (Putney and Kirch, 1981). It finds cut sets of any length and handles the types of gates handled by WAMCUT.

WAMCUT-II evaluates the fault tree by restructuring the logic to obtain and replace independent portions (independent subtrees) with pseudocomponents and to optimize the tree, thus reducing the amount of processing. Events that are input to several gates (replicated events) are moved up as far as possible toward the top of the tree without violating Boolean-algebra rules. After the tree is restructured, cut sets are obtained with a top-down algorithm. The fault-tree minimal cut sets are in terms of the independent subtrees. This form of cut sets is superior to the minimal cut sets of primary events for quantitative calculations. However, if requested, WAMCUT-II can expand the minimal cut sets of independent subtrees to obtain the cut sets of primary events. In certain cases this process can be costly and may be unnecessary.

Input to WAMCUT-II is the fault-tree description and, optionally, the probability of failure for each primary event. The output consists of the fault-tree minimal cut sets and failure probabilities for intermediate gates and the top event.

WAMCUT-II is very similar to WAMCUT in its capabilities, but is usually much faster. The process of restructuring the tree and removing the independent subtrees can reduce the running time considerably. WAMCUT-II is written in Fortran IV for the CDC 7600 computer; it is currently being converted to run on the IBM 370 computer.

6.6.2 COMPUTER CODES FOR QUANTITATIVE ANALYSIS

A variety of codes have been developed for the quantification of accident sequences. Like the qualitative codes discussed in Section 6.6.1, each one has its own uses, and which one is used depends greatly on the size and the complexity of the fault tree. Most of the quantitative programs discussed here are used to make point estimates of the probability of fault-tree top events; several codes, however, have special applications or characteristics. A summary of the quantitative-analysis codes is presented in Table 6-4.

Codes developed for calculating point-estimate probabilities indicate the relative safety of the system by establishing a probability for the top event. A point-estimate code should be capable of describing the relative safety of the system with a numerical value, and it should provide a list of probabilities associated with the dominant minimal cut sets or primary

Table 6-4. Computer codes for quantitative analysis

Code	Input	Quantitative calculations	Importance calculation	Other features	Type of computer and availability[a]
FRANTIC, FRANTIC II	Reduced system equation or minimal cut sets, primary-event failure data	Time-dependent calculation; nonrepairable, monitored, and periodically tested primary events are handled; uncertainty analysis for failure rates in conjunction with time-dependent calculation	No	Can model human-error and dependent-failure contributions; FRANTIC II can handle time-dependent failure rates and incorporates effect of renewal on aging	IBM 360/370 Available from Argonne Software Center
GO	GO chart[b] and fault-tree failure data	Only time-independent calculations for gates and top event; nonrepairable or periodically tested primary events are handled	No	Cut sets for selected gates and probability truncation of cut sets up to order 4	CDC 7600 Available from EPRI Code Center
ICARUS	Reduced system equation, choice of testing scheme, failure data	Average unavailability, optimal test interval, relative contributions of testing, repair, and random failures	No	Three testing schemes available: random testing, uniformly staggered testing, and nearly simultaneous testing	IBM 360/370 Available from Argonne Software Center
IMPORTANCE	Minimal cut sets, primary-event failure data	Top-event point-estimate probability or unavailability	Can calculate the following: Birnbaum, criticality, upgrading function, Fussell-Vesely, Barlow-Proschan, steady-state Barlow-Proschan, sequential contributory	Can rank cut sets and primary events on basis of each importance measure	CDC 7600 Available from Argonne Software Center
KITT-1, KITT-2	Minimal cut sets supplied directly or by MOCUS or PREP; primary-event failure data	Time-dependent unavailability for primary events, minimal cut sets, and top event; failure rate, expected number of failures, and unreliability for top event and minimal cut sets	Fussell-Vesely importance calculations for primary events and minimal cut sets	KITT-2 allows each component to have unique time phases and thus failure and repair to vary from phase to phase	IBM 360/370 CDC 7600 Available from Argonne Software Center

Table 6-4. Computer codes for quantitative analysis (continued)

Code	Input	Quantitative calculations	Importance calculation	Other features	Type of computer and availability[a]
RALLY	Fault-tree description, control information, failure data	Average unavailabilities and failure frequencies for top event; time-dependent calculation possible through use of minimal cut sets; uncertainty analysis possible by using minimal cut sets; normal, lognormal, Johnson, extreme value-1, Weibull, gamma, and exponential distributions are handled	Code CRESSEX in RALLY can perform importance calculations	Can handle up to 1500 components and 2000 gates; can determine minimal cut sets using either a simulative or analytical way	IBM 360/370
RAS	Fault-tree description or minimal cut sets; failure and repair rates	Time-independent unavailability, expected number of failures, and frequency of top event	No	Phased-mission analysis possible; if fault tree is input, minimal cut sets will be calculated	CDC 7600 Available from Argonne Software Center
SUPERPOCUS	Minimal cut sets, component failure data, time at which calculations are performed	Time-dependent unavailability, reliability, and expected number of failures for minimal cut sets and top event	Yes	Ranks minimal cut sets on basis of importance; can read cut sets directly from MOCUS or PREP	IBM 360/370 CDC 7600 Available from Dept. of Nuclear Engineering, University of Tennessee
WAM-BAM	Fault-tree description, primary-event failure data	Point unavailability for top event and intermediate gates; no time-dependent analysis possible	No	Extensive error checking possible through WAM; probability truncation of fault tree; sensitivity analysis possible by using WAM-TAP preprocessor instead of WAM	CDC 7600 Available from EPRI Code Center

[a]All the codes listed here are written in Fortran IV.

[b]A GO chart (see Section 3.6.3) is a chart that resembles a schematic of system primary events and their relations via a set of 16 Boolean operators.

events that contribute to system failure. Other quantitative results that are calculated by these codes are importance measures for primary events, minimal cut sets, and modules of the tree; sensitivities; and time-dependent unavailability or reliability. The application of these calculations is discussed elsewhere in this guide.

Computer codes that perform quantitative analyses can be divided into two major groups: those requiring minimal cut sets as input, and those able to perform analyses without computing cut sets as a necessary intermediate step. The latter are called direct-evaluation codes.

FRANTIC

The FRANTIC (Formal Reliability Analysis including Testing Inspection and Checking) code computes the average and time-dependent unavailability of any general system model like a fault tree (Vesely and Goldberg, 1977). It can be used to assess the effects on system unavailability due to test down-times, repair times, test efficiency, test bypass capabilities, test-caused failures, and different test staggerings. The primary events handled by FRANTIC are primary events involving periodically tested, nonrepairable, and monitored components; human-error and dependent-failure contributions can also be modeled.

FRANTIC uses a system equation that represents the general system model much as a fault tree does. The system equation must be formulated by the user before the FRANTIC run. The primary events of the system equation are assigned an exponential distribution to describe hardware failures. At different instants of time the unavailability associated with each primary event is calculated. A Monte Carlo version of FRANTIC can be used to input sampling distributions for primary-event failure rates.

The input to FRANTIC consists of the system equation, primary-event failure rates, and test and repair characteristics; other inputs include the time period for the calculations as well as print and plot options. The output consists of system unavailability at different instants of time and, if requested, Calcomp plots of the time-dependent system unavailability.

A second version of the code, FRANTIC II, has been developed to enhance the capability to model the time-dependent unavailability of primary events and systems over their total in-service lifetime (Vesely et al., 1981b). The effects of the initial burn-in period, the time region of normal operation, and finally the wearout period can be modeled (the bathtub model). For this FRANTIC uses the Weibull distribution, which has a time-dependent failure rate. In addition, FRANTIC II allows the investigation of discontinuous changes in the failure rate as a function of the number of tests performed. This is essentially a demand-related, rather than a time-related, burn-in and wearout model. FRANTIC II also incorporates the effects of renewal on aging by introducing "good as new" or "good as old" primary events.

The FRANTIC and FRANTIC II codes are very simple to use. There is essentially no limit on the number of primary events in the system equation, but the construction of a system equation for a large system containing a large number of primary events is a nontrivial task. FRANTIC and FRANTIC II are written in Fortran IV for the IBM 360/370.

GO

GO (see Section 3.6.3) calculates the probabilities of all operating and nonoperating states for a system (Gateley et al., 1968). It uses a set of standardized functional operators to model physical primary events with mathematical entities that are easily identified as primary events. The modeling technique produces the GO chart, which corresponds closely to the physical layout, diagram, or schematic.

In the modeling procedure, 16 GO operators are used. Some of them are similar to fault-tree gates, but in addition to logic functions, time delays and switches can be modeled as well as complementary events and mutually exclusive states. The development of the GO chart consists of selecting the functional operators and connecting them with arrows to represent the flow of information. The GO code performs the logical connections and generates the minimal cut sets.

Required input is the GO chart and probabilities associated with the possible operational modes of each primary event, which is analogous to applying probabilities for the primary events of a fault tree. The output consists of probabilities for several output events in several operating states. In addition, cut sets of up to order 4 are generated.

Like WAMCUT, the GO code reduces storage requirements by eliminating low-probability paths at an intermediate stage of the processing and at the same time keeps track of the total of the discarded path. Because of the diversity and detail of the GO operators and the need to include all system primary events, the modeling process is quite complex. Furthermore, a change in probabilities often requires a complete rerun. However, the GO chart can be useful for design and system engineering.

ICARUS

The code ICARUS (Vaurio and Sciandone, 1979) is capable of calculating the average unavailability, optimum test interval, and relative contributions of testing, repair, and random failures for any one of three testing schemes: random testing, uniformly staggered testing, and nearly simultaneous testing.

ICARUS was developed to handle only primary events involving periodically tested components that are constantly unavailable, nonrepairable, or monitored. It is capable of calculating the average unavailability only in the asymptotic state. Consequently, the user must choose one of the three available testing schemes rather than create a particular testing scheme through the input. ICARUS evaluates the average unavailability analytically, and in this regard it is capable of calculating the optimum test interval by direct differentiation.

The input consists of the choice of the testing scheme and various failure rates, testing downtime, and probabilities of failure detection for the primary events in the system under study. The output consists of the testing scheme and failure-mode probabilities specified by the user and the average unavailability, optimum test interval, and average unavailability

at the optimum test interval for the system. Also provided are average unavailability contributions due to testing, repair, and random failures.

The advantage of ICARUS over a similar code like FRANTIC includes the use of analytical treatment for calculating unavailability, which avoids any inherent numerical error. It also includes three failure modes not found in FRANTIC: failure to start on a true demand, failure to detect a failure, and failure to repair a failure. Disadvantages include the ability to handle only periodically tested primary events and the restriction to only three testing schemes. ICARUS is written in Fortran IV for the IBM 360/370.

IMPORTANCE

IMPORTANCE was developed to rank primary events and cut sets according to various available importance measures (Lambert and Gilman, 1977). It is capable of handling fault trees with time-dependent primary events under the assumption that primary events are statistically independent and that their failure and repair distributions are exponential in time.

The importance measures that are included in the IMPORTANCE code are as follows:

1. Birnbaum (Birnbaum, 1969).
2. Criticality (Lambert, 1975).
3. Upgrading function (Lambert, 1975).
4. Fussell-Vesely (Fussell, 1975).
5. Barlow-Proschan (Barlow and Proschan, 1975).
6. Steady-state Barlow-Proschan (Barlow and Proschan, 1975).
7. Sequential contributory (Lambert, 1975).

The input is a list of cut sets and primary-event failure data. (The cut sets generated by FTAP or SETS can be received directly.) Input events can have up to eight-character alphanumeric names. The output consists of the probability, importance, and ranking of top events, primary events, and cut sets on the basis of one or more of the above-mentioned measures.

IMPORTANCE is written in Fortran IV for the CDC 7600. It has been used in several PRA studies.

KITT-1 and KITT-2

KITT-1 and KITT-2 are used for the quantitative reliability analysis of systems. They calculate time-dependent reliability characteristics for primary events, minimal cut sets, and the top event. The calculated characteristics include unavailability, failure rate, expected number of failures, unreliability, and importance.

The KITT codes calculate conservative approximations of the top-event reliability characteristics or can be used to bracket these characteristics. If the bracketing is carried to completion, the exact values are calculated. KITT-1 assumes that the primary events have exponentially distributed times to failure and constant repair times (if the event is repairable). Inhibit conditions have a constant probability of occurrence.

KITT-2 assumes that the primary events have exponentially distributed times to failure and repair (if repairability is applicable). The parameters in these distributions (failure and repair rates) can be changed at times specified by the user. Primary events can also be assigned probabilities of being failed initially if the assumption is not made that they are working at time zero. Inhibit conditions have a constant probability.

Required input consists of control information, primary-event information (failure rates, repair times, and optional names), time points at which the characteristics are calculated, and the list of minimal cut sets. The control parameters control the bracketing options and allow multiple-parameter runs to be performed. Each parameter run uses the same minimal sets, but if one or more of the primary-event failure rates or repair times are changed, the reliability characteristics are recalculated. The output from KITT-1 and KITT-2 consists of unavailability, unreliability, and the expected number of occurrences for primary events, minimal cut sets, and the top event; failure rates for minimal cut sets and the top event; and importance for primary events and minimal cut sets.

KITT-1 and KITT-2 are written in Fortran IV for the IBM 360/370 and the CDC 7600 computers. Some input-error checking is available. The cut sets can be input directly from PREP or MOCUS. However, for large fault trees the use of the KITT codes would be very limited. No external routine is required for running these codes.

RALLY

The code package RALLY, developed by the Gesellschaft fuer Reaktorsicherheit (1978), is capable of evaluating fault trees with up to 1500 primary events and 2000 gates, including AND, OR, NOT, and K-of-N gates.

RALLY consists of the codes TREBIL, TIMBER, CRESSEX, FESIVAR, CRESSC, CRESSCN, SLAP-MP, KARI, and STREUSL. TREBIL was based on the PREP preprocessor for fault-tree synthesis, optimization, and data acquisition for the other programs of the RALLY package. TIMBER plots the fault tree. CRESSEX calculates the average unavailability and failure frequency by means of Monte Carlo simulation. FESIVAR is similar to CRESSEX except that it is capable of performing importance calculations. Minimal cut sets are calculated by either a simulation method with CRESSC (or CRESSCN if the fault tree contains NOT gates) or an analytical method with the programs SLAP-MP and KARI. STREUSL performs a time-dependent fault-tree quantification based on the minimal cut sets of the tree. The average unavailability and failure rate are calculated by the AVAGS code, which is used in conjunction with STREUSL. For uncertainty calculations the following distributions are handled by AVAGS: normal, lognormal, Johnson-SL, extreme value 1, Weibull, gamma, and exponential. RALLY was used in the German Risk Study and is written in Fortran IV for the IBM 360/370.

RAS

RAS (Reliability Analysis System) is an integrated package of computer codes for the quantification of fault trees (Rasmuson et al., 1977). It is based on MOCUS, POCUS, KITT-1, SRTPAN, and COMCAN. The package can be used for an entire system analysis with up to five system phases, or it can be

used to do only one section of the analysis, such as cut-set determination or fault-tree reduction.

The amount of input required for RAS depends on whether all capabilities will be used or if only one or two tasks will be required. Either the fault-tree logic equation or the cut sets can be input. Failure-rate data (exponential distribution assumed), repair rates, and mission times are required for calculating unreliability. If more than one mission is desired, this information must be input for each phase. It should be noted that the phases refer to system phases; cut sets or fault-tree equations can be different for each phase. In this RAS differs from KITT-2, which allows the phasing of primary-event information only and cannot readily handle system phases.

The output of RAS can be in printed, punched-card, or file-storage form. The input information is printed out, which allows for easy error detection. The specific information output depends on the options called within the program. The output from cut-set algorithms includes a fault-tree summary, the number of cut sets of each size. A listing of the cut sets is obtained by requesting it as an input option.

If KITT-1 or POCUS is called, reliability characteristics--including availability, expected number of failures, and failure rates--are listed for the top event. This information can be output for the cut sets and primary events by exercising an option. POCUS also has the option of ranking the primary events and cut sets by their unavailability importance.

When phased missions are required, the mission cut sets can be reduced by a cancellation subroutine and mission unreliability bounds can be optionally calculated. The output from the bounds calculation includes the time-dependent upper bound on mission unreliability for each phase.

RAS is convenient to use because one package can perform a wide range of options without additional input, and several codes that accomplish different functions are included. However, several of these codes have long running times, and their use may not be justified. It should also be noted that, as these codes are relatively new, there is little actual operating experience, which could affect the overall practicality of their use. The RAS package is written in Fortran IV for the CDC 7600 computer.

SUPERPOCUS

SUPERPOCUS is used for quantitative reliability analyses (Fussell et al., 1977). It calculates time-dependent unavailability, unreliability, unavailability importance, and unreliability importance for primary events and ranks the primary events by importance. For the minimal cut sets, this code calculates unavailability, reliability, expected number of failures, unavailability importance, and unreliability importance. The calculated top-event characteristics are unavailability, expected number of failures, and failure rates.

SUPERPOCUS is very efficient because it uses a tightly bounding approximation method. The approximations always overpredict failure characteristics. Primary events are assumed to have exponentially distributed

times to failure and repair (if the event is repairable). Inhibit conditions have a constant probability of occurrence.

Input consists of control information, primary-event information (failure rates, repair times, and optional names), time points at which the characteristics are calculated, and the list of minimal cut sets. The control parameters can be used to edit the output. Any or all of the output information can be suppressed except the top-event information.

The SUPERPOCUS algorithm is superior to that of the KITT codes. It accepts the initial unavailability for primary events. It can read the cut sets directly from MOCUS or PREP output. SUPERPOCUS is written in Fortran IV for the CDC 7600 and the IBM 360/370 computers. A routine for input-error checking is available, and no external routine is required.

WAM-BAM

WAM-BAM, which calculates point probabilities for the top events (Leverenz and Kirch, 1976), actually consists of four codes: WAM, WAMTAP, BAM, and CUT. WAM and WAMTAP are input preprocessors for the evaluation code BAM (Boolean Arithmetic Model). The WAM preprocessor is designed to ease the input description of the fault tree and the event probabilities. If requested, the input to BAM can be saved and subsequently modified by WAMTAP. WAMTAP allows the probability of single or grouped primary events to be changed for sensitivity studies. The use of WAM-CUT has been already discussed in this section.

The evaluation code BAM uses a combination of concepts from the GO method and fault-tree analysis: it uses the GO computational scheme but models the operations as gates on a fault tree. The probability of the top event is computed by forming a truth table, each line of which represents a product term (P-term) event disjoint from all the other P-terms. The product of the probabilities of the event in each P-term gives the probability of the P-term, and the union of the applicable P-term gives the probability of the top event. Like the GO code, WAM-BAM keeps track of the total probability of the discarded path during a probability truncation.

WAM-BAM is very easy to use. However, the new version of WAMCUT may be faster and more efficient for calculating top-event probabilities. WAM-BAM is written in Fortran IV for the CDC 7600 computer.

6.6.3 CODES FOR UNCERTAINTY ANALYSIS

Uncertainty analyses are important parts of PRA studies because of the statistical uncertainty in the failure and event-frequency data. To model statistical uncertainties first, failure and initiating-event frequency-data distributions are selected. Then, based on the logical relationship (e.g., cut sets) of these distributions, they are combined.

The computer codes developed to deal with uncertainty analysis can be divided into two categories: codes that perform the analysis through Monte

Carlo simulation (e.g., SAMPLE and STADIC-II) and codes that perform the analysis by mathematically combining the distributions (e.g., BOUNDS and SPASM). Most of the uncertainty programs can handle a variety of statistical distributions, normal, lognormal, uniform, and empirical distributions being most commonly used. However, some of these codes use more sophisticated distributions, such as the beta, gamma, Student-t, and Johnson distributions. Table 6-5 presents a summary of the codes for uncertainty analysis.

BOUNDS

BOUNDS is used to find probability intervals of system unavailability (Lee and Apostolakis, 1976). Multiple system functions with multiple data input descriptions can be processed in one run.

In the first step of the procedure BOUNDS computes, from primary-event failure rates, the first two moments of primary-event probabilities. Next it uses the information on minimal cut sets to obtain the moments for the occurrence probabilities of the minimal cut sets. From this last step, it calculates the moments of the top-event probability. It matches these moments to produce the Johnson-type distribution that possesses the same moments and then uses the fitted distribution to obtain the uncertainty bounds of the top event.

In input and output BOUNDS is similar to SAMPLE. The code can handle up to 1000 primary events. The number of input minimal cut sets is limited to 500, and it is assumed that there are no more than 5 primary inputs in any minimal cut set. BOUNDS is written in Fortran IV for the IBM 360/370 computer.

MOCARS

MOCARS is a Monte Carlo code for determining the means, the standard deviation, and distribution for fault-tree models (Matthews, 1977). It is essentially the same as SAMPLE, with added capabilities. The method for Monte Carlo simulation is the same as that in SAMPLE, but MOCARS can also handle the following distributions: exponential, Cauchy, Weibull, Pearson type IV, and empirical.

Input is a system-unavailability function specified either in Fortran statements or in terms of cut sets. The output is similar to that of SAMPLE, but MOCARS has the additional option of microfilm plotting with the integrated graphics system and the ability to perform a Kolmogorov-Smirnov goodness-of-fit test. This test shows whether the output distribution resembles a normal, lognormal, or exponential function. The probability distribution for the top event of the fault tree can be plotted as an optional output.

MOCARS is no more complex to use than SAMPLE. Its extra capabilities (e.g., plotted output) give it advantages. Because of the added capabilities, MOCARS is considered applicable to PRA programs and could be more useful than SAMPLE. It is written in Fortran IV for the CDC 7600 computer.

Table 6-5. Computer codes for uncertainty analysis

Code	Input	Method of uncertainty analysis	Type of statistical distribution	Other features	Type of computer and availability[a]
BOUNDS	Reduced system equation or minimal cut sets, primary-event failure data	Mathematical combination of uncertainties; output includes two moments of minimal cut sets and the top event	Johnson, empirical	Can handle multiple system functions with multiple data input descriptions; can fit Johnson-type distribution to the top event	IBM 360/370 Available from University of California at Los Angeles
MOCARS	Minimal cut sets or reduced system equation, primary-event failure data	Monte Carlo simulation	Exponential, Cauchy, Weibull, empirical, normal, lognormal, uniform	Microfilm plotting of output distribution; Kolmogorov-Smirnov goodness-of-fit test on output distribution is possible	CDC Cyber 76 Available from Argonne Software Center
PROSA-2	Reduced algebraic function for system representation, failure data	Monte Carlo simulation	Normal, lognormal, uniform, any distribution in the form of a histogram, truncated normal, beta	Can correlate input parameters; no sorting necessary to obtain the top-event histogram	IBM 370 Available from Argonne Software Center

Table 6-5. Computer codes for uncertainty analysis (continued)

Code	Input	Method of uncertainty analysis	Type of statistical distribution	Other features	Type of computer and availability[a]
SAMPLE	Minimal cut sets or reduced system equation, primary-event failure data	Monte Carlo simulation	Uniform, normal, lognormal	Used in the Reactor Safety Study; output is a probability distribution for the top event	IBM 360/370 Available from Argonne Software Center
SPASM	Fault tree or reduced system equation, component-failure data	Mathematical combination (similar to BOUNDS)	Lognormal	Works in conjunction with WAMCUT	CDC 7600 Available from EPRI Code Center
STADIC-II	Reduced system equation, primary-event failure data	Monte Carlo simulation (similar to SAMPLE)	Normal, lognormal, log-uniform, tabular input distribution	Has a better and efficient method of sorting the probabilities obtained in each trial	PRIME, UNIVAC-1180, CDC 7600 Available from General Atomic Company

[a]All the codes listed here are written in Fortran IV.

PROSA-2

PROSA-2 is an advanced version of PROSA-1, which provides a response-surface solution to probability distributions for the consequences of postulated nuclear accidents (Vaurio, 1981). However, the code can be used for uncertainty analysis by a direct simulation of general analytical functions.

The method for Monte Carlo simulation is similar to that of SAMPLE, but PROSA-2 has a different selection of input distributions; it can handle partially correlated input parameters and forms the top-event histograms without the comparative sorting method used in SAMPLE. The following types of distributions are available in PROSA-2: uniform, truncated normal, exponential, beta, and lognormal.

The input data include the simplified system equation, failure data, and the type of distribution used for the events in the equation. The output includes the probability-distribution histograms for top events and the statistical-error estimates for the histograms.

PROSA-2 can handle dependent (correlated) input parameters and can calculate conditional distributions. The maximum number of variable input parameters that can be analyzed simultaneously is 12. The correlations (if any) between the input parameters are limited to linear correlations. The program can plot the output histogram. PROSA-2 is written in Fortran IV for the IBM 370 computer.

SAMPLE

SAMPLE calculates the mean, the standard deviation, the distribution, and the probability bounds of a function. It was used in the Reactor Safety Study (USNRC, 1975). It uses the Monte Carlo simulation method and allows multiple system functions with multiple data input descriptions to be processed in one run.

The Monte Carlo simulation used in SAMPLE is performed by sampling primary-event values from their input distributions and finding the system-failure probability corresponding to this "trial." After many trials, the system-failure probabilities are sorted and probabilities corresponding to various confidence levels are obtained. SAMPLE can use primary-event data with either a normal, lognormal, or log-uniform distribution. Once selected, the same type of distribution is used for all primary events throughout the problem. After all these trials, results are sorted and the accuracy is tested. Finally, median and 90th percentile confidence bounds are calculated by using the sorted results.

Input includes a probability function derived from the logical configuration of the primary events, primary-event failure rates, and error factors. The output includes a listing of input data, the median value of the point estimates, as well as the system-failure probability in various increments and distribution confidence limits. The output distribution is presented in terms of estimated empirical probability percentiles from which the estimated median and upper and lower bounds can be easily read. The output also includes the estimated mean and standard deviation of the distribution and a tabular histogram of the system density function.

SAMPLE is inefficient with respect to its sorting procedure for the failure probabilities calculated in each trial. Also, the provision of the system unavailability function is a nontrivial task for large fault trees. However, it is very easy to use. SAMPLE is written in Fortran IV for the IBM 360/370 computer.

SPASM

SPASM (System Probabilistic Analysis by Sampling Methods) is an uncertainty-analysis code designed to complement the WAM series (Leverenz, 1981). Its main purpose is to provide an approximation to the top-event probability distribution from an input system model and primary-event probability distribution. While SPASM can be used in conjunction with WAMCUT, it can also be used independently. When using SPASM with WAMCUT, the system analyst chooses an option in WAMCUT that builds a system model for SPASM from the fault-tree Boolean equation. The analyst then inputs the model to SPASM together with the distributions for each event in the model.

The method used in SPASM is similar to that of BOUNDS. However, if SPASM is used in conjunction with WAMCUT, the process of preparing and inputting the system equation is eliminated. This makes the use of SPASM very easy and practical for large fault trees.

Input is very simple, especially if SPASM is used with WAMCUT (the input in WAMCUT stays essentially the same). Only the first and second moments of the fault-tree primary events must be input. If WAMCUT is not used, the analyst should construct the system model in Fortran IV to replace the cut sets generated by WAMCUT. The output consists of the first and second moments of the top event. SPASM is currently programmed for a CDC 6600/6700 computer, but conversion to IBM machines is in progress.

STADIC-II

STADIC uses a Monte Carlo simulation to generate pseudo-random-sample statistical distributions for user-defined output functions (Cairns and Fleming, 1977). STADIC-II (Orvis and Frank et al., 1981) is an improved version. STADIC was used in the uncertainty analysis of the PRA study for high-temperature gas-cooled reactors (General Atomic Company, 1978).

STADIC-II uses a "binning" procedure that eliminates the need to store and sort all of the sample (Monte Carlo trial) values generated for an output function. It also uses a very efficient algorithm for calculating normally distributed random variables. In the binning procedure the complete range of output-function variability, from the 0th to the 100th percentile, is partitioned into user-defined intervals called bins. The programmed default is 20 bins with intervals concentrated around the 50th and 95th percentiles. STADIC-II internally calculates bin boundaries in terms of the output-function values corresponding to the preselected percentiles. A counter is established for each bin. As each random-sample value of the output function is generated, it is compared with the bin boundaries, the bin within which it belongs is identified, and the corresponding counter is incremented by one. Up to 10 functions using up to 75 different variables can be analyzed simultaneously.

Input consists of the user-specified functions to be evaluated, the parameters of the selected statistical probability density function, and the number of trials desired. The user can specify any of the normal, log-normal, or log-uniform distributions--or select an arbitrary tabular distribution--for any of the variables. The input variables can have different distributions within the same functional expression. The output of STADIC-II consists of a complementary cumulative distribution function and a probability density function for each input function; the mean, variance, standard deviation, coefficient of skewness, and coefficient of kurtosis; and the Monte Carlo sampling error.

STADIC-II is considerably faster than SAMPLE because of the binning procedure. Another attractive feature is the flexibility of using different distribution functions for the variable of a given function. STADIC-II is written in Fortran IV and is currently available on UNIVAC-1180, CDC Cyber 7600, and PRIME computers.

6.6.4 CODES FOR DEPENDENT-FAILURE ANALYSIS

Dependent-failure analysis is becoming increasingly important in system reliability and safety studies, because it has been recognized that such failures can often dominate random hardware failures. Dependent-failure analysis attempts to identify the modes of system failure (i.e, minimal cut sets) that have the potential of being triggered by a single, more primary common cause; the minimal cut sets that need to be identified are those with two or more events, all of which are susceptible to a single common-cause failure mechanism.

Codes developed to deal with dependent failures are basically tracking and sorting codes. They are essentially a first effort at providing a formalized method of approaching the difficult problem of identifying and evaluating dependent failures. These codes are summarized in Table 6-6 and briefly described below.

BACFIRE

The BACFIRE code is used as an aid in common-cause failure analysis (Cate and Fussell, 1977). Its objective is to aid in identifying common-cause failures in a system and to point out why this failure potential exists. To this end, each minimal cut set is individually searched for a commonality among all the primary events in that cut set.

BACFIRE uses exactly the same method as COMCAN. However, BACFIRE allows the use of multiple locations for primary events involving components like pipes and cables. For example, if a cable passes through several different-susceptibility compartments, COMCAN can assign only one of these compartments to the cable, but BACFIRE can assign different compartments. The input and output characteristics of BACFIRE are similar to those of COMCAN.

Table 6-6. Computer codes for dependent-failure analysis

Code	Input	Method of common-cause analysis	Other features	Type of computer and availability[a]
BACFIRE	Cut sets, component susceptibilities and locations, and susceptibility domains	Examines cut sets for possible common generic causes or links between all components; prints out cut sets that are common-cause candidates	Has same features as COMCAN, but allows use of multiple locations for primary events (e.g., pipes and cables)	IBM 360/370 Available from Dept. of Nuclear Engineering, University of Tennessee
COMCAN	Cut sets, component susceptibilities and locations, and susceptibility domains	Examines cut sets for possible common generic causes or links between all components	Cut sets that are common-cause candidates can be ranked by significance of common-cause failure output	IBM 360/370 Available from Argonne Software Center
COMCAN-II	Fault tree, component susceptibilities and locations, and susceptibility domains	Same as COMCAN	FATRAM is used to generate cut sets before common-cause analysis; other features are similar to those of COMCAN	CDC 7600 Available from Argonne Software Center
MOCUS-BACFIRE	Fault tree, component susceptibilities and locations, and susceptibility domains	Same as BACFIRE	Similar to BACFIRE, but does not need cut-set input: cut sets are generated by MOCUS and automatically passed to BACFIRE	IBM 360/370 Available from Dept. of Nuclear Engineering, MIT

Table 6-6. Computer codes for dependent-failure analysis (continued)

Code	Input	Method of common-cause analysis	Other features	Type of computer and availability[a]
SETS	Fault tree	Adds generic causes and links to fault tree; cut sets that include one or more generic causes are obtained and identified as common-cause candidates	Can handle large fault trees and can identify partial dependency in cut sets; attractive features of SETS as cut-set generator justify use for dependent-failure analysis	CDC 7600 Available from Argonne Software Center
WAMCOM	Fault tree with susceptibilities added	Uses modularization and SETS to more effectively identify cut sets that contain critical events, critical random events, and significant common-cause events or to describe common-cause sets for each random failure	Can identify common total or partial links between fault-tree components; can handle very large fault trees	CDC 7600 Available from EPRI Code Center

[a]All the codes listed here are written in Fortran IV.

BACFIRE is written in Fortran IV for the IBM 360/370 and the CDC 7600 computers. There is an extensive error-checking routine, and no external routine is needed to run the code.

COMCAN

COMCAN is used to identify potential common-cause failures in a system or combination of systems (Burdick et al., 1976). It individually searches each cut set of system failures for commonality among all the primary events in that cut set.

A minimal cut set will be identified as a common-cause candidate by one of two criteria. The first criterion is met when all the primary events in a minimal cut set share a special condition that alone can result in the simultaneous failure of all the primary events in the cut set. An example of a common special condition is a common maintenance crew servicing all of the primary events implied by the primary events of a minimal cut set. The second criterion is met if all the primary events in a minimal cut set are susceptible to the same secondary-failure cause and are located in the same domain with respect to that failure cause. An example is a minimal cut set with primary events that will all occur when the associated components get wet and no water barrier exists between them.

The input consists of secondary-failure susceptibilities and applicable special conditions for primary events, domain maps for secondary-failure causes, and the list of minimal cut sets. The output provides the analyst a listing of minimal cut sets that have potential for dependent failures. The number of these common-cause candidates can be limited to those that are probably most important.

The method used in COMCAN does not provide partial common-cause dependences in systems under study. The inputting of cut sets (most often minimal cut sets are numerous) is very difficult. COMCAN is written in Fortran IV for the IBM 360/370 and has error-checking routines.

COMCAN-II, an improved version of COMCAN (Rasmuson et al., 1978, 1979), was developed to circumvent COMCAN's dependence on minimal cut sets that must be obtained by other codes. COMCAN-II uses the qualitative code FATRAM (discussed in Section 6.6.1) to obtain minimal cut sets before COMCAN analysis. This eliminates the cumbersome task of inputting all the cut sets. COMCAN-II is written in Fortran IV for the CDC Cyber 7600 computer.

MOCUS-BACFIRE

MOCUS-BACFIRE, obtained by coupling MOCUS and BACFIRE, is used to aid in identifying potential dependent failures in a system directly from the fault tree (Modarres et al., 1980a, b). It eliminates the need for generating cut sets before running BACFIRE and simplifies the input process.

The method used in MOCUS-BACFIRE is the same as described for MOCUS and BACFIRE individually. MOCUS-BACFIRE is written in Fortran IV for the IBM 360/370 computer. There is an extensive error-checking routine, and no external routine is required.

SETS

The SETS code, described earlier, can also be used for dependent-failure analysis (Worrell and Stack, 1978). The analysis is conducted in a manner similar to that of COMCAN by inputting generic cause susceptibilities for each primary event. A transformation of variables incorporates the dependent-failure susceptibilities into the Boolean equation for the top or any intermediate gate of the fault tree, and a few simple manipulations allow the user to display the cut sets that are dependent-failure candidates. The use of SETS for dependent-failure analysis has an advantage in that SETS can handle very large trees, which other dependent-failure codes are unable to do.

WAMCOM

The WAMCOM package (Putney, 1981) is designed for the dependent-failure analysis of large, complex fault trees. It can handle up to 2000-i primary events (i being the number of gates) affected by the common-cause events.

The WAMCOM dependent-failure analysis consists of model preparation and computer analysis. Model preparation is accomplished in four primary steps: the identification of potential common-cause events, fault-tree construction, the definition of individual common-cause events, and the creation of a primary-event effectivity table. The computer analysis is based on a package of three computer codes: LEVEL, WAMCOM, and SETS. LEVEL generates a solution structure for WAMCOM and SETS by partitioning the fault tree into subtrees, called "levels," that are solved individually. LEVEL develops a scheme for rebuilding the tree by reintroducing groups of subtrees into the main tree trunk. The WAMCOM program consists of a preprocessor and a SETS user's-program generator.

The SETS program generator writes a SETS user's program for each of four computer runs called "modes." This user's program is developed from the solution structure generated by LEVEL. Each mode uses as input the solution structure, fault-tree structure, and a component-susceptibility table along with information generated from previous modes.

The input consists of the fault-tree structure and a component-susceptibility table that identifies the susceptibility of each component to a generic cause. The output consists of a listing of the fault-tree input and level processing, the solution of the tree (top-down), and the output of various modes. The output of mode 1 consists of all critical common-cause events (a critical common-cause event is an event that can individually cause enough primary events to fail to place the entire system in a failed state) in the fault tree. Mode 2 output is a list of all critical random-failure events, all combinations of two significant common-cause events, and all combinations of significant common-cause events. (A significant common-cause event is an event that does not by itself lead to system failure but can cause enough primary events to fail such that the existence of a second event, either a dependent or a random failure, will place the system in a failed state.)

Mode 3 output consists of combinations of significant common-cause events with significant random-failure events affected by noncritical common-cause events. The output of mode 4 provides descriptive cause sets for each critical or significant common-cause event input.

The advantages of the WAMCOM package include a fast-running code for the dependent-failure analysis of large trees and the flexibility offered by the code to an experienced analyst. The WAMCOM package is written in Fortran IV for the CDC 7600 computer.

6.6.5 COMPUTER CODES FOR OTHER RELATED PROBABILISTIC ANALYSES

A variety of codes have been developed to aid in probabilistic analyses of accident sequences that are not used directly for qualitative or quantitative analyses of the sequences. Examples are codes that are used to perform a Bayesian updating analysis on failure data or codes that are used to perform cause-consequence analyses (to identify common characteristics among accident sequences). All of these codes are briefly discussed in this section. However, because of their variety and different applications, they were not included in Tables 6-3 through 6-6.

BROLS

BROLS (Orvis and Frank et al., 1981) is a small, fast-running code that facilitates calculations associated with using Bayes' theorem. The code calculates the posterior distribution given the prior and the likelihood distributions.

The user can choose from eight analytical statistical distributions programmed in the code, and different distributions can be selected for the prior and the likelihood. The available distributions are the normal, lognormal, Poisson, binomial, beta, hyperbinomial (or beta binomial), exponential, and uniform. An option allows the user to provide an arbitrary statistical distribution input as a discrete-probability histogram. The program makes extensive use of the International Mathematical and Statistical Library (IMSL) routines.

The input consists of the choice of the prior and likelihood functions, either one of the built-in functions or a user-specified histogram. The output consists of a table containing the probability histograms for the prior, the likelihood, and the posterior. The mean values of the prior and the posterior are also printed. BROLS is written in Fortran IV and is available for UNIVAC 1180, CDC Cyber 7600, and PRIME computers.

EXCON

EXCON is used to aid in performing risk assessments of engineered plants, facilities, or systems (Arendt et al., 1978). It is used in conjunction with cause-consequence analysis.

Required input consists of control information, consequence category descriptions, accident-sequence specifications, and search specifications.

Searches can be performed to analyze the entire set of accident sequences or any subset with the common characteristics specified in the search data.

The output information resulting from a search consists of the expected occurrence frequency of accidents resulting in consequences within each of the categories. A listing of major contributors to the expected occurrence frequency, by category, is also printed. This allows the analyst to determine which accident sequences are inconsistently large contributors to overall system risk. EXCON generates risk curves of the "Farmer" type.

EXCON is written in Fortran IV for the IBM 360/370 and the CDC 7600 computers. It has an extensive error-checking capability and requires no external routine.

6.7 DOCUMENTATION

The documentation of accident-sequence quantification goes beyond providing a frequency estimate for each plant-damage bin. It is very important to document the process by which these results were obtained. This documentation should include detailed descriptions of all simplifying assumptions and approximations used to obtain the results. If possible, the quantitative effects of the assumptions and approximations should be discussed. The documentation should also, by providing intermediate results, include enough information for the reader to reconstruct the accident-sequence frequencies from their dominant contributors. These results should identify the dominant contributions to bins, sequences, and systems. Pertinent sensitivities to primary-event point-estimate and uncertainty characteristics should be discussed.

If uncertainty studies have been performed, then the results of such studies and their ranges or distributions should be presented. The equations and distributions used for uncertainty analysis as well as the process of propagation (with pertinent assumptions) should be clearly described.

If the plant model was used to gain insights into plant reliability or the prevention of damage other than core melt, these insights should also be documented. In most cases this is the most valuable result obtained by the PRA study.

6.8 ASSURANCE OF TECHNICAL QUALITY

The assurance of technical quality can be promoted by a thorough documentation of the quantification process along with a comprehensive review of analysis results by the systems and sequence analysts. The details of the quantification should be recorded to permit a reviewer to reconstruct the quantification process and determine the validity of the steps taken and the

assumptions made. In addition to establishing the validity of the quantification process, the review of results by the systems and sequence analysts serves another objective: to ensure that the results are reasonable and that no important failure modes have been left out. Results from similar plants can be examined to establish whether they are consistent and, if they are not, the reasons for the difference.

REFERENCES

Apostolakis, G. E., and S. Kaplan, 1981. "Pitfalls in Risk Calculations," Reliability Engineering, Vol. 2, pp. 135-145.

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

Barlow, R. E., and F. Proschan, 1975. Statistical Theory of Reliability and Life Testing, Holt, Rinehart, and Winston, Inc., New York.

Birnbaum, Z. W., 1969. On the Importance of Different Components in a Multi-System in Multivariate Analysis, Academic Press, New York.

Burdick, G. R., N. H. Marshall, and J. R. Wilson, 1976. COMCAN--A Computer Program for Common Cause Failure Analysis, ERDA Report ANCR-1314, Aerojet Nuclear Company.

Cairns, J. J., and K. N. Fleming, 1977. STADIC--A Computer Code for Combining Probability Distributions.

Cate, C. L., and J. B. Fussell, 1977. BACFIRE--A Computer Program for Common Cause Failure Analysis, NERS-77-02, Nuclear Engineering Department, University of Tennessee, Knoxville.

Corynan, G. C., 1982. STOP: A Fast Procedure for the Exact Computation of the Performance of Complex Probabilistic Systems, UCRL-53230, Lawrence Livermore National Laboratory, Livermore, Calif.

Engelbrecht-Wiggans, R., and D. R. Strip, 1981. On the Relation of Various Reliability Measures to Each Other and to Game Theoretic Values, SAND80-2624, Sandia National Laboratories, Albuquerque, N.M.

Erdmann, R. C., F. L. Leverenz, and H. Kirch, 1978. WAMCUT, A Computer Code for Fault Tree Evaluation, EPRI-NP-803, prepared by Science Applications, Inc., Palo Alto, Calif., for the Electric Power Research Institute.

Fussell, J. B., 1975. "How to Hand Calculate System Reliability Characteristics," IEEE Transactions of Reliability, Vol. R-24, No. 3.

Fussell, J. B., E. B. Henry, and N. H. Marshall, 1974. MOCUS--A Computer Program To Obtain Minimal Sets from Fault Trees, USAEC Report ANCR-1156, Aerojet Nuclear Company.

Fussell, J. B., D. M. Rasmuson, and D. Wagner, 1977. SUPERPOCUS--A Computer Program for Calculating System Probabilistic Reliability and Safety Characteristics, NERS-77-01, Nuclear Engineering Department, University of Tennessee, Knoxville.

Gateley, W. Y., et al., 1968. GO, A Computer Program for Reliability Analysis of Complex Systems, KN-67-704(R), Kaman Sciences Corporation.

Gesellschaft fuer Reaktorsicherheit, 1978. Deutsche Risikostudie Kernkraftwerke: Eine Untersuchung zu dem durch Stoerfaelle in Kernkraftwerken verursachten Risiko (German Risk Study), Verlag TUEV, Rheinland, Federal Republic of Germany.

Green, A. E., and A. J. Bourne, 1972. Reliability Technology, Wiley-Interscience, New York.

Hahn, F. E., 1966. Applied Boolean Algebra, 2nd edition, Macmillan, New York.

Henley, E. J., and H. Kumanoto, 1981. Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J.

Kaplan, S., 1981. "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations," Risk Analysis, Vol. 1.

Lambert, H. E., 1975. Fault Trees for Decision-Making in Systems Analysis, Ph.D. thesis, UCRL-51829, Lawrence Livermore National Laboratory, Livermore, Calif.

Lambert, H. E., and F. M. Gilman, 1977. The IMPORTANCE Computer Code, ERDA Report UCRL-79269, Lawrence Livermore National Laboratory, Livermore, Calif.

Lee, Y. T., and G. E. Apostolakis, 1976. Probability Intervals for the Top Event Unavailability of Fault Trees, UCLA-ENG-7663, University of California, Los Angeles.

Leverenz, F. L., 1981. SPASM, A Computer Code for Monte Carlo System Evaluation, EPRI NP-1685, Electric Power Research Institute, Palo Alto, Calif.

Leverenz, F. L., and H. R. Kirch, 1976. User's Guide for the WAM-BAM Computer Code, EPRI-217-2-5 (PB-240-624), prepared by Science Applications, Inc., Palo Alto, Calif., for the Electric Power Research Institute.

Leverenz, F. L., and H. R. Kirch, 1978. WAMCUT--A Computer Code for Fault Tree Evaluation, NP-803, Electric Power Research Institute, Palo Alto, Calif.

Matthews, S. D., 1977. MOCARS: A Monte Carlo Simulation Code for Determining Distribution and Simulation Limits, ERDA Report TREE-1138, EG&G Idaho, Inc., Idaho Falls, Idaho.

McKnight, C. W., et al., 1966. Automatic Reliability Mathematical Model, NA-66-838, North American Aviation, Inc., Downey, Calif.

Modarres, M., N. C. Rasmussen, and L. Wolf, 1980a. Reliability Analysis of Complex Technical Systems Using the Modularization Technique, MITNE-228, Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, Mass.

Modarres, M., N. C. Rasmussen, and L. Wolf, 1980b. A User's Guide for MODCUT and PL-MODMC Computer Codes for Fault Tree Analysis, USNRC Report NUREG/CR-1461.

Olman, M. D., 1981. Quantitative Fault Tree Analysis Using the SET Evaluation Program (SEP), USNRC Report NUREG/CR-1935.

Olmos, J., and J. Wolf, 1977. A Modular Approach to Fault Tree and Reliability Analysis, MITNE-209, Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, Mass.

Orvis, D. D., M. V. Frank, et al., 1981. Guidebook for the Reliability and Maintainability Analysis of NWTS Repository Equipment, ONWI-334, Office of Nuclear Waste Isolation, Battelle Memorial Institute, Columbus, Ohio.

Pande, P. K., M. E. Spector, and P. Chatterjee, 1975. Computerized Fault Tree Analysis: TREEL and MICSUP, ORC-75-3 (AD-A010 146), Operations Research Center, University of California, Berkeley.

Putney, B. F., 1981. WAMCOM, Common Cause Methodologies Using Large Fault Trees, NP-1851, Electric Power Research Institute, Palo Alto, Calif.

Putney, B. F., and H. R. Kirch, 1981. WAMCUT-II--A Fault Tree Evaluation Program, SAI-SR-234-81-PA, Science Applications, Inc., Palo Alto, Calif.

Rasmuson, D. M., and N. H. Marshall, 1978. "FATRAM--A Core Efficient Cut Set Algorithm," IEEE Transactions on Reliability, Vol. R-37, No. 4, pp. 250-253.

Rasmuson, D. M., N. H. Marshall, and G. R. Burdick, 1977. User's Guide for the Reliability Analysis System (RAS), ERDA Report TREE-1168, EG&G Idaho, Inc., Idaho Falls, Idaho.

Rasmuson, D. M., et al., 1978. COMCAN II: A Computer Program for Common Cause Failure Analysis, USDOE Report TREE-1289, EG&G Idaho, Inc., Idaho Falls, Idaho.

Rasmuson, D. M., N. H. Marshall, J. R. Wilson, and G. R. Burdick, 1979. COMCAN II--A Computer Program for Automated Common Cause Failure Analysis, USDOE Report TREE-1361, EG&G Idaho, Inc., Idaho Falls, Idaho.

Rooney, J. J., and J. B. Fussell, 1978. BACFIRE II--A Computer Program for Common Cause Failure Analysis of Complex Systems, Department of Nuclear Engineering, University of Tennessee, Knoxville.

Science Applications, Inc., 1978. Fire Related Accident Sequences at CRBRP, SAI-125-78-PA, Palo Alto, Calif.

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

Van Slyke, W. J., and D. E. Griffing, 1975. ALLCUTS--A Fast Comprehensive Fault Tree Analysis Code, ERDA Report ARH-ST-112, Atlantic Richfield Hanford Company.

Vaurio, J. K., 1981. PROSA-2: A Probabilistic Response Surface Analysis and Simulation Code, ANL-81-33, Argonne National Laboratory, Argonne, Ill.

Vaurio, J. K., and D. Sciandone, 1979. Unavailability Modeling and Analysis of Redundant Safety Systems, ANL-79-87, Argonne National Laboratory, Argonne, Ill.

Vesely, W. E., 1977. "Reliability Quantification Technique Used in the Rasmussen Study," Reliability and Fault Tree Analysis, Society for Industrial and Applied Mathematics, Philadelphia, Pa., pp. 775-804.

Vesely, W. E., and F. F. Goldberg, 1977. FRANTIC--A Computer Code for Time-Dependent Unavailability Analysis, USNRC Report NUREG-0193.

Vesely, W. E., and R. E. Narum, 1970. PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree, USAEC Report IN-1349, Idaho Nuclear Corporation, Idaho Falls, Idaho.

Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl, 1981a. Fault Tree Handbook, USNRC Report NUREG-0492.

Vesely, W. E., et al., 1981b. FRANTIC II--A Computer Code for Time-Dependent Unavailability Analysis, USNRC Report NUREG/CR-1924.

Waddington, J. G., and A. Wild, 1981. The Fault Tree as a Tool in Safety Analysis in Nuclear Power Plants, INFO-0036, Atomic Energy Control Board, Ottawa, Canada.

Wagner, D. P., C. L. Cate, and J. B. Fussell, 1977. "Common Cause Failure Analysis for Complex Systems," in Nuclear Systems Reliability and Risk Assessment, J. B. Fussell and G. R. Burdick (editors), Society for Industrial and Applied Mathematics, Philadelphia, Pa.

Willia, R. R., 1978. Computer-Aided Fault Tree Analysis, ORC-78-14, Operations Research Center, University of California, Berkeley.

Worrell, R. B., and D. W. Stack, 1977. Common-Cause Analysis Using SETS, SAND77-1832, Sandia National Laboratories, Albuquerque, N.M.

Worrell, R. B., and D. W. Stack, 1978. A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, Sandia National Laboratories, Albuquerque, N.M.

Worrell, R. B., and D. W. Stack, 1981. "A Boolean Approach to Common Cause Analysis," in 1980 Proceedings, Annual Reliability and Maintainability Symposium, San Francisco, Calif., pp. 363-366.

Chapter 7

Physical Processes of Core-Melt Accidents

7.1 INTRODUCTION

This chapter describes procedures for predicting the progression of core-melt accidents and the associated physical processes, developing containment event trees, and quantifying probabilities for branches of the containment event tree for each accident sequence. It discusses the various physical processes that must be analyzed in a risk study that includes the estimation of accident consequences, the degree to which these processes are understood, unresolved issues, and available methods of analysis. Because of the state of development of core-melt analysis, the procedures provide for considerable flexibility in the selection of models. The need for sensitivity studies is emphasized.

Although this chapter provides guidance for the analysis of physical processes, the procedures described here are not as prescriptive as those in some other chapters of the guide. It is the intent of this guide to reflect commonly accepted practice, not to develop new procedures. The state of the art in this particular area is advancing rapidly.

The analyst should recognize that experience in the analysis of core-melt accidents is very limited and that improvements in methods can be expected over the next few years. Very few risk analyses that have been performed to date have attempted a complete analysis of consequences. The principal example of consequence analysis in a risk study is the Reactor Safety Study (USNRC, 1975). At the time of the Study, however, the methods available for analyzing the physical processes of core-melt accidents were primitive. Considerable experimentation and model development have occurred since the Reactor Safety Study, but the methods of analysis are for the most part not validated. There has also been very little experience in the use of these computer codes in risk analyses. The most complete treatment of the physical processes of reactor accidents in a recent PRA has been the Zion study (Commonwealth Edison Company, 1981).

The procedures described in this guide for the analysis of physical processes are limited to core-melt accidents. Two questions are frequently asked about such accidents: "If these accidents are expected to be very unlikely, why is there so much emphasis on their analysis?" and "Should not primary emphasis be placed on understanding the consequences of accidents that are more likely to occur?" The results of the Reactor Safety Study have indicated that the consequences of core-melt accidents are potentially so much greater than those of more likely accidents that the contribution from these accidents dominates the predicted risk to the public (Hall et al., 1979). It cannot be assumed, however, that the relative risk from core-melt accidents will exceed the risk from less severe accidents for all plant designs. Although methods for analyzing degraded-cooling sequences

that are arrested before a complete meltdown of the core are not addressed in this chapter, the treatment of such sequences is not precluded by the guide.

This chapter discusses a number of physical processes that must be evaluated in a risk study of core-melt accidents. The computer codes that are available for performing these analyses are also described. The analyst should recognize that these models are continually being upgraded and that other models are being developed by ongoing research. Because of these rapid developments in modeling, this guide does not recommend the use of any specific set of computer codes.

7.2 OVERVIEW

Figure 7-1 shows the tasks involved in analyzing the physical processes of severe core-damage accidents. As described in Section 7.10, the activities performed in each of these tasks can differ with the intended application of the PRA.

The first two tasks are concerned with the collection of data and the modeling of the plant for analysis. They require a good understanding of the plant, which can be obtained through close cooperation with the utility and through plant visits. Also necessary is interaction with the system analysts who are defining the success and failure criteria for safety systems. Frequently, analyses will be required to determine which plant conditions or accident sequences result in core melt. Modeling of the plant cannot be completed until after the methods of analysis and the specific sequences for analysis have been selected. In the third task, potential failure mechanisms for the containment and levels of failure are investigated in preparation for the construction of the containment event tree. The potential failure mechanisms must also be recognized before the methods of analysis are selected.

The accident sequences provided to the analyst of physical processes for analysis are the output of the system event trees. To reduce the number of sequences that must be analyzed, these sequences can be grouped into plant-damage states or bins. Alternatively, the selection of accident sequences for analysis can be based on their likelihoods. In the binning process, sequences are grouped according to accident characteristics that affect the response of the containment and the release of radionuclides into the environment. The development of bins and the development of the containment event tree are therefore very closely related. The representative sequences are then analyzed with the core-melt codes, and the results (accident timing, temperatures, flows, pressures, and rate of leakage from containment) are supplied to the radionuclide-transport task. Conditions associated with the leakage from containment are also provided to the environmental transport and consequence analysts. Sensitivity studies are performed as required to quantify event-tree branching probabilities and to estimate the contribution of uncertainties in physical processes to the uncertainties in the total risk.

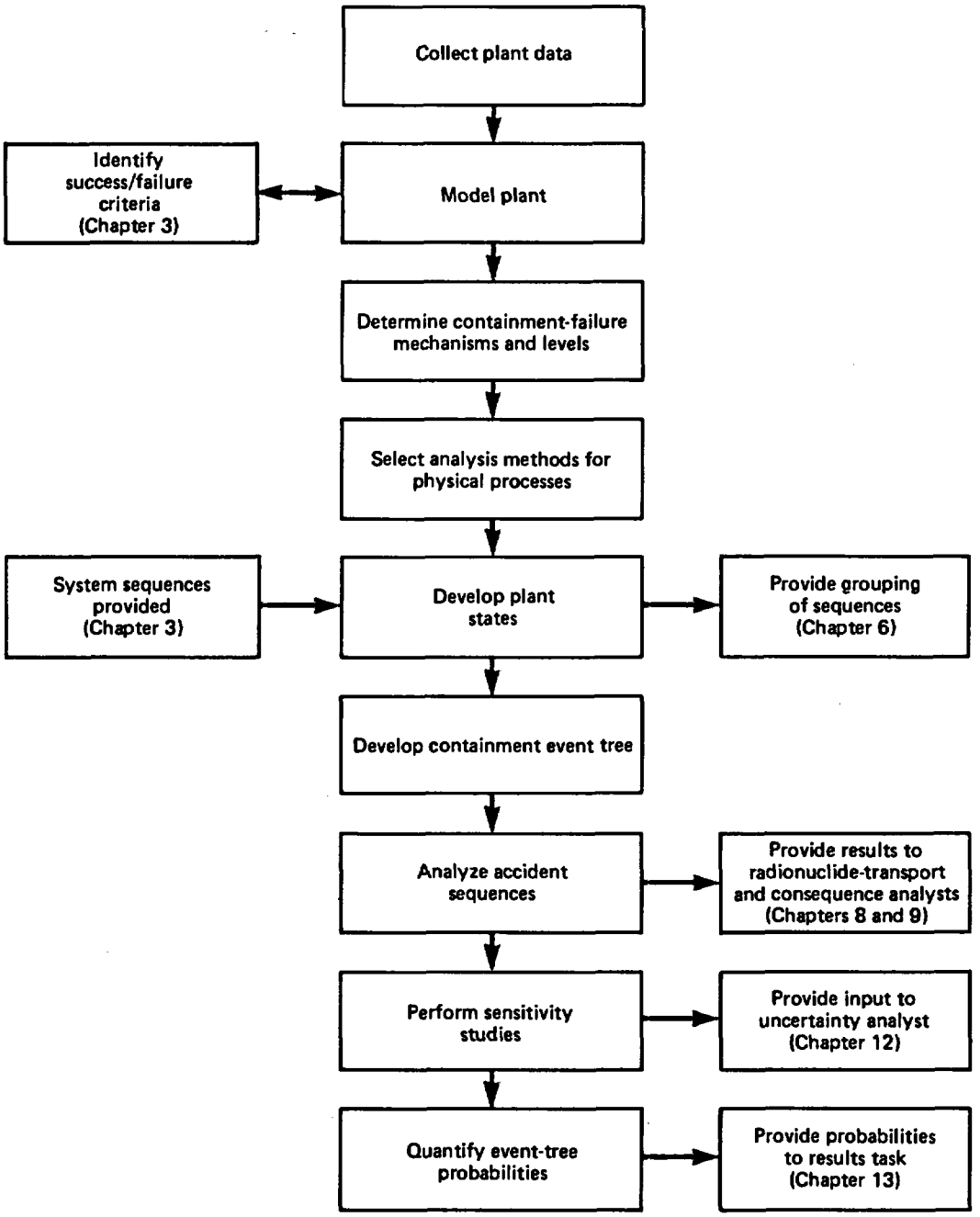


Figure 7-1. Activities diagram for the analysis of physical processes.

Figure 7-1 does not show the iterative nature of the effort. The analysis of accident sequences, for example, may lead to the need to modify assumed containment-failure mechanisms and the containment event tree. Sensitivity studies may also indicate the need for different methods of analysis. If sequence bins are not used, some iteration will be required with the system analysts to ensure that a sufficient number of accident sequences has been analyzed.

7.3 PHYSICAL PROCESSES OF CORE-MELT ACCIDENTS

Many of the physical processes of core-melt accidents are analyzed by the core-melt system codes, which integrate them with other processes. Because research into core-melt processes is limited and the computer codes have not been validated in some areas, the computer codes cannot be used routinely without understanding the limitations of the models and thoroughly understanding the physical processes involved in the progression of a core-melt sequence inside the containment. This section briefly reviews the physical processes and examines the status of current knowledge about the underlying phenomena.

7.3.1 IN-VESSEL BEHAVIOR

The core-melt sequences that are analyzed in PRAs typically involve an imbalance between the power level in the fuel and the availability of cooling water. In these sequences the inventory of water in the reactor-coolant system boils away and the fuel becomes uncovered, heats up, and melts. As already mentioned, degraded-cooling sequences (in which inoperative safety systems are restored in time to arrest the progress of core damage before the reactor vessel is penetrated) have not been analyzed in detail in PRAs in the past. The discussion that follows pertains primarily to accidents postulated to result in complete fuel melting. However, some modeling work that is in progress could be useful in determining the limits of degraded-core coolability (BMFT, 1980; Allison et al., 1981).

7.3.1.1 Pressurized-Water Reactors

The core of a PWR is characterized by an open array of Zircaloy-clad fuel rods. The fuel assemblies rest on a core-support plate that is suspended from the reactor vessel by the core barrel. Tubes containing neutron-absorber material fit into open spaces in each assembly of fuel pins (square arrays of 14 to 17 lattice positions) and are inserted as a cluster from above the core.

As the water level drops in the core region, the exposed fuel heats up. Phenomena affecting the rate of heating are the decay-heat level, fission power level in cases of failure to scram, zirconium oxidation at high temperatures, convective heat transfer to steam and hydrogen, radiative heat transfer to steam, and radiative heat transfer to structures. As the fuel heats, cladding swelling and rupture would occur. The extent of swelling and the failure temperature depend on the heating rate and reactor-coolant-system pressure. At sufficiently high temperatures (approximately 1900°C) the interaction between unoxidized zirconium and uranium dioxide at the cladding interface would result in the formation of a liquid phase (Hagen and Malauschek, 1979). A further rise in temperature could result in an expansion of the molten eutectic region and the melting of the zirconium, zirconium oxide, and uranium dioxide (Peehs et al., 1979). Molten material

would slump and resolidify in lower portions of the core, and some degree of flow blockage in the channels would occur.

Similarly, control rods would be heated by radiation transport and radiative heat absorption. For silver-indium-cadmium control rods in particular, melting might occur early in the core-melt accident and possibly influence the distribution of flow through the core.

A molten zone is expected to grow and progress downward, following the receding water level. The next major phase of the accident begins when the molten fuel leaves the original core region to enter the lower plenum. A variety of modes of fuel relocation can be postulated. Small portions of the fuel could conceivably fall out of the core region and into the lower plenum as they become molten. Or fuel relocation could take place on a larger scale but still progressively as portions of the core-support plate heat up and weaken sufficiently to release the fuel above it. Grid plates below the core-support plate might also impede the progress of the molten material entering the lower plenum. A massive relocation of molten fuel could take place when a portion of the support structure fails, with the molten fuel subsequently pouring into the lower plenum. Alternatively, the molten core material might progress radially outward, overheat the core barrel, and drain into the lower plenum.

When the molten fuel in the lower plenum comes into contact with the water, an interaction will occur, dispersing the fuel and generating steam. Under some conditions, a particularly energetic reaction, referred to as a "steam explosion," could occur with the potential to threaten containment integrity. The possibility of steam explosions is discussed in Section 7.3.4. After the molten fuel has drained into the lower plenum, the remaining water is expected to boil away in a comparatively short time. Additional reactions of steam with zirconium or steel could occur during this period, producing more hydrogen and heat. The core debris would then reheat and begin to attack the reactor vessel. Heat from the core debris would be transferred into the walls of the vessel by conduction, and after the fuel has remelted, heat transfer would be enhanced by internal convection. The fraction of the bottom head of the vessel exposed to fuel debris would be heated in this manner. Under the stress loads of the weight of the core and possibly a high internal pressure in the vessel, the bottom head could then yield and fail. In addition to the general attack on the bottom head, a localized attack on the in-core instrumentation tubes that penetrate the vessel would also occur. A failure of the instrumentation tubes would lead to a small available flow area and a more protracted release of core material, followed by steam and hydrogen, into the reactor cavity.

The release of radionuclides and inert aerosols from the fuel depends on the time-temperature history of fuel heatup. Unfortunately, the modeling of the fuel-melting regime in the existing core-melt system codes is not very mechanistic. More-detailed models are therefore being developed to improve predictions of the temperature of the fuel as a function of time after the start of melting (Allison et al., 1981; Tuerk et al., 1980). None of the currently available codes describe the temperatures and rates of flow throughout the reactor-coolant system during core degradation, but improvements are being made in the MARCH code to perform this analysis.

Since many of the processes described above are treated approximately by existing core-melt codes, a number of modeling efforts are under way to treat some of the processes more mechanistically. Examples are the SCDAP code (Allison et al., 1981) being developed by the Nuclear Regulatory Commission, the MAAP code (Fauske and Henry, 1982) being developed by the Industry Degraded Core Rulemaking (IDCOR) Program, and the CORMLT code (Denny, 1982) being developed by the Electric Power Research Institute. Some aspects and uncertainties regarding in-vessel behavior are described in more detail by Rivard et al. (1981) and in the Zion PRA (Commonwealth Edison Company, 1981).

7.3.1.2 Boiling-Water Reactors

In a BWR, the in-vessel behavior of a melting core is expected to differ in some respects from that described for the PWR. The fuel assemblies in a BWR have fewer pins (49 or 63) than those of a PWR and are enclosed in a shroud. The enrichment of uranium in the fuel pins varies with location within a bundle. A cruciform control blade is inserted upward from the lower plenum between a set of four neighboring bundles. Each bundle is supported by the associated control-rod-drive housing.

Because each bundle is enclosed at elevations above the grid plate, coolant flow cannot redistribute between bundles so long as the shrouds remain intact. In addition, water levels can vary among the bundles. Core melting would proceed in a manner quite similar to that described for the PWR except that radiative heat transport to the shroud and neighboring control blades would provide a major heat sink. Cooling of the shroud by core sprays or bypass flow can be effective in cooling fuel within the bundle. As the shrouds and control blades become molten during core melt, communication would be established among the bundles. Since the fuel bundles are individually supported, there is little potential for a "coherent" dumping of the molten fuel into the lower plenum. In addition, the lower plenum is closely packed with an array of housings for the control-rod drives. The progression of the molten core behind a receding water level would proceed in a series of slumping, solidification, and remelting steps; in the lower plenum of a BWR, its behavior might be similar to that expected in the core region.

The housings of the control-rod drives penetrate the bottom head of the reactor vessel. This appears to be the most likely pathway for the release of molten fuel to the cavity beneath the vessel. A gross attack on the vessel head could also lead to the failure of the head.

7.3.2 IN-CONTAINMENT BEHAVIOR

The accident processes that are described in this section begin with the entry of hot core debris into the region beneath the reactor vessel. Included in this discussion is the pressure and temperature response of the containment.

7.3.2.1 Pressurized-Water Reactor: Large Dry Containment

After the reactor vessel has failed, hot and possibly molten core material would drop or be injected under pressure into the reactor cavity. The subsequent behavior would depend on whether water is present in the reactor cavity and on the geometric configuration of the cavity region.

Interactions Between Molten Fuel and Water

The presence of water in the reactor cavity would depend on both the design and the accident sequence. In some sequences, the activation of the accumulators after vessel penetration would introduce water into the cavity. As molten core material interacts with the water, fuel fragmentation, rapid heat transfer, and steam production would ensue. Depending on the rate of steam production, the total quantity of steam produced, and the strength of the containment, the potential for containment failure could exist at this time. Moreover, this interaction of the core debris with water could lead to a dispersal of the debris throughout the containment. This may make the debris more coolable and avert its attack on concrete, but it may also lead to a greater release of radionuclides, rapid heating of the containment atmosphere, etc.

The generation of containment-threatening missiles from a steam explosion does not appear to be a possibility at this stage of the accident. The size of the fuel particles produced in the interaction could, however, have a major effect on the subsequent coolability of the resulting debris bed if the debris remains in the reactor cavity. (See the Zion PRA (Commonwealth Edison Company, 1981) for a more detailed discussion.) If pathways and mechanisms for the release of steam from the cavity and for the refluxing of condensed water back into the cavity exist, it is possible that a coolable debris bed could result (Commonwealth Edison Company, 1981; Lipinsky, 1980). Considerable experimentation and correlation development have been undertaken, particularly in the LMFBR program, in regard to the coolability of debris beds (Baker et al., 1977; Dhir and Catton, 1977; Hardee and Nilson, 1977; Lipinsky, 1980; Rivard, 1978; Squarer et al., 1981). The potential for arresting further core degradation and concrete attack at this stage is important not only because it would remove a possible containment-failure mode (basemat penetration) but also because it could limit the long-term generation of combustible gases once the core debris is cooled.

For some designs, if the reactor vessel is at an elevated pressure at the time of vessel penetration, some of the core debris could be swept out of the cavity to other regions of the containment (Commonwealth Edison Company, 1981). Since this material would be widely distributed, it would probably be cooled without attack on concrete or after limited attack.

Debris-Concrete Interaction

If water is not initially present in the reactor cavity or is boiled away--or if the core-debris bed is not coolable--the hot core material will attack the concrete basemat, not only eroding the concrete but also inducing the generation of hot (including combustible) gases. Experimental

observation and analysis have indicated that the attack on concrete by the hot fuel could go through a number of phases (Muir et al., 1981; Powers and Arellano, 1981; Powers et al., 1977). The initial attack is expected to involve rapid gas generation and vigorous mixing of the molten core material. At first, the oxide phase of the molten material is expected to be at the bottom of the pool if stratification occurs. After a short time, however, the products of concrete decomposition will mix with the oxidic phase, lowering its density. The layers will then invert, leaving the metallic phase on the bottom.

The principal source of radioactive-decay heat will remain in the oxidic phase, but several significant chemical reactions will take place between the products of concrete decomposition and the metallic phase. As steam and carbon dioxide are released from the concrete, they will pass through the metallic phase and be reduced to hydrogen and carbon monoxide. As the heat source decreases with time and is diluted with inert materials, the metallic phase and later the oxidic phase will solidify. The concrete will probably continue to erode, but at a reduced rate. To date, most of the experiments and model development have been concerned with the concrete-attack phase that precedes solidification. Eventually, the concrete basemat might be penetrated, introducing a pathway for the release of radionuclides.

Containment Pressurization

Throughout the accident, steam and noncondensable gases will be released to the containment atmosphere. All large dry PWR containments have spray systems that could act to condense this steam. Of course, for a given sequence, the spray system could be inoperative or ineffective in condensing steam. Many designs also have fan coolers. Regardless of whether these engineered safety features are operable in a given sequence, steam would condense on steel and concrete structures in the containment.

In the early stages of an accident, heat transfer to structures may be controlled by the flux of steam to the walls. Later in the accident, the heat transfer is limited by the conduction of heat within the structure itself. If an adequate means for removing heat from the containment is not available in an accident sequence, the containment will eventually overpressurize and fail.

Some of the conditions and phenomena that must be considered in performing the containment-response analysis for a core-melt accident include the following:

1. Gas composition (steam, oxygen, combustible gases, and inert gases).

2. Coefficients of condensing heat transfer to structures.

3. Temperature profiles in structures.

4. The effects of containment sprays, containment coolers, and suppression systems.

5. Hydrogen combustion.

6. Heat-source redistribution.

7. Flows between compartments.

The output of the containment analyses is required as input to the analysis of radionuclide transport as well as for predicting containment-failure modes. It may therefore be necessary to have a multicompartment capability for the analysis of containment conditions.

Burning of Combustible Gases

The combustible gases generated in a core-melt accident can threaten the integrity of the containment through combustion as a source of heat or flame impingement, through deflagration as a source of elevated temperature and pressure, and through detonation as a source of shock waves. The conditions leading to various modes of combustion for hydrogen are being investigated experimentally by both the industry and the government (USNRC, 1981a; Berman, 1981a,b). Reports on NRC- and EPRI-sponsored workshops provide a good review of the state of the art (Berman, 1981c). Current plants with large dry containments do not have engineered safety features designed to control the rapid rates of hydrogen generation associated with a core-melt accident. Important sources of hydrogen during an accident arise from the oxidation of metals by high-temperature steam, including the Zircaloy cladding, the steel internals, the steel in the lower head of the vessel, and rebar in the concrete basemat. Carbon monoxide and some methane can also be produced by attack on the concrete. Over a longer term, additional sources of hydrogen can arise from radiolysis and corrosion. The combustion of gases in the containment atmosphere may be possible at various stages of the accident. One critical time period follows the meltthrough of the vessel head and the rapid release of hydrogen from the vessel. Rapid steam generation could follow shortly after a deflagration event, superimposing the two sources of pressure.

High concentrations of steam have the effect of suppressing ignition. In a large dry PWR containment, steam inerting is frequently predicted for accident sequences in which containment safety features are inoperative. If the steam concentration is reduced in such an accident sequence--for example, by the delayed actuation of air coolers--the conditions in the containment atmosphere could rapidly move into a highly combustible range (USNRC, 1981b).

7.3.2.2 Pressurized-Water Reactor: Ice-Condenser Containment

Because of the arrangement of the reactor cavity and the sump, it is unlikely that the cavity would be filled with water at the time of vessel meltthrough. In some sequences, the accumulators would discharge after head failure, releasing water into the cavity. In general, however, conditions in the cavity and the subsequent attack on the concrete would be expected to be similar to the dry-cavity scenario discussed in the preceding section.

The features of the ice-condenser containment that particularly affect its response to core-melt conditions are the ice bed and the low design pressure. As long as it remains, the ice is expected to effectively condense steam even in those sequences where electric power is not available. Because of the small pressure-volume capacity, however, the production of noncondensable gases could eventually cause containment failure even with no significant partial pressure of steam. The low design pressure also makes the containment susceptible to failure in a hydrogen-burning event. For example, if a stoichiometric mixture of hydrogen and air burns rapidly in the containment, the resulting pressure rise will be approximately 150 psi, more than enough to fail the containment. In the future, all ice-condenser designs will have mitigation features that are intended to prevent the accumulation of hazardous levels of hydrogen.

7.3.2.3 Boiling-Water Reactor

There are some differences between the in-containment behavior postulated for core-melt accidents in PWRs and BWRs. Except for the physical layout of the drywell and the suppression pool, the design characteristics of the Mark I and Mark II BWR containments are quite similar. Both have small volumes and are therefore susceptible to failure through overpressure due to the generation of noncondensable gases. Since both are operated with inerted atmospheres, hydrogen burning is not possible except for unlikely circumstances involving a failure of the inerting function.

During the period of time preceding bottom-head failure, steam and hydrogen will be released to the drywell or directly to the suppression pool. If the blowdown from the reactor-coolant system flows into the drywell, the pressure in the drywell will increase to the point at which the vent lines to the suppression pool are cleared, and flow will be established from the drywell into the suppression pool.

After the vessel has failed, molten fuel will enter the cavity. The presence of water in the reactor cavity at the time of vessel meltthrough will depend on the accident sequence. In a LOCA, water is expected to be present in the cavity. In a transient sequence, however, RCS blowdown would be directed to the suppression pool and no water would be present in the cavity, except for cases where the suppression pool is overheated and steam may be condensed in the drywell. Because of the small containment volume, a steam explosion in the reactor cavity, rapid RCS blowdown, or the sweep-out of the fuel from the reactor cavity could threaten the integrity of the containment.

The progress of the molten-core attack on the basemat will be similar to that of the scenario described for the PWR. For the Mark II design, penetration of the concrete pad would be followed by entry into the suppression pool, fragmentation, rapid steam production, and possibly a cooled debris bed. The high temperatures produced in the drywell during the core attack on concrete could affect the integrity of the penetration seals.

Although the volume of the Mark III containment is larger than that of the earlier designs, the design pressure is lower. Thus, noncondensable-gas

generation and hydrogen combustion are potential causes of containment failure. In the future, all Mark III designs will have some type of safety feature for hydrogen control to prevent conditions that could result in deflagration (USNRC, 1981c).

Because of the small size of the drywell, very high temperatures could be produced during the period of concrete attack. Since the outer containment region surrounds the drywell in the Mark III design, leakage from the drywell would not be as critical as it would be for the other designs.

7.3.3 MECHANISMS LEADING TO CONTAINMENT FAILURE

The reactor containment building is a very effective safety feature. If it remains intact, the offsite consequences of the accident will be minor. Conversely, if the containment fails at about the time of core meltdown, current methods of analysis predict major consequences (USNRC, 1981d). For this reason, a risk estimate can be very sensitive to the treatment of containment-failure modes. Table 7-1 lists the mechanisms that might lead to containment failure in a core-melt accident. The mechanisms that are typically considered in risk studies are identified.

The manner and the location of containment failure can be very important. If the size of the breach is small, more time will be available for retention mechanisms to be effective before radioactive material leaks to the environment. Radionuclides may also be retained along the path of leakage. The location of failure can have a particularly large effect on the predicted consequences of accidents in pressure-suppression containments. A location that involves bypassing the pressure-suppression device could involve substantially larger releases to the environment. The elevation of release and the energy content of the gases leaving the containment also affect the offsite consequences.

Table 7-1. Potential containment-failure modes and mechanisms

Direct bypass[a]	Core-concrete interaction
Failure to isolate[a]	Basemat penetration[a]
Vapor explosions	Structural failure and tearout of penetrations
Blast	Blowdown forces
Missile generation[a]	Pipe whip
Quasi-static pressure rise[a]	Vessel thrust forces
Overpressurization	Pressure-vessel burst
Steam[a]	Missile generation
Noncondensable gases[a]	Meltthrough
Combustion processes (hydrogen, carbon monoxide, methane)	Direct contact of containment liner with fuel debris
Blast	
Missile generation	
Quasi-static pressure rise[a]	

[a]Mechanisms typically analyzed in risk studies.

A number of processes that could result in containment failure such as hydrogen combustion and core-concrete attack were described briefly in this section. Sections 7.3.4 and 7.4 discuss the potential for containment failure from a steam explosion and the containment structural response to overpressurization loads (resulting from steam generation, noncondensable-gas production, and the burning of combustible gases).

Two other failure modes that should be carefully considered are failure to isolate the containment and a direct bypass of the containment. The latter type of sequence was the single largest risk contributor identified for the reference PWR in the Reactor Safety Study (USNRC, 1975).

7.3.4 STEAM-EXPLOSION RESPONSE

One of the potential modes of containment failure considered in the Reactor Safety Study (USNRC, 1975) was a steam explosion in the lower plenum of the reactor vessel, which was postulated to cause a slug impact on the upper head of the vessel and the launching of the head as a missile. Steam explosions could be important risk contributors because of the potentially high consequences, even if their likelihood is low. Experimentation and analysis conducted since the Study have indicated that this scenario is very unlikely (Corradini, 1981). At present, it is not possible to give definitive advice to the analyst as to whether or not steam explosions should be considered in a risk study. There is good evidence that the triggering of steam explosions is suppressed at high system pressures (Corradini, 1981; Henry and Fauske, 1979). Sandia National Laboratories has attempted to refine the probability estimates for steam explosions resulting in containment failure that were presented in the Reactor Safety Study (Corradini and Swenson, 1981).

In considering steam explosions, a number of different effects should be evaluated: the rapid generation of steam, missile production, major vessel motion, and (possibly) shock-wave propagation. Although the primary concern in a steam explosion would be containment failure, the possibility of a steam explosion changing the course of an accident should also be considered. A steam explosion could result in an early failure of the reactor vessel, the dispersal of fuel, and a greater release of radionuclides from the fuel.

7.4 ANALYSIS OF CONTAINMENT CAPACITY

The integrity of the containment--or, in the event of containment failure, the mode and the time of failure--can have a major influence on the radiological consequences of a core-melt accident. The results of PRAs indicate that, in terms of public risk, the failure mode of greatest concern is containment overpressurization. Such a failure can result from the generation of steam and noncondensable gases or from the burning of combustible gases. This section discusses the response of different containment designs

to internal overpressurization transients.* The discussion is limited to events in which the rate of pressurization is small in comparison with the mechanical-response time of the structure.

7.4.1 CONTAINMENT DESIGNS

The function of the containment is to provide a leaktight barrier against the release of radionuclides to the environment. To perform this function, the containment must contain the pressure resulting from a blowdown of the reactor-coolant system in the event of an accident. In practice, pressure containment is achieved either by providing a sufficient design pressure capacity and containment volume to accommodate the steam released in an RCS blowdown or by using efficient heat sinks (a suppression pool or an ice bed) to remove steam from the containment atmosphere.

Two major types of structural designs are used in the United States: steel containments and concrete containments (Walser, 1980). Steel containments employ welded steel plate to provide both structural strength and a leaktight barrier. A reinforced-concrete building around the steel containment provides biological shielding and protection against external threats. In concrete containments, the structural strength comes from reinforcing bars or prestressing tendons. The concrete provides biological shielding against direct radiation. A thin steel liner is used to form a leaktight barrier against the release of radioactive material.

Steel containment buildings are designed in accordance with the Boiler and Pressure Vessel Code of the American Society of Mechanical Engineers (ASME, 1980), Section III, Division 1, Subsection NE for Class MC components. A number of concrete reactor containments had been constructed in the United States before an ASME Code committee was formed; these were designed and constructed in accordance with variations of the ACI codes. The current code is ASME Code Section III, Division 2 (ASME, 1980).

The codes embody certain safety factors in the relationships between the allowable working stresses and limiting-stress levels, such as yielding or ultimate failure. The specific safety factors vary with the nature of the loadings as well as with the applicable portions of the Code; for example, the safety factors for primary membrane stresses are different from those for secondary stresses. The design of containment structures must also take into account a variety of load combinations, internal as well as external, normal as well as those induced by accidents. Thus, for any containment structure it is not easy to determine the available safety margins between design loadings and those at which the structure can be expected to fail.

---

*It may be necessary to also consider the response of the containment to external events (airplane impacts, tornadoes, or earthquakes--see Chapters 10 and 11), internal missiles, and hydrogen-detonation loads.

7.4.1.1 PWR Containment Designs

Most of the PWR designs in the United States are of the large dry type. These typically have large free volumes (~2 x 10^6 ft^3) and high design pressures (~30 to 45 psi for steel containments and ~45 to 60 psi for concrete).

The earliest steel containments were spherical. This design option was chosen for West German PWRs and is again becoming popular in the United States. A number of PWRs have cylindrical steel containments with elliptical bottoms and hemispherical heads. Many recent plants have used a hybrid design: a cylindrical steel containment supported by a steel-lined reinforced-concrete basemat.

The concrete PWR containment buildings are cylindrical, with a hemispherical or shallow dome and a flat-slab basemat. The first designs used conventionally reinforced concrete. More recently, prestressed-concrete containments have been constructed; these may be partially or fully prestressed.

The other type of PWR containment system uses packed beds of ice to condense the steam released from the reactor-coolant system. Nearly all of these ice-condenser designs have steel containments with typical volumes of 1.2 x 10^6 ft^3 and a design pressure of 12 to 15 psi.

7.4.1.2 BWR Containment Designs

Boiling-water reactors use suppression pools to condense the steam released from the reactor-coolant system in an accident. Three configurations--Mark I, Mark II, and Mark III--have evolved with time. In each configuration, the reactor-coolant system is located inside a drywell. In the event of an accident involving a break in the reactor-coolant system, steam would be released into the drywell and would flow into the suppression pool to be condensed. Noncondensable gases would flow into the vapor region of the wetwell. In other accidents, steam from the reactor-coolant system may be released directly to the suppression pool through safety relief valves.

The Mark I is called the "lightbulb-and-torus design" because the drywell is shaped like a lightbulb. The suppression pool is inside a torus that runs around the drywell at a lower elevation. The Mark I designs are steel structures with volumes of approximately 2.8 x 10^5 ft^3 and design pressures of 60 psi.

The Mark II is often referred to as the "over-and-under" design because the suppression pool is directly beneath the drywell. These reinforced-concrete containments have volumes of about 3 x 10^5 ft^3 and design pressures of 45 to 60 psi.

The most recent design variation, the Mark III, is a cylindrical containment that can either be concrete or a hybrid with a steel dome and body and a reinforced-concrete basemat. The suppression pool is in an annulus at the lower periphery of the containment. The vapor space of the wetwell is

much larger than that of the other two pressure-suppression designs and forms an outer containment volume that encloses the drywell. The volume of the containment is approximately 1.7×10^6 ft^3, and the design pressure is about 15 psi.

7.4.2 FAILURE PRESSURES, CRITERIA, AND MODES

7.4.2.1 Failure Criteria

In order to establish the pressure at which a structure will fail, it is necessary to define one or more failure criteria for the structure: a limiting stress, strain, or some other condition (Commonwealth Edison Company, 1981; Murfin, 1980). For idealized structures of well-defined material (e.g., a free-standing spherical steel shell) a failure criterion characterized by limiting stresses or strains would appear reasonable. As the geometry of the structure becomes more complicated (e.g., a cylindrical shell with a hemispherical or dished head and a flat rigid bottom), the definition of a failure criterion becomes more difficult, but may still be based on a limiting stress, strain, or the onset of instability. Real containments are, however, far removed from idealized structures, being characterized by gross as well as local geometrical discontinuities, local reinforcements, changes in wall thickness, and the like. Thus, the definition of failure criteria and the associated failure pressures is far from straightforward.

The problem becomes even more complex in reinforced-concrete containments, whose overall behavior depends on interactions among the reinforcement (or prestressing), the concrete matrix, and the leaktight liner. For small deformations (i.e., response in the linear range) the behavior of the composite structure is quite predictable. As increased loadings take part of such a structure into the plastic regime, a variety of failure modes can occur, and the overall behavior becomes more and more difficult to determine. While the reinforcing or prestressing is the principal strength member, it relies on the concrete matrix for support and the transmission of internal pressure loads; both of the former depend on the integrity of the liner for effective performance of their functions. A failure of any one of the three principal components will result in a functional failure of the structure. Although it is to be expected that a concrete containment will fail when the ultimate strength of the principal load-bearing members is exceeded, it must be recognized that a complex structure can also fail by other mechanisms, such as the tearing of the liner. The definition of a failure criterion for the establishment of a failure pressure should recognize the widely differing stress-strain characteristics of the several components of a concrete containment. Many actual containments consist of a combination of conventional reinforcement and prestressing, thus offering the possibility of different behavior in, and requiring different failure criteria for, the several parts of the total structure.

In order to establish failure criteria, the analyst may need to decide what constitutes a functional containment failure. On the one hand, it may not be sufficient to assume that the ultimate strength of the structure can be reached without any loss of leaktightness; on the other hand, minor

increases in leakage should not be defined as failure. In the Reactor Safety Study (USNRC, 1975) it was observed that containment leak rates of up to 100 vol.% per day would not significantly alter the response of the containment to some key accident sequences. This leak rate would of course depend on the containment design and the accident sequences considered.

7.4.2.2 Mode of Failure

Another difficult problem is the characterization of the mode of containment failure or the size of the hole associated with the failure. The mode of containment failure could be closely related to the failure criterion that is deemed to be appropriate. For example, if the failure criterion is related to the blowout or degradation of some of the penetrations, then the magnitude of the leakage can be defined reasonably well. If the failure criterion is associated with the ultimate strength of the structure, it may be necessary to assume a large break.

7.4.2.3 Distribution of Failure Pressures

For the purposes of PRA, a realistic failure pressure is of interest, not the nominal design pressure. Because of uncertainties in the conditions leading to failure, a specific failure pressure cannot be determined. For example, it should not be assumed that the gross ultimate strength of the structure can be reached without the prior loss of function. What is needed for a PRA is a density function describing the probability of failure as a function of loading (pressure) (USNRC, 1975). The shape of such a density function will vary with the containment design, level of analysis, and knowledge of the details of the actual containment. Among the variables that should be considered in assessing the uncertainty in the failure pressure are the validity of the selected failure criterion, the accuracy of the computational methods, the possibility of construction faults, and variations in material properties.

7.4.2.4 Analysis

Containments can generally be characterized as axisymmetric thin-shell structures. Thus, structural analyses at loadings close to design levels are relatively straightforward, and a wide variety of applicable analytical tools are available, ranging from hand calculations to detailed finite-element computer codes. At the high loadings where a structural failure of the containment can reasonably be expected (i.e., after the yielding of the principal load-bearing members) large deformations will typically be encountered, and simple analytical approaches or even many of the detailed design codes may no longer be applicable. While there are a number of sophisticated codes for elastic-plastic structural analysis that are capable of treating large deformations in complex structures (Commonwealth Edison Company, 1981; Murfin, 1980; Murray et al., 1979), these are generally not used by utility or architect-engineer firms in the design of plants.

There is little experimental data on which to base the predictions of the failure levels of containment structures. In the past, some work was done on the explosion-containment potential of steel structures; this is of little interest in the present context. A considerable number of scale-model experiments have been conducted for the prestressed-concrete pressure vessels of gas-cooled reactors; these, however, have been thick-walled structures with again limited applicability to the present problem. There have been only a few experiments in which scale-model containments have been tested to failure under the conditions of interest here (Aoyagi et al., 1979; Atchison et al., 1979; Donten et al., 1979; Rav, 1975). An experimental program (Von Riesemann et al., 1981) that has been initiated at Sandia National Laboratories should provide data that can be used in validating analytical models of containment response at loadings to failure.

The degree of effort and/or sophistication that should enter into the development of a failure pressure may vary with the scope of a particular PRA as well as the nature of the accident sequences that are found to be important. For example, for the class of accident sequences characterized by a loss of containment-heat removal, the pressure in the containment will, in the absence of recovery, increase monotonically to many times the design level, and failure may be a virtual certainty. If such sequences are found to be significant contributors to the risk profile for a particular design, it may be more meaningful to analyze the probability of recovering heat removal as a function of time than to try to pinpoint the failure level of the structure. As another example, the occurrence of large rapid hydrogen burns in certain types of containment can lead to pressures many times the design level. Here again, precise knowledge of the failure level would not be very important.

Analyses of core-melt accidents in various reactor and containment designs have indicated that pressures several times the design levels could be produced by a variety of mechanisms. At such pressure levels, the possibility of failure must clearly be considered. The degree of confidence to which a failure pressure or a failure criterion must be known must inevitably be related to the degree of reliance that is placed in the integrity of the structure at such extreme load conditions. At a minimum, analyses should be conducted to define the simple yield and ultimate-strength levels for the base structure. It should be possible to determine the former quite reliably with even a simplified analysis (Walser, 1980). While the ultimate strength of a thin-shell structure can also be determined quite simply, the validity of the results could be quite suspect since a simplified analysis would not account for nonlinear effects associated with large plastic strains and for interactions among the various components of a complex structure.

In addition to considering the gross behavior of the structure, special consideration should be given to localized conditions, such as the following:

1. Penetrations, including electrical penetrations and major openings (e.g., equipment and personnel hatches).

2. Major discontinuities, such as the transitions from the cylindrical shell to the top head and the basemat.

3. Layout and anchorage of the reinforcement.

4. Liner walls and anchoring.

5. Interactions with surrounding structures at large deformations.

While all of the above areas are considered in the design process, such considerations are limited to a well-defined envelope and may not be applicable far outside the normal region of consideration--for example, in situations involving large plastic strains.

In the analyses, actual property data should be used, where available, rather than general material specifications. In baselining the analysis, advantage may be taken of actual test data on the structure. For example, load-versus-deflection curves obtained during the strength testing could be compared against the analytical predictions, as could the concrete-cracking patterns that may be observed. The extent to which actual data can be used will obviously depend on the state of the plant for which the PRA is conducted. Clearly at the conceptual design stage general material specifications would have to be used, whereas for an existing plant actual measurements should be available.

While the internal pressure loading appears to be the principal determinant of potential containment failure, some consideration should be given to the possible effects of accident temperatures on the response of the containment. Temperature effects may be indirect, in that they may influence the strength characteristics of the structural materials, as well as direct: they may lead to the direct degradation of materials like penetration seals. The potential temperature effects on containment response would be expected to vary with the design of the structure; for example, large-volume containment structures may be less sensitive to temperature effects than are smaller structures, such as the BWR drywell, which has a smaller gas volume and heat sink for the superheated gases from a molten core.

7.5 GROUPING OF SEQUENCES

Chapter 3 describes the development of system event trees, whose end points represent plant conditions that can lead to accident sequences. In the preceding chapters these plant conditions were themselves called "accident sequences," but here the term "system sequence" is used; "accident sequence" is reserved for the end points of the containment event tree.* In a typical PRA, the number of system sequences that are identified is very large--much too large for the physical processes of each to be analyzed.

*For a given plant condition, the containment event tree describes the various pathways that the accident might follow, particularly in terms of the physical processes that could lead to containment failure. A discrete pathway corresponds to a unique accident sequence.

Two approaches have been used to treat this problem: probability screening and the development of plant-damage bins. The former was used in the Reactor Safety Study Methodology Applications Program (Carlson et al., 1981). In this approach, a number of system sequences are selected by using point estimates to identify those with the highest frequencies. These are provided to the physical process analysts for evaluation. If the results of the analysis indicate that the spectrum of potential accident consequences is not well represented (e.g., there are no sequences that fall into large release categories), the level of discrimination is reduced and more sequences are analyzed. One problem with this approach is that it does require iteration and some judgment in deciding when the process is complete. It is consistent, however, with an approach to atmospheric dispersion and consequence analysis in which each dominant accident sequence is analyzed rather than grouped into release categories.

In the other approach, which has been used in a number of recent studies, the analyst develops groups of system sequences referred to as "plant-damage bins," "plant-damage states," or "plant event-sequence categories." The categories are identified by the characteristics of the system sequence that affect the release of radionuclides to the environment. All system sequences within a bin are assumed to have the same containment event tree, in that the branching probabilities are the same, and the end points are assigned to the same radionuclide release categories.

A potential problem with binning is that it presupposes a level of knowledge and skill that many analysts may not have. A combination of the two approaches might therefore be used: a variety of sequences are selected for analysis, and the binning is done after a significant number of sequences have been evaluated.

Some of the characteristics that are used to define bins are listed in Table 7-2 for a typical PWR. Other engineered safety features would, of course, be considered for a BWR or an ice-condenser plant. In practice, it is not necessary to consider a bin for each combination of these characteristics. Most bins would be vacant. In the Zion study, the system sequences were grouped into 21 plant-damage states.

Table 7-2. Bin characteristics[a]

Initiating event	Timing of core melt
Small LOCA	Early
Large LOCA	Late
Transients[b]	Performance of engineered containment safety features
Interfacing-systems LOCAs	No sprays or coolers
Vessel rupture	Coolers only
	Sprays only

[a]For a typical large dry PWR containment.
[b]A number of different types may be identified.

The development of bins requires interactions among the analysts involved in the activities described in Chapters 3, 6, 7, 8, and 9. The systems analysts (Chapter 3) provide a description of the initiating events and system faults of interest for the specific plant to the analysts of physical processes (Chapter 7). After some preliminary analysis, the analysts of physical processes identify the system-sequence characteristics that define the bins. This selection must be done cooperatively or in consultation with the analysis of radionuclide transport (Chapter 8) and environmental consequences (Chapter 9) because the ultimate criterion for grouping system sequences into one bin is the pattern of radionuclide release to the environment. The system sequences are then assigned to bins and returned to the quantification task (Chapter 6).

7.6 CONTAINMENT EVENT TREES AND THEIR QUANTIFICATION

By considering the success or failure states of active plant systems, the event trees described in Chapter 3 trace an accident sequence from the initiating event, through the onset of core damage, and to the point where a stable condition with intact fuel is achieved or where the fuel will overheat and proceed to melt. The containment event tree is developed to describe the progression of an accident sequence from the start of core melt to the release of radionuclides after containment failure, with particular emphasis on branch points that can result in containment failure or significantly affect the release of radionuclides.

The final branch points of the containment event tree are referred to as "accident sequences." The activities in performing a probabilistic risk analysis can be conceptually reduced to estimating the absolute frequency and consequences of all the sequences.

7.6.1 DEVELOPMENT OF CONTAINMENT EVENT TREES

Typically, containment event trees follow from the final branch points of system event trees. In the Limerick study (Philadelphia Electric Company, 1981) the concept of a bridge tree was used for special accident sequences in which there was an interaction between containment failure and subsequent core meltdown.

In the Reactor Safety Study (USNRC, 1975), the headings of the containment event tree were events postulated to lead to containment failure. However, it might be appropriate to include in the containment event tree events that significantly change accident consequences without failing the containment. For example, if an accident pathway could result in the formation of a coolable debris bed in the reactor cavity rather than attack on the concrete basemat, the consequences of the accident could be altered even if the modes of containment failure were unaffected.

7.6.1.1 Time and Location of Containment Failure

It might also be appropriate to recognize the potential for a particular type of containment failure or a particular event to occur at different times. Two important examples are steam overpressurization and hydrogen deflagration. In some sequences postulated for large dry PWR containments, the containment can be threatened by a rapid release of steam after the bottom head of the pressure vessel melts through. If the containment survives this steam spike, it may be challenged many hours later by the buildup of steam and noncondensable gases. The potential consequences of the later failure could be much smaller because of the time available for deposition processes to reduce the concentration of radionuclides in the containment atmosphere. Thus, a number of possible failure times should be included in the containment event tree.

Hydrogen combustion is subject to similar uncertainties. As the concentration of hydrogen in the containment increases, there could be a broad time period during which deflagration could occur, depending on the availability of an adequate ignition source. The potential for containment failure and the subsequent release of radionuclides would depend on the time of the ignition. The analyst might therefore decide to include a number of possible times for hydrogen-combustion events in the event tree. The containment event tree should not be expanded unnecessarily, however, because the number of subsequences that must be analyzed increases rapidly.

The location of containment failure can also be an important variable that can appear on the containment event tree. This is particularly true for pressure-suppression containments, in which the effectiveness of the suppression system (pools or ice beds) could be affected by the location of the failure.

7.6.1.2 Special Cases

The analysis may identify special cases that cannot be conveniently fit into the generalized containment event tree. An example is vessel rupture as an initiating event or as the result of a transient. Such an event could lead to missile generation and containment failure. This mechanism would not appear on the event tree for most accident sequences.

Another special case is containment isolation after an accident. This is an operation which would be expected to appear on the system event tree but which corresponds to a preexisting failure of the containment. In the Reactor Safety Study, containment-isolation failure appeared explicitly in the containment event tree. Indeed, for the BWR, several leak sizes as well as two isolation-failure locations were considered because of their possible influence on predicted behavior.

Another option, which keeps the functions of the system event tree and the containment event tree separate and more clearly defined, is to treat containment isolation as a separate case with its own containment event tree.

The interfacing-system LOCA sequence, in which the containment is bypassed before the meltthrough of the reactor vessel, is also a special case that can be assigned its own containment event tree.

It is convenient to set up the containment event tree in a time sequence because this allows logically nonsequential branches to be easily eliminated.

7.6.1.3 Examples of Containment Event Trees

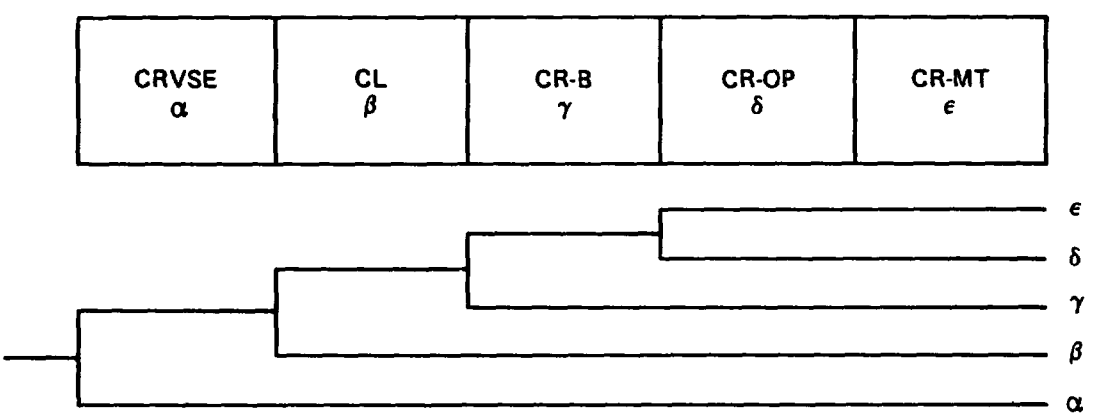
Containment Event Trees for PWRs

Figure 7-2 shows the simple containment event tree that was used in the Reactor Safety Study (USNRC, 1975). In the Zion PRA, a number of additional branch points were considered (Commonwealth Edison Company, 1981). The Zion event tree was first divided into key time periods of interest; for each time period the key binary branching decisions were identified (see Table 7-3). The specific binary decisions will depend on the design of the plant and the use of the PRA. Binary decisions that might be added to those in Table 7-3 are the following:

1. Does an in-vessel steam explosion result in containment failure?

2. Does an out-of-vessel steam explosion result in containment failure?

3. Does pocketing of hydrogen result in hydrogen detonation and subsequent containment failure?



CRVSE	Containment failure from in-vessel steam explosion
CL	Containment isolation failure
CR-B	Containment failure from hydrogen combustion
CR-OP	Containment failure from overpressurization
CR-MT	Containment failure through basemat penetration

Figure 7-2. Example of a containment event tree. From the Reactor Safety Study (USNRC, 1975).

Table 7-3. Typical binary branching decisions for the containment event tree of a large dry PWR containment[a]

EVENTS BEFORE CORE MELT
Is the containment pressure resulting from the initiating transient before any core degradation within the containment pressure limit?
Is sufficient hydrogen generated and released before core melt, and do conditions for the ignition of this hydrogen exist?
Is the containment pressure within the containment pressure limit?
EVENTS RELATED TO IN-VESSEL PHENOMENA
Does the postulated fuel melting progress noncoherently?
Is the pressure generated by the core debris-water interaction inside the reactor vessel within the pressure-boundary failure limits?
Is sufficient hydrogen generated and released before vessel failure, and do conditions for the ignition of this hydrogen exist?
Is the containment pressure within the containment pressure limit?
Do the conditions for in-vessel cooling of the core debris exist?
Is most of the core debris forcibly ejected after vessel failure?
EVENTS RELATED TO OUT-OF-VESSEL PHENOMENA AFTER VESSEL FAILURE
Is water present in the reactor cavity at the time of vessel failure?
Is the basemat perforated immediately after vessel failure?
Do the accumulators discharge, or does water return to the cavity after vessel failure?
Does the containment pressure from steaming alone exceed P_0 = 70 psia in the transient immediately after vessel failure?
Is the containment pressure from steaming alone within the containment pressure limit?
Is sufficient hydrogen available immediately after vessel failure, and do conditions for the ignition of this hydrogen exist?
Is the containment pressure within the containment pressure limit?
EVENTS RELATED TO ULTIMATE CORE DEBRIS DISPOSITION AND COOLABILITY
Does a coolable debris bed form initially?
Does the containment pressure remain within the containment pressure limit?
Is basemat failure prevented?

[a]From the Zion Probabilistic Safety Study (Commonwealth Edison Company, 1981).

Containment Event Trees for BWRs

The form of the containment event tree depends on the design of the plant. The types of nodal questions that define the branch points in a BWR containment event tree will be different from those in a PWR event tree. Table 7-4 lists a number of nodal questions that would be appropriate for a Mark III BWR containment.

Table 7-4. Typical binary branching decisions for the containment event tree of a Mark III BWR containment

Does containment failure precede melting?
Does containment failure result in the disruption of the suppression pool?
Is the suppression pool bypassed?
Does a steam explosion occur during core meltdown?
Does a steam explosion cause containment failure?
Is the hydrogen-control system functional?
Does hydrogen combustion lead to containment failure?
Is there water in the reactor cavity before vessel meltthrough?
Does a steam explosion fail the containment?
Do drywell penetration seals fail because of high temperatures?
Does the suppression pool boil after containment failure?
Does basemat penetration occur?

7.6.2 QUANTIFICATION OF THE CONTAINMENT EVENT TREE

It is not possible to provide detailed guidance on the quantification of the branch points in the containment event tree. Some judgment will be required from the analyst. Since the state of knowledge about many of the key physical processes is changing rapidly, risk analysts will have to follow the results of research closely to remain abreast of developments.

The meaning of branching probabilities is frequently treated with some ambiguity. Because of the uncertainties in the prediction of physical processes, it is sometimes not possible to state with complete confidence which pathway an accident sequence will take. The branching probability in this sense represents a lack of knowledge about the physical processes that are involved.

In the real world one of the branches would be followed for all similar sequences. However, because of our inability to model the process with confidence, we cannot say which path that would be. Thus, we must judge the likelihood of each path being the correct one.

A branch point can also be attributed to variability in accident processes. For example, a specified composition of hydrogen and air may be within flammability limits, but, for burning to occur, an adequate ignition source must be present as well. The availability of ignition sources for practical purposes can be considered as a random process. Thus, in some accident sequences burning may occur, while in other, essentially identical sequences, burning would not occur. By grouping accident sequences in very narrow bins, some of the aspects of variability can be minimized.

Each approach that has been taken in assigning probabilities to the branch points of the containment event tree has required some degree of subjectivity. For some events it is possible to develop a prescription that can be applied to the results of analyses to determine the branch-point probabilities directly. In this approach the judgment enters in the development of the formulas for estimating the probabilities. For other events the analyst may not have sufficient information to do more than make a purely subjective judgment of branching probability. Some examples for various containment-failure modes are given in Sections 7.6.2.1, 7.6.2.2, and 7.6.2.3.

Another type of condition that can be encountered within the containment event tree is one in which the analyst has a high degree of confidence in the outcome, but recognizes a residual probability that he could be wrong. In this case, a small probability (e.g., 1×10^{-2} to 1×10^{-4}) may be assigned to the alternative branch point to ensure that this potential is recognized. This approach was used in the treatment of debris-bed coolability in the Zion study (Commonwealth Edison Company, 1981).

7.6.2.1 Overpressurization Failures

One of the most important types of containment failure involves overpressurization caused by the generation of steam (rapid or steady), the production of noncondensable gases, or the burning of hydrogen. The pressure level at which the containment would fail can be calculated (as discussed in Section 7.4), but only within some range of uncertainty; the same is true of the pressure history within the containment. In a prescriptive approach to determining failure probability for a specific accident sequence, the analyst develops a curve that shows the probability of failure as a function of containment pressure. Some judgment is required in developing this curve, but there are some points that can be determined easily. For example, at the design pressure, the probability of containment failure is near zero because the containment has been tested at this pressure; at the ultimate strength of the structure, the probability of failure must be unity.

In defining the rest of the curve, the analyst should consider the natural variability in material properties, uncertainties in analyzing the failure level for the structure, and the possibility of construction

defects. For a given sequence, the estimated probability of failure is the integral of the overlap of the peak pressure with its uncertainty distribution and the failure pressure with its uncertainty distribution. The approaches taken in the Reactor Safety Study (USNRC, 1975) and the Zion PRA (Commonwealth Edison Company, 1981) basically followed this type of procedure.

If the burning of hydrogen is involved in the particular containment overpressure failure, it might be appropriate to include a conditional probability of hydrogen combustion in the predicted failure probability. For the treatment of hydrogen combustion, it is possible to develop a prescriptive approach that is analogous to that described for overpressure failure. The conditions resulting in combustion (e.g., a flame-temperature criterion or a region on a ternary air-steam-hydrogen diagram) can be described with uncertainties. If the conditions predicted by the calculational method with their uncertainties overlap the conditions required for combustion, a probability of combustion can be estimated.

7.6.2.2 Steam-Explosion Failures

In the Reactor Safety Study, the probability of a steam explosion that would fail the containment was estimated by dividing the overall probability into three components: the probability of a coherent drop of a large mass of molten fuel into water, the probability of a steam explosion, and the likelihood that, given a steam explosion, the containment would fail. Each probability was determined subjectively but was based on a number of auxiliary calculations and a review of known steam-explosion mechanisms.

Recently, a more-detailed approach to estimating the probability of containment failure was undertaken for a PWR and a BWR (Corradini, 1981), using the results of experimental work performed since the Reactor Safety Study. In this work, the conditional probabilities of events that would result in containment failure were characterized as density functions and the overall probabilities were estimated by a Monte Carlo propagation.

7.6.2.3 Basemat Penetration

Although considerable research has been performed, major uncertainties remain in modeling the long-term behavior. In assigning a probability for this failure mode, the analyst must exercise considerable subjective judgment. In the Reactor Safety Study, it was assumed that basemat penetration was a certainty; the question that was considered was whether penetration would precede and prevent overpressure failure by releasing the gases in the containment into the ground. On the basis of parametric analyses, an uncertainty band (assumed Gaussian) was established around the time of basemat penetration. The time calculated for overpressure failure was then compared with this band to estimate the probability that penetration will precede containment failure through overpressure.

7.7 AVAILABLE METHODS OF ANALYSIS

The subsequent discussion of computer codes used in analyzing the physical processes of core-melt accidents covers only the codes that are publicly available. There is no intent to suggest that proprietary codes should not be used in PRAs. However, if proprietary codes are used, some documentation of the models will be required in the PRA, and it would be preferable to show how the results of the proprietary code compare with those of publicly available codes or with experiment.

The descriptions that follow are quite general. Furthermore, no attempt is made to list their limitations, because changes in the codes are being made so quickly that such a listing would be out of date by the time this guide is published. Some comparisons of code capabilities have been presented by other authors (see, for example, Rivard et al., 1981, Tables 5-II through 5-V).

The codes used in the analysis of physical processes are divided into three categories, according to their function: thermal-hydraulics, core melt, and core-concrete interactions. As shown in Table 7-5, they are available from the National Energy Software Center at the Argonne National Laboratory or the EPRI Software Center. Also discussed briefly are some of the codes that are used to analyze the structural response of the containment. These codes are not included in Table 7-5 because a great many codes with similar capabilities are available.

Table 7-5. Computer codes used in the analysis of physical processes

Code	Type	Source	Reference
RELAP5	System thermal-hydraulics transient	National Energy Software Center	Ransom et al. (1980)
RETRAN	System thermal-hydraulics transient	EPRI Software Center	Moore et al. (1978)
TRAC	System thermal-hydraulics transient	National Energy Software Center	Los Alamos National Laboratory (1981)
MARCH 1.1	Core-melt system code	National Energy Software Center	Wooton and Avci (1980)
RACAP	Core-melt system code	EPRI Software Center	Electric Power Research Institute (1981)
KESS	Core-melt system code	EPRI Software Center	Gulden et al. (1980)
CORCON-MOD1	Core-concrete interactions	National Energy Software Center	Muir et al. (1981)

7.7.1 CODES FOR ANALYZING THE THERMAL-HYDRAULICS OF TRANSIENTS AND LOCAS

The core-melt codes treat the initial phase of a core-melt accident simplistically, either by inputting tables of mass and enthalpy leak rates or by using a single-control-volume approximation. To provide assurance that the timing of core uncovering is not in significant error, it is advisable to analyze the early time period with a system thermal-hydraulics code like RETRAN (Moore et al., 1978), RELAP (Ransom et al., 1980), or TRAC (Los Alamos National Laboratory, 1981). The results of these analyses can be used as input to, or for the initialization of, the core-melt system codes, or they can be used to adjust parameters in the core-melt code.

Of the codes that are generally available for analyzing this phase of the accident, RETRAN has the most detailed treatment of the secondary and control systems. Some validation of the code has been made against mild plant transients. RELAP and TRAC are quite similar to RETRAN, however, in terms of the basic approach, strengths, and limitations. They all require a significant amount of computer time to analyze a typical transient or small-break LOCA. A sizable reduction in computation time has, however, been achieved with RELAP5, the newest version of the code.

7.7.2 CORE-MELT SYSTEM CODES

There are three core-melt system codes that are potentially available for use in performing risk analyses for LWR plants: MARCH, KESS (Gulden et al., 1980), and RACAP (EPRI, 1981). Of these, the MARCH code has been the most widely used and reviewed (Rivard et al., 1981). In addition, the MAAP code (Fauske and Henry, 1982), which is being developed by the Industry Degraded Core Rulemaking Program (IDCOR), should be available in the near future.

This guide does not recommend any one of these codes in preference to another. However, whichever code or method is selected, great care must be taken in its use. None of the codes have been validated against experimental data. Because the codes are in a developmental stage, many versions are in use. This can lead to ambiguity regarding the underlying assumptions of the model. The NRC has established a process for freezing reference versions of MARCH, updating the code, and informing users of identified problems.

This section describes the principal features of each of the core-melt system codes. Because of the developmental status of the codes, the comments made here about the limitations and the capabilities of the codes may become rapidly outdated. Before using one of these codes, the analyst should examine it in depth and should become thoroughly familiar with it. The codes should not be routinely applied without a continuing reevaluation of the applicability of models and assumptions for the conditions under consideration.

7.7.2.1 The MARCH Code

MARCH (Meltdown Accident Response Characteristics--Wooton and Avci, 1980) was written as a follow-on to the Reactor Safety Study. There were three principal objectives in its development:

1. To provide a consistent and integrated treatment of the stages of core melt.

2. To develop the capability to analyze transients and small-pipe-break accidents in addition to large-pipe-break accidents.

3. To develop generalized models capable of analyzing a variety of LWR containment designs.

MARCH was written to be compatible with the input needs of the CORRAL codes, which predict radionuclide transport and deposition inside the containment. Figure 7-3 shows the interfacing between MARCH and CORRAL II.

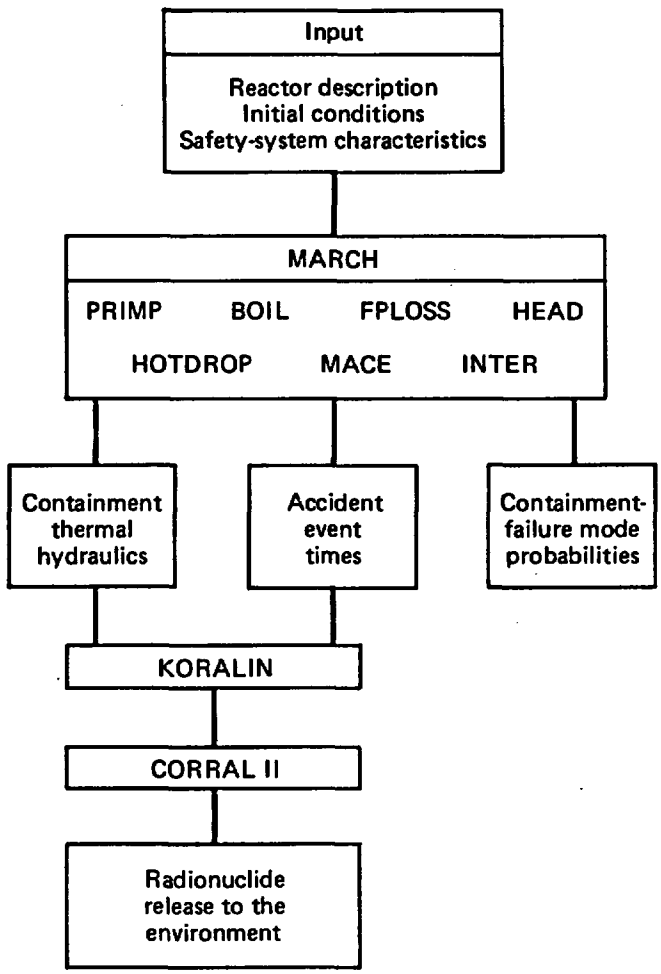


Figure 7-3. Flow diagram for MARCH/CORRAL analyses.

Subroutines in MARCH describe the major physical processes expected in a core-melt accident (see Figure 7-4). The analysis begins with the description of the hydraulic response of the system to the initiating event and proceeds to the uncovering of the core, the heatup of the fuel, the oxidation of the cladding, the liquefaction and slumping of the fuel, the boil-off of water in the lower plenum, attack on the reactor pressure vessel, interactions between the molten fuel and water in the reactor cavity, and attack on concrete. During the stages of core melt, the transient temperature and pressure history of the containment atmosphere is predicted. If the pressure exceeds an input criterion, containment failure is predicted to occur and the subsequent depressurization is analyzed. Hydrogen concentrations in the containment volumes are also followed, and the consequences of hydrogen combustion can be examined.

MARCH predicts the behavior of many complex physical processes. It contains, however, a number of well-recognized deficiencies. An examination of its limitations has been undertaken for the NRC (Rivard et al., 1981). Some limitations in the MARCH models arise from an inadequate supporting-data base. Others could have been corrected by improvements that are within the state of the art, but the necessary funding has not been available.

7.2.2.2 The RACAP Code

The RACAP code package (EPRI, 1981) includes modules for the analysis of the physical processes of core-melt accidents, radionuclide behavior, and offsite consequences. Interactions among the routines are shown in Figure 7-5. The INCOR part of RACAP corresponds to the MARCH code, and some of the INCOR modules are very similar to the subroutines in MARCH. The BOIL routines in MARCH and RACAP are both derivatives of the Reactor Safety Study's BOIL code. The INTER code is the basis for the modeling of core-concrete interactions in both code packages.

To predict the containment temperature and pressure transient, RACAP uses the CONTEMPT code. CONTEMPT performs a more rigorous treatment of intercompartment flow than does the MACE routine in the MARCH code. In particular, CONTEMPT can account for pressure differences between interconnected compartments during periods of rapid pressure change. The analysis of reactor-vessel meltthrough also differs from the treatment in MARCH.

7.7.2.3 The KESS Code

The KESS code package (Gulden et al., 1980) was developed in the Federal Republic of Germany. KESS is designed on a modular basis, using an executive-code management approach that allows for a number of modeling options and close coupling between models at some expense in computation time. The two levels of control and data transfer in the executive program are shown in Figure 7-6. The computer codes currently available in the KESS system are shown in Figure 7-7. In general, alternative modules can be

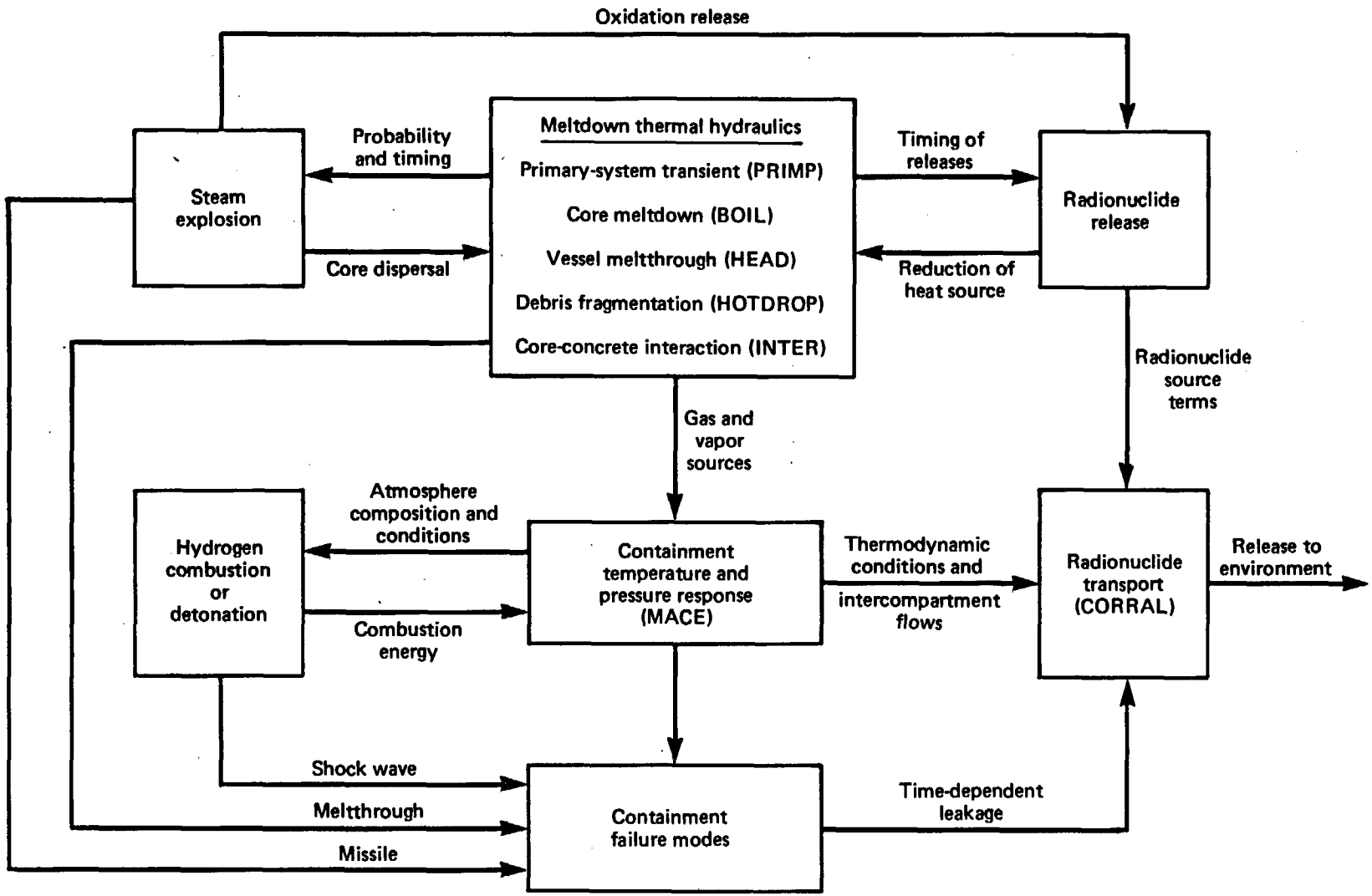


Figure 7-4. Core-melt processes.

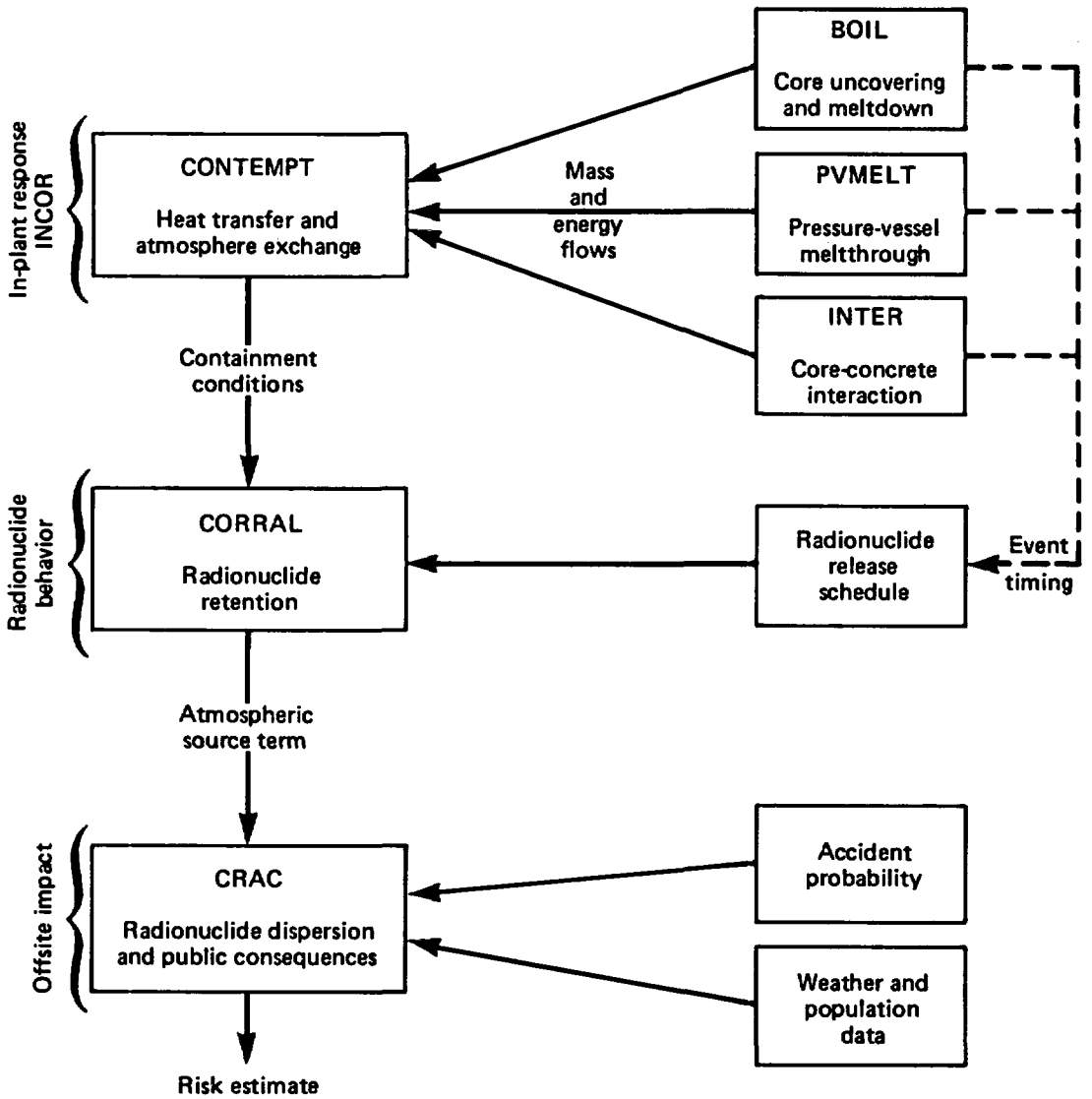


Figure 7-5. The RACAP code network for accident-consequence analysis.

selected for each phase of the accident--a simple model and a more complex model.

Some of the models in KESS are more detailed than the analogous models in MARCH. For example, the MELSIM model is more detailed in the description of fuel slumping than the slumping models in BOIL. Similarly, the RAUHZ module examines heat transfer from a pool in which natural convection is driven by internal heat generation. This mechanism is not considered in the HEAD routine of MARCH. Further experimentation and analysis are required, however, to determine which models are more appropriate under different conditions.

The KESS code has been made available in the United States through information-exchange arrangements with the NRC and EPRI. The currently

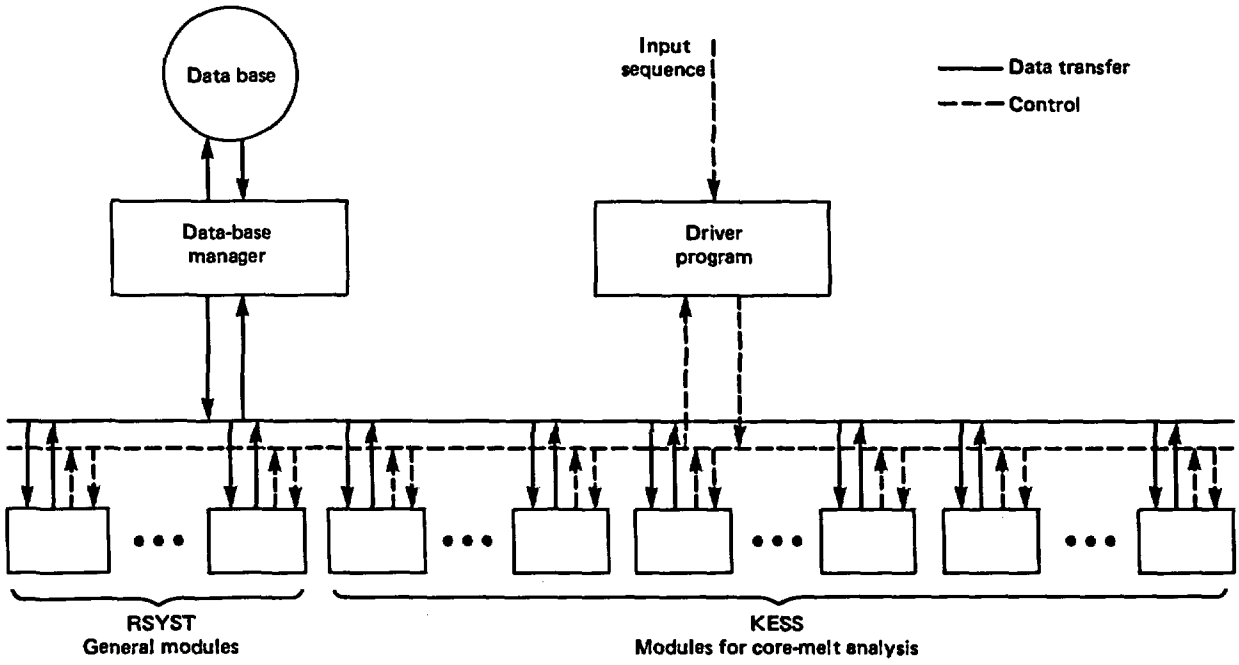


Figure 7-6. Control and data transfer in the KESS executive program.

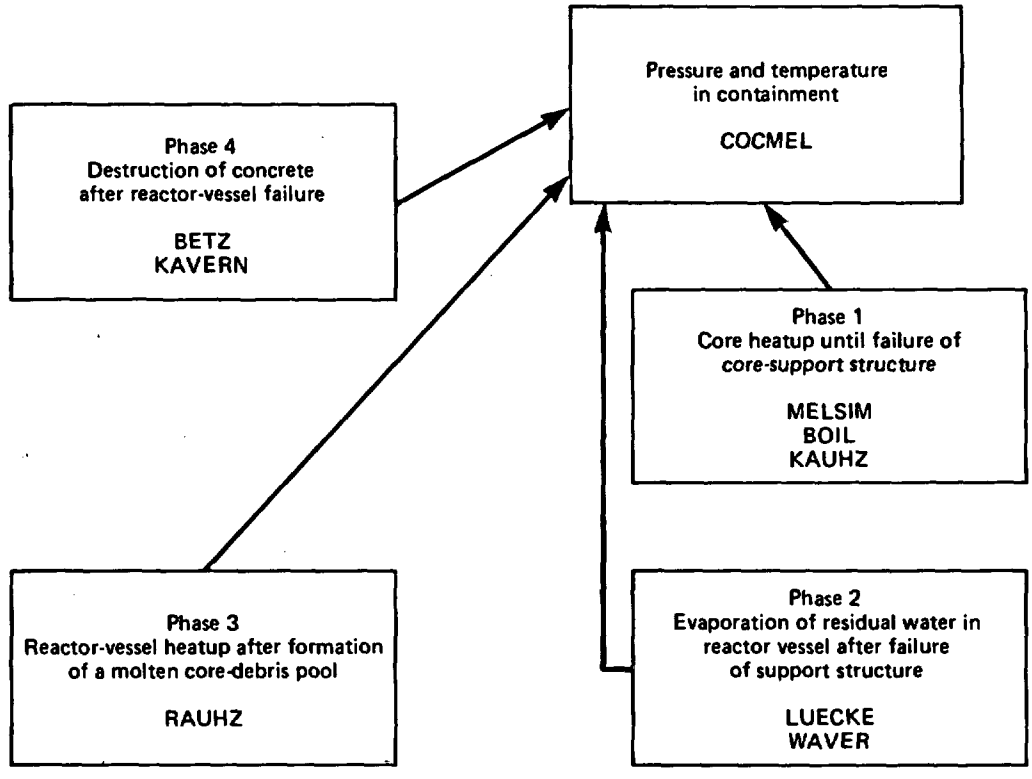


Figure 7-7. Computer codes incorporated into KESS.

available version has some significant limitations for use in risk analyses. This version does not have the capability to analyze transients and small-pipe-break accidents, nor does the containment code have spray, suppression-pool, or ice-condenser models. A number of additional modules are being added to KESS by the German researchers, and updated versions of the routines in KESS should be soon available in the United States.

7.7.2.4 Separate-Effects Codes

The conditions that would lead to a containment failure by overpressurization are well beyond those that are analyzed in the design of the containment. However, a number of computer codes are available for analyzing the behavior of the containment through the range of gross yielding. Among the codes that are generally available are HONDO (Key et al., 1978), ADINA (Bathe, 1978), NASTRAN (MacNeal, 1978), and MARC (Marcal, 1975). Codes of this type normally use finite-element methods and can perform two- or three-dimensional nonlinear analyses for complex materials like concrete. Multipurpose shock-hydrodynamics codes are also available to evaluate the impact on the containment wall of shock waves or missiles that could be generated in a steam explosion or a hydrogen detonation.

The most advanced American code for modeling core-concrete interactions is CORCON (Muir et al., 1981), which has been included in some experimental versions of MARCH. The principal components of the CORCON model are the concrete cavity, the molten pool of core debris, and the gas atmosphere and surroundings above the pool. CORCON considers mass and energy transport and conservation within this system. Analytical models are provided for the pertinent physical phenomena and chemical interactions, including heat transfer, the ablation of concrete and changes in the shape of the reactor cavity, heat transfer inside the molten pool and from the surface of the pool to the atmosphere and the surroundings, chemical reactions between the molten pool and gases, and decay-heat generation in the molten pool. The MOD1 version is applicable only to the high-temperature phase of core-concrete interactions, when the core debris is hot enough to be entirely liquid and to erode the concrete at a relatively rapid rate.

7.7.2.5 Codes Under Development

Three computer codes that are currently under development will examine specific aspects of core-melt processes. These codes are SCDAP, CONTAIN, and HECTR. The SCDAP code (Allison et al., 1981) was developed at the Idaho National Engineering Laboratory to model fuel behavior during core heatup and melting inside the reactor pressure vessel. It is being validated by comparison with the results of the NRC's experimental program on severe fuel damage.

CONTAIN (Senglaub et al., 1981) will analyze containment processes in severe accidents in either light-water reactors or liquid-metal fast breeders. The analysis couples radionuclide transport with the thermal-hydraulic behavior. The objective of this code, which is being developed at Sandia National Laboratories, is to provide detailed mechanistic models for containment processes--models that can be used as a benchmark for other codes.

The HECTR code (Berman, 1981a) is being developed at Sandia National Laboratories in close conjunction with the NRC research program on hydrogen behavior. It will treat the combustion of hydrogen in a more mechanistic manner than do the models in existing core-melt system codes.

7.8 UNCERTAINTY ANALYSIS

7.8.1 SOURCES OF UNCERTAINTY

Uncertainties in the analysis of the physical processes of core-melt sequences enter into the results of a probabilistic risk assessment in two ways. First, the uncertainties affect the estimates of the frequencies of accident sequences. These uncertainties are therefore reflected as the probabilities of branches in the containment event tree or as distributions on these probabilities. Second, the uncertainties appear as variations in the output variables from the analysis. These variables (e.g., temperatures, compositions, flows) are used as input to the models of radionuclide release and transport in the plant and in the environment. These uncertainties can therefore be propagated through the radionuclide-transport models and be represented as distributions on the radiological consequences of the accident sequences.

Some of the principal modeling uncertainties that affect the predictions of radionuclide release and transport are related to the following:

1. The thermal history of the fuel.
2. Temperature distributions and flows in the reactor-coolant system and the containment.
3. The relative timing of core melt and containment failure.
4. The mode of containment failure.
5. The coolability of core-debris configurations.
6. The generation and combustion of hydrogen.
7. Fuel-coolant interactions.

7.8.2 METHODS OF ANALYSIS

The use of some subjective judgment in assigning uncertainties to accident consequences appears to be unavoidable. For some input parameters, experimental data are available, and from these data distributions can be inferred. Frequently, however, the experimental bases for input variables and models of physical processes are quite limited. Judgment is therefore required in the assignment of uncertainties.

There is some concern that the subjective assignment of uncertainties implies more knowledge about the results of a PRA than actually exists. On the other hand, the estimated uncertainties in the risk provide very important insights even if they only represent the best judgment of the analyst. The effect of assumptions underlying the subjective representation of uncertainties can be determined by performing sensitivity studies. It is therefore recommended that, when a potentially controversial judgment is made regarding the progress of an accident, the effect of the judgment be evaluated by also performing the analysis with a different (possibly more conservative) assumption.

Chapter 8 presents the results of formal uncertainty analyses for the MARCH and CORRAL codes. This type of analysis is useful in determining how uncertainties in the input variables for physical process analysis affect radiological consequences. It can also be used to some extent to evaluate the implications of different models for radiological consequences. Since the analyses are performed within the context of existing models in computer codes, they cannot fully account for all sources of uncertainty. Informed judgment must therefore be used to extend the ranges of uncertainty obtained by formal methods of uncertainty analysis.

7.8.3 AVAILABLE INFORMATION ON UNCERTAINTY AND VARIABILITY

An uncertainty analysis has been performed with the MARCH and CORRAL codes for some specific accident sequences. Some of the results are tabulated in Chapter 8.

7.9 INFORMATION REQUIREMENTS

A large amount of plant design information is needed to analyze the physical processes of core-melt accidents. Since some of the output (compartment temperatures and intercompartment flows) is used as input for the analysis of radionuclide release and transport, the two groups of analysts must agree on the appropriate breakdown of the containment into control volumes.

The initial source of plant data is the final safety analysis report (FSAR). The FSAR will not contain all of the necessary information,

however. Liaison with the utility or the equipment vendor and architect-engineer must be established to obtain detailed plant drawings and specifications. At least one plant tour should also be made at a point midway in the data-acquisition stage to confirm assumptions and answer questions.

Table 7-6 identifies plant data that must be input to a core-melt code. Some analysis is required to convert raw plant data into this form. For the reactor-coolant system, the following information is required: fuel design, core power distribution, masses and quantities of different materials, the design of the upper and lower internals, and the design of the reactor vessel. For the containment it is necessary to know the overall dimensions, air volume, the dimensions and material compositions of heat sinks (noting whether heat sinks are one-sided or two-sided), and interconnections between subregions.

Table 7-6. Plant-data input to core-melt codes

System or component	Parameters included
General containment data	Total volume; number of compartments; volume and dimensions of compartments; initial pressure, temperature, and humidity
Heat sink	Number and compartment location of heat-sink slabs; materials in slab, including density, heat capacity, and thermal conductivity; heat-transfer area, thickness, and heat-transfer coefficient for the liner-concrete interface
Ice condenser (if applicable)	Mass of ice; temperature of ice; temperatures of water drained from ice bed; temperature of gas leaving ice bed
Suppression pool (if applicable)	Mass of water; temperature of water; water volume; air volume
Containment floor (for core-concrete interactions)	Thickness, density, thermal conductivity, temperature, and composition of concrete containment floor
ECC tanks	Pressure, temperature, and water mass of accumulators and/or upper head injection tanks
ECC pumps	Start time, nominal flow rate, nominal and shut-off pressure of all pumps, including high-pressure injection, safety injection, low-head pumps, and any additional pumps; minimum temperature to avoid pump cavitation
ECC heat exchangers	Heat-exchanger capacity; primary and secondary flow rates and temperatures for ECC and containment-spray heat exchangers
Containment coolers (if applicable)	Number and location of coolers; air-flow rate and inlet temperature; secondary flow rate and inlet temperature
Containment sprays	Flow rate, temperature, and spray-drop diameter of containment-spray system

Table 7-6. Plant-data input to core-melt codes (continued)

System or component	Parameters included
Auxiliary feedwater (if applicable)	Flow, temperature, and start time of auxiliary feedwater pumps
Water-supply parameters	Mass of water in condensate-storage tank; mass of water in the refueling-water storage tank (RWST); fractional value of RWST to start recirculation of ECC and containment sprays; minimum sump mass to avoid cavitation
Core	Initial thermal power; total number of lattice positions in core; total number of fuel rods in core; active fuel height; liquid level; mass of UO_2, Zircaloy, and miscellaneous metal; fuel-rod diameter; fuel-pellet diameter; hydraulic diameter; cladding thickness; density, conductivity; and heat capacity of core material; peaking factors
Vessel	Code diameter; flow area; cross-sectional area; mass, heat capacity, temperature, and heat-transfer area of internal structures; mass, diameter, and thickness of bottom head
Reactor-coolant system	Volume; initial primary steam volume; pressure; safety-relief-valve pressure setpoint and rated capacity
Steam generator	Initial mass of water in steam generator; volume of steam generator; setpoint of secondary steam-generator relief valve

Information is also needed about the engineered safety features (ESFs): the number, capacity, requirements for net positive suction head, failure mechanisms, and the temperature of the source water. The analyst must know the logic of ESF operation: What triggers their operation? Are there alternative operating modes? Does more than one system compete for the same source of water? Emergency operating procedures must be reviewed to determine how the operator will interact with the system for a particular accident situation. The analyst must remember that the intent of the analysis is realism. The flow rates and water-source temperatures provided in SARs are frequently conservative. The analyst must also decide what constitutes an operable state for a system. If the emergency core-cooling (ECC) system is operational and two of three pumps must function for success, should the analyst assume that two or three pumps are operating? In the Reactor Safety Study, a minimum safeguards assumption was made. This assumption does not necessarily represent the most likely mode of operation, nor is it necessarily conservative. Emergency operating procedures may provide quidance, but consideration should also be given to sensitivity studies.

7.10 PROCEDURES

The depth at which physical processes should be analyzed in a risk assessment depends on the use of the study. Procedures for two types of analysis are described in this section. The first set of procedures outlines the steps that would be undertaken in a detailed PRA in which an in-depth treatment of accident consequences is performed. For a reliability-oriented risk study, like those conducted in the Interim Reliability Evaluation Program (Mays et al., 1981), a more limited treatment of physical processes is sufficient. The steps in this type of analysis are presented as the second set of procedures. The depths of analysis that are described for the two sets of procedures are actually end points on a spectrum of possibilities. The analyst must decide the appropriate depth of analysis for the specific application. The major tasks are illustrated in Figure 7-1.

7.10.1 DETAILED ANALYSIS OF PHYSICAL PROCESSES

Task 1: Collect Plant Data

1. Review the FSAR. Collect data on system design, ESF operating levels, etc., as required to provide the data listed in Table 7-6.

2. Establish liaison with utility staff, the vendor of the nuclear steam supply system, and the architect-engineer. Obtain plant drawings and operating procedures. Provide a list of missing data (as early as possible).

3. Make one or two plant visits to answer questions and verify assumptions about the plant layout (e.g., connections to the sump, flow paths between compartments).

Task 2: Model Plant

1. Develop plant model to be used in core-melt analyses for each accident sequence (e.g., MARCH analyses). This must be done in cooperation with the radionuclide release and transport task (Chapter 8).

2. Develop models for separate-effects analyses (e.g., containment structure, shock-hydrodynamic analysis of hydrogen detonation, debris-bed coolability) as required. The level of detail in these models will depend on the specific application and the requirements of the analysis techniques.

3. Reduce plant data to the engineering units required as code input.

4. Assist in the development of success and failure criteria for engineered safety features. This step is usually the responsibility of the systems analysts (Chapter 3). However, separate-effects analyses are frequently required to determine which conditions or sequences result in core melt. In the Reactor Safety Study, it was

assumed that if the criterion for the peak cladding temperature (2200°F) is exceeded, core melt will result. From experimental data and the behavior observed in the accident at Three Mile Island, it may be possible to defend a criterion that is less conservative.

Task 3: Determine Containment-Failure Mechanisms and Levels

1. Identify a comprehensive list of potential containment-failure mechanisms (see Table 7-1 for example).

2. Perform structural analyses of the containment to determine the steady internal pressure resulting in containment failure. Identify possible modes and locations of failure. The analysis should recognize that a range of possible failure pressures could exist from some level above the design pressure up to the ultimate strength of the containment, including the potential for stress concentrations and manufacturing defects. A density function for failure pressure should be developed.

3. Perform separate-effects analyses for the other potential mechanisms of containment failure to determine (a) whether the mechanism is credible, (b) the conditions under which containment failure would result, and (c) the likely locations and modes of containment failure.

Task 4: Select Analysis Methods for Physical Processes

1. Identify analysis requirements. Consider the special features of the reactor design that could require separate-effects analyses or changes in existing codes.

2. Select a code for the core-melt analysis (e.g., MARCH) and separate-effects codes as necessary.

3. Develop models or modify codes as required.

Task 5: Develop Bins for Accident Sequences

1. Receive system sequences from the task of accident-sequence definition and system modeling (Chapter 3).

2. Identify the initiating events, ESF states, and core-melt characteristics that can be used to group system sequences (see Table 7-2). This should be done in consultation with the analysts of radionuclide release and transport as well as the analysts of environmental transport and consequences to ensure that the release categories assigned to different sequences within a bin are common and that the branching probabilities on the containment event tree are the same.

3. Assign system sequences to plant-damage bins and provide to the analysts who will perform the accident-sequence quantification (Chapter 6).

Alternative Procedure

Receive from the task of accident-sequence quantification a small set of dominant system sequences that have been identified by probability discrimination. After release categories for these sequences are determined, consider the need for analyzing more sequences.

Task 6: Develop Containment Event Tree

1. Divide the accident into the major time periods of interest as in Table 7-3.

2. Select event-tree headings. The nodal questions in Tables 7-3 and 7-4 can be used as a guide. Add or delete headings, depending on the special features of the plant.

3. Order event-tree headings and describe the structure of the tree. The size of the tree is affected by the order of events. In general, events should be ordered on the tree in the temporal sequence in which they would actually occur. Unnecessary or meaningless branches may be removed from the tree.

Task 7: Analyze Accident Sequences

1. Provide preliminary assistance to the analysts involved in accident-sequence definition and system modeling in identifying plant conditions leading to core melt as required.

2. Select a representative sequence for each bin.

3. Determine the status of operating systems for the accident sequence. This includes not only whether a system is operating but also the level of operation (e.g., two of three pumps at 150 gpm each). Describe initial and boundary conditions.

4. Perform analyses to describe the transient power, thermal, and hydraulic behavior before core damage. Benchmark or tune the core-melt code.

5. Identify the containment-failure modes to be evaluated for each sequence. An accident sequence associated with each containment-failure mode will be analyzed.

6. Analyze the physical processes for each accident sequence using the core-melt code. Separate-effects analyses may be necessary to determine the time and the conditions of containment failure. Provide the results to the analysts of radionuclide release and transport as well as environmental transport and consequences.

Task 8: Perform Sensitivity Studies

1. Identify potentially sensitive parameters. In particular, consider parameters that could affect the likelihood or the time of containment failure.

2. Perform sensitivity studies by varying assumptions and values of input parameters over the range of uncertainty.

3. Provide results to the uncertainty-analysis task.

Task 9: Quantify Containment Event Tree

1. Develop a systematic approach to the characterization of branch-point probabilities, with or without uncertainties, consistent with the overall philosophy of the study.

2. Compare the predicted pressure profile for each sequence with the distribution function for failure pressure to determine the probability of containment failure (including sequences with hydrogen burning).

3. On the basis of the results obtained in tasks 8 and 9, use subjective judgment to predict branch-point probabilities (and uncertainty bands).

4. Provide results to the uncertainty-analysis task and to the integration task.

7.10.2 LIMITED ANALYSIS OF PHYSICAL PROCESSES*

Task 1: Collect Plant Data

Collect and review FSAR data on the design of the containment and the nuclear steam supply system. Compare with analogous features from previous risk studies.

Task 2: Model Plant

1. Develop plant model to be used in core-melt analyses of selected accident sequences.

2. Reduce plant data to the engineering units required as code input.

Task 3: Determine Containment-Failure Mechanisms and Levels

1. Identify containment-failure mechanisms by analogy with similar plants.

2. Estimate the containment-failure pressure on the basis of building-code requirements for the specific structure (e.g., a factor of 2 to 3, depending on the type of design).

---

*Since sensitivity studies would usually not be performed in this level of analysis, task 8 of Section 7.10.1 is omitted.

Task 4: Select Analysis Methods for Physical Processes

Select a code for core-melt analysis.

Task 5: Develop Bins for Accident Sequences

1. Receive system sequences from the task of accident-sequence definition and system modeling.

2. Select bin characteristics.

3. Assign system sequences to bins and provide to the task of accident-sequence quantification.

Alternative Procedure

Do not use binning approach.

Task 6: Develop Containment Event Tree

Develop a containment event tree by analogy with similar plant designs.

Task 7: Analyze Accident Sequences

1. Identify sequences for analysis. Sequences that are expected to have small consequences or are comparable to sequences analyzed previously in a similar plant would not be analyzed. The criteria for selecting sequences for analysis are as follows:

   a. It is unclear whether the sequence leads to core melt, or

   b. It is unclear whether the sequence leads to containment failure, or

   c. The sequence is substantially different from those analyzed previously.

2. Perform core-melt or separate-effects analyses as required.

Task 8: Quantify Containment Event Tree

Estimate branch-point probabilities by analogy with other studies or from the results for the few sequences analyzed specifically for the plant.

7.11 METHODS OF DOCUMENTATION

The amount of documentation that is required for the analysis of physical processes depends on the purpose of the study. In general, it should not be necessary to provide so much information that a reviewer can independently operate the computer codes to duplicate the calculations. It

should be assumed, however, that the risk analysis will be subjected to an extensive review by peers. Some of the information that should be documented in the report is listed below.

1. Sources of data.
2. Tables of plant-design data.
3. Computer codes (names and brief descriptions).
4. Major model options.
5. Tables of sequence probabilities and uncertainties.
6. Tables of accident event times and containment conditions.
7. Figures illustrating containment conditions for selected sequences.
8. A list of all assumptions.
9. A list of all limitations of the study.
10. Data documenting and justifying the containment event tree.
11. A justification and description of the basis for branching probabilities.

7.12 DISPLAY OF FINAL RESULTS

The outputs of this task are the thermal-hydraulics conditions for each accident sequence as required for the analysis of radionuclide transport and the conditional probabilities of sequences. If the core-melt code and the radionuclide-transport code are compatible (e.g., MARCH and CORRAL), the interface between the codes can be automatically determined--for example, by storing the output files of the physical process analysis on tape for later use in the radionuclide-transport code. If there is no formal link between the analysis methods, close liaison between the radionuclide-transport task and the physical process task will be necessary to ensure that the data are provided in a convenient format. Since a limited amount of thermal-hydraulics data produced by the core-melt codes is used in the transport codes, care must be exercised in the interpolation or averaging of the thermal-hydraulics data to be certain that the reduction process gives truly representative and reproducible results.

The probabilities of sequences can be characterized by point estimates or distributions, depending on the method selected for the propagation of uncertainties.

7.13 ASSURANCE OF TECHNICAL QUALITY

None of the currently available core-melt codes have been adequately validated against experiments. As the testing and validation of these codes progress, it would be advisable to use controlled versions of the codes that can be referenced. Since there are a number of available options in the core-melt codes, the selected options should be documented. Before any analyses are made it would be advisable to identify (list) all of the options available in the code. A conscious selection of options should then be made and frozen. If at a later time changes in options are advisable, they should be made with the approval of the project management and not left to the judgment of the analysts. This does not mean that a variety of code options should not be used to test the importance of modeling assumptions.

A formal procedure should be established for checking code input and results. The cost of review can be very high, and project management must decide the extent of review that is warranted. It should be recognized, however, that experience indicates a very high incidence of errors in preparing code input. Reference cases should be performed with the computer codes to demonstrate that the codes are operating correctly.

REFERENCES

Allison, C. M., B. O. Hagrman, S. Hsieh, E. T. Laats, and J. W. Spore, 1981. Severe Core Damage Analysis Package (SCDAP), Code Conceptual Design Report, EGG-CDAP-5937, EG&G Idaho, Inc., Idaho Falls, Idaho.

American Society of Mechanical Engineers, 1980. 1980 ASME Boiler and Pressure Vessel Code, An American National Standard, Section III Rules for Construction of Nuclear Power Plant Components, Philadelphia, Pa.

Aoyagi, Y., et al., 1979. "Behaviours of Reinforced Concrete Containment Models Under Thermal Gradient and Internal Pressure," in Transactions of the 5th SMIRT Conference, Paper No. J4/5, Berlin.

Atchison, R. J., G. J. K. Asmis, and F. R. Campbell, 1979. "Behavior of Concrete Containment Under Over-Pressure Conditions," in Transactions of the 5th SMIRT Conference, Paper No. J3/2, Berlin.

Baker, L., Jr., et al., 1977. Post Accident Heat Removal Technology, ANL/RAS 77-2, Argonne National Laboratory, Argonne, Ill.

Bathe, K. J., 1978. ADINA: A Finite Element Program for Automatic Dynamic Incremental Nonlinear Analysis, Report 82448-1, prepared by the Massachusetts Institute of Technology for the National Aeronautics and Space Administration. (Published in September 1975; revised in December 1978.)

Berman, M., 1981a. Monthly Progress Report on Sandia Hydrogen Programs, October and November of 1981, Sandia National Laboratories, Albuquerque, N.M.

Berman, M., 1981b. Light Water Reactor Safety Research Program Quarterly Report, January-March, 1981, USNRC Report NUREG/CR-2163 (SAND81-1216, Sandia National Laboratories, Albuquerque, N.M.).

Berman, M., 1981c. Proceedings of the Workshop on the Impact of Hydrogen on Water Reactor Safety, USNRC Report NUREG/CR-2017 (SAND81-0661, Sandia National Laboratories, Albuquerque, N.M.).

BMFT (Bundesministerium fuer Forschung und Technologie), 1980. Investigation of Partial Core Meltdowns, BMFT-RS-380, quarterly reports for 1979, Bonn, Federal Republic of Germany.

Carlson, D. D., et al., 1981. Reactor Safety Study Methodology Applications Program: Sequoyah #1 PWR Power Plant, USNRC Report NUREG/CR-1659, Vol. 1.

Commonwealth Edison Company, 1981. Zion Probabilistic Safety Study, Chicago, Ill.

Corradini, M. L., 1981. Analysis and Modelling of Steam Explosion Experiments, USNRC Report NUREG/CR-2072 (Sandia National Laboratories, Albuquerque, N.M.).

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

Denny, V. E., 1982. "Analytical Models for Core Heatup, Liquefaction, and Slumping," International Meeting on Thermal Nuclear Reactor Safety, August 1982.

Dhir, V. K., and I. Catton, 1977. Study of Dryout Heat Fluxes in Bed of Inductively Heated Particles, USNRC Report NUREG-0262.

Donten, K., et al., 1979. "Results of Strength Tests on a 1:10 Model of Reactor Containment," in Transactions of the 5th SMIRT Conference, Paper No. J4/8, Berlin.

EPRI (Electric Power Research Institute), 1981. RACAP-1: Reactor Accident Consequences Analysis Program, First Version, EPRI NP-1871, Palo Alto, Calif.

Fauske, H. K., and R. E. Henry, 1982. "IDCOR Modular Accident Analysis Program, An Enhanced Analytic Capability To Model Core Degradation Phenomena," Transactions of the American Nuclear Society, Vol. 41.

Gulden, W., et al., 1980. KESS, A Program System for the Analysis of Hypothetical Core Meltdown Accidents, USNRC Translation 837A.

Hagen, S., and H. Malauschek, 1979. "Bundle Experiments on the Meltdown Behavior of PWR Fuel Rods," Transactions of the American Nuclear Society, Vol. 33.

Hall, R. E., et al., 1979. A Risk Assessment of a Pressurized-Water Reactor for Class 3-8 Accidents, USNRC Report NUREG/CR-0603 (Brookhaven National Laboratory, Upton, N.Y.).

Hardee, H. C., and R. H. Nilson, 1977. "Natural Convection in Porous Media with Heat Generation," Nuclear Science and Engineering, Vol. 63, p. 119.

Henry, R. E., and H. K. Fauske, 1979. "Nucleation Processes in Large Scale Vapor Explosions," Journal of Heat Transfer, Vol. 101, pp. 280-287.

Key, S. W., Z. E. Bersinger, and R. D. Krieg, 1978. HONDO II, A Finite Element Computer Program for the Large Deformation Dynamic Response of Axisymmetric Solids, SAND78-0422, Sandia National Laboratories, Albuquerque, N.M.

Lipinski, R. J., 1980. Assessment of Core Penetration of a PWR Reactor Vessel and Particulate Debris Coolability in TMLB', S2D and ABG Accidents, USNRC Report NUREG/CR-1518 (SAND80-0701, Sandia National Laboratories, Albuquerque, N.M.).

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

MacNeal, R. H., 1978. NASTRAN: Theoretical Manual Level 17.6, National Aeronautics and Space Administration, Washington, D.C.

Marcal, P. V., 1975. MARC User Information Manual, Vol. 1, MARC Analysis Corporation.

Mays, S. E., J. P. Poloski, W. H. Sullivan, J. E. Trainer, R. C. Bertucio, and T. J. Leahy, 1981. Draft Report--Risk Assessment for Browns Ferry Nuclear Plant, Unit 1, prepared for the U.S. Nuclear Regulatory Commission.

Moore, K. V., et al., 1978. RETRAN--A Program for One-Dimensional Transient Thermal-Hydraulic Analysis of Complex Fluid Flow Systems, CCM-5, prepared by Energy Incorporated for the Electric Power Research Institute, Palo Alto, Calif.

Muir, J., et al., 1981. CORCON-MOD1: An Improved Model for Molten-Core/Concrete Interactions, USNRC Report NUREG/CR-2142.

Murfin, W. B., 1980. Report of the Zion/Indian Point Study, USNRC Report NUREG/CR-1410, Vol. 1, Chapter 3.

Murray, D. W., L. Chitnuyanondh, and C. Wong, 1979. "Modelling and Predicting Behavior of Prestressed Concrete Secondary Containment Structures Using BOSOR5," in Transactions of the 5th SMIRT Conference, Paper No. J3/5, Berlin.

Peehs, M., K. Hassmann, and S. Hagen, 1979. "Analysis of a Hypothetical Core Meltdown Accident of a PWR," Siemens Forschungs und Entwicklungsberichte, Siemens, Erlangen, Federal Republic of Germany.

Philadelphia Electric Company, 1981. Probabilistic Risk Assessment, Limerick Generating Station, Docket Nos. 50-352, 50-353, U.S. Nuclear Regulatory Commission, Washington, D.C.

Powers, D. A., and F. E. Arellano, 1981. Large Scale, Transient Tests of the Interactions of Molten Steel with Concrete, USNRC Report NUREG/CR-2282 (SAND81-1753, Sandia National Laboratories, Albuquerque, N.M.).

Powers, D. A., D. A. Dahlgren, J. F. Muir, and W. D. Murfin, 1977. Exploratory Study of Molten Core Material/Concrete Interactions, SAND77-2042, Sandia National Laboratories, Albuquerque, N.M.

Ransom, V. H., et al., 1980. RELAP5/MOD1 Code Manual, USNRC Report NUREG/CR-1826.

Rav, TVSR Appa, 1975. "Behavior of Concrete Nuclear Containment Structures up to Ultimate Failure with Special Reference to MAPP-1 Containment," Inelastic Behavior, Report 4-SM-THEME/75, Structural Engineering Research Centre, Madras, India.

Rivard, J. B., 1978. Post Accident Heat Removal: Debris Bed Experiments D-2 and D-3, USNRC Report NUREG/CR-0421 (SAND78-1238, Sandia National Laboratories, Albuquerque, N.M.).

Rivard, J. B., et al., 1981. Interim Technical Assessment of the MARCH Code, USNRC Report NUREG/CR-2285 (SAND81-1672, Sandia National Laboratories, Albuquerque, N.M.).

Senglaub, M. E., J. P. Odom, M. J. Clauser, J. E. Kelly, and P. S. Pickard, 1981. CONTAIN, a Computer Code for the Analysis of Containment Response to Reactor Accidents--Version 1A, draft USNRC Report NUREG/CR-2224 (SAND81-1495, Sandia National Laboratories, Albuquerque, N.M.).

Squarer, D., A. T. Pieczynski, and L. E. Hochreiter, 1981. "Dryout in Large Particle, Deep Debris Beds," Transactions of the American Nuclear Society, Vol. 36.

Tuerk, W., F. A. R. Schmidt, and H. Unger, 1980. "An Experimentally Verified Fuel Rod Meltdown Model," Transactions of the American Nuclear Society, Vol. 35.

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

USNRC (U.S. Nuclear Regulatory Commission), 1981a. Long Range Research Plan, NUREG-0740.

USNRC (U.S. Nuclear Regulatory Commission), 1981b. Preliminary Assessment of Core Melt Accidents at the Zion and Indian Point Nuclear Power Plants and Strategies for Mitigating Their Effects, NUREG-0850, Vol. 1.

USNRC (U.S. Nuclear Regulatory Commission), 1981c. Federal Register, Vol. 46, No. 246, pp. 62281-62285.

USNRC (U.S. Nuclear Regulatory Commission), 1981d. Technical Bases for Estimating Fission Product Behavior During LWR Accidents, NUREG-0772, Washington, D.C.

Von Riesemann, W. A., et al., 1981. "Structural Safety Margins of Containments," Ninth Water Reactor Research Information Meeting, October 1981, U.S. Nuclear Regulatory Commission, Washington, D.C.

Walser, A., 1980. "An Overview of Reactor Containment Structures," Nuclear Engineering and Design, Vol. 61, pp. 113-122.

Wooton, R. O., and H. I. Avci, 1980. MARCH (Meltdown Accident Response Characteristics) Code Description and User's Manual, USNRC Report NUREG/CR-1711 (Battelle's Columbus Laboratory, Ohio).

Chapter 8
Radionuclide Release and Transport

8.1 INTRODUCTION

This chapter describes methods for the evaluation of radionuclide releases to the environment during degraded-core accidents at light-water reactors. Overheating or melting of the reactor fuel in such accidents can result in the release of radionuclides from the fuel and their eventual release to the environment. Structural materials from the core and the reactor-coolant system can also be released with the radionuclides and are likely to affect not only the behavior of radionuclides in the reactor-coolant system and the containment but also eventual releases to the environment.

The methods discussed in this chapter include those used for establishing the initial inventories of radionuclides and structural materials in the fuel and the reactor; the analysis of radionuclide and structural material releases from the core; and the analysis of radionuclide transport, deposition, and release in the reactor-coolant system and the containment. These steps in a PRA are usually preceded by an analysis of the physical processes that can occur during degraded-core accidents since the presently available radionuclide-behavior models require input information on the timing of various events and the thermal-hydraulic conditions in the reactor. The analyses needed to obtain such information were discussed in Chapter 7.

The principal output of the radionuclide release and transport calculations is a set of release fractions to the environment. These express the quantities of radionuclides released to the environment as a fraction of the reactor-core inventory at the beginning of the accident. This information is required for analyzing, as described in Chapter 9, the transport of radionuclides through the environment and the consequences of the accident to public health and safety.

Radionuclides can be released from the reactor either into the air or into the ground. The pathways of releases into the ground are likely to result in significant attenuation of most radionuclides during their passage through soil, and thus accident sequences involving releases into the air are of much greater radiological importance. If radionuclides come in contact with groundwater, however, they may dissolve and be transported much more readily. Only cursory analyses of releases into the ground have been performed to date. For completeness, a summary of the treatment of ground releases in the Reactor Safety Study (USNRC, 1975) is given in Appendix G. This chapter deals only with the evaluation of releases into the air.

8.2 OVERVIEW

The evaluation of radionuclide releases that result from severely degraded core accidents involves the four elements shown in Figure 8-1:

1. Inventories of radionuclides and structural materials.
2. Radionuclide and structural material source term from the core.
3. Transport, deposition, and release in the reactor-coolant system.
4. Transport, deposition, and release in the containment.

Also shown in Figure 8-1 are the input needed from the analysis of physical processes (Chapter 7) and the output provided for the analysis of environmental transport and consequences (Chapter 9). The analysis proceeds sequentially, starting with the inventories of radionuclides and structural materials. This involves the determination of the quantities of radionuclides and structural materials that are present at the beginning of the accident. The next step is the evaluation of the radionuclide and structural material source term from the core. This entails the determination of the quantities of radionuclides and structural materials that are released

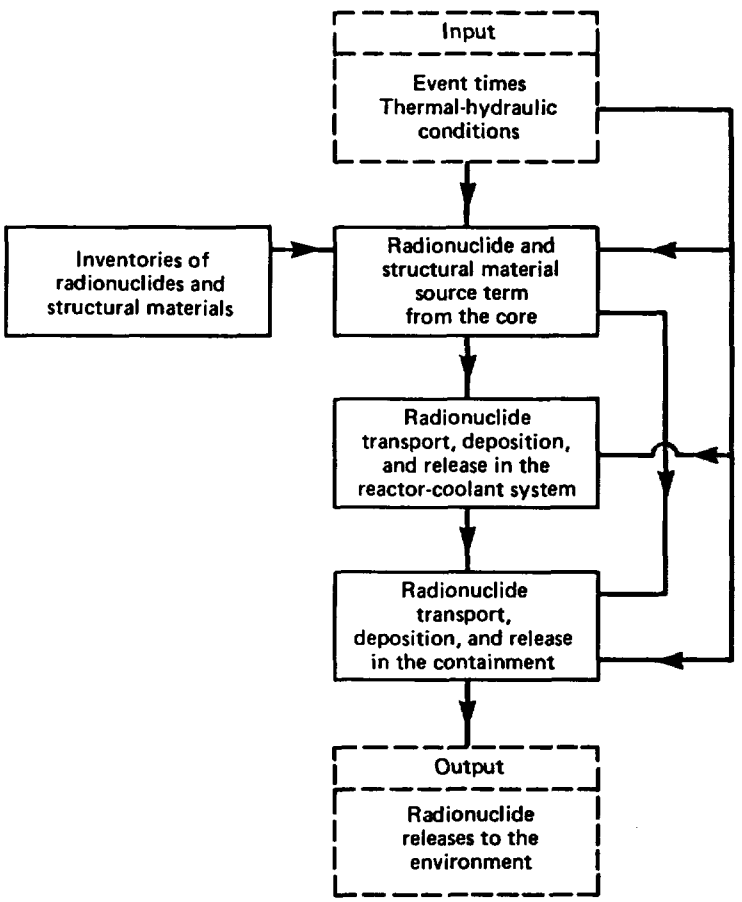


Figure 8-1. Elements in the analysis of radionuclide behavior in the reactor.

from the core to the reactor-coolant system or to the containment. (Direct releases of radionuclides and structural materials from the corium--the melted core and structural materials--to the containment can occur in core-melt accidents after the pressure vessel has melted through and the corium is interacting with the concrete basemat.) This source term is then used in the analysis of radionuclide transport, deposition, and release in the reactor-coolant system. The analysis considers the various deposition processes that can occur in the coolant system. The result is the source term for release from the coolant system to the containment; it is used in the analysis of transport, deposition, and release in the containment. This analysis takes account of the various deposition processes that can occur in the containment, and it estimates the quantities of radionuclides that are released from the containment to the environment.

It should be noted that, although the primary objective of the radionuclide transport and deposition calculations for the reactor-coolant system and the containment is the evaluation of source terms for releases to the containment and to the environment, respectively, the analyses can also provide information on the distribution of radionuclides deposited in the reactor-coolant system and the containment. This information may be of value for any cleanup and decontamination operations that may be necessary after an accident.

The four steps in the analysis of radionuclide release and transport are described in greater detail below.

8.2.1 INVENTORIES OF RADIONUCLIDES AND STRUCTURAL MATERIALS

The starting point in the analysis of radionuclide behavior during degraded-core accidents is the determination of the inventories of materials that can be released to the reactor-coolant system and the containment. This includes radionuclides, fuel, stable isotopes produced by the decay of radionuclides during reactor operation, and structural materials like cladding, control rods, core supports, and instrument tubes. Released structural materials can have a significant impact on the behavior of radionuclides in the coolant system and the containment, primarily by their effects on such aerosol behavior as agglomeration. It should be noted that the transport and deposition behavior of the stable isotopes of a particular nuclide is indistinguishable from that of the radioisotopes of the same nuclide. It is important to account for the effect of stable isotopes on mass-balance calculations since their inventories can be greater than those of the corresponding radioisotopes.

Radionuclide and stable-nuclide inventories can be determined with an isotope generation and depletion code that accounts for fission, transmutation, and decay. Such codes need nuclear constants (cross sections, decay rates, fission yields) and information on the initial nuclide inventory, the percentage uranium enrichment, the specific power of reactor operation, and burnup. Information on the quantities of structural materials present in the core can be found in documents on the reactor design, such as the safety analysis report and design drawings, or it can be obtained from the utility or the vendor.

8.2.2 RADIONUCLIDE AND STRUCTURAL MATERIAL SOURCE TERM FROM THE CORE

Releases of radionuclides from fuel can be expected to depend on the chemistry of the radionuclides within the fuel (kinetics and thermodynamics), the physical form of the fuel (e.g., cladding intact or failed, fuel solid or molten, fuel surface-to-volume ratio), and the environment to which the fuel is exposed (e.g., temperature, fluid composition, and steam/water/air/hydrogen ratio). The specification of the source term from the fuel should include not only the magnitudes of the releases but also the release rates and the chemical and physical forms (especially particle size) of the released materials. Releases can occur by a variety of processes. These release processes are classified here phenomenologically rather than mechanistically since this is more consistent with the state of knowledge of the subject. The release processes presently believed to be possible in degraded-core accidents are described below. It should be noted that each of these processes may actually represent several mechanisms of release.

Cladding-Rupture Release. When the fuel-rod cladding ruptures, which is usually considered to result from overheating, part of the radionuclide inventory that accumulates in the fuel-to-cladding gap during normal reactor operation will be released from the pressurized fuel rod. The radionuclides thus released will consist of the noble gases and the radionuclides that are in volatile form; there is also the possibility that any loose debris present in the gap, such as fuel powder, may be entrained in the gases flowing out of the rod. The cladding-rupture release can be expected to be a small component of the overall source term in a core-melt accident, but it could be an important contributor in other degraded-core accidents. Although it is usually considered to occur instantaneously at the time of cladding rupture, some diffusion may continue over a longer period of time. The release will not occur in all fuel rods at the same time, as it depends on the heatup rates of individual rods. This release process was called the "gap release" in the Reactor Safety Study (USNRC, 1975).

Diffusion Release. When the fuel is held at an elevated temperature and the cladding has failed, radionuclides will diffuse from inside the fuel matrix to the surface, where they will be released. Such a release may occur, for example, after the cladding fails and as the fuel is heating up but before the fuel melts. This release process can be important in degraded-core accidents where the core does not melt but stays at an elevated temperature for a significant period of time.

Leach Release. When water comes into contact with the fuel, radionuclides in the fuel will be leached into the water. This process can only occur, of course, after the cladding has failed. A release of this type may have occurred during the accident at Three Mile Island.

Melt Release. Occurring when fuel melts, this process involves the diffusion of radionuclides from inside the melt and their escape from its surface. It is believed that significant amounts of structural materials can be released with the radionuclides by this process. The rates of such a release can be expected to depend on the way the core melts down and will not be uniform across the core.

Melt/Concrete Release. This can occur after pressure-vessel melt-through, when the molten core and structural materials (corium) are in contact with the concrete basemat in the reactor cavity. Gases from the decomposition of the concrete will sparge the corium and can remove radionuclides contained within it. Large quantities of concrete components can be expected to be released with the radionuclides. This release was termed the "vaporization release" in the Reactor Safety Study. The process of vaporization can, and does of course, occur at other times--for example, during the melt release.

Fragmentation Release. Steam explosions that may result from the contact of a mass of fuel with water either in the pressure vessel or in the containment could result in the fragmentation of the fuel. (The likelihood of steam explosions is discussed in Chapter 7.) Other energetic events could cause a similar fragmentation; for example, the forces involved in pressure-vessel meltthrough may be sufficient for this purpose. If such an event occurs in an oxidizing atmosphere, a release of radionuclides from the dispersed fuel may result from (1) fuel oxidation with the attendant increase in surface area and a greater opportunity for the escape of radionuclides by diffusion or (2) the oxidation of radionuclides within the fuel. In particular, it has been suggested that there may be an enhanced release of radionuclides that have volatile oxides (USNRC, 1975), an example being ruthenium. (Molybdenum can also be oxidized by steam.) This release process was called the "oxidation release" in the Reactor Safety Study.

It should be noted that the volatile radionuclides that would be most likely to escape as a result of fuel oxidation may not be present in the fuel at the time of fuel oxidation, owing to their earlier release by other processes. The oxidizing atmosphere needed for this release derives either from air in the containment or air in the environment. It is also possible that fuel dispersal into an inert or reducing atmosphere may occur. In this case, the relocation of the fuel and the radionuclides it contains can be an important factor. This is also true of fuel dispersal in an oxidizing environment since not all radionuclides will escape from the fuel, and the location and ultimate fate of the remaining nuclides must be considered. If fragmented fuel becomes immersed in water, radionuclides can be released by leaching from the fuel with its increased surface area. For example, such a release could occur in the event of a steam explosion in the containment when there is water in the reactor cavity.

It should be noted that release by oxidation does not require fuel dispersal in a finely divided form. It may occur if the fuel is held at a high temperature in the presence of an oxidizing agent--such as oxygen, steam, or carbon dioxide--for a reasonable amount of time. Releases by this mechanism may contribute to some of the other release processes described above, for example, the melt/concrete release.

The release processes discussed above represent those believed to be possible during severely degraded core accidents. Not all processes will necessarily occur in every accident since they are dependent on the particular conditions of each accident. Although this discussion represents current understanding of the release processes, it is also possible that processes not discussed above may occur.

In order to analyze radionuclide and structural material releases from the core, information is needed on radionuclide and structural material inventories, the physical processes that occur, and physical and chemical data needed to model each of the release processes. Information on the physical processes determines which radionuclide-release processes occur, provides data on the atmosphere in the reactor-coolant system, describes the manner and timing of core degradation, and specifies the time at which various events occur (e.g., cladding failure, core-melt initiation and termination, pressure-vessel failure).

8.2.3 TRANSPORT, DEPOSITION, AND RELEASE IN THE REACTOR-COOLANT SYSTEM

The analysis of radionuclide transport and deposition in the reactor-coolant system (RCS) must consider both chemical and physical processes that may influence the behavior of the radionuclides. Radionuclides and structural materials can be released from the fuel to the reactor-coolant system as vapors or particulates. Vapors can condense on coolant-system surfaces, within the RCS fluid to form particulates, or on suspended particulates. Particulates or condensed materials can also be vaporized if appropriate temperatures are encountered. Particulates can also agglomerate to form larger particles. In addition, materials released from the core can react chemically with one another or with the components of the carrier fluid (steam, hydrogen, and possibly air). Vapor materials can be removed from the RCS atmosphere by interaction with water (e.g., injected emergency core coolant) or by natural deposition processes like sorption on surfaces. Particulate material can also be removed by interaction with water and by such natural deposition processes as diffusion, diffusiophoresis, thermophoresis, impaction, and gravitational settling. It should be recognized that deposited material can be resuspended. For example, particulates can be reentrained in the fluid flow, and deposited vapors can be revaporized.

In order to perform such analyses, information is needed on the radionuclide and structural material source terms released to the reactor-coolant system (quantities of materials, release rates, time dependence, chemical forms, particle-size distribution, and particle composition), physical conditions in the reactor-coolant system (e.g., pressure, fluid temperature, surface temperature, fluid flow rate, fluid composition, flow path), the geometric configuration of the reactor-coolant system and the materials of RCS surfaces, and the physical and chemical properties of the released materials (e.g., vapor pressures, chemical reaction rates).

8.2.4 TRANSPORT, DEPOSITION, AND RELEASE IN THE CONTAINMENT

The analysis of radionuclide transport and deposition in reactor containments is similar in many ways to the analysis of radionuclide behavior in reactor-coolant systems. In principle, the processes that can occur in the coolant system can also occur in the containment. However, the conditions in containments during degraded-core accidents are very different from the conditions in reactor-coolant systems. This means that the actual

behavior of radionuclides in the containment is likely to be quite different from that in the coolant system. Furthermore, material suspended in the containment can be removed by various engineered safeguards, such as sprays, filters, ice condensers, and suppression pools, depending on the design of the reactor.

Input information needed for the analysis is of the same general type as for the RCS analyses but also includes information on the characteristics and functionability of the engineered safeguards and information on the mode and timing of containment failure.

8.3 METHODS

Severely degraded core accidents are rare events for which an experimental data base on radionuclide releases consequently does not exist. Therefore, recourse must be made to analytical methods in order to evaluate radionuclide releases to the environment. Available methods are discussed below for the four parts of radionuclide release and transport analysis that were described in Section 8.2.

8.3.1 INVENTORIES OF RADIONUCLIDES AND STRUCTURAL MATERIALS

The ORIGEN computer code is often used to estimate radionuclide inventories in fuel (Bell, 1973; Croff, 1980); it analyzes fission, transmutation, and decay. Cross sections, which are averaged over ranges of neutron energy, are used in predicting the reaction rates for fission and transmutation. Standard descriptions of radioactive-decay chains and accepted values of nuclear constants, such as half-life and fission yield, have been incorporated into the code. ORIGEN cannot predict the spatial distribution of nuclides within the reactor; it can, however, be used to estimate either the average inventory in the reactor or the inventory in a particular region of the reactor if the power generation in that region is specified as a function of time. Predictions made with ORIGEN have been compared with measurements of the inventories of actual fuel rods (Croff, 1980). The agreement has been typically within approximately 30 percent of the measured value.

Input data needed by ORIGEN include the initial nuclide inventory, the percentage uranium enrichment, the specific power of reactor operation, and burnup.

Computer codes other than ORIGEN are available for calculating radionuclide inventories. Many of them are proprietary, but one that is in the public domain is CINDER. It differs from ORIGEN in the technique used to solve the decay equations and in the data base employed. A comparison of CINDER and ORIGEN calculations is under way (T. England, Los Alamos National Laboratory, personal communication, 1981).

8.3.2 RADIONUCLIDE AND STRUCTURAL MATERIAL SOURCE TERM FROM THE CORE

In order to characterize concisely the radionuclide source term from the fuel and to facilitate analyses of radionuclide behavior, it is desirable to classify the large number of fission and activation products that occur in reactor fuel into a small set of categories, each of which is similar in physical and chemical behavior and can consequently be represented by a single nuclide. Such a classification was employed in the Reactor Safety Study (RSS--USNRC, 1975), and it has achieved a measure of popularity. It is shown in Table 8-1.

Table 8-1. Radionuclide-classification scheme used in the Reactor Safety Study[a]

Noble gases	Xe, Kr
Halogens	I, Br
Alkali metals	Cs, Rb
Tellurium group	Te, Se, Sb
Alkaline earths	Sr, Ba
Transition metals	Ru, Mo, Pd, Rh, Tc
Lanthanides and actinides	La, Nd, Eu, Y, Ce, Pr, Pm, Sm, Np, Pu, Zr, Nb

[a]In subsequent parts of this chapter, the various radionuclide groups will be denoted by the symbol for the first element listed in each group.

At present, there is no generally accepted comprehensive method for estimating radionuclide releases from the fuel during degraded-core accidents. However, several models are available in the literature. One of the earliest models is that used in the FRCRL2 computer code (Ritzman and Morrison, 1971). This code considers cladding-rupture, diffusion, and melt releases of radionuclides for a nodalized core (core divided into regions from each of which radionuclides are released independently). It is based on the earlier codes FRACREL and REGAP (USNRC, 1975). These models and available experimental data were used in the development of the RSS release fractions (see Table 8-2). The RSS source term has achieved some popularity, but the validity of the release-fraction values has been questioned. Furthermore, the RSS source term considers only the cladding-rupture, melt, vaporization, and oxidation release processes and does not consider possible structural material releases. In addition, the RSS source-term model assumes that the release processes apply to the whole core, with no core nodalization.

Available models for each of the six release processes discussed in Section 8.2.2 are described below.

8.3.2.1 Cladding-Rupture Release

An improved model for the cladding-rupture releases of cesium and iodine has been developed at the Oak Ridge National Laboratory (Lorenz et

Table 8-2. Release fractions used in the Reactor Safety Study for radionuclide releases from the fuel

Nuclide	Gap[a]	Melt[a]	Vaporization[b]	Oxidation[b]
Xe, Kr	0.03	0.87	0.1	0.9
I, Br	0.017	0.885	0.1	0.9
Cs, Rb	0.05	0.76	0.19	0
Te[c]	1.0×10^{-4}	0.15	0.85	0.6
Sr, Ba	1.0×10^{-6}	0.1	0.01	0
Ru[d]	0	0.03	0.05	0.9
La[e]	0	0.003	0.01	0

[a]Fraction of initial core inventory released.
[b]Release fraction applies to the core inventory remaining after previous releases.
[c]Release fractions also apply to Se and Sb.
[d]Release fractions also apply to Mo, Pd, Rh, and Tc.
[e]Release fractions also apply to Nd, Eu, Y, Ce, Pr, Pm, Sm, Np, Pu, Zr, and Nb.

al., 1979, 1980). Experiments were performed to measure radionuclide releases from several types of LWR fuel rods into which defects had been introduced. The experiments were conducted in steam over the temperature range 500 to 1200°C, and a model was fit to the collected data. It was found that in the temperature range 700 to 900°C, this release can be expressed by

$$M_B = \alpha V_B \left(\frac{M_0}{A}\right)^a \exp\left(-\frac{C}{T}\right)$$

where

M_B = mass of radionuclide released in the burst (g).
V_B = volume of plenum gas vented at 0°C and system pressure (cm^3).
M_0 = radionuclide inventory in the fuel-to-cladding gap (g).
A = internal area of the cladding associated with M_0 (cm^2).
T = temperature at rupture location (K).

Values of the adjustable constants α, a, and C were obtained by fitting the model to the experimental data (see Table 8-3).

In addition to the burst release, a longer term diffusion release was measured in the experiments and fit, over the temperature range 500 to 1200°C, with the model

$$M_D = M_0\left[1 - \exp\left(-\frac{R_0 t}{M_0}\right)\right]$$

Table 8-3. Values of parameters in burst and diffusion release models for cesium and iodine[a]

Parameter	Cesium	Iodine
α $[(g/cm^3)\cdot(g/cm^2)]$	3.49	0.163
a	0.8	0.8
C (K^{-1})	7.42×10^3	3.77×10^3
σ $[(g\cdot MPa/\mu m\cdot hr)\cdot(g/cm^2)^{-a}]$	1.90×10^3	1.22×10^2
γ (K^{-1})	1.98×10^4	1.48×10^4

[a]From Lorenz et al. (1980).

where M_D is the mass of radionuclide released by diffusion (g), t is the time at diffusion temperature (hr), and R_0 is the initial rate of release by diffusion (g/hr), given by

$$R_0 = \sigma\left(\frac{W}{P}\right)\left(\frac{M_0}{A}\right)^a \exp\left(-\frac{\gamma}{t}\right)$$

where W is the width of the radial gap (μm) and P is the system pressure (MPa). Again, values of the adjustable constants σ and γ were obtained by fitting the model to the experimental data (see Table 8-3). In general, the models were found to represent the data on which they were based within a factor of 3.

The models require knowledge of the initial radionuclide inventory in the gap. This inventory can be estimated on the basis of experimental observation or by using analytical methods. Several techniques were discussed in the Reactor Safety Study, including the use of the REGAP computer code.

The models were applied to the analysis of a loss-of-coolant accident (LOCA) for a typical pressurized-water reactor. Release fractions for iodine and cesium were found to be 5.3×10^{-4} and 2.5×10^{-4}, respectively--one to two orders of magnitude lower than the RSS release fractions. However, the cladding-rupture release is a very small contributor to the total source term for a meltdown accident.

In using these models, it is necessary to recognize their limitations. Their validity can only be ensured when applied to situations within the range of the test parameters used in the experiments on which they are based. These experiments used short sections of fuel rods with low gap inventories, but the authors of the model believe the model is applicable to full-length rods.

8.3.2.2 Diffusion Release

Classical models can be employed to model diffusion (Booth, 1957), but a supporting data base of diffusion coefficients is needed. A computer code called GRASS can be used for a mechanistic analysis of the diffusion of radionuclides from fuel to the fuel-to-cladding gap (Rest, 1978). It treats such processes as gas-bubble nucleation, diffusion, fuel microcracking, and grain boundary diffusion. The code does not treat radionuclides other than the noble gases, but extensions are planned (R. Sherry, U.S. Nuclear Regulatory Commission, personal communication, 1981). Although it was developed for steady-state conditions, GRASS has also been applied to transients (Rest, 1982).

Some experimental data of a scoping nature have been developed for irradiated LWR fuel heated to 1300-1600°C in steam. The tests simulated fuel rods with ruptured cladding. Heating times were short (0.4 to 10 minutes), and the fuel was of high burnup (30,000 MWd/MT) and low initial gap inventory (0.3 percent for cesium and iodine). The results showed a large increase in the release of noble gases, cesium, and iodine when the fuel is heated uniformly to a minimum of 1350 to 1400°C. Within 2 minutes at 1400°C, approximately 4 to 9 percent of the noble gases, cesium, and iodine in the fuel rod was released. Releases at 1- to 10-minute heating times were estimated to differ by factors of 0.8 to 1.2, respectively, from those at 2 minutes. At 1600°C, the releases in 2 minutes were about 17 to 25 percent of the total inventory. LWR fuel with different irradiation histories can be expected to give different release results in the temperature range 1300 to 1600°C.

Experimental work in progress should provide more data at higher temperatures (T. Kress, Oak Ridge National Laboratory, personal communication, 1981).

Diffusion releases of radionuclides in degraded-core accidents have not received a great deal of attention, because they have been viewed as unimportant in meltdown accidents. Their actual importance depends on the accident sequence that is modeled, and it is quite possible that they may be significant contributors to the total radionuclide source term for some accidents.

8.3.2.3 Leach Release

Until recently, leach releases have received little attention in analyses of degraded-core accidents owing to the perception that they are not important. Their actual importance depends on the details of the accident. The accident at Three Mile Island has helped focus attention on their potential contribution to the radionuclide source term.

Data on the leaching of radionuclides by water from fuel are sparse. Some work on spent fuel has been done at the Pacific Northwest Laboratory (Katayama et al., 1980). The leaching of cesium and strontium from corium-concrete mixtures has been studied by Johnstone and Braithwaite (USNRC, 1978). Powers and Westrich (USNRC, 1981) have also investigated the leaching of a variety of species from corium-concrete mixtures.

8.3.2.4 Melt Release

Experiments investigating the melt release have been conducted for the past several years in the Federal Republic of Germany, in the SASCHA facility of the Kernforschungszentrum Karlsruhe (KfK) (Albrecht et al., 1978, 1979). The experimental apparatus consists of a high-frequency induction furnace in which corium is heated to melting in a thoria crucible under air, argon, and steam atmospheres. The materials released from the corium are trapped in a collection train for analysis. Experiments have been reported for small samples (30 to 150 grams) of corium and corium traced with fission products. The experiments are designed to determine the melt release of both radionuclides and structural materials from the corium. Releases were generally found to increase on changing the atmosphere from steam to argon to air. The release fractions in air at 2700°C were found to be 0.004 to 0.007 for Fe, Cr, and Co and 0.04 to 0.11 for Sn, Sb, and Mn; for air at 2150°C, release fractions in the range 0.2 to 0.4 were found for Se, Cd, Te, and Cs. Generally, the melt temperature had the greatest effect on the releases, but chemical reactions among the melt constituents and with the atmosphere also played a significant role. The most probable sizes of the aerosol particles formed in air at temperatures between 1800 and 2700°C were less than 0.5 micrometer. Species of low volatility were concentrated in the larger particles, while those of high volatility were concentrated in the smaller particles.

Recent experiments at KfK were performed with sample sizes of 150 to 250 grams (Albrecht and Wild, 1981). Release information was obtained for a variety of species. More than 90 percent of iodine and cesium was released when a temperature of 1700°C was maintained for 10 minutes. Since total radionuclide releases for actual accident sequences will be dependent on specific time/temperature histories, release rates expressed as percent release per unit time at a particular temperature were calculated where possible for use in source-term evaluations.

The results of these experiments were compared with the melt-release values of the Reactor Safety Study. They indicate that the RSS melt-release values are underestimated for Te and Sb by a factor of 3 to 5 and overestimated for Ba, Mo, Zr, Ru, La, Ce, Pr, Nd, and Np by a factor of about 10.

The KfK release rates were also used to estimate the amounts of structural materials that would be released in a core-melt accident at the Biblis-B PWR. It was predicted that, of the total fuel and structural material inventory of 181 metric tons, a total aerosol mass of 3.5 metric tons would be formed before pressure-vessel meltthrough. Of this, 1.8 metric tons was estimated to come from the silver in the control rods and about 0.45 metric ton each from UO_2 and Fe/FeO.

In experiments planned at the Oak Ridge National Laboratory (ORNL), sections of irradiated fuel rods will be heated to melting and material releases measured (M. Silberberg, U.S. Nuclear Regulatory Commission, personal communication, 1981). These experiments will be extensions of the work that produced the ORNL cladding-rupture release model described in Section 8.3.2.1.

The results of these various melt-release experiments will eventually be used to develop a new model for this release process. However, no such model is available at present. In the interim, it is possible that the presently available results can be used to provide some indication of appropriate melt-release fractions. If such data are used, the user must consider their extrapolation to the actual conditions of full-scale core meltdowns.

A model that improves on the RSS model and accounts for diffusion and melt releases was recently proposed (USNRC, 1981). The model has the form

$$\frac{dM_x}{dt} = -k_x(t)M_x$$

where M_x is the mass of material x in the corium, k_x is a temperature-dependent release-rate coefficient, and t is time. This model allows the radionuclide releases from the fuel to be related to the core-heatup time. Release-rate coefficients were determined for several radionuclides by fitting to a wide range of experimental data (see Figure 8-2). Coefficients for fuel, cladding, and other structural material were developed from data collected at the SASCHA facility (see Table 8-4). The fractional radionuclide-release rates of Figure 8-2 and Table 8-4 were approximated by the equation

$$k(t) = Ae^{Bt} \qquad (8\text{-}1)$$

where A and B are constants determined by curve-fitting procedures (see Table 8-5).

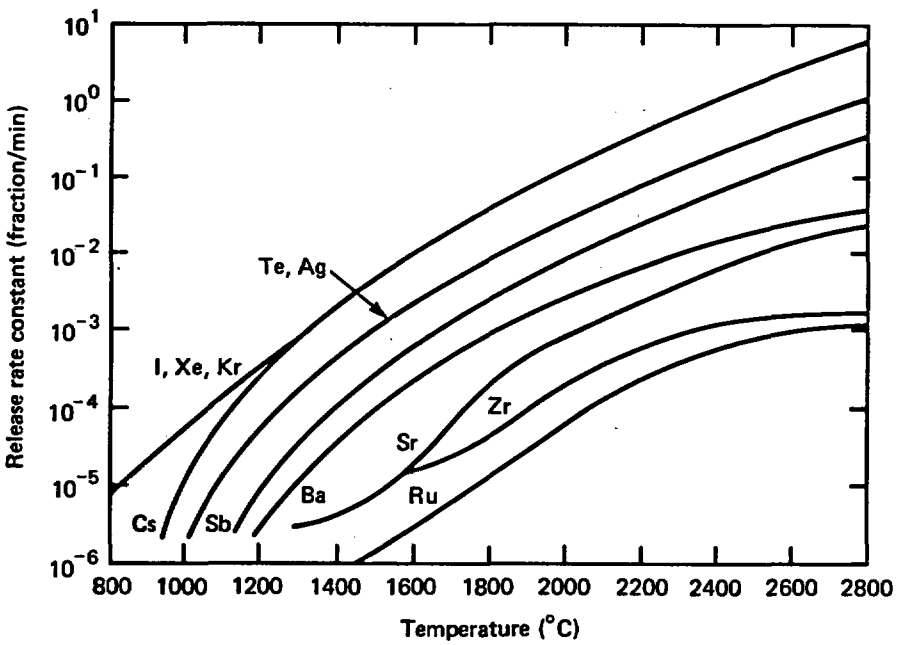


Figure 8-2. Release-rate coefficients for various radionuclides. From NUREG-0772 (USNRC, 1981).

Table 8-4. Release-rate coefficients for inert material[a]

Material	Temperature (°C)	Coefficient (1/m)
Fuel	2400	1×10^{-6}
	2700	1×10^{-5}
Cladding	2200	1×10^{-6}
	2500	1×10^{-5}
Structure	1800	1×10^{-6}
	2200	1×10^{-5}

[a]From NUREG-0772 (USNRC, 1981).

A comparison of results obtained with this new model and the results reported in the Reactor Safety Study for the large-pipe-break meltdown-accident sequence AB showed general agreement for all radionuclides except Te and Sb, for which the new model predicted considerably higher releases (USNRC, 1981). The usefulness of the model depends on the accuracy of the release-rate coefficients. The available values are thought to be quite uncertain (USNRC, 1981).

Table 8-5. Values of the constants A and B for release-rate coefficients[a,b]

Element	1000°C < T < 2200°C		T > 2200°C	
	A	B	A	B
Fuel (UO_2)	1.0×10^{-14}	0.00768	Same	Same
Cladding (Zr, Sn)	4.6×10^{-14}	0.00768	Same	Same
Structure (Fe)	3.2×10^{-11}	0.00576	Same	Same
Ru	1.36×10^{-11}	0.00768	8.49×10^{-7}	0.00262
Zr	8.3×10^{-10}	0.00622	1.44×10^{-5}	0.00173
Ba	7.28×10^{-11}	0.00677	6.40×10^{-7}	0.00377
Sb	1.0×10^{-8}	0.00667	1.55×10^{-6}	0.00303
Te, Ag	2.96×10^{-8}	0.00677	1.17×10^{-5}	0.00404
Cs, I	1.65×10^{-7}	0.00667	1.89×10^{-5}	0.00451

[a]From NUREG-0772 (USNRC, 1981).
[b]See Equation 8-1.

8.3.2.5 Melt/Concrete Release

For the past several years, an experimental program has been under way at Sandia National Laboratories to investigate the interaction of molten corium with concrete. Its principal objective has been to study the rate of concrete decomposition and the behavior of the melt. Information has also been obtained on aerosol generation (USNRC, 1980). It was found that the aerosol was composed mostly of nonfuel material and that the multimodal particle-size distribution of the aerosol was sharply peaked at a mean aerodynamic diameter of 2 micrometers. A preliminary model has been developed for the rate of aerosol release from the surface of molten corium interacting with concrete. This model has the form

$$\frac{dM}{dt} = C_a A_s V_s$$

where

M = released aerosol mass (g).
C_a = aerosol concentration in the plume rising above the melt (g/m^3).
A_s = melt surface area (plume cross section) (m^2).
V_s = superficial gas velocity (m/sec).
t = time (sec).

The aerosol concentration, C_a, was related empirically to the melt temperature and the superficial gas velocity by

$$C_a = A_0 \exp\left(-\frac{E}{RT}\right)\left(\beta V_s + \alpha\right)$$

where R is the universal gas constant = 1.987 cal/mole, T is the melt temperature (K), and the empirical constants E, β, α, and A_0 have the following values:

$$E/R = 19{,}000$$
$$\beta = 24$$
$$\alpha = 3.3$$
$$A_0 = 10^4$$

In order to estimate the aerosol release, a knowledge of the geometric configuration of the melt and a thermal analysis of the melt-concrete interaction are needed. The WECHSL (Reimann and Murfin, 1978) and CORCON (Murfin, 1977) computer codes are presently being developed to perform such analyses. Examples of the application of this model are the Zion and Indian Point probabilistic risk assessments (USNRC, 1980).

It should be noted that the model does not provide information on the release of radionuclide aerosols from the melt. It applies to materials like the oxides of silicon, calcium, and aluminum, which derive from the concrete. The model is also based on only a limited data base, and it depends on the results of a thermal analysis that are somewhat uncertain.

It is likely that the model provides order-of-magnitude accuracy, but it becomes worse at low (<1700°C) and high (>2600°C) melt temperatures (D. A. Powers, Sandia National Laboratories, personal communication, 1981).

Experiments are planned in the Federal Republic of Germany to examine material releases that result from corium-concrete interactions (Albrecht and Wild, 1981).

8.3.2.6 Fragmentation Release

Little information is available on the oxidation release that results from fuel fragmentation beyond that provided in the Reactor Safety Study. This release process was called the "oxidation release" in the Reactor Safety Study. The RSS release fractions for fragmentation were based on measurements of radionuclide releases during fuel oxidation by air at elevated temperatures.

8.3.2.7 Fuel Oxidation Release

A preliminary model has been published recently for the release of radionuclides from damaged fuel rods in a steam environment (Cubicciotti, 1981). The model describes a release that occurs as a result of fuel oxidation by steam and the ensuing grain growth. It is based on the experimental observation that the rate of sintering of UO_2 is significantly greater in a steam atmosphere than in an inert or reducing atmosphere and that the release of noble gases from heated UO_2 fuel is enhanced in the presence of steam. For the noble gases the model has the form

$$F = 1 - \left[1 - 4\left(\frac{\tau_H}{\pi}\right)^{1/2}\right]\left[1 - 4\left(\frac{\tau_\rho}{\pi}\right)^{1/2} + \tau_\rho\right] \qquad (8\text{-}2)$$

where

F = fractional release of radionuclide.

$\tau_L = D_c t/L^2$.

D_c = chemical diffusion constant representing the penetration of oxidant into the UO_2 (m^2/sec): $D_c = 9.9 \times 10^{-3} \exp(-28{,}600/T)$, T being the temperature (K).

L = height (H) or radius (ρ) of a fuel pellet (m).

t = time (sec).

An extension of the model to handle volatile radionuclides has been proposed (Cubicciotti, 1981). It was suggested that the factor $[1 - \exp(-P_i/P_T)]$, where P_T is the total pressure in the system and P_i is the vapor pressure of the volatile radionuclide, be used for that

purpose. This factor is unity for the noble gases and highly volatile radionuclides. For less volatile materials, the factor depends on the vapor pressure of the chemical form of the material. Preliminary calculations indicate that releases in steam are one to two orders of magnitude greater than releases in inert atmospheres (Cubicciotti, 1981).

8.3.2.8 Important Issues and Work in Progress

An experimental program has recently been started at the Oak Ridge National Laboratory to study the release of material from fuel during heatup to melting (T. Kress, Oak Ridge National Laboratory, personal communication, 1981). No results are presently available, however. In a separate analytical program at Battelle's Columbus Laboratories, a computer code called START is being developed to predict the releases of radionuclides and structural materials during degraded-core accidents, including meltdown accidents. Using semimechanistic models, the code presently accounts for releases by the cladding-rupture, diffusion, leach, melt, vaporization, and oxidation processes. It provides a detailed time dependence for material releases. A paper describing a preliminary version of the START code has recently been published (Baybutt et al., 1981).

Little information is available on the chemical forms of the materials that may be released from the core or the sizes of particulates. The Reactor Safety Study (USNRC, 1975) assumed that iodine will be released as elemental iodine (I_2) in vapor form and other radionuclides as particulates, but no information was provided on particle sizes. It has been suggested, on the basis of recent experiments, that iodine will be released from fuel not as elemental iodine but as cesium iodide (Campbell et al., 1981). It is possible that this could significantly change any resulting release of iodine to the environment. This issue is discussed further in Section 8.4. Lack of knowledge of chemical forms represents a significant uncertainty in the evaluation of radionuclide and structural material source terms.

Another major uncertainty is the timing of radionuclide and structural material releases. This depends partly on the timing of the physical processes that occur, especially the rate at which the fuel heats up, and partly on the chemical and physical properties of the radionuclides and structural materials. It should also be noted that the radionuclide-release rates will affect the core-heatup rate. For a given release process, it is quite possible that different materials will have different release rates owing to their different properties. Little work has been done to date to study such differences.

Since wide variations in physical conditions can be expected across degraded cores, it is important, in performing analyses of releases from the core, to partition, or nodalize, the core into regions within which the physical conditions are approximately uniform. The analyses are then performed for each individual region. It is quite possible that different regions of the core will experience different release processes at the same time.

8.3.3 TRANSPORT, DEPOSITION, AND RELEASE IN THE REACTOR-COOLANT SYSTEM

The TRAP computer code is the only model that is presently available to analyze radionuclide transport and deposition in reactor-coolant systems during degraded-core accidents (Baybutt and Jordan, 1977; Jordan et al., 1979). Analyses of the transport of radionuclides through reactor-coolant systems were performed in the Reactor Safety Study (USNRC, 1975) for both particulates and elemental iodine, and it was concluded that, except in two special BWR cases, the retention of radionuclides in the coolant system would be minimal. However, the analyses were based on the thermal-hydraulics information available at the time, which was not detailed and did not consider the effects of structural material releases on radionuclide behavior in the reactor-coolant system. The coagulation of structural material aerosols with radionuclides could result in significant radionuclide removal.

The TRAP code models mechanistically the behavior of both radionuclide vapors and particulates (Jordan et al., 1979). It includes models for vapor sorption on surfaces, vapor condensation and evaporation onto and from particles and surfaces in the reactor-coolant system, particle deposition by diffusion from laminar and turbulent flow, inertial particle deposition from turbulent flow, particle deposition by thermophoresis, and particle agglomeration by Brownian and turbulent processes. The reactor-coolant system is represented in the code as a set of interconnected compartments (control volumes) within which the thermal-hydraulic conditions are uniform at any instant in time and the radionuclides are well mixed. Radionuclide transport is superimposed on the fluid flow between compartments without being coupled to it. The control volumes can be connected arbitrarily by fluid flow, and a source term of radionuclides can be placed in any volume. The modeling of radionuclide transport is based on the concept of a radionuclide state in which a particular physical form is associated with a radionuclide location (e.g., particulates suspended in steam). The transport of radionuclides can occur among the states of an individual control volume or between certain states of different control volumes if these are connected by fluid flow. Radionuclide-transport rates are modeled by using correlations for mass-transfer coefficients in a system of differential equations.

Data required as input to TRAP include the physical properties of the radionuclides, the geometric configuration of the reactor-coolant system and the material of surfaces, the source term from the core, the flow path through the coolant system, and thermal-hydraulic conditions. TRAP provides as output the radionuclide masses present in each state within each control volume as a function of time. This includes the amounts of radionuclides released to the containment from the breach in the reactor-coolant system.

TRAP does not model the gravitational agglomeration of particles, which can be important if, as is likely, large amounts of structural materials are released with the radionuclides. Neither does it account for chemical reactions that may occur during the transport of radionuclides through the reactor-coolant system, the sorption of vapors on particulates, radioactive decay, particle resuspension, or the interaction of radionuclides with water in the coolant system. The code was designed for accidents in which there is no water in the flow path to the containment. The TRAP code is being

developed further in a continuing program at Battelle's Columbus Laboratories (J. A. Gieseke, Battelle's Columbus Laboratories, personal communication, 1981). In particular, some of the processes identified above are being incorporated into the code.

To support the development of TRAP, experiments are being performed at Sandia National Laboratories to determine the vapor pressures of radionuclide compounds and to identify the chemical compounds that can result from reactions among materials released from the fuel to the reactor-coolant system and from reactions between these materials and the atmosphere of the reactor-coolant system (R. M. Elrick, Sandia National Laboratories, personal communication, 1981). For materials typical of the surfaces in the reactor-coolant system, radionuclide-vapor deposition velocities under conditions characteristic of accidents are being measured in a project at Battelle's Columbus Laboratories (S. L. Nicolosi, Battelle's Columbus Laboratories, personal communication, 1981). The results of these experiments will be incorporated into TRAP as they become available.

8.3.4 TRANSPORT, DEPOSITION, AND RELEASE IN THE CONTAINMENT

There are several computer codes that describe radionuclide transport and deposition in reactor containments. One of the earliest of these was MIRA, which accounts for the removal of iodine by natural deposition, filtration, PWR sprays, and scrubbing in a BWR wetwell (Ritzman, 1971). This code was superseded by CORRAL, which was developed as part of the Reactor Safety Study. CORRAL treats all radionuclides that can be released from the fuel and employs the classification of Table 8-1. It assumes that iodine is present in the containment as elemental iodine or organic iodide (e.g., methyl iodide). Other radionuclides, except the noble gases, are assumed to be present as particulates. Noble gases and organic iodides are assumed to pass through the containment without attenuation. Models for the removal of methyl iodide by charcoal filters and sprays were described in the Reactor Safety Study but were not programmed in the CORRAL code.

Models for the removal of elemental iodine and particulates by both natural processes and the operation of engineered safeguards are included in CORRAL. These models are semiempirical and are based largely on results obtained in the Containment Systems Experiments (Postma and Johnson, 1971). Natural deposition of elemental iodine is modeled by natural convection to the containment walls as a result of a temperature gradient between the containment atmosphere and walls. For particulates, natural deposition is modeled by gravitational settling. The code accounts for the removal of both elemental iodine and particulates by sprays, filters, and suppression pools. The containment is represented as a set of interconnected compartments (control volumes) within which the thermal-hydraulic conditions are assumed to be uniform at any instant in time, and the radionuclides are well mixed. Radionuclide transport is superimposed on the fluid flow between compartments without being coupled to it.

CORRAL places some restrictions on the time dependence of the source term that is used. The cladding-rupture and fragmentation/oxidation

releases are assumed to occur instantaneously, the melt release is assumed to occur in 10 equal parts spaced equidistantly over a time period specified by the user of the code, and the melt/concrete release is assumed to occur in two parts, each composed of 10 exponentially decreasing amounts characterized by an empirical half-life. The size of the particulates is assumed to decrease linearly from 15 to 5 micrometers over a period specified by the user. This behavior approximates results obtained in the Containment Systems Experiments and is believed to represent the evaporation of water from particulates on which water had condensed (Postma and Johnson, 1971).

Data required as input to CORRAL include the geometric configuration of the containment, the source term to the containment, the flow path through the containment, thermal-hydraulic conditions, the times of various events that occur during the accident, and information on the operation of containment safeguards. CORRAL provides as its principal output a set of cumulative radionuclide-release fractions for environmental transport analyses. It also provides information on the quantities of radionuclides deposited in each compartment.

CORRAL does not model the behavior of any structural materials released to the containment, nor does it account for any chemical reactions that may occur among released materials or reactions between released materials and the atmosphere or the materials in the containment. It does not model explicitly the agglomeration of particles or the condensation of steam on particles, although, since the code is empirically based, their effects can be considered to be included to some degree. Furthermore, CORRAL does not consider radioactive decay, phase changes in radionuclides, or the resuspension of deposited radionuclides. The removal of radionuclides in ice condensers and during their passage through leak pathways in the containment to the environment is not specifically modeled, but can be accounted for by using intercompartmental decontamination factors that are supplied by the user. The removal of particulates by diffusion, thermophoresis, and diffusiophoresis is not modeled, nor is the sorption of vapors on particulates.

The accuracy with which CORRAL predicts the actual radionuclide behavior that would occur in a degraded-core accident naturally depends on how far the conditions in the containment during the accident depart from those used in the Containment Systems Experiments, on which CORRAL is based. These experiments were performed in an isothermal environment, where radionuclide deposition by convective flow and diffusiophoresis is likely to be less than would be experienced under actual accident conditions. A limitation of CORRAL is that it is not designed to treat situations where airborne mass concentrations of particulates are high and agglomeration becomes a controlling factor. The aerosol concentrations employed in the Containment Systems Experiments were well below those that can be expected for some degraded-core accidents. CORRAL is best suited for those cases where steam condensation on particles occurs in the containment.

The version of CORRAL that was used in the Reactor Safety Study was tailored specifically to the Surry and Peach Bottom reactors. The version available from the National Energy Software Center is designated CORRAL-2 and has been generalized to accommodate other reactor designs. The radionuclide-behavior models do not differ from the RSS version.

The NAUA computer code has been developed at Kernforschungszentrum Karlsruhe in the Federal Republic of Germany to describe the behavior of aerosols in containments during core-melt accidents (Bunz and Schoeck, 1980; Bunz et al., 1981). The code is based on first principles. NAUA treats the Brownian and gravitational coagulation (agglomeration) of particles, the condensation or evaporation of water vapor onto or from particles, and the deposition of particles by sedimentation (gravitational settling), diffusion, and thermophoresis. The code assumes homogeneous mixing of the atmosphere in the containment, which it treats as a single volume. It can handle all possible particle-size distributions, such as lognormal, Gaussian, and monodisperse, with any time dependence for the aerosol source term to the containment. NAUA takes into account a size-dependent composition of the particles. The particle contents of water and solid material are averaged over the size of each size fraction but not over the whole size distribution. The radioactive nonvolatile nuclides are assumed to be homogeneously distributed over the solid fraction of the particles. The possible reaction of volatile radionuclides with the particles and droplets is not modeled, nor are the transport and deposition of radionuclide vapors or the resuspension of particulates. Radionuclide decay is not modeled, nor is the removal of particles by engineered safeguards like sprays. Application of the code depends on a detailed knowledge of the thermal conditions in the containment that control steam condensation.

Data required as input to NAUA include the geometric configuration of the containment, thermal-hydraulic conditions, and aerosol and steam source terms to the containment. Output includes the mass and number concentration of the aerosol as a function of time and particle size, and the quantities released to the environment.

An experimental program in the Federal Republic of Germany is aimed at providing data for the further development of NAUA (Bunz and Schoeck, 1980). Particular attention is being focused on water-vapor condensation on particulates and walls. Measurements of condensation on particulates have been made. Work is continuing on the examination of wall condensation and the dynamics of latent heat transfer. Aerosol experiments are also being performed in the NSPP facility at ORNL to investigate steam-condensation effects (T. Kress, Oak Ridge National Laboratory, personal communication, 1981).

The COSMO code has been written at the Japanese Atomic Energy Research Institute to analyze the removal of inorganic, organic, and particulate iodine (Nishio et al., 1981). It represents an extension of the MIRA code (Ritzman, 1971). A code called FISSCON has also been written recently in Canada (Fluke, 1981). It analyzes the behavior of radionuclides in the containments of CANDU reactors. FISSCON is very similar to CORRAL.

Aerosol-behavior codes, such as HAARM-3 (Gieseke et al., 1978) and QUICK (Gieseke and Lee, 1980), which were developed for the containment analysis of liquid-metal fast breeder reactors (LMFBRs), have been applied to LWR containments when steam condensation is not excessive (USNRC, 1981). HAARM-3 includes models for Brownian, gravitational, and turbulent agglomeration; gravitational, diffusional, and thermophoretic deposition on surfaces; particle removal by filtration; and leakage to the environment. The code assumes that aerosol concentration is spatially homogeneous throughout

the containment and that the aerosol-size distribution is lognormal. It cannot handle multiple compartments, the behavior of radionuclide vapors, or the condensation of steam on particles.

QUICK is similar to HAARM-3 in the processes it treats, but no simplifying assumptions are made regarding the aerosol-size distribution. An extended version of QUICK, called ZONE (Jordan et al., 1980), has the provision to treat the containment as three compartments interconnected by fluid flow. In addition, a code called MSPEC, which is similar to QUICK but also treats many chemical species, is under development (H. Jordan, Battelle's Columbus Laboratories, personal communication, 1981). Other LMFBR aerosol codes that are available include PARDISEKO (Jordan et al., 1974), HAA-3 (Hubner et al., 1973), AEROSIM (Walker et al., 1978), and MAEROS (Gelbard, 1981). However, not all of these codes have yet seen extensive use. Several of them have been shown to predict reliably experimental results with aerosol concentrations of less than 30 g/m^3 in vessels up to 850 m^3 in volume (Reed et al., 1980). However, it is possible that local aerosol concentrations higher than 30 g/m^3 may occur in some accident sequences, and the present codes have not been tested against experiments in this higher concentration regime. Consequently, care should be exercised in the use of these codes when the aerosol concentrations depart significantly from those for which the codes have been validated.

The ability of engineered containment safeguards to remove radionuclides is an important element in modeling the behavior of radionuclides in the containment. Radionuclide removal by filters and PWR sprays is relatively well understood. However, significant uncertainties exist for ice condensers and BWR suppression pools.

Experimental data for the removal of elemental iodine in ice beds have been obtained by the Westinghouse Electric Corporation (Malinowski, 1970). The fraction of air mixed with the steam was found to have a major effect on the decontamination factor for iodine. The effect of different additives to the ice on the amount of iodine retention was also investigated. There are no directly relevant data for particulate removal, however.

Presently, there are no detailed models available for radionuclide removal by scrubbing in BWR suppression pools, although a code called SUPRA is under development (I. B. Wall, Electric Power Research Institute, personal communication, 1981). It is also possible that existing models for bubble rise in steam generators (Baybutt et al., 1980) could be adapted. Pool scrubbing is usually treated with empirically obtained decontamination factors. Their values are very sensitive to the conditions of the experiments. In particular, the extent of radionuclide removal can be expected to depend very sensitively on whether the suppression-pool water is subcooled or boiling. More experimental and model-development work is needed. Recently, a program to perform measurements and develop models for decontamination factors was started (J. C. Cunnane, Battelle's Columbus Laboratories, personal communication, 1981).

The risk-dominant accidents of the Reactor Safety Study involved a gross failure of the containment, which provides a leak pathway with a large cross-sectional area for the escape of radionuclides to the environment.

For accidents involving a containment leak path with a smaller cross-sectional area, it is quite possible that the leak could be plugged by condensing steam or escaping material, or that some fraction of the escaping material would deposit along the leak path. It should be noted that our present understanding of the structural response of the containment building during accidents is not well developed and consequently represents a significant uncertainty in the modeling of radionuclide behavior.

In the Containment Systems Experiments, it was observed that leaks were plugged by condensed steam (Witherspoon and Postma, 1971). Measurements were made on the decontamination of radionuclides during passsage through leakage pathways, and significant attenuation was found (Hilliard and Postma, 1981).

A simple model has been developed for the plugging by aerosol deposits of ducts that are circular in cross section (Vaughan, 1978). This model has been recently compared with experimental data on the behavior of aerosols passing through leaks. The comparison indicated that the model was valid for a variety of aerosols over a range of duct diameters from 100 micrometers to 30 centimeters (Morewitz, 1981, 1982). In the process of plugging leak paths, the aerosols attach to the walls or to previously deposited aerosols. Some of the agglomerates can break off and be resuspended in the air stream so that the sizes of aerosols exiting from leaks can be increased (Morewitz, 1981).

It should be noted that the model described above was developed for idealized cracks. Most vessel cracks or leak pathways in a containment can be expected to be irregular, and therefore the actual aerosol removal may be higher than that predicted by the model.

A new code, MATADOR, that improves on CORRAL-2 is being developed at Battelle's Columbus Laboratories (Baybutt and Raghuram, 1981). The CONTAIN computer code, which was developed for the analysis of aerosol behavior during LMFBR accidents, is being extended at Sandia National Laboratories to handle radionuclide behavior in LWR containments during degraded-core accidents (Clauser et al., 1981). The TRAP code, originally developed for the analysis of radionuclide behavior in reactor-coolant systems and described in the preceding section, is being extended to treat the containment.

8.4 CURRENT ISSUES IN RADIONUCLIDE BEHAVIOR

The phenomena that occur during degraded-core accidents are complex. As a result, we do not have a complete understanding of the processes that occur, and there are a number of questions about radionuclide behavior that remain unanswered. As more research is performed, we can expect these issues to be resolved, but it is likely that new questions will arise. It is important that any analysis of radionuclide behavior take account of unresolved issues--for example, by providing estimates of the uncertainties they cause in the results of the analyses. This can, however, be a difficult task.

Some issues that remain unresolved at present and their probable impacts on public risk are listed in Table 8-6 and briefly discussed below.

Table 8-6. Unresolved issues in radionuclide behavior and their probable impacts on public risk

Issue	Probable impact
Aerosol generation from structural materials	High
Agglomeration of aerosols	High
Radionuclide removal by water pools and ice condensers	High to medium
Resuspension of deposited radionuclides	Medium
Chemical form of the radionuclide	High
Presence of organic iodides	Medium to low
Hydrogen combustion	Medium to low
Chemical reactions of radionuclides with materials in the containment	Medium to low
Radioactive decay	Medium
Radiation effects	Low
Coupling of thermal-hydraulics and radionuclide-behavior models	Medium
Verification and validation of computer codes	High to medium

8.4.1 AEROSOL GENERATION FROM STRUCTURAL MATERIALS

A variety of structural materials are present in the reactor. They include fuel cladding, control rods, core supports, and instrument tubes. Some of these materials can be released to the reactor-coolant system and the containment with radionuclides. In addition, the components of concrete can be suspended in the containment atmosphere as a result of the interaction between the molten core and the concrete basemat. These released structural materials can exert a significant impact on the behavior of radionuclides in the reactor-coolant system and the containment, primarily by their effects on such aerosol behavior as agglomeration.

Some data on structural material releases are available from fuel-melt experiments (Albrecht et al., 1978, 1979, 1981). These data, however, were obtained in small-scale experiments, and the extrapolation of the data to prototypic core-meltdown conditions is questionable. Larger-scale experiments, currently in progress, may help to solve this problem.

Limited experimental data on aerosol generation as a result of core-concrete interactions are available, and a preliminary model has been developed (USNRC, 1980). However, the model is accurate at best to within

an order of magnitude (D. A. Powers, Sandia National Laboratories, personal communication, 1981). Its application also requires a knowledge of the geometric configuration of the melt and a thermal analysis of the melt-concrete interaction, both of which are subject to significant uncertainties.

8.4.2 AGGLOMERATION OF AEROSOLS

It is likely that dense aerosols (with high concentrations per unit volume) will be generated in the reactor-coolant system and possibly parts of the containment as a result of the release of structural materials with radionuclides. Such aerosols will agglomerate and form particles of much larger sizes, which will then be subject to more rapid settling by gravitational deposition. In turn, this would significantly reduce the radionuclide release to the environment.

Little experimental work has been done under conditions appropriate for degraded-core accidents. However, some experiments are now under way (T. Kress, Oak Ridge National Laboratory, personal communication, 1981).

The importance of agglomeration in the reactor-coolant system has recently been assessed with the QUICK code (USNRC, 1981). For accident sequences with low aerosol concentrations and short residence times in the coolant system, such as the sequence AD in the Reactor Safety Study (USNRC, 1975), it was found that agglomeration and settling would result in less than 1 percent of the released materials being retained in the reactor-coolant system. For other accident sequences with longer residence times and higher aerosol concentrations, such as TMLB', QUICK predicted that 99 percent or more of the released materials will be retained in the reactor-coolant system. The importance of agglomeration as a contributor to particle retention thus depends on the characteristics of the particular accident sequence.

8.4.3 RADIONUCLIDE REMOVAL BY WATER POOLS AND ICE CONDENSERS

Little information exists on the removal of radionuclides by BWR suppression pools, PWR ice condensers, or water pools that may exist in PWRs (e.g., in the pressurizer). If the radionuclides released from the fuel do pass through water pools, significant radionuclide attenuation may occur. Whether such attenuation occurs depends on the nature of the accident. Of particular importance are the radionuclide-flow pathway to the environment and whether the pool water encountered is subcooled or boiling.

Some experimental data for the removal of elemental iodine in ice beds have been obtained by the Westinghouse Electric Corporation (Malinowski, 1970), but there are no directly relevant data for particulate removal. Existing information on the removal of radionuclides by water pools is poor. A program of research to measure aerosol attenuation by pool scrubbing has just been initiated at Battelle's Columbus Laboratories (J. C. Cunnane, Battelle's Columbus Laboratories, personal communication, 1981) with funding by the Electric Power Research Institute. No data are available yet, however.

A full understanding of radionuclide interactions with water pools requires a knowledge of the aqueous chemistry of radionuclides. The aqueous chemistry of iodine has been summarized in a recent report (USNRC, 1981).

8.4.4 RESUSPENSION OF DEPOSITED RADIONUCLIDES

Radionuclides that are deposited on surfaces in the reactor-coolant system or the containment can be resuspended; for example, particulates can be reentrained in fluid flow, and deposited vapors can be revaporized. To date, few analyses of radionuclide behavior have considered resuspension. In principle, the vaporization of condensed vapors is easily handled, and indeed the TRAP code treats this process. However, little information is available on the resuspension of chemisorbed vapors. Some data are available on the resuspension of particulates, but this process has not received attention in analyses of radionuclide behavior.

Radionuclides that dissolve in water can also become resuspended in the reactor atmosphere. The processes responsible for this resuspension are partitioning effects and the flashing of the water to steam to leave the dissolved materials. Other than the equilibration of elemental iodine in the water of the containment sprays, treated in CORRAL, these processes have not been modeled in analyses of radionuclide behavior.

8.4.5 RADIONUCLIDE CHEMICAL FORMS

The chemical form in which a radionuclide is released from the fuel can be expected to influence its subsequent behavior in the reactor-coolant system and the containment as well as the quantity that is eventually released to the environment. (It is also likely that the chemical form will influence the behavior of radionuclides in the environment.) The properties that exert an effect on radionuclide behavior include volatility or vapor pressure, solubility, and chemical reactivity, which vary among the possible chemical forms of a given radionuclide. At present, there is little information on the chemical forms of the radionuclides released from the core, and thus considerable uncertainty in analyses of radionuclide behavior can be introduced from this source.

Over the past year or so, questions have been raised on the chemical form of iodine released from fuel in degraded-core accidents.* For many years it has been assumed that iodine is released in elemental form.

---

*The interested reader can consult the following correspondence, available in the NRC Public Document Room: letter from W. R. Stratton, A. P. Malinauskas, and D. O. Campbell to NRC Chairman J. Ahearne, dated August 14, 1980; letter from Chauncey Starr to NRC Commissioner J. Hendrie, dated September 2, 1980; and letter from the Nuclear Safety Oversight Committee to President Jimmy Carter, dated December 21, 1980.

However, experiments at the Oak Ridge National Laboratory suggest that the actual form is cesium iodide (Campbell et al., 1981). Thermodynamics calculations performed in the Reactor Safety Study and more recently (USNRC, 1981) support this conclusion. Some evidence has also been found for the formation of cesium iodide deposits in the fuel-to-cladding gap (Cubicciotti and Sanecki, 1978). However, the experimental evidence is not definitive, and thermodynamics conclusions alone cannot necessarily be expected to determine chemical forms (kinetics is also important).

The Nuclear Regulatory Commission attempted to resolve this issue by funding a study to examine the state of the technology of iodine behavior. The results of the study have been recently reported (USNRC, 1981). The report summarized and evaluated available information on radionuclide releases from fuel, the chemistry of cesium and iodine, and radionuclide transport in the reactor-coolant system and the containment. The primary objectives were to determine, if possible, the most likely chemical form of iodine and to determine the effect of chemical form on the quantity of iodine released to the environment. The report concluded:

> The current data base suggests that cesium iodide will be the expected predominant iodine chemical form under most postulated light water reactor accident conditions. The current evidence regarding the chemical form of iodine released from fuel at high temperatures (>1400°C) is inconclusive. However, thermodynamic calculations predict that formation of CsI should occur in the gaseous reducing atmosphere in the reactor coolant system following release from fuel even if iodine is not released from the fuel as CsI. The formation of some more volatile iodine species (e.g., elemental iodine and organic iodines), however, cannot be precluded under certain accident conditions.
>
> The assumed form of iodine (either cesium iodide or elemental iodine) was not predicted to have a major influence on the estimated magnitude of iodine attenuation in the containment for severe accident sequences with early containment failure in which there is little time for natural fission product retention mechanisms to be effective. However, the assumed chemical form of iodine can influence the predicted attenuation within the reactor coolant system, where, in general, the attenuation factor will be greater for cesium iodide than for elemental iodine (i.e., less iodine will escape into the containment).

It should be recognized that, though these conclusions are based on the current state of the technology, there are significant uncertainties in the analyses and the supporting data base, and thus the conclusions cannot be regarded as definitive.

Questions can also be raised about the chemical forms of other radionuclides and their effects on radionuclide releases to the environment. This is an area in which experimental research is badly needed. Some work is in progress at Sandia National Laboratories to investigate the radionuclide chemical forms that may be present in reactor-coolant systems during degraded-core accidents (R. M. Elrick, Sandia National Laboratories, personal communication, 1981). Some insights into likely chemical forms can

be obtained by consulting thermodynamics tables or performing thermodynamics calculations with such computer codes as SOLGASMIX (Bessmann, 1977). However, these tables and codes do not contain data for all likely radionuclide chemical forms. Moreover, thermodynamics considerations alone cannot be used to predict chemical forms since chemical kinetics also plays an important role. A summary of available information on the chemistry of volatile radionuclides has recently been compiled (USNRC, 1981).

8.4.6 PRESENCE OF ORGANIC IODIDES

It is possible that iodine will react with organic materials (e.g., lubricating oils present in the containment), after it has been released from the fuel, and form organic iodides, such as methyl iodide. In the Reactor Safety Study, for example, it was assumed that a small percentage of the iodine in the containment is converted to organic iodides (USNRC, 1975). Both radiolytic and nonradiolytic formation mechanisms were considered. The importance of this phenomenon is that organic iodides differ from other chemical forms in their transport and deposition behavior. It is also possible that volatile forms of iodine, such as hydrogen iodide (HI) and hypoiodous acid (HOI), may be formed. Some recent work has provided evidence for the existence of HOI (C. C. Lin, General Electric Company, personal communication, 1981). The presence of such forms can have important implications for the transport and deposition of iodine and for the partitioning of iodine between water and the reactor atmosphere.

The information base on this topic is quite sparse, and the estimation of the quantities in which such materials may be formed is subject to large uncertainties. More experimental work is needed to resolve these issues.

8.4.7 HYDROGEN COMBUSTION

During degraded-core accidents, hydrogen can be formed by metal-water reactions or possibly by radiolysis under boiling conditions (see Chapter 7). In the latter case, free oxygen gas can be liberated. Hydrogen can burn or detonate in the containment if air is present, certain hydrogen concentrations are reached, and an ignition source is present. If such an event were to occur, it might affect the deposition rates and the chemical forms of the radionuclides in the containment. No information is presently available on such effects.

8.4.8 CHEMICAL REACTIONS OF RADIONUCLIDES WITH MATERIALS IN THE CONTAINMENT

A wide variety of materials are present in the containments of light-water reactors, from lubricating oils to paints on containment surfaces. It is possible that these materials will react chemically with the radionuclides released into the containment and thus possibly alter their behavior. The formation of organic and other forms of iodine provides a specific example. Little is known about such reactions.

8.4.9 RADIOACTIVE DECAY

Most analyses of radionuclide behavior do not account for radioactive decay because it has been assumed that decay would exert little effect on the results, owing to the relatively short time periods involved. However, for certain accidents, the time periods can be on the order of days, and there are some transformations, such as that of tellurium to iodine, that could be important. The treatment of radioactive decay is especially important if short-lived isotopes are to be considered.

8.4.10 RADIATION EFFECTS

It is possible that the radiation fields in reactor accidents may influence radionuclide behavior either by physical (e.g., charge) or chemical effects. Studies of charging effects on aerosol behavior have concluded that there is minimal impact (Reed et al., 1977). The formation of organic iodides is controlled, in part, by radiolytic mechanisms (Postma and Zavadoski, 1972). It is also possible, as discussed earlier, that the formation of hydrogen and oxygen by the radiolysis of water may affect radionuclide behavior. Little other work pertinent to reactor-accident conditions has been done.

8.4.11 COUPLING OF THERMAL-HYDRAULICS AND RADIONUCLIDE-BEHAVIOR MODELS

The state of the art in the modeling of radionuclide behavior artificially decouples the evaluation of thermal-hydraulic conditions. The computer codes that describe radionuclide behavior use information on thermal-hydraulic conditions as input. Radionuclide transport and deposition are superimposed on fluid flow. Although at present this approximation is believed to be reasonable, considering the level of sophistication of current models, it is possible that, as the state of the art in radionuclide behavior is advanced, an integration with the thermal-hydraulics analyses may be warranted. The assumption of well-mixed, homogeneous control volumes, which is used in virtually all radionuclide-behavior codes, may also need to be reassessed.

8.4.12 VERIFICATION AND VALIDATION OF COMPUTER CODES

It is important that computer codes for the analysis of radionuclide behavior and the models they contain be verified (independently assessed to determine that they function as specified and there are no coding errors) and validated (assessed to determine the accuracy of the analyses by comparison with experimental results). Few of the available codes have either been verified or validated, in the latter case mainly owing to the lack of experimental data.

8.5 INFORMATION REQUIREMENTS

This section discusses the information needed for analyses of radionuclide behavior and describes where such information can be obtained. Each of the steps in the analysis is addressed in turn.

8.5.1 INVENTORIES OF RADIONUCLIDES AND STRUCTURAL MATERIALS

Computer codes that calculate radionuclide inventories require information on the operating history of the reactor (Bell, 1973; Croff, 1980). Such information is available from the utility operating the reactor. They also require a set of nuclear constants; these are often incorporated in the codes as data libraries. Information on the amounts of structural materials in the system can be found in documents containing design data, such as safety analysis reports, or in design drawings, or it can be obtained from the utility or the vendor.

8.5.2 RADIONUCLIDE AND STRUCTURAL MATERIAL SOURCE TERM FROM THE CORE

The analysis of the release of radionuclides and structural materials from the core requires information on the following:

1. Inventories of radionuclides and structural materials (taken from the previous step).

2. The physical processes of core-melt accidents (provided by the analyses described in Chapter 7).

3. Physical and chemical data needed by each of the release models (sources were discussed in Section 8.3.1).

Information on the physical processes of core-melt accidents specifies which radionuclide-release processes will occur, provides data on the atmosphere in the reactor-coolant system (e.g., amount of hydrogen present), describes the manner of core degradation, and specifies the times at which various events occur (e.g., cladding failure, core-melt initiation and termination, and pressure-vessel failure).

8.5.3 TRANSPORT, DEPOSITION, AND RELEASE IN THE REACTOR-COOLANT SYSTEM

This element of the analysis requires information on the following:

1. Radionuclide and structural material source terms from the core. Data on quantities, release rates, time dependence, chemical forms, and particle-size distribution and composition are needed. (Provided by the previous step.)

2. The geometric configuration of the reactor-coolant system and the materials of its surfaces. (Provided by sources of information on the reactor design, such as the safety analysis report.)

3. Physical conditions. Information is needed on fluid flow rates and flow paths, fluid composition, fluid temperatures, surface temperatures, and system pressure, all as a function of time. (Provided by the analyses described in Chapter 7.)

4. Physical and chemical properties of radionuclides for the models of radionuclide behavior. (Sources were discussed in Section 8.3.2.)

8.5.4 TRANSPORT, DEPOSITION, AND RELEASE IN THE CONTAINMENT

The information needed for this task can be summarized as follows:

1. Radionuclide and structural material source terms. Data on quantities, release rates, time dependence, chemical forms, and particle-size distribution and composition are needed. (Provided by the previous step.)

2. Steam source term. Data on the quantity and release rate are needed. (Provided by the analyses described in Chapter 7.)

3. The geometric configuration of the containment and the materials of its surfaces. (Provided by sources of information on the reactor design, such as the safety analysis report.)

4. Physical conditions. Information is needed on fluid flow rates and flow paths, fluid composition, fluid temperatures, surface temperatures, system pressure, and steam condensation, all as a function of time. (Provided by the analyses described in Chapter 7.)

5. Engineered safeguards. Information is needed on their functionability (provided by the analyses described in Chapter 7) and operational characteristics, such as spray flow rates and water-droplet size, and filter efficiencies. (Provided by sources of information on the reactor design, such as the safety analysis report.)

6. Containment failure. Information is needed on the time and the mode of containment failure and such leak-path characteristics as length, cross-sectional areas, and tortuosity. (Provided by the analyses described in Chapter 7.)

7. Physical and chemical properties of radionuclides for the models of radionuclide behavior. (Sources were discussed in Section 8.3.3.)

8.6 UNCERTAINTIES IN THE ANALYSIS OF RADIONUCLIDE BEHAVIOR

8.6.1 SOURCES OF UNCERTAINTY

Uncertainties are present in both the data and the models used in analyzing the behavior of radionuclides. Data may be imprecise or unavailable, and models may only approximate the processes they are intended to describe. The omission of important processes because certain phenomena are not completely understood or because they cannot be modeled represents another source of uncertainty. Such sources of uncertainty were identified in Section 8.3. The most significant sources are summarized in Table 8-7.

All these sources of uncertainty propagate through to the results of the analyses. It is important for the assessment and utilization of the results of a PRA study that uncertainties in the results be evaluated and presented with the risk estimates. It is also important to represent the sources of uncertainty and to present their contributions to the total uncertainty because this information is of value in establishing priorities for further work and providing insights into the results of the probabilistic risk assessment.

8.6.2 RECOMMENDED PROCEDURES FOR UNCERTAINTY ANALYSIS

Ideally, in a probabilistic risk assessment, uncertainties should be assessed for the actual analyses that were performed. On some occasions a purely qualitative assessment will suffice, while on others, numerical estimates will be needed. The level of quantification can range from the simple application of engineering judgment for evaluating bounds on the predicted radionuclide releases into the environment to the development of input uncertainty estimates and their propagation through the computer codes by one of several available methods.

Various techniques of uncertainty analysis are described in Chapter 12. One method that has been developed for the analysis of uncertainties in radionuclide behavior uses statistical design and response-surface methods (Baybutt et al., 1981). The response-surface method is described in Chapter 12. Since relatively little work has been done in this area, it is not possible to recommend any specific techniques of uncertainly analysis as most appropriate. Consequently, the analyst of uncertainties in radionuclide behavior should select a technique from those discussed in Chapter 12, basing his choice on the needs of the probabilistic risk assessment being performed and the methods used for the analysis of radionuclide behavior.

One simple way to estimate uncertainties in releases to the environment is to use values that have been developed in other studies. Obviously, care must be taken to ensure that the selected values are appropriate for the case at hand. The section that follows provides a summary of such information that is available.

Table 8-7. Significant sources of uncertainty in the analysis of radionuclide behavior

Element of analysis	Sources of uncertainty
Inventories of radionuclides and structural materials	No significant uncertainties
Radionuclide and structural material source term from the core	Mode of core degradation and core-melt behavior Quantities of structural material released Chemical forms of released radionuclides Timing of radionuclide and structural material releases Adequacy of experimental data base on releases Validity of extrapolation of correlations based on small-scale experiments to prototypic reactor-accident conditions
Transport, deposition, and release in the reactor-coolant system	Source term from the core (magnitude, physical and chemical form, timing) Particle agglomeration Chemical reactions Water scrubbing of radionuclides Thermal-hydraulic conditions Vapor pressures of radionuclides Validity of computer codes
Transport, deposition, and release in the containment	Source term from the reactor-coolant system (magnitude, physical and chemical form, timing) Removal of radionuclides by ice condensers and BWR suppression pools Thermal-hydraulic conditions, particularly steam condensation on particles and hydrogen combustion Particle agglomeration Radionuclide attenuation during passage through containment cracks Chemical reactions Validity of computer codes

8.6.3 AVAILABLE INFORMATION ON UNCERTAINTIES

Only beginning efforts at the quantification of uncertainties in the analysis of radionuclide behavior have been made. One such effort was a project at Battelle's Columbus Laboratories to develop and apply methods for evaluating uncertainties in the predictions of the MARCH and CORRAL codes of radionuclide releases to the environment (Baybutt and Kurth, 1980). A series of reports on this work are being prepared, and some of the results have been published (Kurth et al., 1980).

Tables 8-8, 8-9, and 8-10 show the results of uncertainty analyses for three meltdown-accident sequences from the Reactor Safety Study: TMLB'-δ, ACDF-α, and TC-γ. Typically, standard deviations were 40 to 60 percent of the mean release fractions. Both data and model uncertainties were considered, but only the variables and models that were believed to be the dominant contributors were included in the analyses. Thus the actual uncertainties are likely to be larger. The results of the calculations also depend on the variable and model input uncertainties that were used and the method of uncertainty analysis that was employed. Furthermore, the analyses do not include uncertainties associated with the validity or the completeness of the MARCH and CORRAL codes. These can be expected to be substantial; consequently, the results of Tables 8-8, 8-9, and 8-10 should not be used as estimates for uncertainties in radionuclide releases to the environment without modification to account for the additional sources of uncertainty.

Similar methods have been applied to the evaluation of uncertainties in TRAP calculations of radionuclide deposition in the reactor-coolant system (Baybutt et al., 1980). Calculations were made for the BWR accident sequence TC-γ with a source term containing elemental iodine, cesium hydroxide, and plutonium dioxide. The results are shown in Table 8-11, where the standard deviation expressed as a percentage of the mean deposition fraction is seen to range from 48 to 75 percent. The qualifications given for the MARCH/CORRAL uncertainty estimates also apply to those for TRAP.

8.7 RELEASE CATEGORIES

Ideally, in a comprehensive risk assessment, analyses of radionuclide behavior should be made for all accident sequences of interest. However, such an exercise can become prohibitively expensive. In order to circumvent this problem, it is possible to categorize sequences by their characteristics in such a way that members of the same category have similar radionuclide-release fractions. A set of release categories is then defined such that all accidents assigned to the same category are assumed to have the same set of release fractions. It is then necessary to perform analyses of radionuclide behavior for only one accident sequence in each category in order to determine the set of release fractions for that category. This is the approach that was used in the Reactor Safety Study (USNRC, 1975) for radionuclide releases to the environment, and the release categories defined in the Study are shown in Table 8-12 as an example.

Table 8-8. Uncertainty estimates for the environmental radionuclide-release fractions of the TMLB'-δ PWR meltdown-accident sequence[a]

Radionuclide group[b]	Best-estimate release fraction[c]	Mean release fraction[d]	Standard deviation
I	0.59	0.18	0.08
Cs	0.55	0.38	0.17
Te	0.18	0.35	0.16
Sr	0.07	0.05	0.03
Ru	0.02	0.06	0.03
La	0.003	0.01	0.006

[a]From analyses by P. Baybutt, D. C. Cox, and R. E. Kurth, Battelle's Columbus Laboratories (work in progress). See qualifications in the text of Section 8.6.3 on what these estimates do and do not include.

[b]See Table 8-1 for definitions.

[c]Obtained from the CORRAL code with best-estimate input data.

[d]Obtained from a statistical analysis.

Table 8-9. Uncertainty estimates for the environmental radionuclide-release fractions of the ACDF-α PWR meltdown-accident sequence[a]

Radionuclide group[b]	Best-estimate release fraction[c]	Mean release fraction[d]	Standard deviation
I	0.49	0.38	0.06
Cs	0.36	0.38	0.16
Te	0.19	0.34	0.15
Sr	0.04	0.06	0.03
Ru	0.19	0.29	0.12
La	0.002	0.01	0.006

[a]From analyses by P. Baybutt, D. C. Cox, and R. E. Kurth, Battelle's Columbus Laboratories (work in progress). See qualifications in the text of Section 8.6.3 on what these estimates do and do not include.

[b]See Table 8-1 for definitions.

[c]Obtained from the CORRAL code with best-estimate input data.

[d]Obtained from a statistical analysis.

Table 8-10. Uncertainty estimates for the environmental radionuclide release fractions of the TC-γ BWR meltdown-accident sequence[a]

Radionuclide group[b]	Best-estimate release fraction[c]	Mean release fraction[d]	Standard deviation
I	0.04	0.08	0.05
Cs	0.15	0.25	0.11
Te	0.11	0.27	0.12
Sr	0.02	0.03	0.02
Ru	0.01	0.05	0.03
La	0.001	0.01	0.006

[a]From analyses by P. Baybutt, D. C. Cox, and R. E. Kurth, Battelle's Columbus Laboratories (work in progress). See qualifications in the text of Section 8.6.3 on what these estimates do and do not include.

[b]See Table 8-1 for definitions.

[c]Obtained from the CORRAL code with best-estimate input data.

[d]Obtained from a statistical analysis.

Table 8-11. Uncertainty estimates for the reactor-coolant-system deposition fractions[a] of the TC-γ BWR meltdown-accident sequence[b]

Radionuclide	Mean deposition fraction	Standard deviation
Iodine	0.04	0.03
Cesium	0.29	0.14
Plutonium	0.1	0.06

[a]Defined as the ratio of material deposited to that released.

[b]From Baybutt et al. (1980). See qualifications in the text of Section 8.6.3 on what these estimates do and do not include.

Table 8-12. Radionuclide-release categories used in the Reactor Safety Study

Release category	Fraction of core inventory released[a]							
	Noble gases	Organic iodine	I	Cs	Te	Ba	Ru	La
PWR-1	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}
PWR-2	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}
PWR-3	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}
PWR-4	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}
PWR-5	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}
PWR-6	0.3	2×10^{-3}	8×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}
PWR-7	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}
PWR-8	2×10^{-3}	5×10^{-6}	1×10^{-4}	5×10^{-4}	1×10^{-6}	1×10^{-8}	0	0
PWR-9	3×10^{-3}	7×10^{-9}	1×10^{-7}	6×10^{-7}	1×10^{-9}	1×10^{-11}	0	0
BWR-1	1.0	7×10^{-3}	0.40	0.40	0.70	0.05	0.5	5×10^{-3}
BWR-2	1.0	7×10^{-3}	0.90	0.50	0.30	0.10	0.03	4×10^{-3}
BWR-3	1.0	7×10^{-3}	0.10	0.10	0.30	0.01	0.02	3×10^{-3}
BWR-4	0.6	7×10^{-4}	8×10^{-4}	5×10^{-3}	4×10^{-3}	6×10^{-4}	6×10^{-4}	1×10^{-4}
BWR-5	5×10^{-4}	2×10^{-9}	6×10^{-11}	4×10^{-9}	8×10^{-12}	8×10^{-11}	0	0

[a]See Table 8-1 for definitions of the radionuclide groups I, Cs, etc.

Such categorizations are likely to be dependent on both the design of the reactor and the methods used for radionuclide-behavior analyses. Furthermore, their establishment and use involves subjective judgment. It is possible that generic release categories applicable to several different reactor designs could be developed.

Little work has been done on constructing release categories or establishing procedures for the development of release categories since the time of the Reactor Safety Study. However, some work on this topic is being performed as part of the Oconee PRA (W. J. Parkinson, Science Applications, Inc., personal communication, 1982).

8.8 PROCEDURES

A step-by-step set of procedures for analyzing radionuclide behavior in degraded-core accidents is provided below.

Task 1: Establish level of analysis to be performed. The level of analysis can range from the simple use of radionuclide-release categories developed in previous studies to the use of the most sophisticated methods available. The appropriate level of analysis depends on the objectives of the PRA, available resources, and time constraints.

Task 2: Select techniques to be used for analysis. Presently available methods are described in Section 8.3. The selection of techniques is governed by the level of analysis to be performed, the availability of needed data, the objectives of the PRA, available resources, and time constraints. The techniques that are selected may need to be adapted to the specific problem at hand. The analyst should also determine that the methods account for all phenomena likely to be of importance. Any improvements made in the analytical techniques subsequent to the publication of this procedures guide should be reviewed for possible inclusion in the work.

Task 3: Collect needed input data. The information identified in Section 8.5 as needed for analyses of radionuclide behavior must be collected.

Task 4: Determine inventories of radionuclides and structural materials. Available methods are described in Section 8.3.1. Often the ORIGEN computer code (Bell, 1973; Croff, 1980) is employed to estimate the radionuclide inventory in the core at the outset of the accident. Alternative codes like CINDER should be considered for possible use. The choice depends on how accurately the core inventory must be predicted, and therefore it is necessary to establish the degree to which the codes considered agree with experimental results. The quantities of structural materials can be determined from sources of information on the reactor design, an example being the safety analysis report.

Task 5: Determine radionuclide and structural material releases to the reactor-coolant system. Available methods are described in Section 8.3.2.

There are no generally accepted techniques. New methods are under development, but until they become available, special assessments of radionuclide and structural material releases will have to be made case by case, using whatever information is available when the assessments are made.

Task 6: Determine radionuclide releases to the containment. Available methods are described in Section 8.3.3. The only computer code presently available for performing such analyses is TRAP (Baybutt and Jordan, 1977; Jordan et al., 1979). However, this code does not include all processes that are likely to be important for all accidents (see Section 8.3.3). If necessary, for the cases to be analyzed, code modifications or special assessments must be made to account for important processes not modeled in TRAP. Aerosol processes like gravitational agglomeration can be modeled with the QUICK or HAA codes.

Task 7: Determine radionuclide releases to the environment. Available methods are described in Section 8.3.4. Several computer codes are available. CORRAL (USNRC, 1975) has been used widely but has a number of deficiencies. New codes are under development. In the meantime, codes like CORRAL and NAUA (Bunz et al., 1981) can be used, but an assessment must be made of the validity of their results in light of their deficiencies or processes not treated. The use of both CORRAL and NAUA may provide more reliable results than either code does individually.

Task 8: Determine uncertainties in radionuclide releases to the environment. A procedure for uncertainty analysis must be selected, and input data and model uncertainties must be quantified. The procedure is then used to propagate the input data and model uncertainties through the analyses of radionuclide behavior to determine the uncertainties in the results of the analyses, namely, the radionuclide releases to the environment.

Task 9: Provide data to analyses of environmental transport and consequences. The output of the analyses of radionuclide behavior is provided as input to the analyses of environmental transport and consequences. This consists of the magnitude of radionuclide releases to the environment as a function of time, particle sizes and compositions, and chemical forms.

8.9 METHODS OF DOCUMENTATION

This section provides an outline of the information that should be in a final report describing the results of the analysis. Sufficient detail should be provided for purposes of peer review.

1. Introduction. The objectives of the radionuclide behavior analysis should be described in light of the overall objectives of the probabilistic risk assessment being performed. The level of analysis should be specified, and any special requirements of the analysis for the reactor design being analyzed should be described.

2. Overview. The elements involved in the analysis should be summarized, and a description should be provided of the procedure that was followed. The methods used in the assurance of technical quality should be discussed.

3. Analytical techniques. A description of the methods used should be provided, with a justification for their selection. Details should be given of any modifications made to existing methods.

4. Input data. References should be provided to the sources of input data employed. A summary should be given of key data.

5. Assumptions. Any assumptions made in the analyses should be specified and discussed.

6. Presentation of results. This section should discuss the particular accidents analyzed and present the results of each step in the procedure. The final results presented should be those needed as input to the analyses of environmental transport and consequences (Chapter 9).

7. Summary. Any pertinent observations on the analyses or their results should be given here.

8.10 DISPLAY OF FINAL RESULTS

This section describes the format of the results of the radionuclide-behavior analyses that are provided as input to the analyses of environmental transport and consequences. The information that is needed consists of (1) the magnitude of radionuclide releases to the environment, (2) the physical form of the released radionuclides, and (3) the chemical form of the released radionuclides. The required format is briefly described below.

In preparing the results on release magnitudes, the radionuclide classification of Table 8-1 should be employed or one that is compatible with the analytical methods used for the evaluation of environmental transport and consequences. Radionuclide releases should be expressed as a fraction of the original core inventory at the beginning of an accident. The time dependence of these releases should be specified.

In presenting results on the physical form of the radionuclides, the distribution of particle sizes and composition as a function of particle size should be given. The chemical forms in which radionuclides are released to the environment should be specified for each radionuclide.

8.11 ASSURANCE OF TECHNICAL QUALITY

Little formal work has been done to develop methods of ensuring that PRAs are performed correctly. Consequently, this section presents only some general suggestions on the procedures that can be used for the assurance of technical quality (AOTQ) in analyses of radionuclide behavior.

The function of ensuring technical quality should be provided at several levels: the levels of the analysts (the persons actually performing calculations), the task leader (the individual directing the analysts), the PRA program manager (the individual directing the overall probabilistic risk assessment), the plant operating personnel, and peer reviewers. In general, these persons should perform AOTQ activities appropriate to their level in the organization and check on the execution of such activities by their immediate subordinates. For analysts these activities would include checking calculations and input data to computer codes and maintaining a written record of all calculations. The task leader would perform spot checks, and the PRA program manager would review the results for any inconsistencies or apparent errors. Review of results for their reasonableness is a valuable approach at all levels. Plant operating personnel should review the analyses to ensure that the design and operation of the plant have been represented properly. Peer reviewers should be used to provide a truly independent appraisal of the analyses performed.

Part of the AOTQ program must address the verification and validation of any computer codes or other tools used in the analyses. In addition, whenever computer codes are implemented on a new computer, they should be thoroughly checked using test cases.

The formal procedures described in Chapter 2 for the assurance of technical quality should be implemented for analyses of radionuclide behavior.

REFERENCES

Albrecht, H., and H. Wild, 1981. "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, Ill.

Albrecht, H., V. Matschoss, and H. Wild, 1978. "Investigation of Activity Release During Light Water Reactor Core Meltdown," Nuclear Technology, Vol. 40, p. 278.

Albrecht, H., V. Matschoss, and H. Wild, 1979. "Experimental Investigation of Fission and Activation Product Release from LWR Fuel Rods at Temperatures Ranging from 1500 to 2800°C," paper presented at IAEA Specialists Meeting on the Behavior of Defected Zirconium Alloy Clad Ceramic Fuel in Water Cooled Reactors, Chalk River, Canada, September 1979.

Baybutt, P., and H. Jordan, 1977. "TRAP: A Computer Code for the Analysis of Radionuclide Transport in LWR Primary Systems During Hypothetical Terminated LOCA's," in Proceedings of Topical Meeting on Thermal Reactor Safety, Sun Valley, Idaho, July/August 1977, CONF-770708, Vol. 3, p. 249.

Baybutt, P., and R. E. Kurth, 1978. Uncertainty Analysis of Light Water Reactor Meltdown Accident Consequences: Methodology Development, Topical Report for the U.S. Nuclear Regulatory Commission, Battelle's Columbus Laboratories, Columbus, Ohio.

Baybutt, P., and S. Raghuram, 1981. "MATADOR--A Replacement for the CORRAL Computer Code for the Analysis of Radionuclide Behavior in LWR Containments," paper presented at the Ninth Water Reactor Safety Research Information Meeting, Gaithersburg, Md., October 26-30, 1981.

Baybutt, P., J. A. Gieseke, H. Jordan, and S. Raghuram, 1980. "An Assessment of LWR Primary System Radionuclide Retention in Meltdown Accidents Using the TRAP Computer Code," in Proceedings, ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, Tennessee, April 1980, CONF-800403, Vol. 2, p. 1322, American Nuclear Society, La Grange Park, Ill.

Baybutt, P., R. E. Cudnik, and S. Raghuram, 1980. "Iodine Scrubbing in Steam Generator Tube Rupture Accidents," Proceedings, ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, Tennessee, April 1980, CONF-800403, Vol. 2, p. 1306, American Nuclear Society, La Grange Park, Ill.

Baybutt, P., S. L. Nicolosi, and S. Raghuram, 1981. "Radionuclide Source Terms for Degraded Core Accidents in Light Water Reactors," 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, Ill.

Bell, M. J., 1973. ORIGEN--The ORNL Isotope Generation and Depletion Code, ORNL-4628, Oak Ridge National Laboratory, Oak Ridge, Tenn.

Besmann, T. M., 1977. SOLGASMIX-PV, A Computer Program To Calculate Equilibrium Relationships in Complex Chemical Systems, ORNL/TM-5775, Oak Ridge National Laboratory, Oak Ridge, Tenn.

Booth, A. H., 1957. Report AECL DCI-27, Atomic Energy of Canada Ltd., Ottawa, Canada.

Bunz, H., and W. Schoeck, 1980. "Measurements of the Condensation of Steam on Different Aerosols Under LWR Core Meltdown Accidents," paper presented at the CSNI Specialists Meeting on Nuclear Aerosols in Reactor Safety, Gatlinburg, Tenn., April 1980.

Bunz, H., and W. Schoeck, 1980. "The Natural Removal of Particulate Radioactivity in an LWR Containment During Core Meltdown Accidents," in Proceedings, ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, Tennessee, April 1980, CONF-800403, Vol. 2, p. 1328, American Nuclear Society, La Grange Park, Ill.

Bunz, H., W. Schikarski, and W. Schoeck, 1981. "The Role of Aerosol Behavior in Light Water Reactor Core Melt Accidents," Nuclear Technology, Vol. 53, p. 141.

Campbell, D. O., A. P. Malinauskas, and W. R. Stratton, 1981. "The Chemical Behavior of Fission Product Iodine in Light Water Reactor Accidents," Nuclear Technology, Vol. 53, p. 111.

Clauser, M. J., M. E. Sanglaub, J. E. Kelly, J. P. Odom, M. F. Young, P. J. Cooper, K. K. Murato, and P. E. Rexroth, 1981. "Development of CONTAIN for LWR Containment Analysis," paper presented at the Ninth Water Reactor Safety Research Information Meeting, Gaithersburg, Md., October 26-30, 1981.

Croff, A. G., 1980. ORIGEN2--A Revised and Updated Version of the Oak Ridge Isotope Generation and Depletion Code, ORNL-5621, Oak Ridge National Laboratory, Oak Ridge, Tenn.

Cubicciotti, D., and J. E. Sanecki, 1978. "Characterization of Deposits on Inside Surfaces of LWR Cladding," Journal of Nuclear Materials, Vol. 78, p. 96.

Cubicciotti, D., 1981. "A Model for Release of Fission Gases and Volatile Fission Products from Irradiated UO_2 in a Steam Environment," Nuclear Technology, Vol. 53, p. 5.

Fluke, R. J., 1981. FISSCON: A Fission Product Behavior Code, Report 79317, Ontario Hydro, Toronto, Canada.

Gelbard, F. MAEROS: Input/Output Manual, draft USNRC Report NUREG/CR-1391.

Gieseke, J. A., H. Jordan, and K. W. Lee, 1980. Aerosol Measurements and Modeling for Fast Reactor Safety, USNRC Report NUREG/CR-1165.

Gieseke, J. A., K. W. Lee, and L. D. Reed, 1978. HARM-3 User's Manual, USNRC Report BMI-NUREG-1991 (Battelle Memorial Institute, Columbus, Ohio).

Hilliard, R. K., and A. K. Postma, 1981. "Large-Scale Fission Product Containment Tests," Nuclear Technology, Vol. 53, p. 163.

Hubner, R. S., E. U. Vaughan, and L. Baurmash, 1973. HAA-3 User's Report, AI-AEC-13038, Atomics International.

Jordan, H., J. A. Gieseke, and P. Baybutt, 1979. TRAP-MELT User's Manual, USNRC Report NUREG/CR-0632.

Jordan, H., W. Schikarski, and H. Wild, 1974. Nukleare Aerosole in Geschlossenem System, KfK-1989, Kernforschungszentrum Karlsruhe, Federal Republic of Germany.

Jordan, H., P. M. Schumacher, J. A. Gieseke, and K. W. Lee, 1980. Multiple Zone Aerosol Behavior Model, USNRC Report NUREG/CR-1294.

Katayama, Y. B., D. J. Bradley, and C. O. Harvey, 1980. Status Report on LWR Fuel IAEA Leach Tests, PNL-3173, Pacific Northwest Laboratory, Richland, Wash.

Kurth, R. E., P. Baybutt, and D. C. Cox, 1980. "Determination of Environmental Radionuclide Release Uncertainties for LWR Meltdown Accidents," Transactions of the American Nuclear Society, Vol. 34, p. 444.

Lorenz, R. A., J. L. Collins, and A. P. Malinauskas, 1979. "Fission Product Source Terms for the Light Water Reactor Loss-of-Coolant Accident," Nuclear Technology, Vol. 46, p. 404.

Lorenz, R. A., J. L. Collins, and A. P. Malinauskas, 1980. Fission Product Source Terms for the LWR Loss-of-Coolant Accident, USNRC Report NUREG/CR-1288.

Lorenz, R. A., J. L. Collins, A. P. Malinauskas, M. F. Osborne, and R. L. Towns, 1980. Fission Product Release from Highly Irradiated LWR Fuel Heated to 1300-1600 C in Steam, USNRC Report NUREG/CR-1386.

Malinowski, D. D., 1970. Iodine Removal in the Ice Condenser System, WCAP-7426, Westinghouse Electric Corporation, Pittsburgh, Pa.

Morewitz, H. A., 1981. "Fission Product and Aerosol Behavior Following Degraded Core Accidents," Nuclear Technology, Vol. 53, p. 120.

Morewitz, H. A., 1982. "Leakage of Aerosols from Containment Buildings," Health Physics, Vol. 42, p. 195.

Murfin, W. B., 1977. A Preliminary Model for Core/Concrete Interactions, SAND77-0370, Sandia National Laboratories, Albuquerque, N.M.

Nishio, G., M. Tanaka, K. Hashimoto, Y. Motoki, M. Naritomi, and S. Kitani, 1981. "Containment Spray Model for Predicting Radioiodine Removal in Light Water Reactors," Nuclear Technology, Vol. 54, p. 68.

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

Postma, A. K., and R. W. Zavadoski, 1972. Review of Organic Iodine Formation Under Accident Conditions in Water-Cooled Reactors, WASH-1233, U.S. Atomic Energy Commission, Washington, D.C.

Powers, D. A., and H. Westrich, 1981. Advanced Reactor Safety Research Quarterly Report, January-March 1980, USNRC Report NUREG/CR-1594.

Reed, L. D., H. Jordan, and J. A. Gieseke, 1977. "Charging of Radioactive Aerosols," Journal of Aerosol Science, Vol. 8, p. 457.

Reed, L. D., K. W. Lee, and J. A. Gieseke, 1980. "The Behavior of Contained Radioactive Suspensions," Nuclear Science and Engineering, Vol. 75, p. 167.

Reimann, M., and W. B. Murfin, 1978. "Calculations for the Decomposition of Concrete Structures by a Molten Pool," paper presented at the PAHR Information Exchange Meeting, Ispra, Italy, October 1978.

Rest, J., 1978. GRASS-SST: Fission Gas Behavior in UO_2, USNRC Report, U.S. Nuclear Regulatory Commission, Washington, D.C.

Rest, J., 1982. "The Prediction of Transient Fission-Gas Release and Fuel Microcracking Under Severe Core-Accident Conditions," Nuclear Technology, Vol. 56, p. 553.

Ritzman, R. L., and D. L. Morrison, 1971. FRCRL2--A Computer Code for Calculating Fission Product Release in Reactor Accident Analyses, BMI-1913, Battelle Memorial Institute, Columbus, Ohio.

Ritzman, R. L., 1971. MIRA--Methods for Iodine Removal Analysis in Reactor Containment Systems, BMI-1915, Battelle Memorial Institute, Columbus, Ohio.

USNRC (U.S. Nuclear Regulatory Commission), 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG 75/014), Washington, D.C., Appendix VII.

USNRC (U.S. Nuclear Regulatory Commission), 1978. Light Water Reactor Safety Research Program Quarterly Report, January-March 1978, NUREG/CR-0324, Washington, D.C.

USNRC (U.S. Nuclear Regulatory Commission), 1980. Report of the Zion/Indian Point Study, Vol. I, NUREG/CR-1410, Washington, D.C.

USNRC (U.S. Nuclear Regulatory Commission), 1981. Technical Bases for Estimating Fission Product Behavior During LWR Accidents, NUREG-0772, Washington, D.C.

Vaughan, E. U., 1978. "Simple Model for Plugging of Ducts by Aerosol Deposits," Transactions of the American Nuclear Society, Vol. 28, p. 507.

Walker, B. C., C. R. Kirby, and R. J. Williams, 1978. Discretization and Integration of the Equation Governing Aerosol Behavior, SRD-R-98, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, London, England.

Witherspoon, M. W., and A. K. Postma, 1971. Leakage of Fission Products from Artificial Leaks in the Containment Systems Experiment, BNWL-1582, Battelle Northwest Laboratories, Richland, Wash.

NRC FORM 335 (11-81) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-2300
Vol. 1

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
PRA Procedures Guide
A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
J. W. Hickman, et al.

5. DATE REPORT COMPLETED
MONTH December YEAR 1982

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Technical Writing Group

DATE REPORT ISSUED
MONTH January YEAR 1983

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
The American Nuclear Society and
The Institute of Electrical and Electronics Engineers

10. PROJECT/TASK/WORK UNIT NO.
FIN G 1004

11. FIN NO.
NRC Grant No. G-04-81-001
NRC Grant No. G-04-81-05

13. TYPE OF REPORT
Technical Report

PERIOD COVERED *(Inclusive dates)*
Not applicable

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

This procedures guide describes methods for performing probabilistic risk assessments (PRAs) for nuclear power plants at three levels of scope: (1) systems analysis; (2) systems and containment analysis; and (3) systems, containment, and consequence analysis. After reviewing its objectives and limitations, this document describes the organization and management of a PRA project and then presents procedures for accident-sequence definition and systems modeling, human-reliability analysis, the development of a data base, and the quantification of accident sequences. Procedures for evaluating the physical processes of core meltdown are presented next, followed by guidance on the evaluation of radionuclide releases from the containment as well as the analysis of environmental transport and offsite consequences. The analysis of external hazards is discussed next, including procedures for seismic, fire, and flood analyses. The guide concludes with suggestions for the development and interpretation of results and the performance of uncertainty analyses.

17. KEY WORDS AND DOCUMENT ANALYSIS 17a. DESCRIPTORS
Probabilistic risk assessment, accident-sequence definition, system modeling, human-reliability analysis, component data base, accident-sequence quantification, containment analysis, radionuclide release and transport analysis, environmental transport and consequence analysis, external hazard analysis, seismic analysis, fire analysis, flood analysis, uncertainty analysis

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unrestricted

19. SECURITY CLASS *(This report)*
unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
unclassified

22. PRICE
$

NRC FORM 335 (11-81)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555