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

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The NRC/GPO Sales Program, U.S. Nuclear Regulatory Commission,
   Washington, DC 20555
3. The National Technical Information Service, Springfield, VA 22161

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

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

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

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

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

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

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

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

GPO Printed copy price: $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

Page

VOLUME 1

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

Page

VOLUME 2

CONTENTS (Continued)

CONTENTS (Continued)

Page

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Continued)

# List of Figures

Figure Title Page

VOLUME 1

LIST OF FIGURES (Continued)

## LIST OF FIGURES (Continued)

VOLUME 2

## 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.

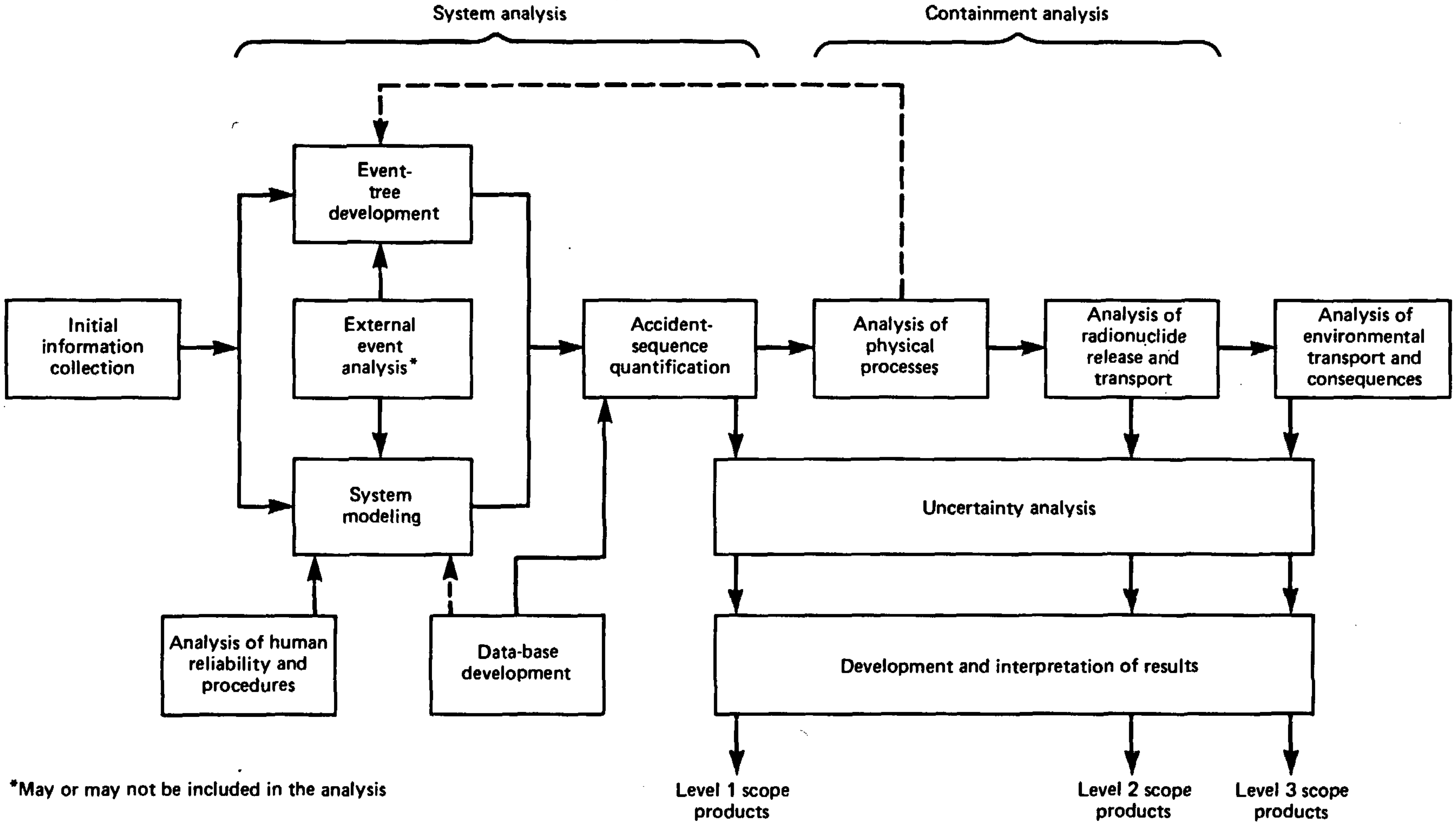
The sections that follow discuss the tasks associated with risk assessments of various scopes. Each task is briefly described, and the relationships between tasks are discussed. The steps involved in the analysis are shown in Figure 2-1.

### 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


System analysis
Containment analysis
Event-tree development
Initial information collection
External event analysis*
Accident-sequence quantification
Analysis of physical processes
Analysis of radionuclide release and transport
Analysis of environmental transport and consequences
System modeling
Uncertainty analysis
Analysis of human reliability and procedures
Data-base development
Development and interpretation of results
Level 1 scope products
Level 2 scope products
Level 3 scope products

*May or may not be included in the analysis

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

| | Manpower estimate (man-months) | | |
|---|---|---|---|
| Function | 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 |

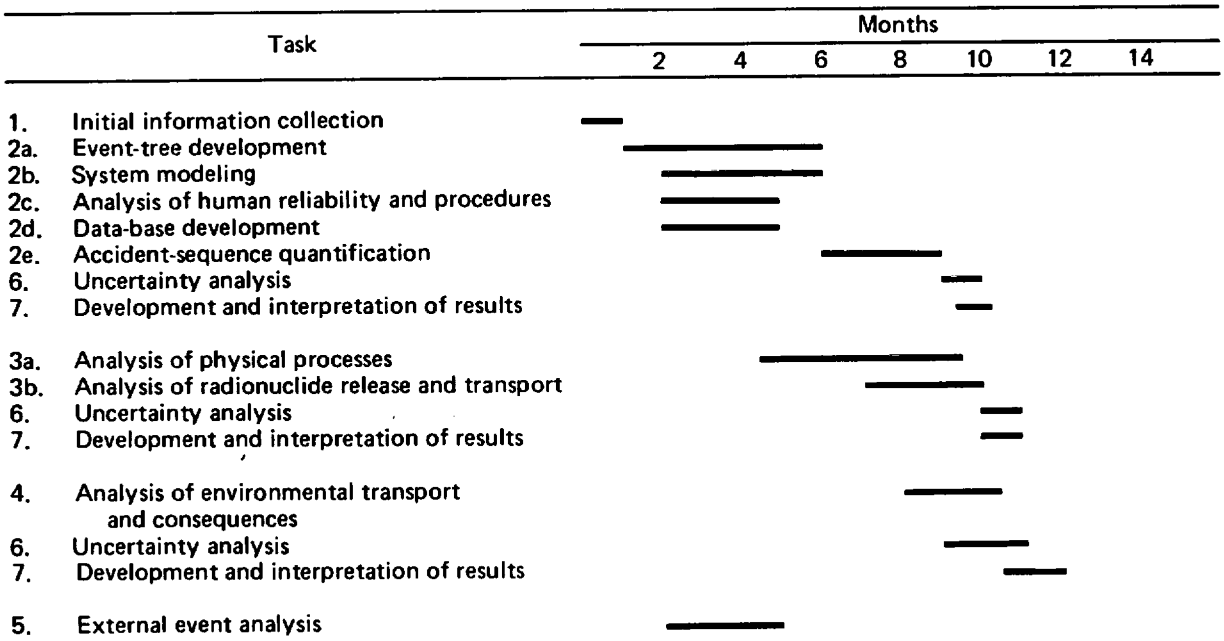


Figure 2-2. Minimum technical schedule. For report preparation and publication, another 6 months should be added.

### 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 | |
| 1 | human-reliability specialist | |
| 1 | data analyst | |
| 2 | sequence-quantification specialists | |
| 3 | physical process analysts | Level 2 |
| 1 | structural analyst | |
| 2 | radionuclide-transport analyst | |
| 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.

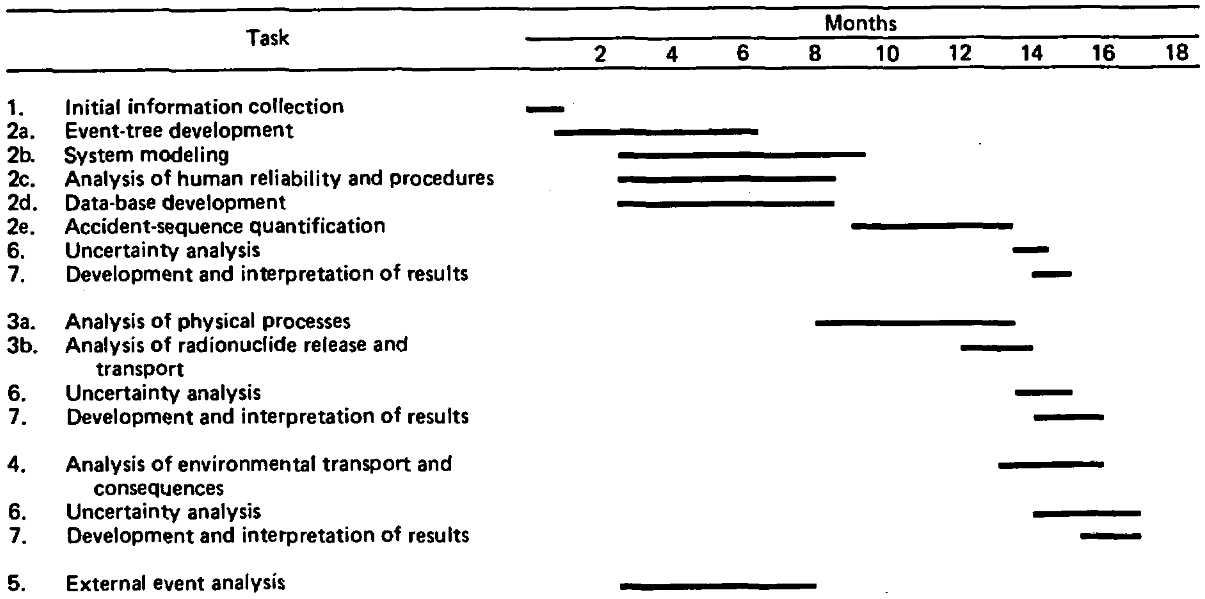


**Figure 2-3. Representative technical schedule. For report preparation and publication, another 7 months should be added.**

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

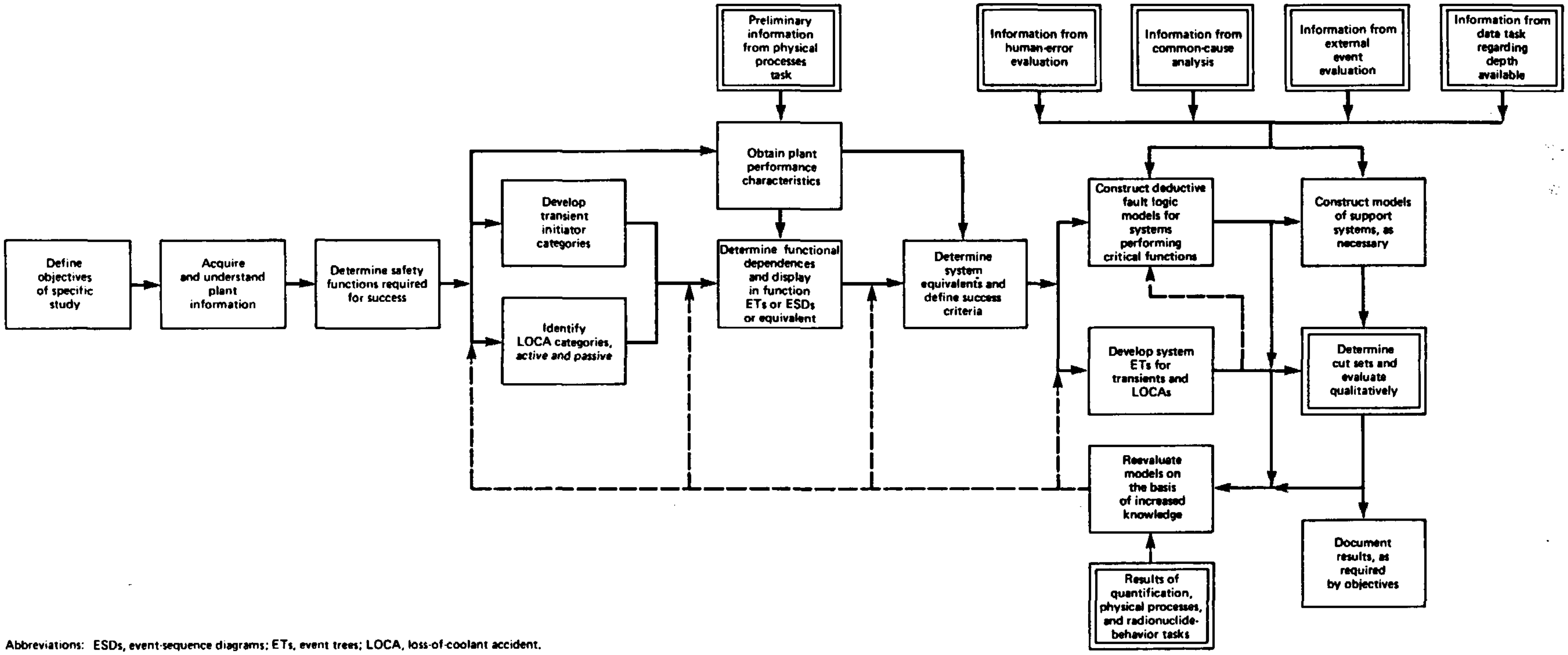
The first step in performing a probabilistic risk assessment is the task of accident-sequence definition and system modeling. This task begins with a definition of the objectives of the study and the acquisition of a substantial amount of information on plant design and operation. It progresses through 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


Preliminary information from physical processes task
Information from human-error evaluation
Information from common-cause analysis
Information from external event evaluation
Information from data task regarding depth available
Obtain plant performance characteristics
Develop transient initiator categories
Identify LOCA categories, *active and passive*
Define objectives of specific study
Acquire and understand plant information
Determine safety functions required for success
Determine functional dependences and display in function ETs or ESDs or equivalent
Determine system equivalents and define success criteria
Construct deductive fault logic models for systems performing critical functions
Construct models of support systems, as necessary
Develop system ETs for transients and LOCAs
Determine cut sets and evaluate qualitatively
Reevaluate models on the basis of increased knowledge
Results of quantification, physical processes, and radionuclide-behavior tasks
Document results, as required by objectives

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

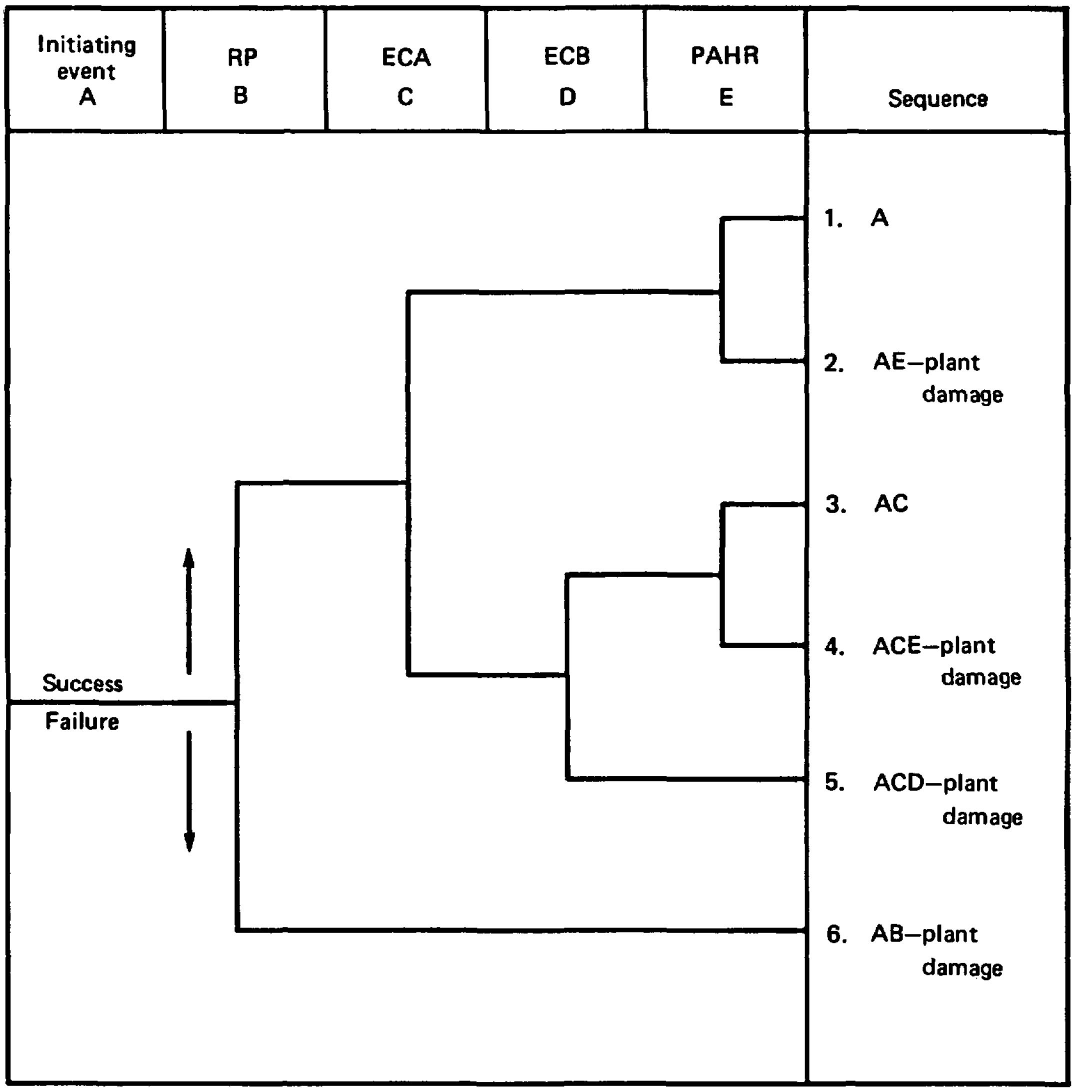


Figure 3-2. An example of a simple event tree. (See page 3-13 for an explanation of symbols.)

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.

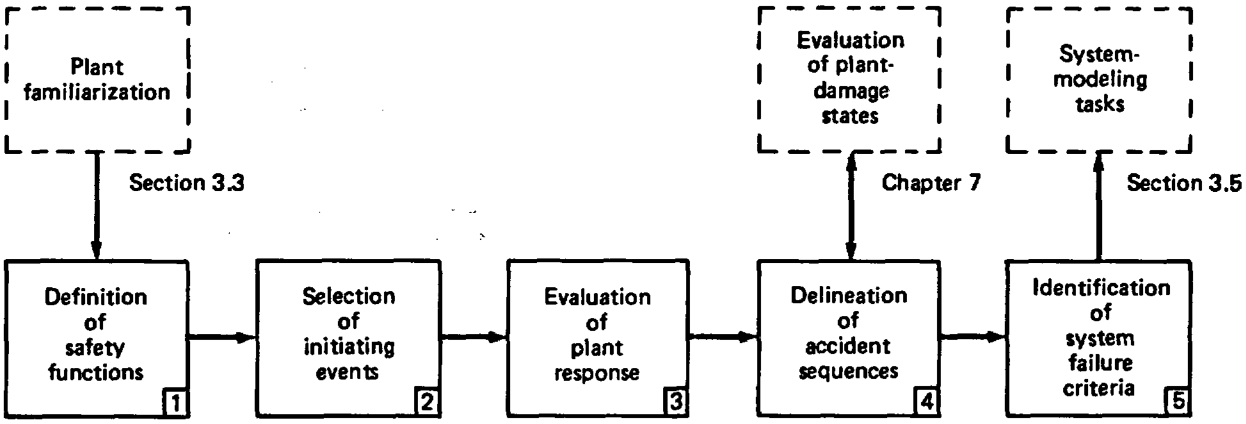

Plant familiarization
Section 3.3
Evaluation of plant-damage states
Chapter 7
System-modeling tasks
Section 3.5
Definition of safety functions
1
Selection of initiating events
2
Evaluation of plant response
3
Delineation of accident sequences
4
Identification of system failure criteria
5

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<br>Coolant recirculation and RHR injection line<br>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)<br>Water break | 1. Rapidly decreasing reactor water level<br>2. Rapidly decreasing reactor pressure<br>3. Drywell pressure unaffected | Rupture of RHR | Reactor scram on low water level | |
| FCV 74-47<br>Coolant recirculation and RHR return line<br>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)<br>Water break | See FCV 74-67 | Rupture of RHR | Reactor scram on low water level | |
| FCV 74-53<br>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)<br>Water break | See FCV 74-67 | Rupture of RHR | Reactor scram on low water level | |
| 13 PCVs<br>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)<br>Steam break | 1. Turbine-pressure regulator will attempt to control pressure<br>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

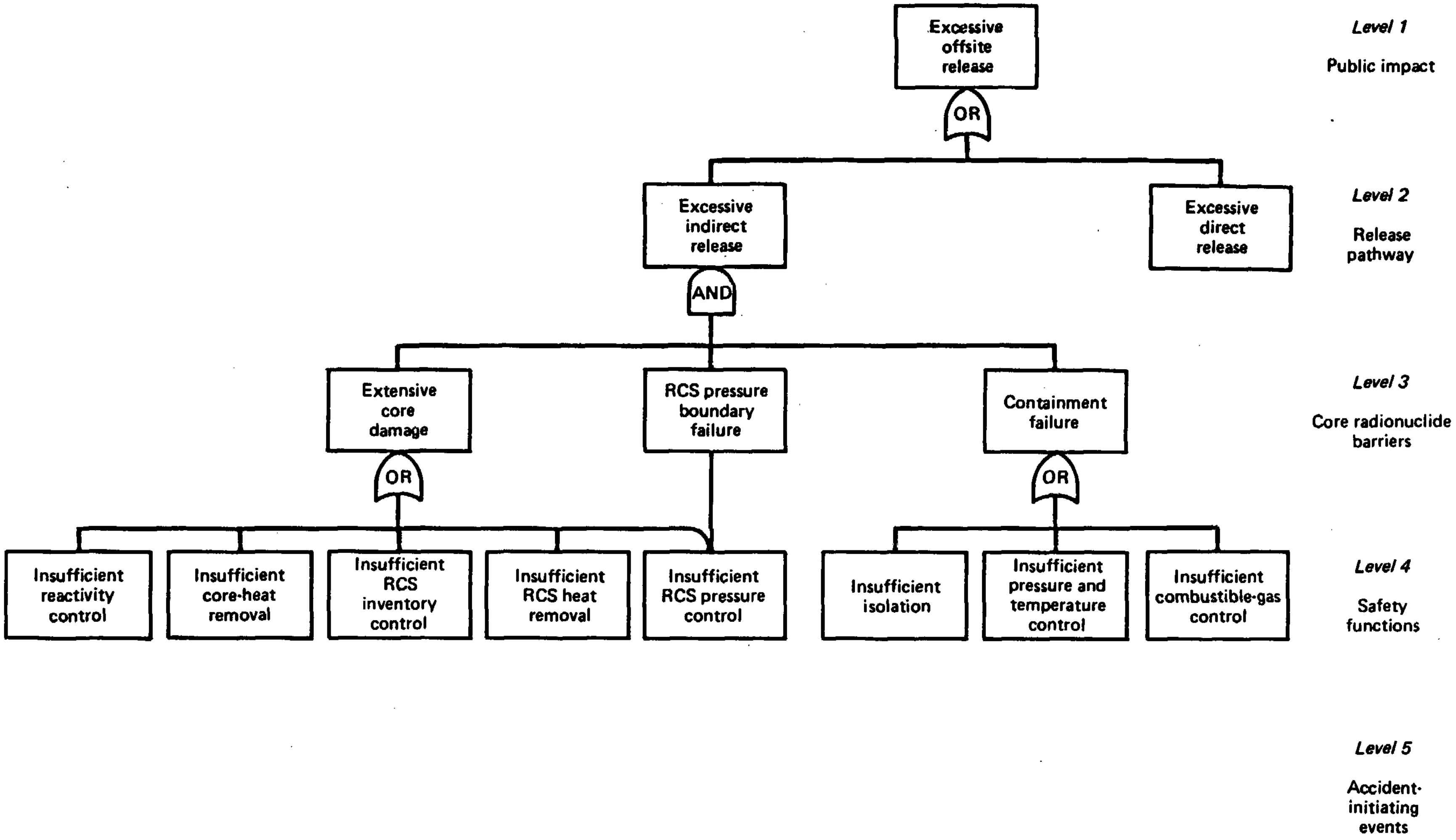

Excessive offsite release
OR
Excessive indirect release
Excessive direct release
AND
Extensive core damage
RCS pressure boundary failure
Containment failure
OR
OR
Insufficient reactivity control
Insufficient core-heat removal
Insufficient RCS inventory control
Insufficient RCS heat removal
Insufficient RCS pressure control
Insufficient isolation
Insufficient pressure and temperature control
Insufficient combustible-gas control
Level 1
Public impact
Level 2
Release pathway
Level 3
Core radionuclide barriers
Level 4
Safety functions
Level 5
Accident-initiating events

**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<br>2. Inadvertent opening of TBV | TBV power failure; momentary decrease in condenser vacuum; turbine pressure failure; ICS malfunction; increase in electrical demand |
| | 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.

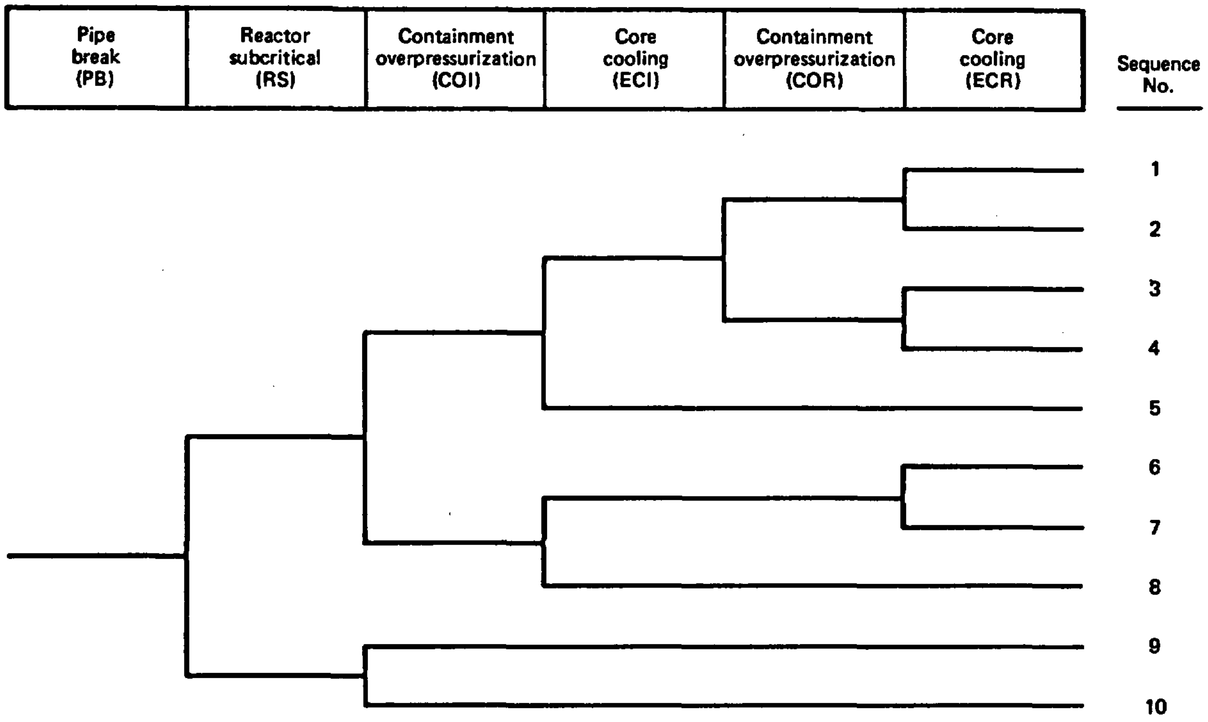
Function event trees are developed for each group of initiators because each group generates a distinctly different plant response. The function event tree is not an end product; it is an intermediate step that provides a baseline of information and permits a stepwise approach to sorting out the complex 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

| | | Coolant injection | | Coolant recirculation | |
|---|---|---|---|---|---|
| Break type and size | Reactor subcritical | 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<br>OR<br>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<br>OR<br>1 of 4 LPCI pumps<br>OR<br>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 | | | |
| | | | 2 of 2 core-spray loops<br>OR<br>1 of 2 core-spray loops and 1 of 4 LPCI pumps | | |
| Steam, 1.4 to 4.1 ft$^2$ | | | 2 of 2 core-spray loops<br>OR<br>4 of 4 LPCI pumps<br>OR<br>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.

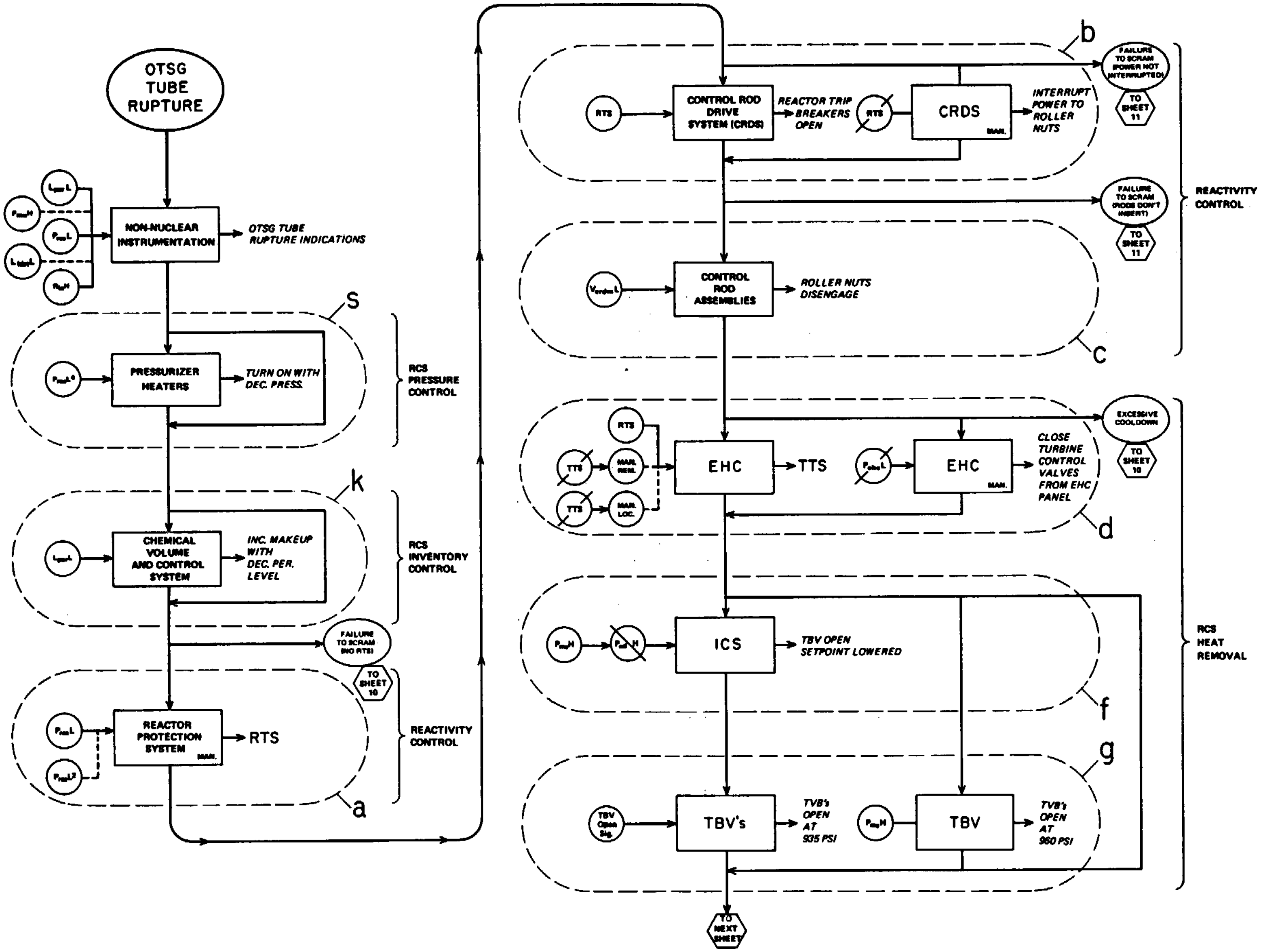


Figure 3-8. Excerpt from an event-sequence diagram.

### 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.

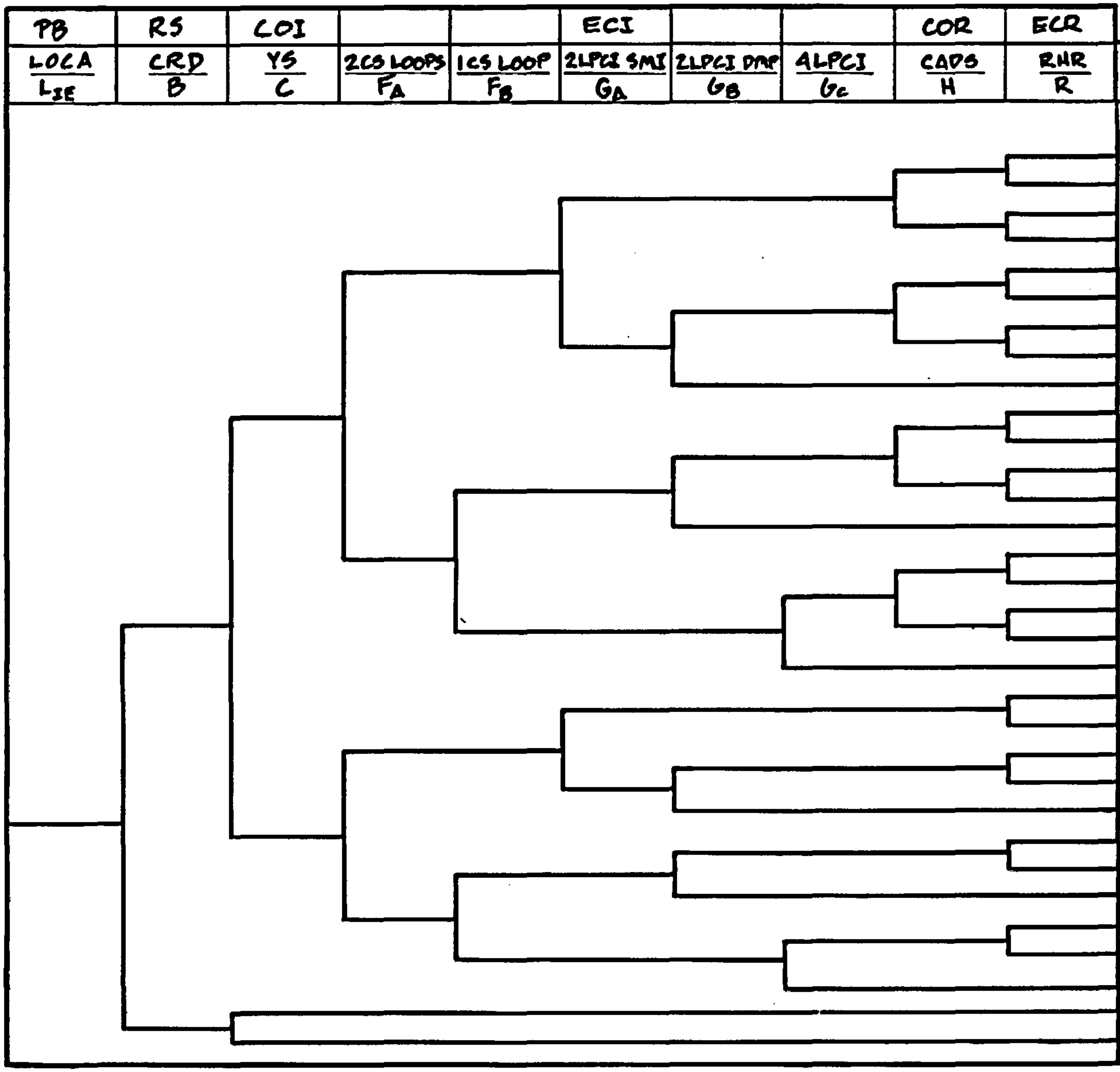
2. If an event-tree heading affects only one other heading, roll them together into a single heading.

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



| Seq. No. | Sequence | RS | COI | ECI | COR | ECA |
|---|---|---|---|---|---|---|
| 1 | $L_{IE}$ | | | | | |
| 2 | $L_{IE}R$ | | | | | X |
| 3 | $L_{IE}H$ | | | | X | |
| 4 | $L_{IE}HR$ | | | | X | X |
| 5 | $L_{IE}G_A$ | | | | | |
| 6 | $L_{IE}G_AR$ | | | | | X |
| 7 | $L_{IE}G_AH$ | | | | X | |
| 8 | $L_{IE}G_AHR$ | | | | X | X |
| 9 | $L_{IE}G_AG_B$ | | | X | N/A | N/A |
| 10 | $L_{IE}F_A$ | | | | | |
| 11 | $L_{IE}F_AR$ | | | | | X |
| 12 | $L_{IE}F_AH$ | | | | X | |
| 13 | $L_{IE}F_AHR$ | | | | X | X |
| 14 | $L_{IE}F_AG_B$ | | | X | N/A | N/A |
| 15 | $L_{IE}F_AF_B$ | | | | | |
| 16 | $L_{IE}F_AF_BR$ | | | | | X |
| 17 | $L_{IE}F_AF_BH$ | | | | X | |
| 18 | $L_{IE}F_AF_BHR$ | | | | X | X |
| 19 | $L_{IE}F_AF_BG_C$ | | | X | N/A | N/A |
| 20 | $L_{IE}C$ | | X | | N/A | |
| 21 | $L_{IE}CR$ | | X | | N/A | X |
| 22 | $L_{IE}CG_A$ | | X | | N/A | |
| 23 | $L_{IE}CG_AR$ | | X | | N/A | X |
| 24 | $L_{IE}CG_AG_B$ | | X | X | N/A | N/A |
| 25 | $L_{IE}CF_A$ | | X | | N/A | |
| 26 | $L_{IE}CF_AR$ | | X | | N/A | X |
| 27 | $L_{IE}CF_AG_B$ | | X | X | N/A | N/A |
| 28 | $L_{IE}CF_AF_B$ | | X | | N/A | |
| 29 | $L_{IE}CF_AF_BR$ | | X | | N/A | X |
| 30 | $L_{IE}CF_AF_BC$ | | X | X | N/A | N/A |
| 31 | $L_{IE}B$ | X | | | | X |
| 32 | $L_{IE}BC$ | X | | | N/A | X |

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.

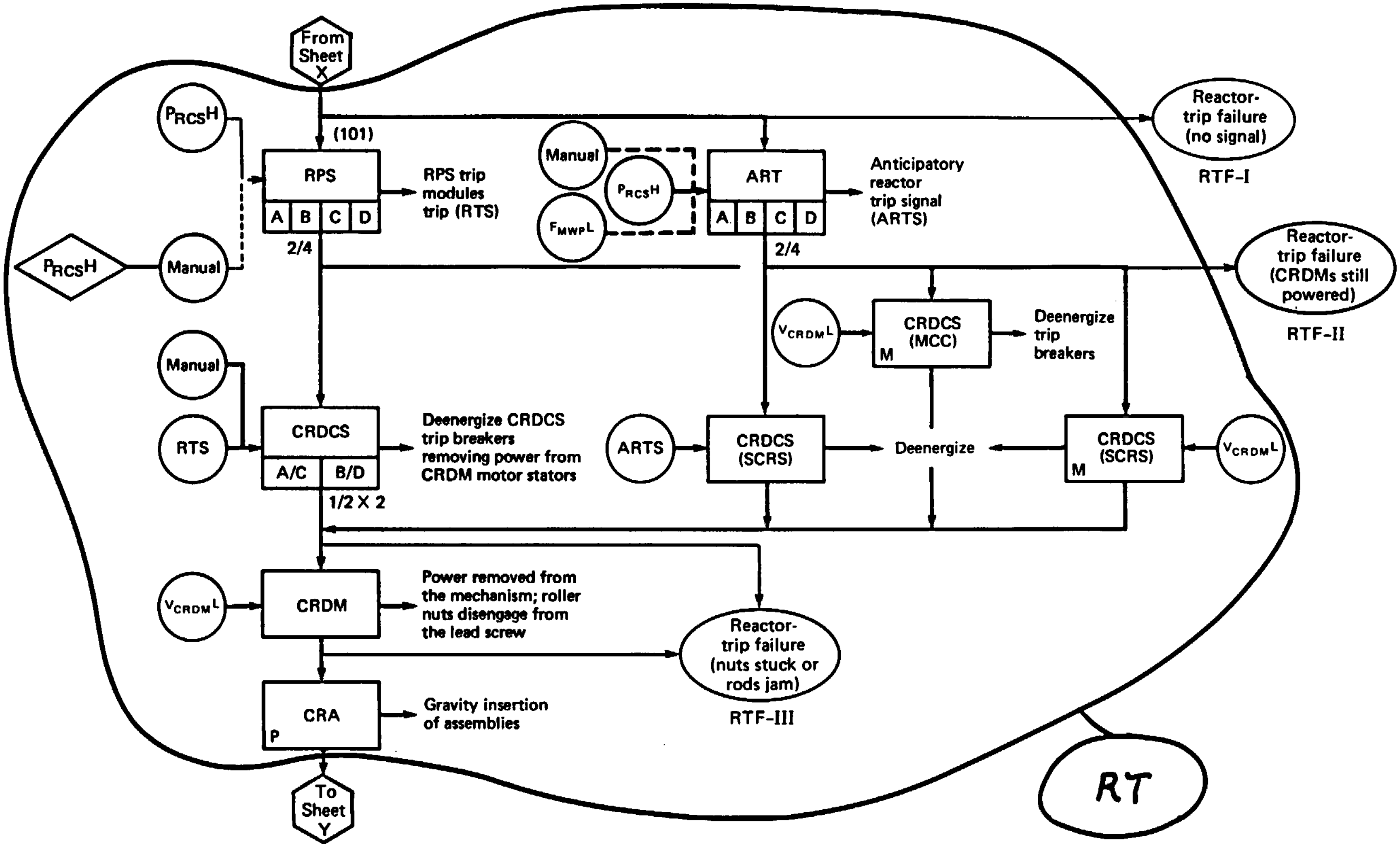
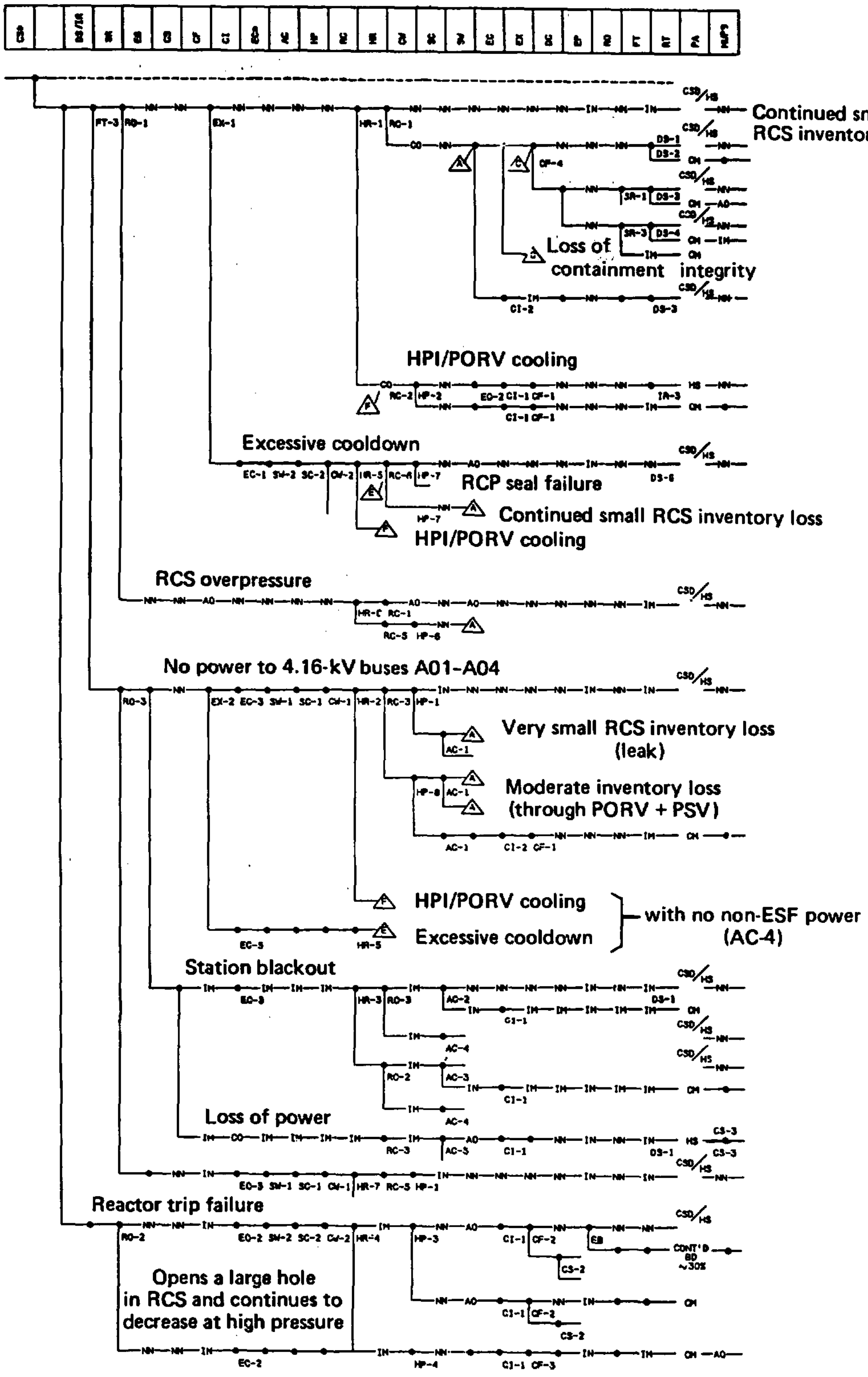

From Sheet X
(101)
$P_{RCS}H$
Manual
$P_{RCS}H$
RPS
A B C D
2/4
RPS trip modules trip (RTS)
Manual
$P_{RCS}H$
$F_{MWP}L$
ART
A B C D
2/4
Anticipatory reactor trip signal (ARTS)
Reactor-trip failure (no signal)
RTF-I
Reactor-trip failure (CRDMs still powered)
RTF-II
$V_{CRDM}L$
CRDCS (MCC)
M
Deenergize trip breakers
Manual
RTS
CRDCS
A/C B/D
1/2 X 2
Deenergize CRDCS trip breakers removing power from CRDM motor stators
ARTS
CRDCS (SCRS)
Deenergize
CRDCS (SCRS)
M
$V_{CRDM}L$
$V_{CRDM}L$
CRDM
Power removed from the mechanism; roller nuts disengage from the lead screw
Reactor-trip failure (nuts stuck or rods jam)
RTF-III
CRA
P
Gravity insertion of assemblies
To Sheet Y
RT

Figure 3–10. Reactor-trip actions.


Continued small RCS inventory loss
Loss of containment integrity
HPI/PORV cooling
Excessive cooldown
RCP seal failure
Continued small RCS inventory loss
HPI/PORV cooling
RCS overpressure
No power to 4.16-kV buses A01-A04
Very small RCS inventory loss (leak)
Moderate inventory loss (through PORV + PSV)
HPI/PORV cooling
Excessive cooldown
with no non-ESF power (AC-4)
Station blackout
Loss of power
Reactor trip failure
Opens a large hole in RCS and continues to decrease at high pressure

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

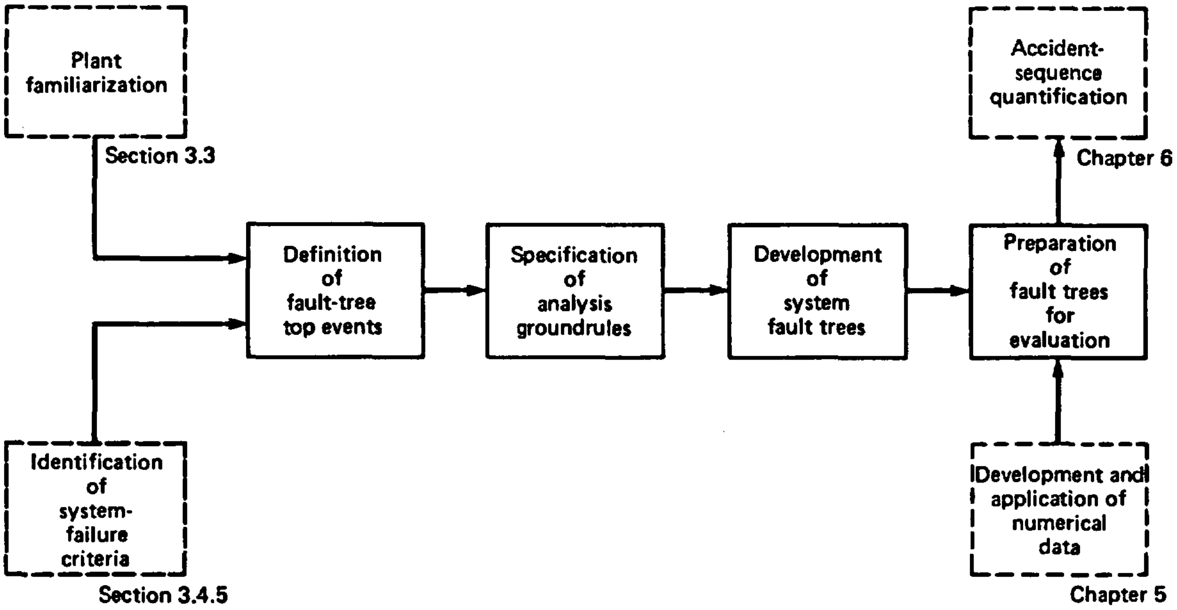

Plant familiarization
Section 3.3
Accident-sequence quantification
Chapter 6
Definition of fault-tree top events
Specification of analysis groundrules
Development of system fault trees
Preparation of fault trees for evaluation
Identification of system-failure criteria
Section 3.4.5
Development and application of numerical data
Chapter 5

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.

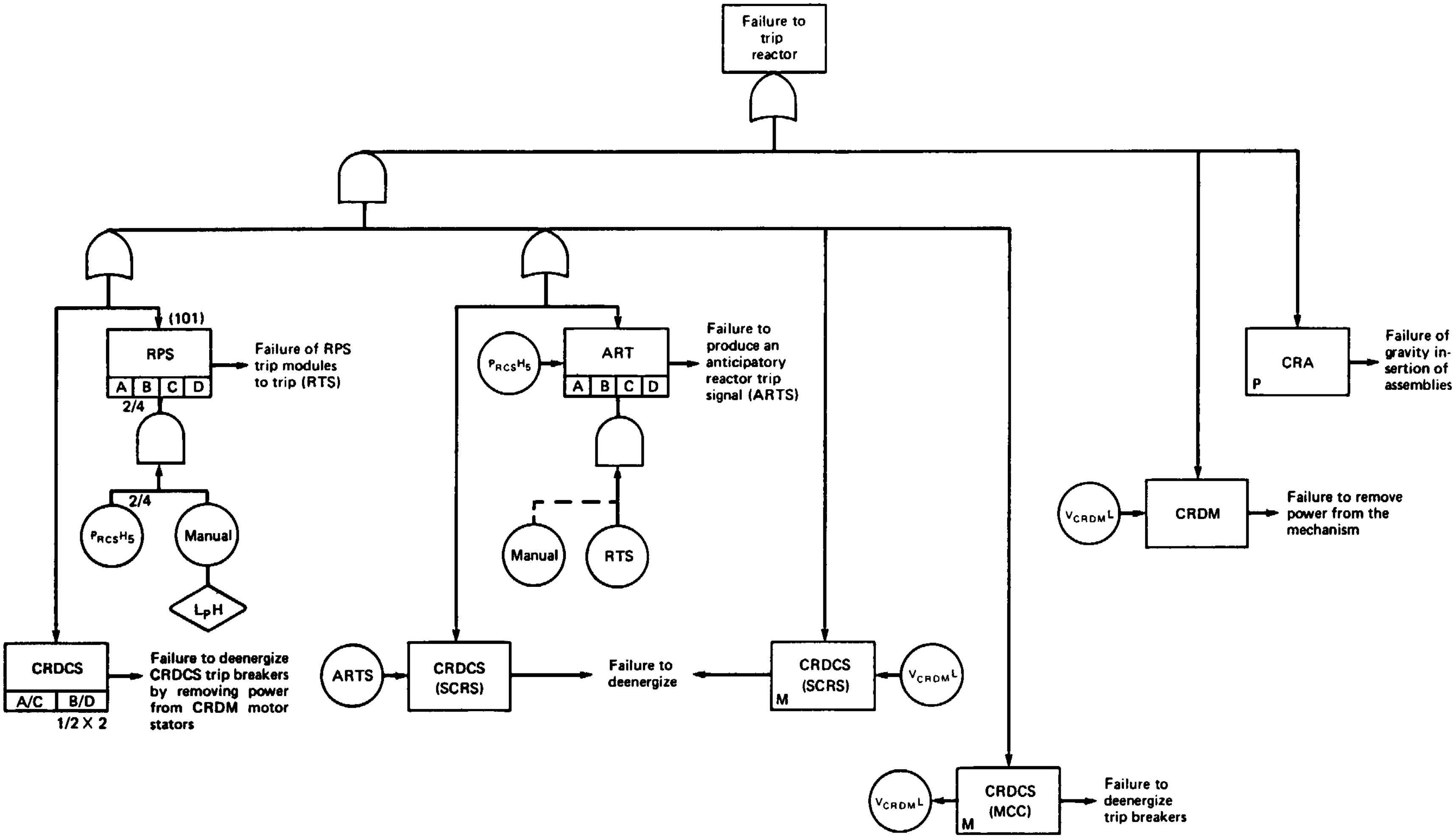

Failure to trip reactor
(101)
RPS
A B C D
2/4
Failure of RPS trip modules to trip (RTS)
2/4
$P_{RCS}H_5$
Manual
$L_pH$
$P_{RCS}H_5$
ART
A B C D
Failure to produce an anticipatory reactor trip signal (ARTS)
Manual
RTS
CRA
P
Failure of gravity insertion of assemblies
$V_{CRDM}L$
CRDM
Failure to remove power from the mechanism
CRDCS
A/C
B/D
1/2 X 2
Failure to deenergize CRDCS trip breakers by removing power from CRDM motor stators
ARTS
CRDCS (SCRS)
Failure to deenergize
CRDCS (SCRS)
M
$V_{CRDM}L$
$V_{CRDM}L$
CRDCS (MCC)
M
Failure to deenergize trip breakers

**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 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| System | Div. | Comp. | System | Div. | Component | Failure mode | Fault effect | Detection | Diagnostics | Comments |
| 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.

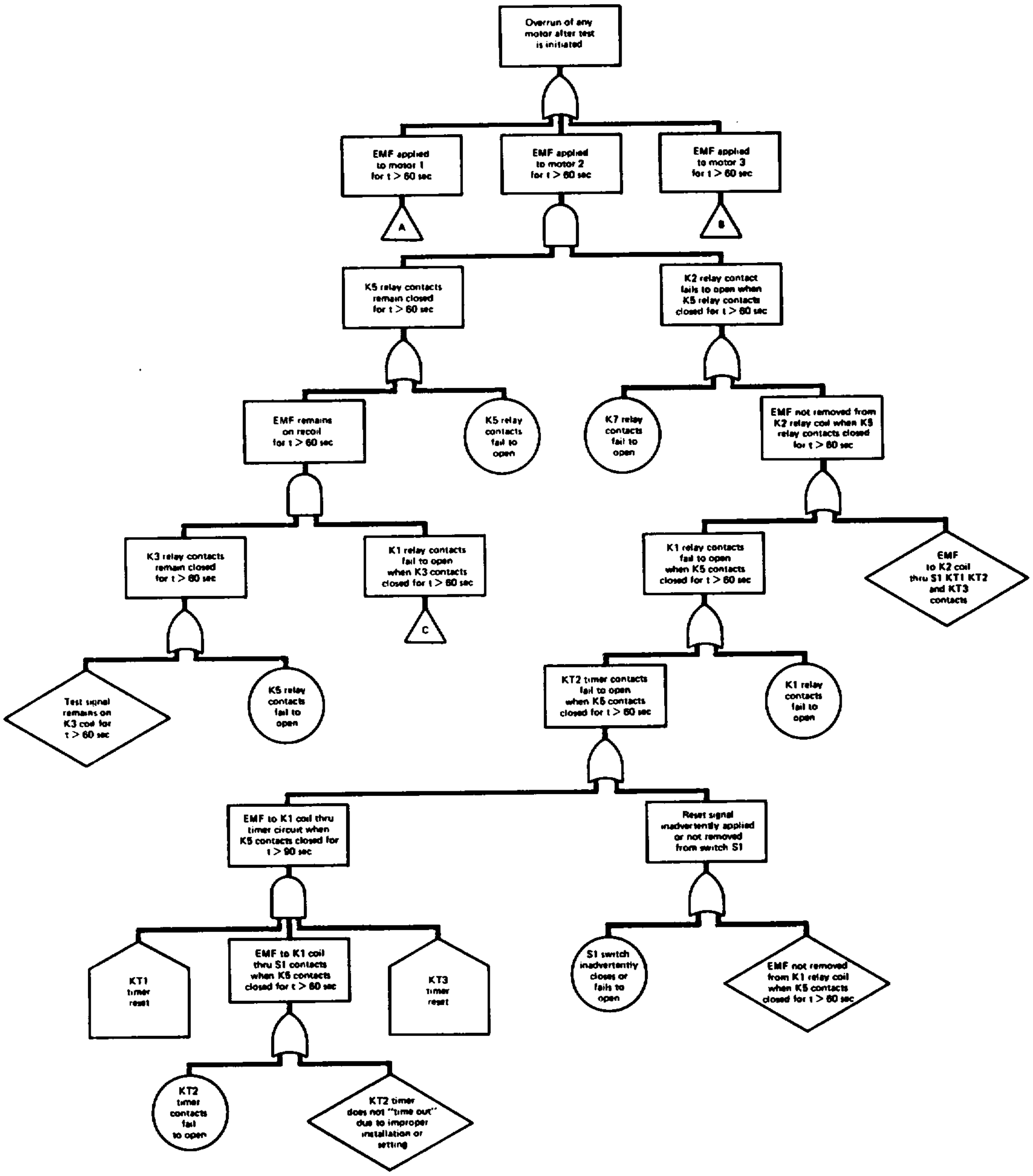
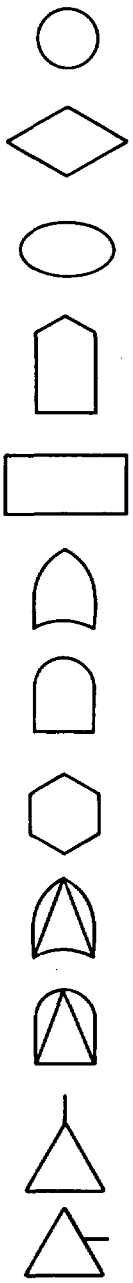

Overrun of any motor after test is initiated
EMF applied to motor 1 for t > 60 sec
EMF applied to motor 2 for t > 60 sec
EMF applied to motor 3 for t > 60 sec
A
B
K5 relay contacts remain closed for t > 60 sec
K2 relay contact fails to open when K5 relay contacts closed for t > 60 sec
EMF remains on recoil for t > 60 sec
K5 relay contacts fail to open
K7 relay contacts fail to open
EMF not removed from K2 relay coil when K5 relay contacts closed for t > 60 sec
K3 relay contacts remain closed for t > 60 sec
K1 relay contacts fail to open when K3 contacts closed for t > 60 sec
C
K1 relay contacts fail to open when K5 contacts closed for t > 60 sec
EMF to K2 coil thru S1 KT1 KT2 and KT3 contacts
Test signal remains on K3 coil for t > 60 sec
K5 relay contacts fail to open
KT2 timer contacts fail to open when K5 contacts closed for t > 60 sec
K1 relay contacts fail to open
EMF to K1 coil thru timer circuit when K5 contacts closed for t > 90 sec
Reset signal inadvertently applied or not removed from switch S1
KT1 timer reset
EMF to K1 coil thru S1 contacts when K5 contacts closed for t > 60 sec
KT3 timer reset
S1 switch inadvertently closes or fails to open
EMF not removed from K1 relay coil when K5 contacts closed for t > 60 sec
KT2 timer contacts fail to open
KT2 timer does not "time out" due to improper installation or setting

**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.

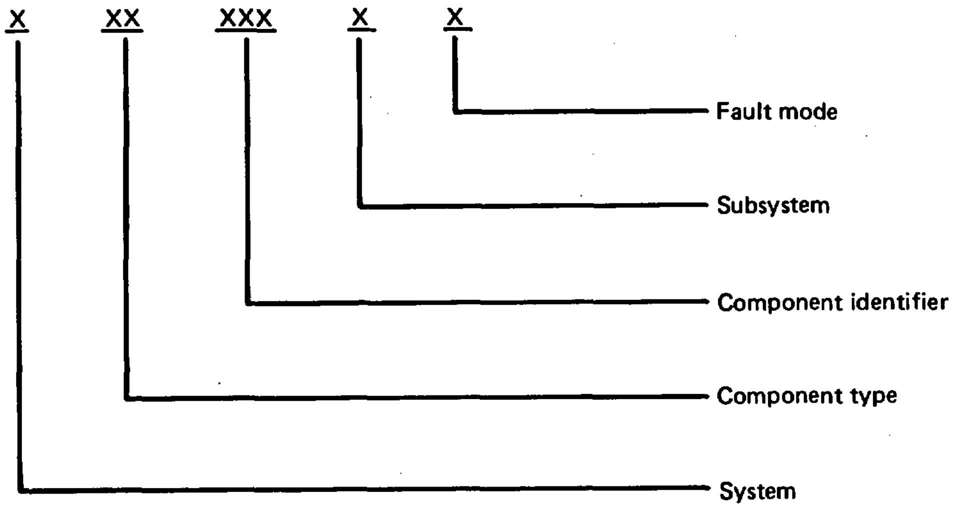


Figure 3-17. Event-naming code.

### 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.

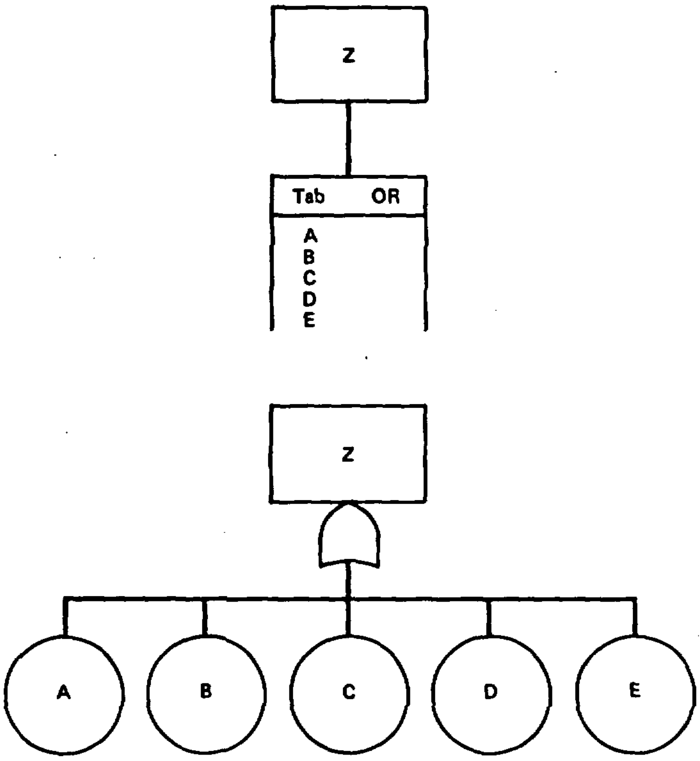


**Figure 3-19. The tabular OR gate (top) and the equivalent fault-tree arrangement.**

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 (deenergize 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 (deenergize 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 comparison 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.

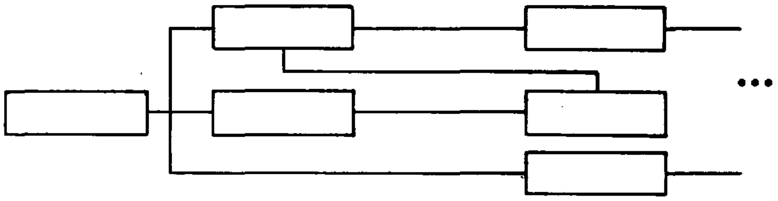
When used in the PRA process, the intent of the RBD is to combine, either directly or using the fault-tree logic as input, similar components that are in series in each system train into one supercomponent and then link together parallel supercomponents to form a summary model of the system. The selection 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.

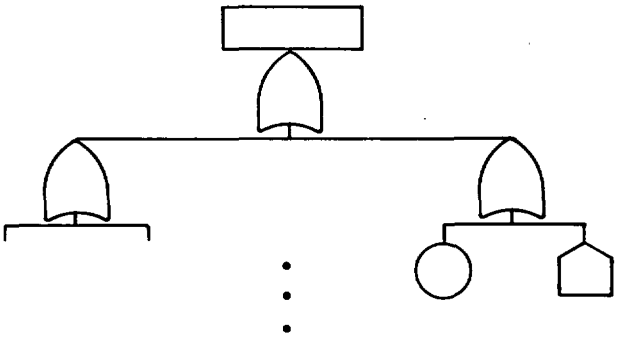
Information about what could possibly cause the failure of all components in a failure set or cut set can be summarized in a cause table. The conceptual form of this table is shown in Figure 3-21. One cause-table page is made for each order of failure set and for each boundary condition on the system. 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) $\{A, B\},\{K, L, M\}\ldots$

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 tounded.

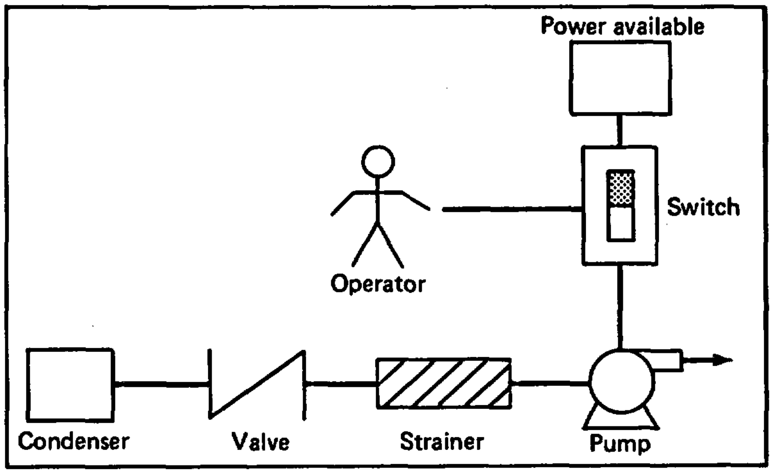


**Figure 3-22. A simplified system for a GO model.**

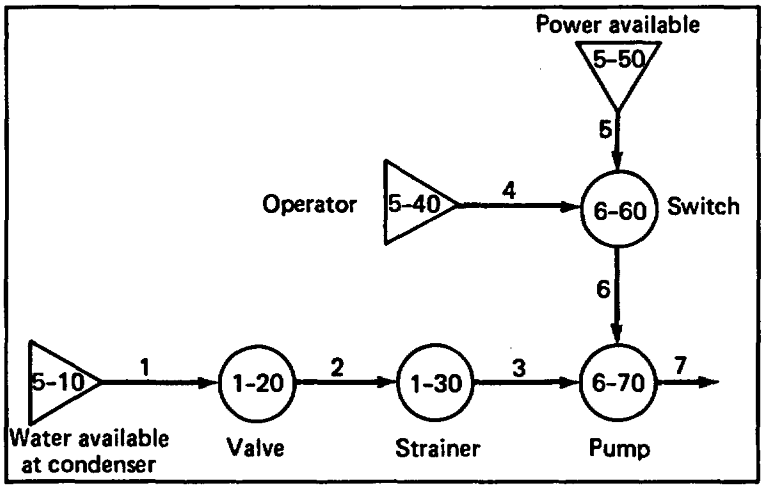


**Figure 3-23. The GO chart for the system shown in Figure 3-22. See page 3-61 for an explanation of the numbers.**

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.

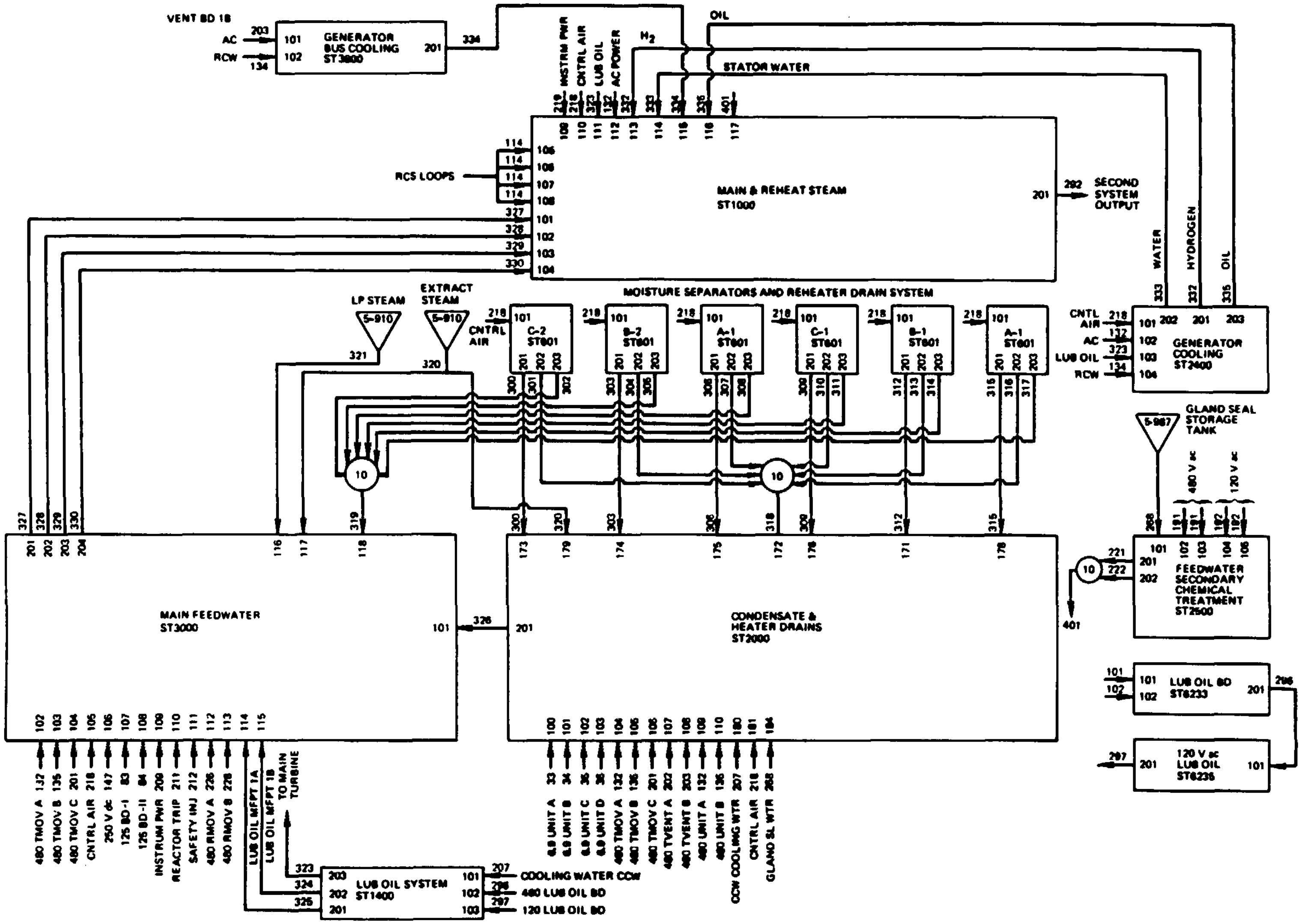


Figure 3-24. GO model for a PWR secondary loop system. Systems are shown as blocked supertypes, with only inputs and outputs showing interfaces depicted. The equipment in the supertypes has been previously modeled by means of elemental GO operators.

### 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.

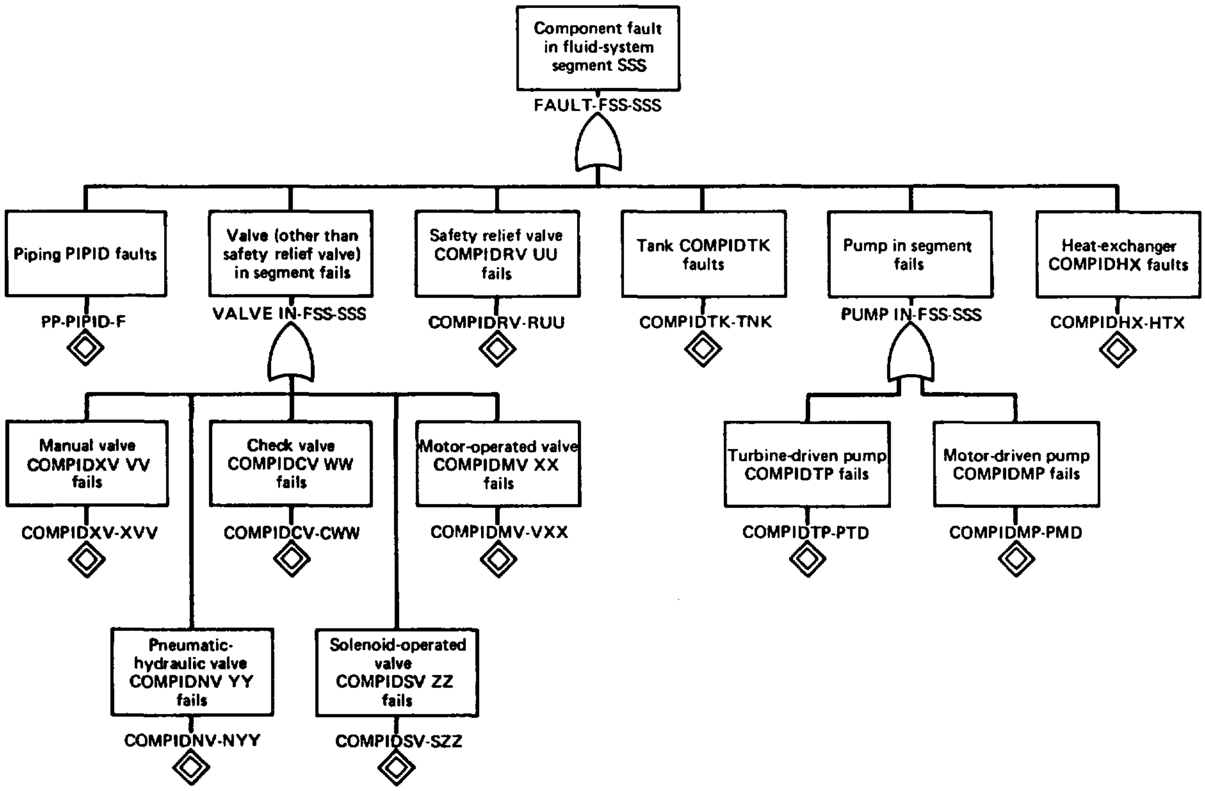

Component fault in fluid-system segment SSS
FAULT-FSS-SSS
Piping PIPID faults
PP-PIPID-F
Valve (other than safety relief valve) in segment fails
VALVE IN-FSS-SSS
Safety relief valve COMPIDRV UU fails
COMPIDRV-RUU
Tank COMPIDTK faults
COMPIDTK-TNK
Pump in segment fails
PUMP IN-FSS-SSS
Heat-exchanger COMPIDHX faults
COMPIDHX-HTX
Manual valve COMPIDXV VV fails
COMPIDXV-XVV
Check valve COMPIDCV WW fails
COMPIDCV-CWW
Motor-operated valve COMPIDMV XX fails
COMPIDMV-VXX
Turbine-driven pump COMPIDTP fails
COMPIDTP-PTD
Motor-driven pump COMPIDMP fails
COMPIDMP-PMD
Pneumatic-hydraulic valve COMPIDNV YY fails
COMPIDNV-NYY
Solenoid-operated valve COMPIDSV ZZ fails
COMPIDSV-SZZ

**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

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

In other words, the frequency of concurrent failure events A and B, $\phi$(A 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. <u>Common-mode failures</u>* are multiple, concurrent, and dependent failures of identical equipment that fails in the same mode. <u>Propagating</u>

*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

| | | | Applicability to steps in risk analysis | | | |
|---|---|---|---|---|---|---|
| Category | | Method | 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. | WAMCOME[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.

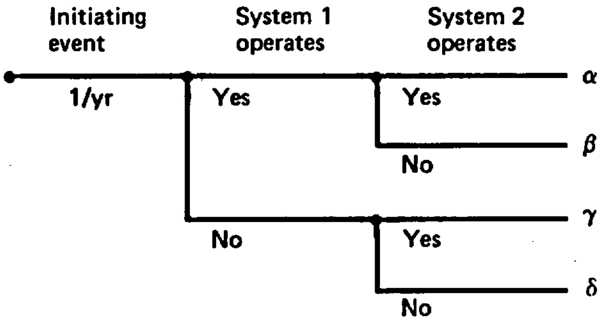
*See Section 6.6 for a description of the computer codes discussed here.

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

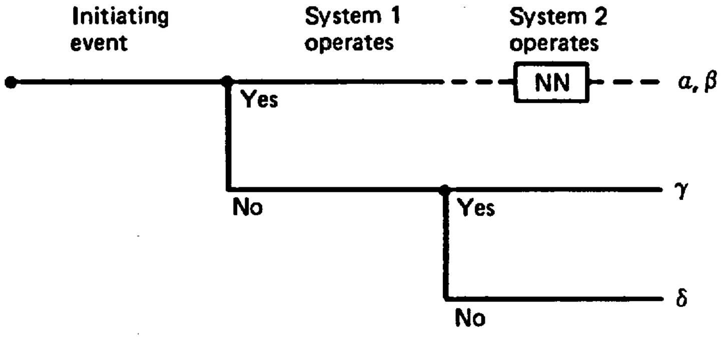
| | | Dependent-failure type | | | | | |
|---|---|---|---|---|---|---|---|
| | Method | Common-cause initiating events 1 | Intersystem functional dependences 2A | Intersystem shared equipment 2B | Intersystem physical interactions 2C | Intersystem human interactions 2D | Inter-component dependences 3 |
| 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

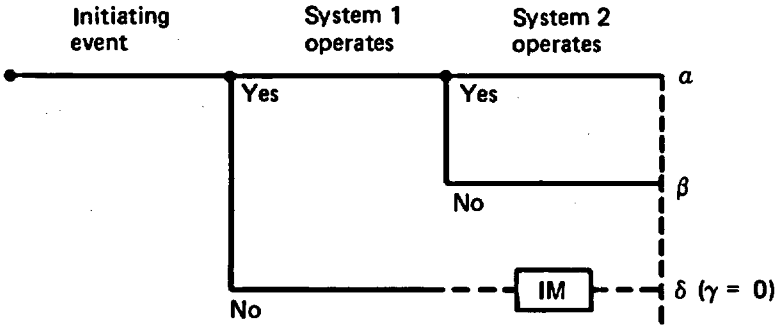
The four types of intersystem dependences (types 2A, 2B, 2C, and 2D) can be analyzed by means of event trees, fault trees, or a combination of them. The variety of approaches available can be explained in terms of a simple event tree:



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:

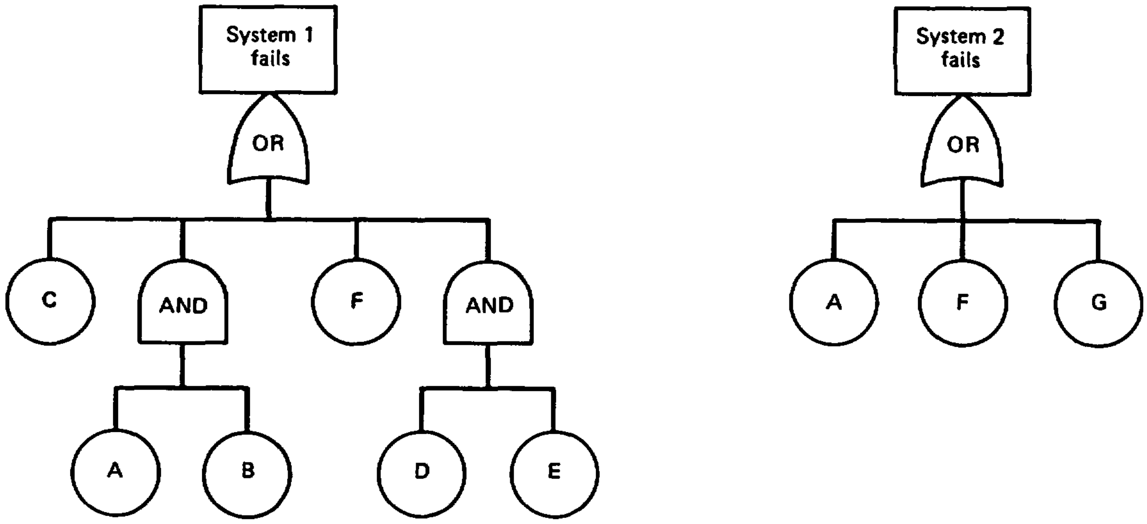


where NN denotes "not needed." Another example of a functional dependence is the case where system 2 can operate only in conjunction with the successful operation of system 1. Such a condition could result from some physical interaction (type 2C) that takes place when system 1 fails. It is reflected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

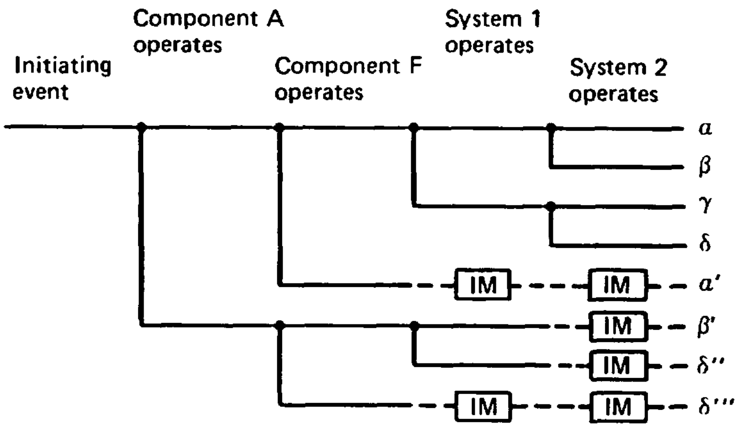


where IM denotes "impossible."

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 $\delta$" 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 $\delta$ 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 $\gamma$, 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 $\gamma$ 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

$$\begin{aligned}\gamma &= 1 \text{ AND } 2\\ &= \left[(A \text{ AND } B) \text{ OR } C \text{ OR } (D \text{ AND } E) \text{ OR } F\right] \text{ AND } (\overline{A \text{ OR } F \text{ OR } G})\end{aligned}$$

After Boolean reduction, the logic is simplified to the form

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

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

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

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 $\gamma$ 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 $\gamma$.

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 tradeoff 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

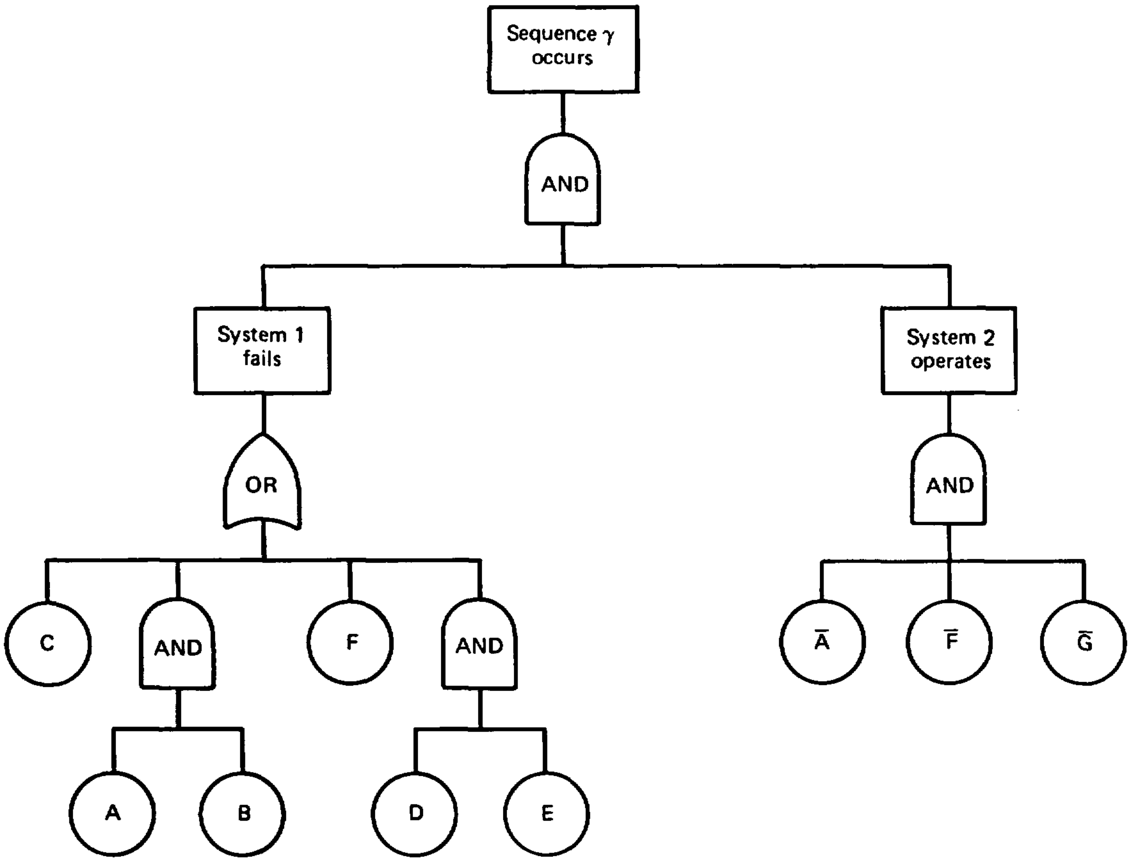


**Figure 3-26. Hypothetical fault tree for sequence γ. Here X denotes failure; $\bar{X}$ denotes the successful functioning of the component.**

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

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

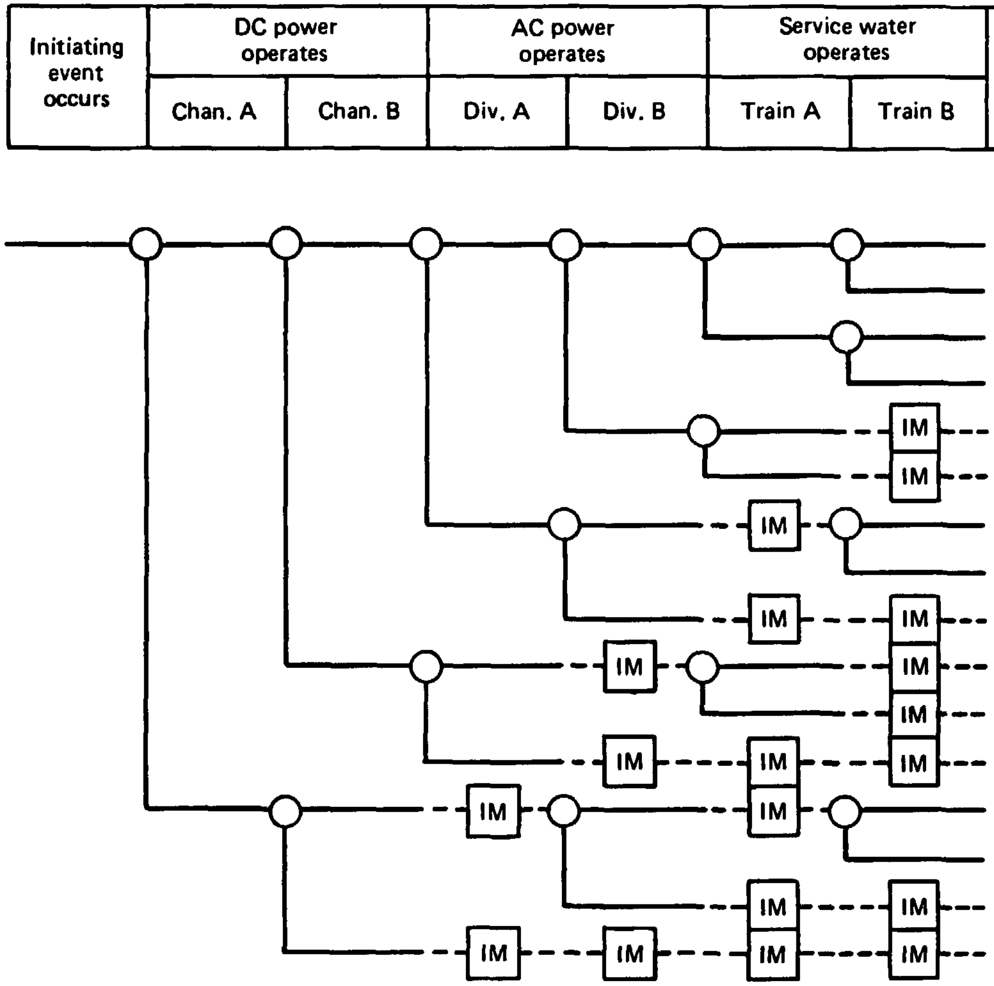
where $\phi(I_k | iE)$ is the total frequency of unique impact vector k given the initiating event occurs and $\phi(I_{jk} | iE)$ is the frequency of the $j^{th}$ event sequence, whose impact vector is identical with $I_k$ given the initiating event occurs.

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 $\ell$ 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 $\ell$ 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



| Sequence |  Sequence impact vector |  |  |  |  |  | Support-system state |  Unique impact vector |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | ECCS |  | AFWS |  | FC |  |  | ECCS |  | AFWS |  | FC |  |
|  | A | B | A | B | A | B |  | A | B | A | B | A | B |
| j |  |  |  |  |  |  | k |  |  |  |  |  |  |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 1 | 0 | 1 | 2 | 0 | 1 | 0 | 1 | 0 | 1 |
| 3 | 1 | 0 | 1 | 0 | 1 | 0 | 3 | 1 | 0 | 1 | 0 | 1 | 0 |
| 4 | 1 | 1 | 1 | 1 | 1 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 1 |
| 5 | 0 | 1 | 0 | 1 | 0 | 1 |  |  |  |  |  |  |  |
| 6 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 7 | 1 | 0 | 1 | 0 | 1 | 0 |  |  |  |  |  |  |  |
| 8 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 9 | 0 | 1 | 0 | 1 | 0 | 1 |  |  |  |  |  |  |  |
| 10 | 0 | 1 | 0 | 1 | 0 | 1 |  |  |  |  |  |  |  |
| 11 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 12 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 13 | 1 | 0 | 1 | 0 | 1 | 0 |  |  |  |  |  |  |  |
| 14 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 15 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |
| 16 | 1 | 1 | 1 | 1 | 1 | 1 |  |  |  |  |  |  |  |

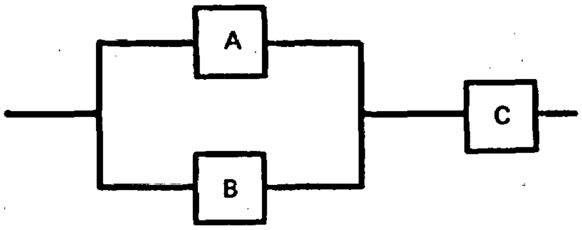
**Figure 3-27. A support-system event tree with impact vectors.**

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 x $10^{-3}$ 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.

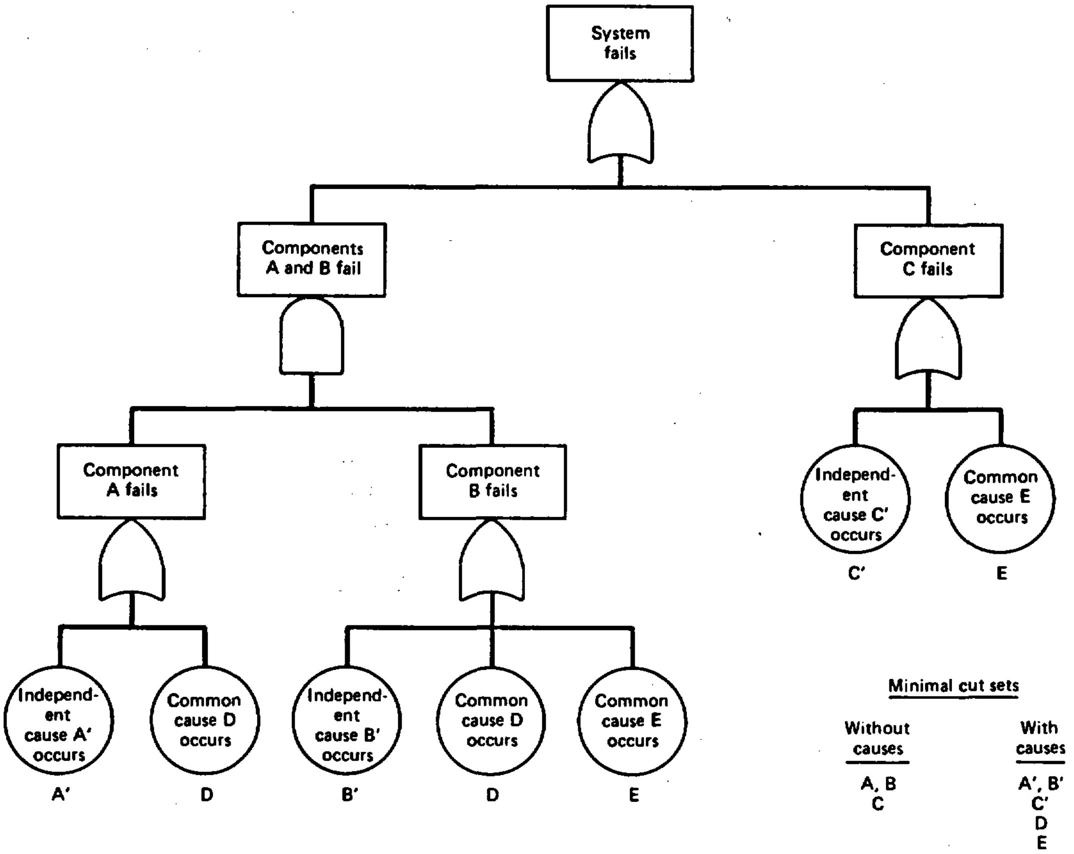


**Figure 3-28. Fault tree for a three-component system with independent and common causes.**

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]

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

[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 $\lambda_i$ is the unit failure rate for independent failures and $\lambda_c$ 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

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

where $\lambda_d$ is the failure-on-demand probability for a single unit and $\beta_d$ 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 $\beta_d$ and $\lambda_d$ 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 $\mu_1$ is the (constant) repair rate of single unit when one unit is failed, $\mu_2$ is the (constant) repair rate of both units when the system is failed, and $\lambda$ and $\beta$ 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 ($\beta$) is not necessarily equal to the beta factor for the failure to start on demand ($\beta_d$).

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 $\beta$. 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

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

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

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 $\beta$ 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

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

where $\lambda_1$ is the single-unit failure rate, $\underset{\sim}{x}$ = (1,0) or (0,1), and $\lambda_2$ 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 $\lambda_x$ depend only on the number of units failed. Each unit can fail individually with a constant failure rate $\lambda$. "Common-cause shocks are assumed to hit the system at random times. The time between shocks is exponentially distributed, with constant occurrence rate $\mu$. 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, $\lambda$, 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 $\mu$. The shock rate $\mu$ 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, $\lambda_1$, 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

$$\lambda_i = \mu\left[\binom{m}{i} p^i q^{m-1}\right] \qquad \text{for } i = 2, m \tag{3-8}$$

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:

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

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

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)

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

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:

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

With $\lambda_1$, $\lambda_+$, and p, an estimate for $\mu$ 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:

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

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

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

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

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

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 $\beta$. 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.

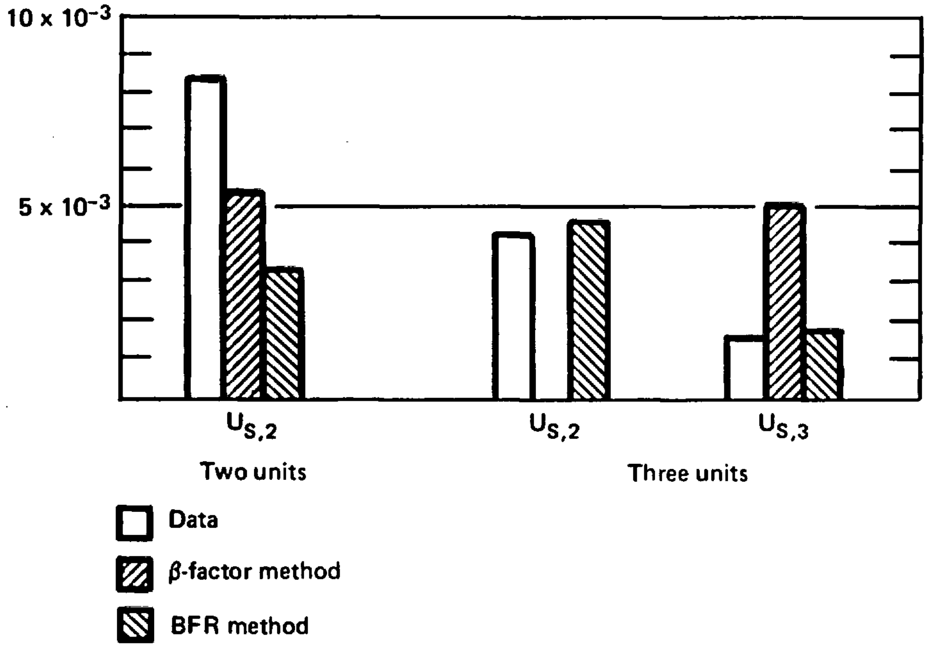


Figure 3-29. Estimated $U_{S,2}$ and $U_{S,3}$ in two- and three-unit systems.

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]

| | | Intersystem dependences | | | | Intercomponent dependences | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 2A | 2B | 2C | 2D | 3A | 3B | 3C | 3D |
| Method of analysis | Common-cause initiators | Functional dependences | Shared equipment | Physical inter-actions | Human inter-actions | Functional dependences | Shared equipment | Physical inter-actions | Human inter-actions |
| 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)<br>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)<br>Human-reliability analysis (e) |
| 3. | Intercomponent dependences | Fault-tree and cause-table analysis (c and d)<br>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

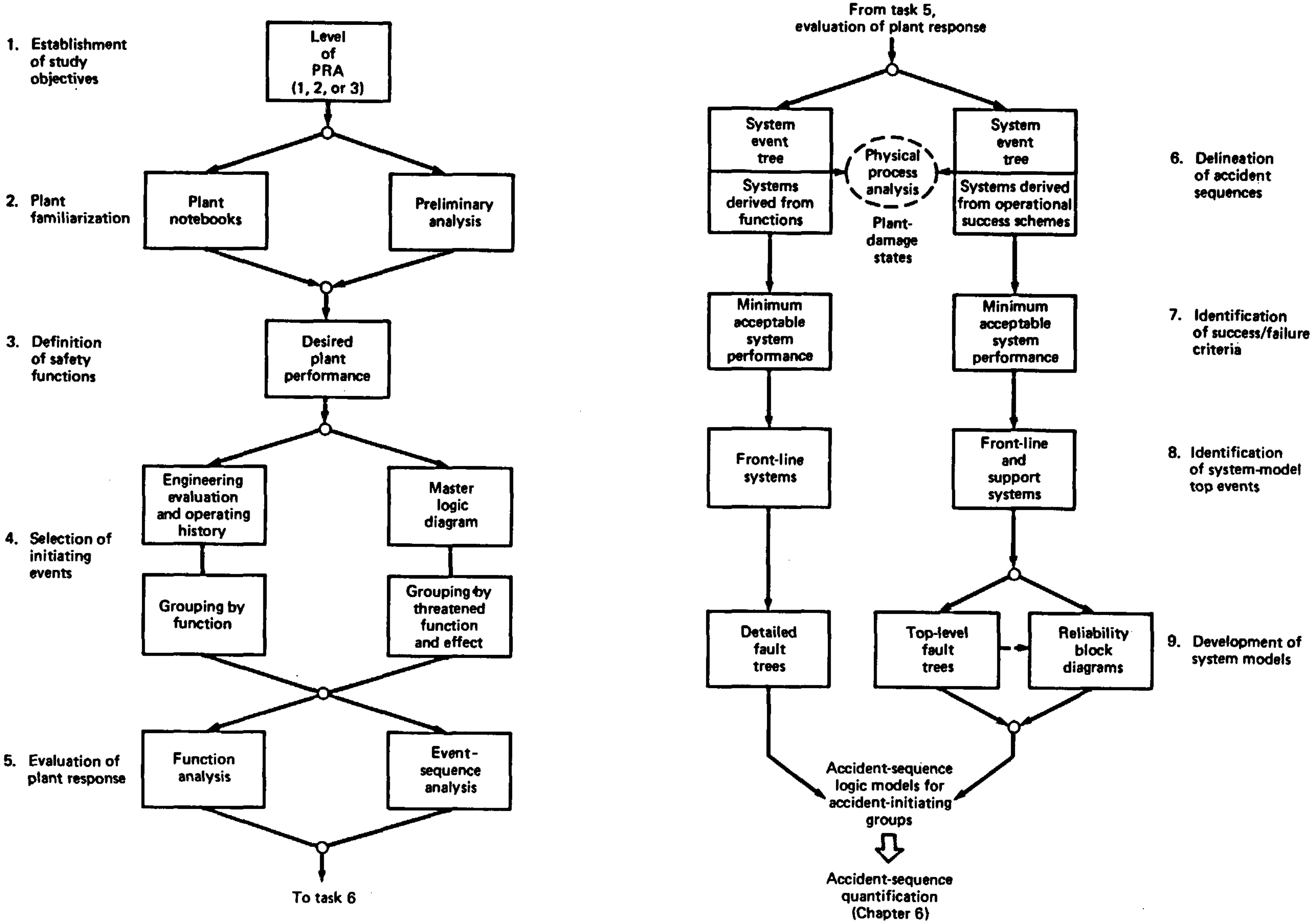

1. Establishment of study objectives
Level of PRA (1, 2, or 3)
2. Plant familiarization
Plant notebooks
Preliminary analysis
3. Definition of safety functions
Desired plant performance
4. Selection of initiating events
Engineering evaluation and operating history
Master logic diagram
Grouping by function
Grouping by threatened function and effect
5. Evaluation of plant response
Function analysis
Event-sequence analysis
To task 6
From task 5, evaluation of plant response
System event tree
Systems derived from functions
Physical process analysis
Plant-damage states
System event tree
Systems derived from operational success schemes
6. Delineation of accident sequences
Minimum acceptable system performance
Minimum acceptable system performance
7. Identification of success/failure criteria
Front-line systems
Front-line and support systems
8. Identification of system-model top events
Detailed fault trees
Top-level fault trees
Reliability block diagrams
9. Development of system models
Accident-sequence logic models for accident-initiating groups
Accident-sequence quantification (Chapter 6)

**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.