

NUREG/CR-4350/1 of 7

SAND85-1495/1 of 7

RG

Printed August 1985

Probabilistic Risk Assessment Course Documentation

Volume 1: PRA Fundamentals

Roger J. Breeding, Timothy J. Leahy, Jonathan Young

Wallis R. Cramond, Project Coordinator

Prepared by

Sandia National Laboratories

Albuquerque, New Mexico 87185 and Livermore, California 94550

for the United States Department of Energy

under Contract DE-AC04-76DP00789

8512270366 850831
PDR NUREG
CR-4350 R PDR

**Prepared for
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 or 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.

Available from
Superintendent of Documents
U.S. Government Printing Office
Post Office Box 37082
Washington, D.C. 20013-7982
and
National Technical Information Service
Springfield, VA 22161

NUREG/CR-4350/1 of 7
SAND85-1495/1 of 7
RG

PROBABILISTIC RISK ASSESSMENT COURSE DOCUMENTATION
VOLUME 1: PRA FUNDAMENTALS

Roger J. Breeding
Timothy J. Leahy
Jonathan Young

Energy Incorporated
Seattle, Washington

Project Coordinator: Wallis R. Cramond

August 1985

Work Performed Under Contract 50-5107
for
Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
for the
U.S. Department of Energy

Prepared for
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A-1321

PREFACE

This series of publications is the course documentation for the primary topics taught in the Probabilistic Risk Assessment Technology Transfer Program during 1982 through 1984. These volumes represent an integrated set of subjects developed from course notes and classroom presentations with student and peer review feedback. The topics included in this series are:

- Volume 1 - PRA Fundamentals
- Volume 2 - Probability and Statistics for PRA Applications
- Volume 3 - System Reliability and Analysis Techniques,
Session A - Reliability
- Volume 4 - System Reliability and Analysis Techniques,
Sessions B & C - Event Trees/Fault Trees
- Volume 5 - System Reliability and Analysis Techniques,
Session D - Quantification
- Volume 6 - Data Development
- Volume 7 - Environmental Transport and Consequence Analysis

The material contained in this series is not intended to be a stand alone set of text books for self-instruction but rather it is designed for use in the classroom or for independent study.

The content of this series does not necessarily reflect the views or policies of the U.S. Nuclear Regulatory Commission or Sandia National Laboratories, nor does mention of trade names, commercial products, or organizations imply endorsement by Sandia or the U.S. NRC or any other agency of the U. S. Government.

ABSTRACT

The full range of PRA topics is presented, with a special emphasis on systems analysis and PRA applications. Systems analysis topics include system modeling such as fault tree and event tree construction, failure rate data, and human reliability. The discussion of PRA applications is centered on past and present PRA based programs, such as WASH-1400 and the Interim Reliability Evaluation Program, as well as on some of the potential future applications of PRA. The relationship of PRA to generic safety issues such as station blackout and Anticipated Transient Without Scram (ATWS) is also discussed.

In addition to system modeling, the major PRA tasks of accident process analysis, and consequence analysis are presented. An explanation of the results of these activities, and the techniques by which these results are derived, forms the basis for a discussion of these topics. An additional topic which is presented in this course is the topic of PRA management, organization, and evaluation. This discussion explains the relationship of sound management, proper organization, and thorough evaluation to the performance of a credible risk assessment.

MAJOR TOPICS

- (1) **RISK ASSESSMENT CONCEPTS.** Includes fundamentals to permit an understanding of PRA, definitions of risk, objectives of and approaches to risk analyses.
- (2) **ELEMENTS OF NUCLEAR PLANT RISK ANALYSES.** Describes the basic elements which comprise a full PRA: system modeling, accident process analysis, and consequence analysis.
- (3) **APPLICATIONS OF PRA.** Provides a broad overview of the applications of PRA, both past and present. An overview of current major PRA-related programs will be presented together with the relationship of PRA to current safety issues.
- (4) **RELIABILITY AND RISK ANALYSIS.** Provides an understanding of the definitions and concepts of reliability and availability. Includes a description of logic models employed in reliability and availability analysis.
- (5) **ACCIDENT INITIATORS.** Explains the process of identifying and selecting accident initiators in nuclear plant PRA.
- (6) **EVENT TREE ANALYSIS.** Describes the purposes and techniques of event tree analysis, including identification of dominant and key accident sequences, and the effect of system and functional interrelationships.
- (7) **FAULT TREE ANALYSIS.** Provides familiarity with terminology, notation, and symbology employed in fault tree analysis, and discusses applicable component failure modes relative to the postulation of fault events.
- (8) **FAULT TREE AND EVENT TREE QUANTIFICATION.** Provides an understanding of the quantitative basis of PRA. Elements of PRA quantification ranging from the selection of component failure rate data to accident sequence quantification will be presented.

- (9) **COMMON CAUSE FAILURES.** Discusses the significance of common cause failures in terms of safety system unavailability and accident sequence probabilities. The definition of common cause failures and several examples will be presented.
- (10) **EXTERNAL EVENTS.** Presents the definition and nature of external events. Discusses the ways in which potential external events are analyzed and incorporated into a plant PRA.
- (11) **ACCIDENT PROCESS ANALYSIS.** Provides a general introduction to the purposes and techniques of examining accident phenomenology and containment response. Describes the role of accident process analysis in PRA.
- (12) **FISSION PRODUCT TRANSPORT AND RELEASE.** Explains the purpose and basis of release categorization. Describes the factors related to accident sequences which determine the type, timing, and magnitude of radiological releases.
- (13) **FUNDAMENTALS OF CONSEQUENCE EVALUATION.** Describes the purposes and elements of accident consequence evaluation, including the primary radionuclide transport and dispersion mechanisms, dosimetry, and health effects.
- (14) **PRA INTEGRATION.** Describes how the diverse elements which comprise a PRA are brought together to form a cohesive, comprehensive study. A discussion of the various levels of PRA and the skills which must be brought to those efforts will be provided.
- (15) **STRENGTHS AND LIMITATIONS.** Discusses the primary strengths and limitations of PRA. Describes the ways in which PRA practitioners attempt to capitalize on the strengths and deal with the weaknesses.
- (16) **NATURE OF PRA RESULTS.** Explains the ways in which PRA results are interpreted and presented. Examples of the kinds of engineering insights which result from a PRA will be presented.
- (17) **LWR PRA APPLICATIONS.** Describes some of the ways in which the interpretations which are drawn from PRA results are actually applied. Current and potential uses of PRA will be discussed.

REFERENCES

- Reactor Safety Study, WASH-1400, NUREG-75/014
- PRA Procedures Guide, NUREG/CR-2300, ANS/IEEE
- Fault Tree Handbook, NUREG-0492

TABLE OF CONTENTS

	<u>Page</u>
Preface	i
Abstract	iii
Table of Contents	v
List of Figures	ix
List of Tables	xii
Acknowledgements	xiv
 1. RISK ASSESSMENT CONCEPTS	 1-2
1.1 The Nature of Risk	1-2
1.2 Risk Assessment Objectives	1-3
1.3 Approaches to Risk Assessment	1-4
1.4 PRA Terminology	1-7
1.5 Summary of Risk Assessment Concepts	1-8
 2. ELEMENTS OF NUCLEAR PLANT RISK ANALYSIS	 2-2
2.1 PRA Study Activities	2-2
2.1.1 System Modeling	2-2
2.1.2 Accident Process Analysis	2-8
2.1.3 Accident Consequence Analysis	2-8
2.2 Levels of PRA	2-13
2.3 PRA Element Quality Assurance	2-13
2.4 Summary	2-14
 3. APPLICATIONS OF PRA	 3-2
3.1 Programmatic Advancements in PRA	3-2
3.1.1 WASH-1400	3-2
3.1.2 Reactor Safety Study Methods Application Program (RSSMAP)	3-3
3.1.3 Interim Reliability Evaluation Program (IREP)	3-4
3.1.4 Integrated Safety Assessment Program (ISAP)	3-5
3.1.5 Utility Studies	3-5
3.2 Current and Future PRA Applications	3-6
3.3 Unresolved issues	3-10
3.4 Role of PRA	3-11
 4. RELIABILITY AND RISK ANALYSIS	 4-2
4.1 Introduction	4-2
4.2 Probability	4-2
4.3 Unavailability	4-3
4.3.1 Failure Probability	4-4
4.3.2 Unavailability Contributions	4-5
4.3.3 Cumulative Failure Probability	4-8
4.4 Range Propagation and Bounding Techniques	4-12

TABLE OF CONTENTS (continued)

	<u>Page</u>
4.5 Reliability and Availability Analysis Tools	4-13
4.5.1 Failure Modes and Effects Analysis	4-13
4.5.2 Reliability Block Diagram	4-14
4.5.3 Parts Count Approach	4-14
4.5.4 Other Techniques	4-14
5. ACCIDENT INITIATORS	5-2
5.1 Nature of Accident Initiators	5-2
5.2 Grouping and Quantification of Accident Initiators	5-6
6. EVENT TREE ANALYSIS	6-2
6.1 Event Tree Analysis Process	6-2
6.2 Functional Event Trees	6-6
6.3 Systemic Event Tree Analysis	6-8
6.4 Summary	6-10
7. FAULT TREE ANALYSIS	7-2
7.1 Introduction	7-2
7.2 Definition and Nature of Fault Tree Analysis	7-2
7.3 Purposes of Fault Tree Analysis	7-4
7.4 The Fault Tree Development Process	7-4
7.4.1 Define Fault Tree Top Event	7-4
7.4.2 Develop and Update Analysis Notebook	7-6
7.4.3 Define Primary System and Interfaces	7-7
7.4.4 Develop Analytical Assumptions and Constraints	7-8
7.4.5 Fault Tree Construction	7-9
7.5 Fault Tree Symbology	7-9
7.6 Ground Rules of Fault Tree Analysis	7-9
7.7 Faults and Failures - Definitions	7-15
7.8 Fault Tree Reduction	7-15
7.9 Summary	7-18
8. FAULT TREE AND EVENT TREE QUANTIFICATION	8-2
8.1 Preparation for Quantification	8-2
8.2 General Procedure	8-3
8.2.1 Fault Tree Linking Method	8-4
8.2.2 Event Trees With Boundary Conditions	8-8
8.3 Simultaneous Test and Maintenance Contribution	8-9
8.4 Human Error	8-10
8.4.1 Sources of Uncertainty In Human Error Estimation	8-13
8.5 Data Base	8-15
8.5.1 Existing Data Sources	8-16
8.6 Treatment of Uncertainty	8-17
8.7 Computer Codes	8-19
8.8 Summary	8-19

TABLE OF CONTENTS (continued)

	<u>Page</u>
9. COMMON CAUSE FAILURES	9-2
9.1 Definition of Dependencies	9-2
9.2 Analysis of Dependencies	9-4
9.3 Summary	9-8
10. EXTERNAL EVENTS	10-2
10.1 Introduction and Overview	10-2
10.2 Earthquakes	10-9
10.2.1 General Discussion	10-9
10.2.2 Characterization of the Seismic Hazard	10-18
10.2.3 Structural and System Response	10-20
10.3 Fires	10-23
10.4 Floods	10-25
10.5 Summary	10-28
11. ACCIDENT PROCESS ANALYSIS	11-2
11.1 Introduction and General Discussion	11-2
11.2 Core Degradation and Melting Within the Reactor Vessel	11-5
11.3 Molten Core Phenomena Outside the Reactor Vessel	11-14
11.4 Relationship Between the Systems Analysis and Accident Process Analysis	11-19
11.5 Containment Considerations	11-24
11.6 Accident Process Analysis Models	11-29
11.7 Summary	11-44
12. FISSION PRODUCT TRANSPORT AND RELEASE	12-2
12.1 Introduction and Overview	12-2
12.2 Types of Release	12-3
12.3 Physical and Chemical States and Removal Processes	12-8
12.4 Release Categorization and Computer Codes	12-12
12.5 Summary	12-17
13. CONSEQUENCE ANALYSIS	13-2
13.1 Introduction	13-2
13.2 Atmospheric Transport and Diffusion	13-2
13.3 Pathways to Man	13-17
13.4 Dosimetry	13-20
13.5 Health Effects	13-25
13.6 Mitigation Measures	13-26
13.7 Computer Codes	13-34
13.8 Items for Further Research	13-45

TABLE OF CONTENTS (continued)

14.	PRA INTEGRATION	14-2
14.1	Introduction	14-2
14.2	Information Requirements	14-3
14.3	PRA Tasks	14-4
14.4	Integration of the Tasks	14-8
14.5	PRA Objectives	14-11
14.6	Schedule and Manpower	14-11
14.7	Assurance of Technical Quality	14-14
14.8	Summary	14-15
15.	STRENGTHS AND LIMITATIONS	15-2
15.1	Introduction	15-2
15.2	Plant Modeling and Model Evaluation	15-3
15.3	Data	15-4
15.4	Human Errors	15-5
15.5	Summary of System Modeling	15-5
15.6	Accident Process Analysis	15-6
15.7	Containment Analysis	15-6
15.8	Fission Product Transport Analysis	15-7
15.9	Summary of Accident Process, Containment, and Fission Product Transport Analysis	15-7
15.10	Consequence Analysis	15-8
15.11	External Events	15-9
15.12	Summary	15-10
16.	NATURE OF PRA RESULTS	16-2
16.1	Quantitative and Qualitative Results	16-2
16.2	Specific Examples of PRA Results	16-5
16.3	Insights From PRAs	16-5
16.3.1	Broad Insights Regarding Core Damage and Offsite Risk	16-5
16.3.2	Insights Regarding Accident Sequences	16-25
16.3.3	Additional Insights on External Initiators	16-26
16.4	Summary	16-26
17.	LWR PRA APPLICATIONS	17-2
17.1	Introduction	17-2
17.2	General Applications	17-6
17.3	Applications of PRA in Regulation	17-8
17.3.1	Allocation of Resources	17-8
17.3.2	Generic Regulatory Applications	17-9
17.3.3	Plant-Specific Regulatory Applications	17-9
17.3.4	PRA and Regulatory Decision-Making	17-10
17.4	Examples of PRA Programs	
APPENDIX A	REFERENCES	A-1

LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
1-1	Frequency of Man-Caused Events Involving Fatalities	1-9
1-2	Frequency of Natural Events Involving Fatalities	1-10
2-1	Elements of PRA	2-3
2-2	General Process for Event Tree Development	2-4
2-3	Simple Event Tree Model	2-5
2-4	Fault Tree Development Process	2-6
2-5	Simple Fault Tree Model	2-7
2-6	Example Reliability Block Diagram	2-9
2-7	Containment and Degraded Core Analysis Flow Chart	2-11
2-8	Environmental Transport and Consequence Analysis	2-12
3-1	Probabilistic Risk Assessment	3-9
4-1	Block Diagram Example	4-15
5-1	Core Cooling Success Criteria for Various LOCAs	5-3
6-1	General Process for Event Tree Development	6-3
6-2	Functional LOCA Event Tree	6-7
7-1	Fault Tree Development Process	7-5
7-2	Fault Tree Symbols	7-10
7-3	Example of Improper Gate-to-Gate Construction	7-14
7-4	Corrected Example of Gate-to-Gate Construction	7-14
7-5	Logic Gate/Boolean Correlation	7-20
8-1	Human Reliability Analysis Event Tree	8-12
10-1	Risk-Assessment Methodology for External Events	10-5
10-2	Family of Hazard Curves	10-6
10-3	Fragility Curves for Wind Loading	10-7
10-4	Combination of Risk from External Events with the Risk from Internal Events	10-8
10-5	The Focus and Epicenter of An Earthquake	10-10
10-6	Summary of Types of Fault Movement	10-11
10-7	The San Andreas Fault Zone, California	10-12
10-8	Accelerograph Record of the 1966 Parkfield, California Earthquake	10-14
10-9	Expected Level of Earthquake Hazards	10-15
10-10	Model of Seismic Hazard Analysis	10-19
10-11	Probability Density Functions of Release Frequencies from Seismic Events	10-22

LIST OF FIGURES (continued)

<u>Figure</u>		<u>Page</u>
11-1	Containment and Degraded Core Analysis Flow Chart	11-4
11-2	Decay Heat Reduction Over Time	11-8
11-3	Early Core Melt Progression	11-10
11-4	General Structure and Features of Meltdown in a Reactor Vessel	11-11
11-5	Visualization of the Downward Progresses of a Coherent Molten Mass as the Below-Core Structure Weakens	11-12
11-6	Visualization of the State Resulting from Failure of the Core Barrel Prior to Penetrations of a Coherent Molten Mass Through the Below-Core Structure	11-13
11-7	Major Sources and Sinks of Thermal Energy	11-15
11-8	Various Possible Modes of Lower Plenum Failure	11-16
11-9	Condition for Potential Steam Explosions	11-18
11-10	Light Water Reactor Loss of Coolant Accident (LOCA) Engineered Safety System (ESF) Functions	11-21
11-11	Relationship of Different Portions of a PRA	11-23
11-12	Steps in the Accident Process Analysis	11-25
11-13	General Compartment Features	11-30
11-14	Overall PRA Relationship Between MARCH and CORRAL	11-35
11-15	Subroutine Flow in MARCH and CORRAL	11-36
11-16	Primary Vessel Water Level-Small LOCA (0.75 in) With Loss of ECC	11-38
11-17	Core Average and Core Hotspot Temperatures-Small LOCA (0.75 in) With Loss of ECC	11-39
11-18	Primary Vessel Pressure-Small LOCA (0.75 in) with Loss of ECC	11-40
11-19	Containment Atmosphere Temperature-Small LOCA (0.75 in) with Loss of ECC	11-41
11-20	Containment Atmosphere Pressure-Small LOCA (0.75 in) with Loss of ECC	11-42
11-21	Hydrogen Concentration in Containment Atmosphere-Small LOCA (0.75 in) with Loss of ECC	11-43
12-1	PRA Elements	12-4
12-2	Elements of the Analysis of Radionuclide Behavior in the Reactor	12-5
12-3	Fission Product Release Rate Constants from Fuel - Smoothed Curves	12-9
12-4	Fission Product States	12-10

LIST OF FIGURES (continued)

Figure		Page
13-1	Consequence Assessment	13-3
13-2	Area Surrounding the Douglas Point Nuclear Generating Station	13-5
13-3	Various Types of Smoke-Plume Patterns Observed in the Atmosphere	13-6
13-4	The Average Diurnal Variation of the Vertical Temperature Structure at the Oak Ridge National Laboratory During September - October, 1950	13-8
13-5	Typical Horizontal Wind-Speed and Direction Traces at Various Heights	13-9
13-6	Map of the Hilly Area Showing Wind Flow by Means of Massed Wind Roses	13-10
13-7	Average Vectors Constructed from Night and Day Wind Observations	13-11
13-8	A Day-Night Wind Rose Showing the Diurnal Effect of the Sea Breeze	13-12
13-9	Representations of a Plume from a Point Source	13-14
13-10	Briggs Rural-Data-Based Dispersion Coefficients (Solid Curves) Compared with the Pasquill-Gifford Coefficients (Broken Curves)	13-16
13-11	Pathways to Man	13-18
13-12	Principal Radionuclide Exposure Pathways	13-21
13-13	Simplified Interdiction Model	13-22
13-14	Retention Model	13-23
13-15	Common Doses from Various Sources	13-27
13-16	Possible Relationships Between Dose and Excess Risk of Cancer	13-29
13-17	Basic Model for Latent Cancer Fatalities	13-30
13-18	Evacuation Area Used for Cost Calculations	13-32
13-19	Concentration of Radioactive Material Outdoors (Curve A) and Indoors (Curve B) as a Function of Time During the Cloud Passage	13-33
13-20	Radionuclide Pathway Interactions	13-35
13-21	Comparison of Single and Double Unit Risk of Early Fatality (Mean Values)	13-46
14-1	PRA Elements	14-5
14-2	General PRA Activity Flow Diagram	14-6
14-3	Linking of Accident and Containment Event Trees	14-10
16-1	Transient Systemic Event Tree	16-6
16-2	Probability Distribution for Early Fatalities Per Reactor Year	16-10
16-3	Limerick/WASH-1400 Risk Comparison	16-11

LIST OF TABLES

<u>Table</u>		<u>Page</u>
2-1	Typical Format for a Failure Mode and Effects Analysis	2-10
3-1	PRA Methodological and Experimental Advance	3-7
3-2	Examples of Applications	3-8
5-1	Initiating Events Used in the ANO-1 Analysis	5-4
5-2	BWR Transient Initiators	5-5
5-3	Transient Classes and Frequencies	5-7
6-1	Specifications of Desired Data for Event Tree Analysis	6-4
7-1	Rules for Fault Tree Construction	7-17
7-2	Rules of Boolean Algebra	7-19
8-1	Computer Codes for Quantitative Analysis	8-20
8-2	Computer Codes for Dependent Failure Analysis	8-22
10-1	Possible External Events	10-3
10-2	Modified Mercalli Scale	10-16
10-3	Earthquake Magnitudes, Energies, Effects, and Frequencies	10-17
10-4	Statistical Evidence of Fires in Light-Water Reactors	10-24
10-5	Propagation Analysis	10-26
10-6	Potential Causes of Flooding	10-27
10-7	External Events	10-29
11-1	Accident Sequence Stages	11-6
11-2	Core Phenomenology	11-7
11-3	Examples of Engineered Safety Features	11-22
11-4	Containment Failure Modes	11-26
11-5	Some of the Phenomena That Must Be Included In A Core-Melt Containment Analysis	11-28
11-6	Summary of Types of Computer Models Utilized In Accident Process Analysis	11-31
11-7	Typical Data Required to Model Core Melt and Containment Response	11-32
11-8	MARCH/CORRAL Code Package	11-34
11-9	MARCH Code Inadequacies	11-37
12-1	Types of Release to Containment Atmosphere	12-6
12-2	Melting and Boiling Points of Reactor Core Constituents	12-11
12-3	RSS Radionuclide Classification Scheme	12-13
12-4	Available Computer Codes	12-15
12-5	Summary of Accidents Involving Core	12-16
12-6	Dominant Accident Sequences Versus Release Categories	12-18
13-1	Gaussian Dispersion Equation and Equations for the Dispersion Coefficients	13-15
13-2	Radiation and Dosage Units	13-24
13-3	Types of Reactor Products	13-26

LIST OF TABLES (continued)

<u>Table</u>		<u>Page</u>
13-4	Codes Available to Compute Accident Consequences	13-36
13-5	U.S. Consequence Codes Common Features	13-37
13-6	Comparison of U.S. Codes	13-39
13-7	Site and Environs Input Data	13-40
13-8	Release Description Input Data	13-41
13-9	Mitigation Input Data	13-42
13-10	Health Effects Input Data	13-43
13-11	Type of Outputs Available	13-44
13-12	Items Deserving Further Study	13-47
14-1	Typical PRA Team Makeup	14-12
14-2	Estimated Manpower Per Task	14-13
16-1	Types of Information Generated by PRA	16-3
16-2	Typical Accident Sequence Description	16-7
16-3	Typical Event Descriptions	16-8
16-4	PWR Large LOCA Accident Sequences vs. Release Categories	16-9
16-5	Surry (RSS) PRA Results	16-12
16-6	Peach Bottom (RSS) PRA Results	16-13
16-7	Oconee (RSSMAP) PRA Results	16-14
16-8	Sequoyah (RSSMAP) PRA Results	16-15
16-9	Grand Gulf (RSSMAP) PRA Results	16-16
16-10	Calvert Cliffs (RSSMAP) PRA Results	16-17
16-11	Crystal River (IREP) PRA Results	16-18
16-12	ANO-1 (IREP) PRA Results	16-19
16-13	Browns Ferry (IREP) PRA Results	16-20
16-14	Big Rock Point PRA Results	16-21
16-15	Limerick (PRA, Rev. 4) PRA Results	16-22
16-16	Zion (ZIP) PRA Results	16-23
17-1	Published U.S. LWR PRA Studies	17-3
17-2	Plant-Specific Risk Assessments	17-4
17-3	PRA Related Studies	17-5
17-4	Industry Degraded Core Program	17-12
17-5	National Reliability Evaluation Program (NREP)	17-13
17-6	DOE Five Year R&D Program	17-14
17-7	IREP Objectives	17-15
17-8	Accident Sequence Evaluation Program	17-16
17-9	Severe Accident Sequence Analysis (SASA)	17-17
17-10	Methods Development	17-18
17-11	Generic Issues	17-19
17-12	Proposed Preventive/Mitigative Concepts	17-20
17-13	Concept Objectives	17-21
17-14	Alternative Decay Heat Removal Concepts	17-22
17-15	Mitigation Concepts	17-23
17-16	Hydrogen Mitigation	17-24
17-17	Alternate Containment Concepts	17-25
17-18	Qualitative Value-Impact Matrix	17-26

ACKNOWLEDGMENTS

The course documentation represents the completion of the documentation process for the PRA Technology Transfer Program.

The authors wish to thank all of the people who contributed to its development -- colleagues and staff, reviewers, sponsors, and especially the students who provided invaluable feedback during several course presentations.

Special appreciation is extended to the leadership of the program and particularly to the following individuals: Wallis R. Cramond, Program Coordinator at Sandia National Laboratories; Ernest V. Lofgren, Peer Review Coordinator, Science Applications International Corporation; Lala J. Curry, Manager of Support Services, SAIC/JRB ; James C. Malaro, J. Calvin Belote, S. Richard Sturges (now retired), and Patricia J. Rathbun of the U.S. Nuclear Regulatory Commission.

The following pages of the PRA Fundamentals Course documentation contain copyrighted material:

- 10-10
- 10-11
- 10-12
- 10-14
- 10-15
- 10-16
- 10-17

Permission to use this material has been received from the copyright owners. Further use of this material is subject to U.S. copyright laws.

TOPIC 1
RISK ASSESSMENT CONCEPTS

1.0 RISK ASSESSMENT CONCEPTS

This Probabilistic Risk Assessment (PRA) Fundamentals course is designed to provide a broad introduction to PRA and its applications. This four day course begins with a general introduction to the field of PRA; proceeds to discuss the methods which are used in system modeling, accident process analysis, and accident consequence analysis; and ends with a discussion of the strengths, limitations, and applications of PRA. In order to illustrate some of the techniques which are important in PRA, several in-class sample problems will be presented.

1.1 The Nature of Risk

Although the application of formalized PRA techniques to nuclear power plants is a relatively new development, the practice of risk assessment on a broader scale is not. Since the earliest times, people have taken actions based on their needs and their understanding of the risks associated with various means of meeting those needs. By essentially asking themselves what can go wrong with some potential course of action, and how likely an undesired outcome might be, people are performing small, informal risk assessments on a daily basis. These informal risk assessments are generally based on people's own limited bases of experience. Sometimes, these informal risk assessments suggest courses of action which may fail to accomplish their intended goals or which have associated undesired consequences. In these instances, the informal risk assessment may have been based on distorted perceptions of likelihood or consequences. In an attempt to improve the accuracy of risk assessments, and thus make them suitable for application to large-scale technologies, formalized risk assessment tools have been developed. These formalized risk assessment tools will be discussed throughout this PRA Fundamentals course.

As indicated by its title, PRA purports to assess risk. It seems reasonable, then, that before discussing the techniques of PRA, one must first define what is meant by "risk". One dictionary definition describes risk as, "the chance of injury, damage, or loss; the degree of probability of loss." Although it is not precise enough to use in the context of PRA, this dictionary definition identifies the essential parameters which are necessary to define risk. Specifically, these parameters are likelihood and consequences. In the context of PRA, the concept of risk can be defined as, "the likelihood of experiencing a defined set of undesired consequences."

Conceptually, it can be said that risk arises from the interaction between two related parameters - hazard and protection. A hazard is defined as a potential source of risk. When the potential is identified, and is deemed to be great enough, various mechanisms of protection may be implemented. For example, although there are a number of hazards in a nuclear power plant, the one which is of most concern is the radionuclide inventory in the core of the reactor. In response to the recognition of this hazard, protective measures such as emergency core cooling systems and a reactor containment building are put in place. The hazard and the protective measures, then, interact resulting in some level of risk. The magnitude of the risk increases as the severity of the hazard and/or the likelihood of failure of the protective measures increase.

Safety is a concept which is even more nebulous and difficult to define than risk. Safety can, in a sense, be thought of as being the degree to which risk is absent. A safe condition is one in which the level of attendant risk is acceptable. Note that safety is not defined as a complete absence of risk. It is important to recognize that no human activity is free of risk. Rather, safety is defined in terms of the relative absence of risk.

An individual's acceptance or rejection of various risks involves two rather subjective parameters. These are the person's perception of the risk and the degree to which the exposure to the risk in question is voluntary or involuntary.

Recognizing that no activity is free of risk, people tend to accept or reject risks based on their perceptions of the degree of risk associated with various endeavors. Ironically, many individuals who gladly travel by automobile, with a statistically high risk, erroneously perceive air travel to be highly risky, and therefore, unacceptable to them. In this case, the perceived level of risk, rather than the actual level of risk, determines the acceptability of the activity.

Although it is very often difficult to determine which risks are voluntary and which are involuntary, it can be said that in general, the public prefers voluntarily accepted risks. Paradoxically, this is true even when a voluntary risk may be somewhat greater than an involuntary risk. Interestingly, actuarial statistics show that approximately 5 percent of the risk which is believed to be totally voluntary in nature is, in fact, involuntary. For example, approximately 5 percent of all of the automobile fatalities involve people who are in their homes or who are walking on sidewalks. That is to say, approximately 5 percent of the automobile fatalities involve people who are not traveling in an automobile, and are, thus, involuntarily subjected to automobile-related risk.

1.2 Risk Assessment Objectives

The assessment of risk with respect to nuclear power plants is intended to achieve four general objectives. These objectives are:

- To identify initiating events and event sequences which might be significant contributors to risk.
- To provide a realistic quantitative measure of the likelihood of these risk contributors.
- To provide a realistic evaluation of the potential consequences associated with hypothetical accident sequences.
- To provide a reasonable risk-based framework for making decisions regarding nuclear plant design, operation, and siting.

One of the products of a nuclear power plant PRA is a list of applicable initiating events (challenges to reactor core integrity) and the sequences of events which could follow these initiating events. It is important to note that a PRA does not, and cannot, identify all of the potential events which might constitute risk contributors. However, through disciplined analysis, and thorough review, it can be reasonably assured that PRA identifies all of the probabilistically significant risk contributors.

By quantitatively evaluating the significance of the identified risk contributors, it is possible to identify the most likely (dominant) accident sequences, or contributors to those sequences, and take corrective action as required. Within the constraints of the available data base, realistic calculations of the probabilities of events which contribute to risk are made.

Although the definition of consequences of interest may vary from one PRA to another, PRAs attempt to realistically evaluate the consequences of hypothetical accident

sequences. Depending on the scope of PRA, the evaluation of accident sequences may include an estimation of the number of latent cancers, the number of immediate fatalities, the probability of core damage, or a number of other possible consequential parameters. Regardless of which parameter is of interest, a PRA attempts to develop a realistic evaluation of accident consequences in terms of that parameter.

By identifying significant risk contributors, evaluating the significance of those contributors, and assessing the consequences of accident sequences, PRA constitutes a comprehensive framework for many types of decision-making. Decisions regarding reactor design, operation, and siting can be made, at least in part, on the basis of a rational, disciplined evaluation of the risks which are associated with a particular facility.

1.3 Approaches to Risk Assessment

Three basic approaches to risk assessment have been used in the nuclear industry. Two of these approaches, the worst-case approach and the actuarial approach, have been used with rather little success. The third approach, the analytical approach, has been much more successfully used. Examples of the past applications of these approaches are presented below.

The worst case approach to risk assessment identifies the worst foreseeable set of consequences associated with an activity but does nothing to assess the likelihood or credibility of those consequences. The first assessment of the risk associated with a nuclear power facility employed the worst-case approach.

In the mid-1950's, the concept of risk with regard to the nuclear industry took on a new perspective. The assessment was performed to aid in establishing a basis for U.S. Government assured indemnification of commercial deployment of nuclear energy. At that time, the risks of generating electrical energy using nuclear power were not understood. The Congress of the United States determined that, in order for the nuclear industry to have a reasonable possibility of growth, some indemnification process needed to be enacted. First, it was necessary to evaluate the extent of damage or hazard that could arise. In the summer of 1956, the first effort to estimate the likelihood and crudely evaluate the consequences of such an event was initiated. The result of this work was entitled Theoretical Possibilities and Consequences of Major Accidents In Large Nuclear Power Plants, otherwise known as WASH-740.

Unlike most recent PRAs, there was little treatment of accident likelihoods in the WASH-740 report. The writers believed that there was not a sufficient basis for making rigorous estimations of accident probabilities. However, in a section called, "The Best Judgment of the Most Knowledgeable Experts," the unanimous opinion was that the likelihood of a major reactor accident was low. The likelihood of significant internal release of fission products from the core, but no release outside the reactor vessel, was estimated to range from 10^{-2} to 10^{-4} per year for each reactor. Estimates of the likelihood of release of significant fission product activity outside the reactor vessel, but not outside the containment building, ranged from 10^{-3} to 10^{-4} . Finally, estimates for the likelihood of major releases of radioactivity outside the containment building were between 10^{-5} to 10^{-9} per reactor year.

The WASH-740 assumptions regarding the mechanisms and amounts of radioactivity releases were simplistic and broad. Three cases were evaluated:

- A. **Contained Case.** All radioactivity was assumed to be released from the core and distributed uniformly throughout the containment building; none escaped to the environment. In this case, the only hazard was direct gamma radiation.
- B. **Volatile Release Case.** This case assumed that all of the volatile fission products and 1 percent of the strontium were released to the environment.
- C. **50% Release Case.** In this case, it was assumed that half of all fission products were released to the environment.

The consequence evaluations were based on these releases and were related to lethal exposure, injury, and property damage. The consequences ranged from no lethal exposure, no injury, and small financial loss for release case A, to a lethal exposure for 3,400 people, injury to 43,000 people, and property damage of \$9.1 billion for release case C with worst-case weather conditions assumed.

The actuarial approach has been used for only very limited purposes in PRA. This approach, the basis of the insurance industry, is based on broad statistical data. In the insurance application, a determination is made of the probability that a person of a given age will live to some future age, and a numerical value of the insurance premium is determined. Given the sparsity of experience with nuclear plant accidents, however, such an approach cannot be successfully used to estimate the probability of future accidents.

To date, the only successful PRA applications of the actuarial approach have been in developing component failure data. This application has been successful because of the large amount of experience with specific components.

The analytical approach has been used successfully since it was first employed in the Reactor Safety Study which was published as WASH-1400 in 1975. This document was prepared by an Atomic Energy Commission team headed by Norman Rasmussen. The effort was charged to evaluate risk associated with operating 100 nuclear power reactors in the United States. The project was a rational "follow-on" to WASH-740, so the U.S. Atomic Energy Commission (AEC) mapped out a plan to perform a systematic and comprehensive assessment of risk which finally resulted in the publication of the Reactor Safety Study (RSS) or WASH-1400. Basic planning, selection of the study director, and assembling of the team of necessary expertise took place in the early 1970's. The final report was published in October of 1975.

The WASH-1400 study described and delineated the various accidents that could lead to significant radioactivity release, and then evaluated the health and economic effects of these releases. Since these evaluations were made within a framework of likelihood or probability, a representation of risk was generated.

Two major findings of the RSS were:

- Consequences of potential reactor accidents are not larger than those of certain nonnuclear accidents.
- The likelihood of such reactor accidents is smaller than that of nonnuclear accidents with similar consequences.

The RSS contributed significantly to the state-of-the-art PRA applications for nuclear power plants. The RSS established that the fault tree/event tree methodology could be used credibly to identify risk-significant accident sequences. A comprehensive data base was established for nuclear power plants. Significant advances were also made in the modeling of physical processes which occur in degraded core accidents. Likewise, areas for future research in this modeling were identified. Finally, significant advances were made in the consequence modeling task of a PRA.

Review and criticism of the study continued through the late-1970's. The most competent and notable review of the WASH-1400 was performed by the Lewis Committee. Although specific calculational techniques were called into question, the overall conclusion was that the study was well done, made a significant contribution to the understanding of sources of risk, and that these methods and techniques should be used more extensively by both the industry and the regulators.

In October of 1975, an effort to extend and refine the techniques used in the WASH-1400 RSS, the NRC initiated a program called the Reactor Safety Study Methods Application Program (RSSMAP). The following objectives of the RSSMAP were stated:

- Identify the risk dominating accident sequences for a broader spectrum of reactor designs.
- Compare these accident sequences with those identified for the reactors studied in the RSS.
- Based on this comparison, identify design differences between the plants which have a significant impact on risk.

The scope of the RSSMAP was limited to system modeling and accident process analysis. Accident consequence modeling was not included.

The accident at Three Mile Island (TMI) in March of 1979, sparked even greater interest in PRA and how it might be used to measure and enhance nuclear reactor safety. The NRC's Interim Reliability Evaluation Report (IREP), initiated in direct response to the TMI incident, was conceived with four specific objectives in mind:

- Identify, in a preliminary way, those accident sequences that dominate the public health and safety risks originating in nuclear power plant accidents.
- Develop a formulation for subsequent, more intensive applications of probabilities, safety analysis, or risk assessment on the subject plants.
- Expand the cadre of experienced practitioners of risk assessment methods within the NRC and the nuclear power industry.
- Evolve procedures for codifying the competent use of these techniques for use in the extension of IREP to all domestic light water reactor plants.

In addition to these major NRC-sponsored PRA programs, a number of industry-sponsored PRA efforts have been completed. These privately funded studies have generally been designed to answer specific safety questions associated with the subject plants. As such, these studies often have been considerably different from the RSS in terms of scope and

methods. While past PRA efforts have often varied from one another in a number of respects, each has enhanced an understanding of the meaning and applications of PRA.

1.4 PRA Terminology

Like many other disciplines, PRA has a body of terminology which is peculiar to it alone, or which has specific meanings within its context. No attempt will be made here to provide a comprehensive listing of PRA-related terms. Instead, however, some of the basic terms which help to begin a discussion of PRA are defined and discussed in this section.

At the very heart of PRA is the term probability. Although several definitions of probability exist, the simplest regards probability as a ratio which is expressed as the number of occurrences of some event of interest divided by the number of opportunities for that event to occur.

A familiar example which illustrates this concept of probability is a box of seven marbles, two of which are black and five of which are white. On any random selection of one marble, there is a 0.286 probability of selecting a black marble.

Likelihood is commonly used interchangeably with probability but actually has a slightly different meaning. The term "likelihood" implies that some kind of a subjective judgment is used as the basis for determining how probable some event of interest is. The term "probability", on the other hand, implies a product of some mathematical calculation.

The concept of reliability can be thought of in terms of automobile performance. Many years ago, for example, automobiles were quite unreliable. On cold mornings they would not start, and flat tires frequently occurred. Over the years, these occurrences have diminished, and cars are considered to be more reliable. That is, it is more likely that today's automobiles will start and operate as required. They are more reliable in the sense that fewer failures occur which disable the automobiles. In more formal terms, reliability is the probability that a system will perform satisfactorily for at least a given period of time when used under stated conditions.

Availability is a PRA-related concept which is similar to reliability but is more comprehensive. Availability is that fraction of total time during which a component or system is available to perform its intended function. Unlike reliability, the concept of availability includes considerations of repair time, testing time, and any administrative time constraints. To again use the automobile analogy, an automobile's availability is that fraction of total time during which it is available for service. This fraction must take into account the time that the automobile is disabled, being repaired, being refueled, or is otherwise taken out of service.

Unavailability is the complement of availability. Unavailability is that fraction of the time during which the automobile is not available for service. This includes not only the time in which the automobile is unable to start or to run, but also any time during which it is being repaired or having routine service performed. It is generally the unavailability of nuclear plant safety systems that is of interest in PRA.

There are, of course, many more terms which are important in PRA. However, the above terms are the most basic and allow the beginning of a discussion of PRA. Other terms will be defined as they are presented throughout the course.

1.5 Summary of Risk Assessment Concepts

PRA provides a rigorous, disciplined means of addressing a number of different questions associated with the safety of nuclear power plants. PRA techniques can be used to assess design, operation, and siting characteristics of nuclear power plants in terms of their associated risks. In addition, PRA provides a means of comparing the risks associated with nuclear power plants relative to other industrial/societal risks.

Figures 1-1 and 1-2 show comparisons of the risks of various natural and man-caused hazards relative to the risks associated with nuclear power plants. These are the now famous cumulative complementary distribution function curves developed in WASH-1400. Such a comparison provides at least a starting point for addressing the most difficult of all regulatory questions, "how safe is safe enough?"

A number of factors may be combined to lead to increased use of PRA techniques in the future. There is always an increasing need to better understand nuclear plant reliability and safety. Nuclear power plants are extremely complex facilities. Engineers are frequently unable to examine nuclear plant system relationships and similar issues because they are unable to look at the plant as a whole. PRA provides a systematic way of conducting such evaluations. In addition, there has been a growing acceptance of these methods as rational and reasonable ways of assessing risk and safety issues. Several review groups, including the Lewis, Rogovin, and Kemeny Committees, have addressed the use of these methods and have concluded that in the regulatory process and in the design process, the PRA method should be employed because it yields insights into plant safety which are not available through any other method.

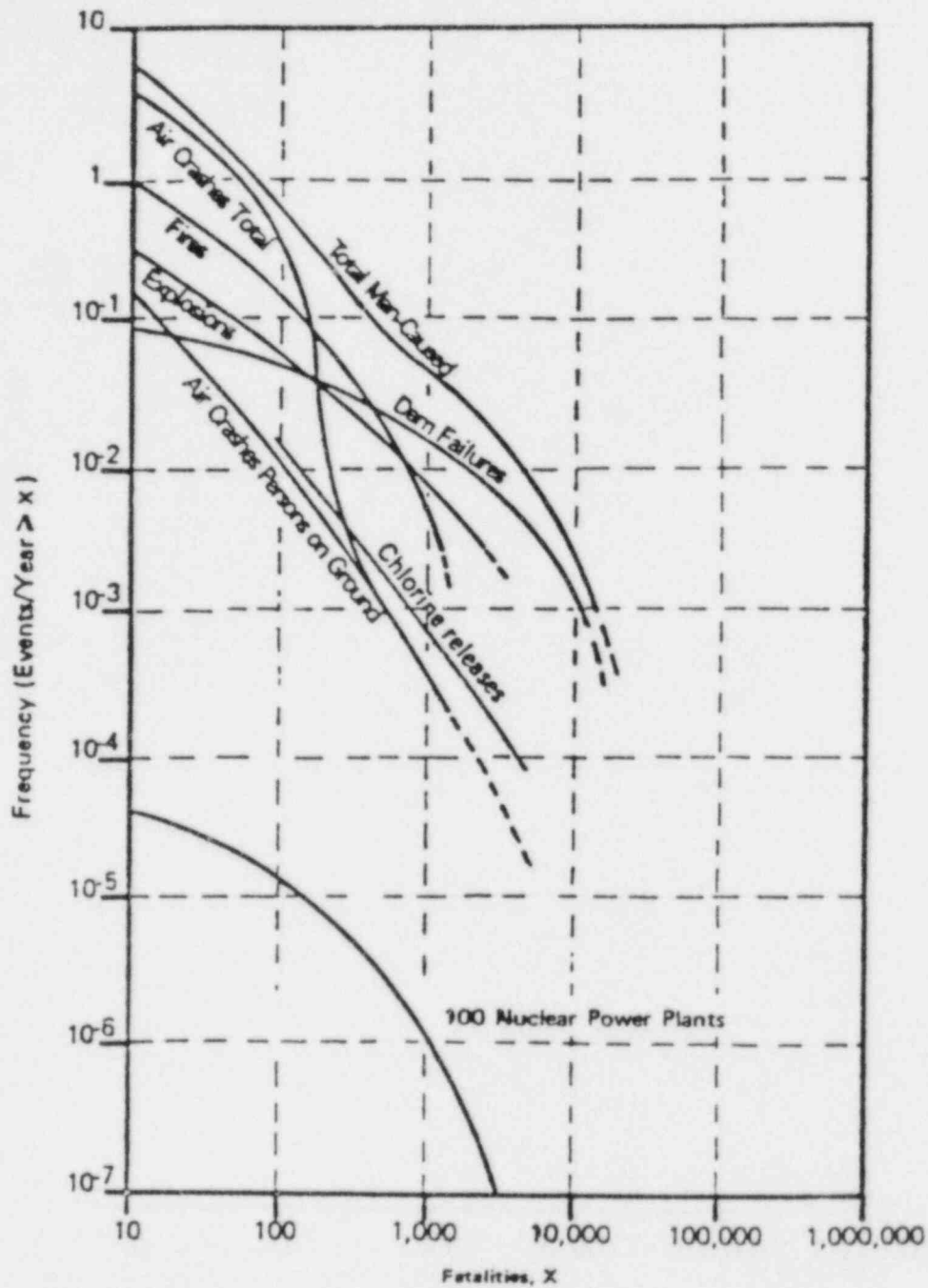


FIGURE 1-1
FREQUENCY OF MAN-CAUSED EVENTS INVOLVING FATALITIES

Source: U.S. Nuclear Regulatory Commission. Reactor Safety Study (WASH-1400) Main Report. 1975, Page 2, Figure 1-1.

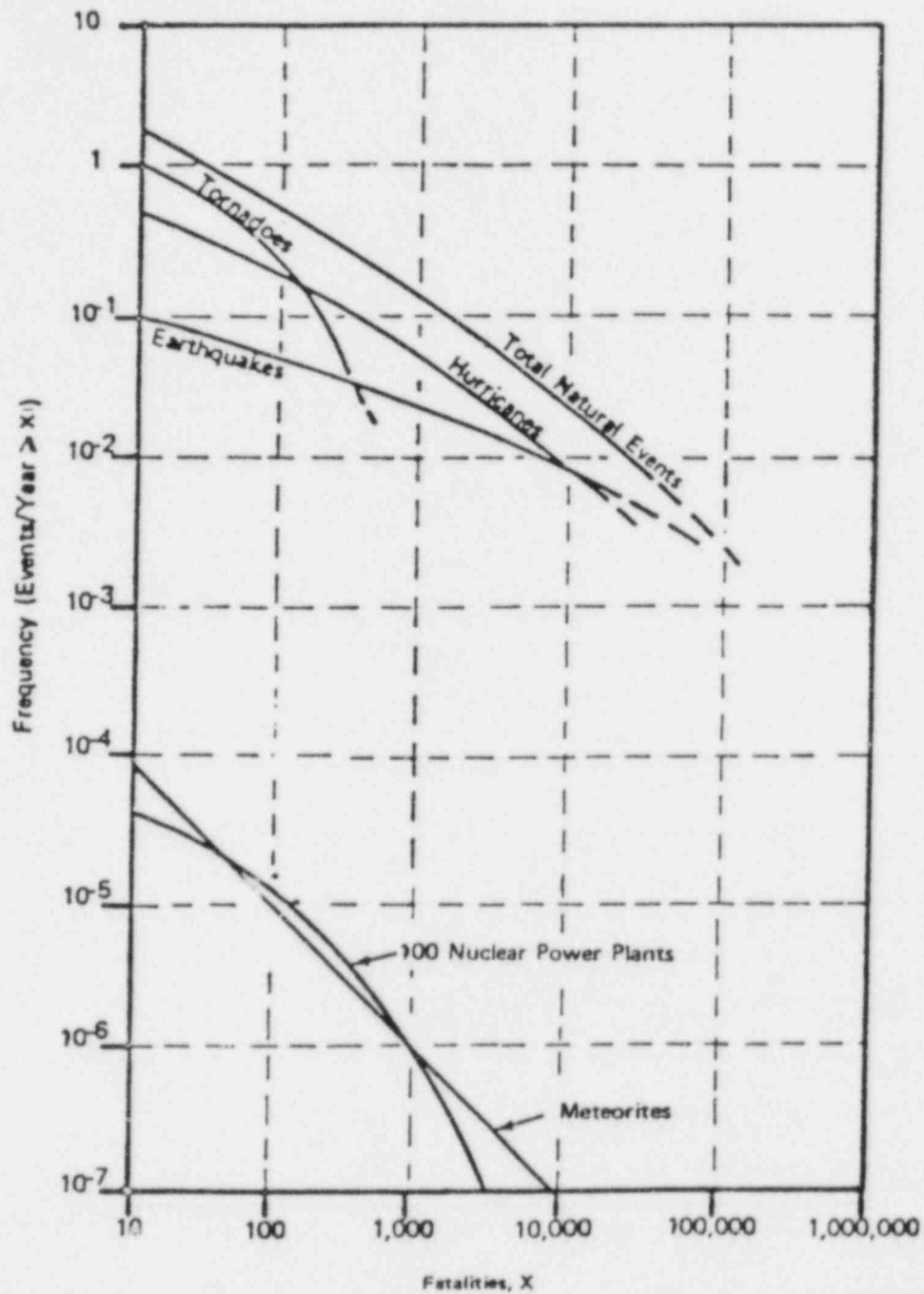


FIGURE 1-2
FREQUENCY OF NATURAL EVENTS INVOLVING FATALITIES

Source: U.S. Nuclear Regulatory Commission. Reactor Safety Study (WASH-1400) Main Report. 1975, Page 2, Figure 1-2.

TOPIC 2
ELEMENTS OF NUCLEAR PLANT RISK ANALYSIS

2. ELEMENTS OF NUCLEAR PLANT RISK ANALYSIS

PRA is a multidisciplinary tool with which to evaluate the risks associated with various technologies. Of course, this PRA training program is directed at PRA as applied to the evaluation of nuclear power plants. As a multidisciplinary tool, PRA is comprised of a number of different elements and techniques. The required scope of the analysis determines what complement of PRA techniques are used in a particular study. The various levels of PRA studies, and the techniques which comprise them, are discussed in this topic.

2.1 PRA Study Activities

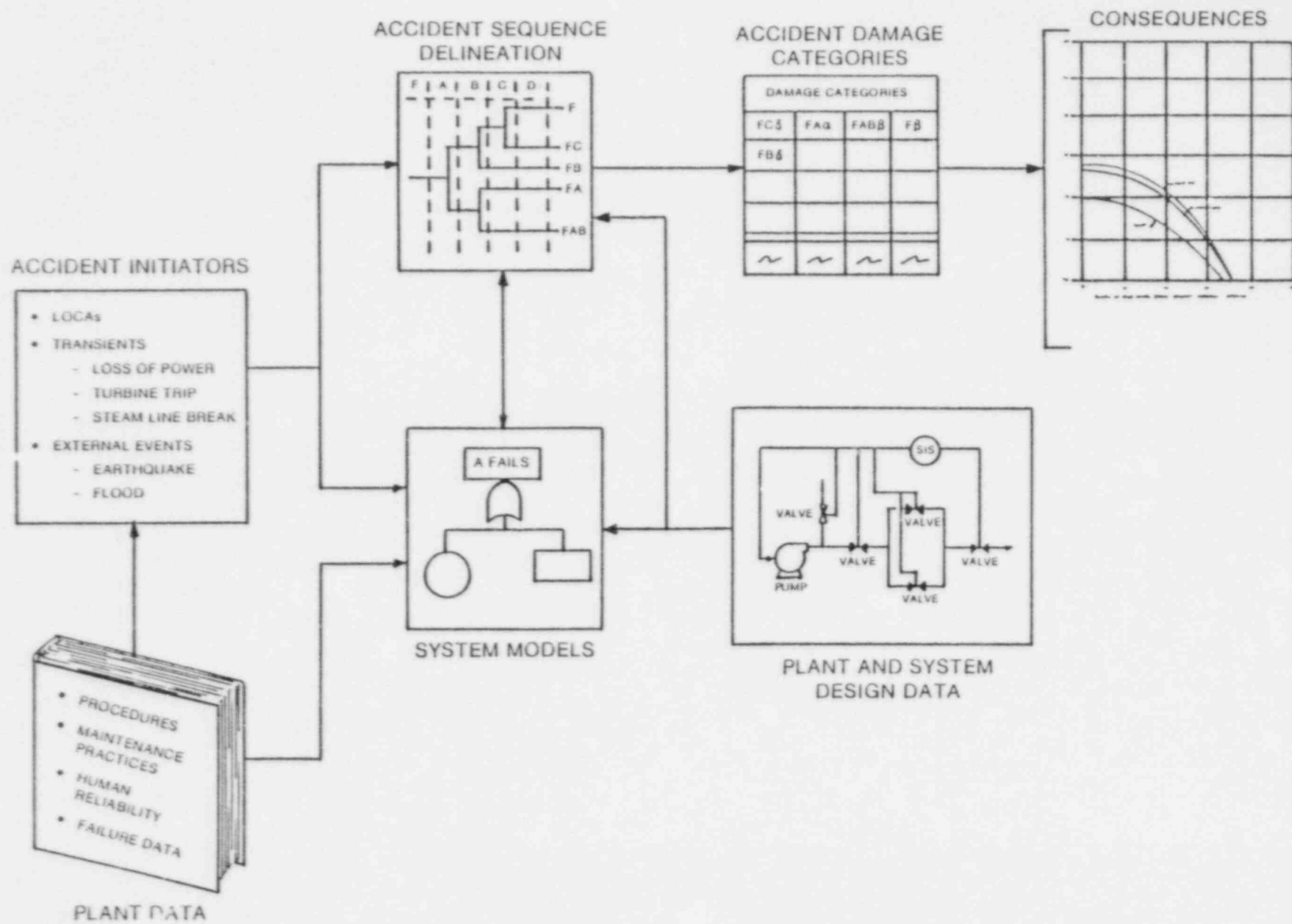
The field of PRA is generally divided into three broad areas: system modeling, accident process analysis, and accident consequence analysis. Although each of these broad areas is discussed more fully later in the course, they are introduced here to illustrate how they interact to produce PRAs of various levels. Figure 2-1 provides a graphic representation of the activities which comprise a risk assessment. Drawing on plant-specific and generic data, a listing of potential accident initiators is first developed. Accident initiators are undesired events which challenge the integrity of the core. These events are discussed in Topic 5. The list of potential accident initiators is used in both the system modeling and accident process analysis portions of the PRA. Finally, based on an understanding of the physical processes which are involved, probabilistic estimates of the consequences associated with specific accident sequences are developed. System modeling, accident process analysis, and accident consequence analysis are discussed briefly below.

2.1.1 System Modeling

In some respects, system modeling is the most basic element of PRA. Various kinds of system models are used to depict the combinations of safety function or system successes and failures which constitute accident sequences, and to develop an understanding of the ways in which the safety systems can fail. Although there are many different system modeling techniques, the two which are used almost exclusively in PRA are called event tree analysis and fault tree analysis.

The event tree model provides a systematic means of delineating accident sequences in terms of the functional or system successes and failures that make up those sequences. The steps in event tree analysis are shown in Figure 2-2. As shown in the simple event tree model, presented in Figure 2-3, the event tree provides end-to-end traceability from the accident initiating event to ultimate accident sequence outcome, in terms of a plant damage state. The identification of initiating events and the process of event tree analysis are discussed in Topics 5 and 6.

Fault tree analysis is performed to identify the potential events or combinations of events which can make the plant safety systems unavailable to respond to initiating events. The system fault tree models can be quantified to obtain probabilities of system unavailability. By using these system unavailability probabilities as inputs to the event tree models, the probabilities of the various accident sequences can be calculated. The process used to develop a fault tree model is shown in the flow chart in Figure 2-4. This process is fully discussed in Topic 7. A very simple fault tree model is shown in Figure 2-5.



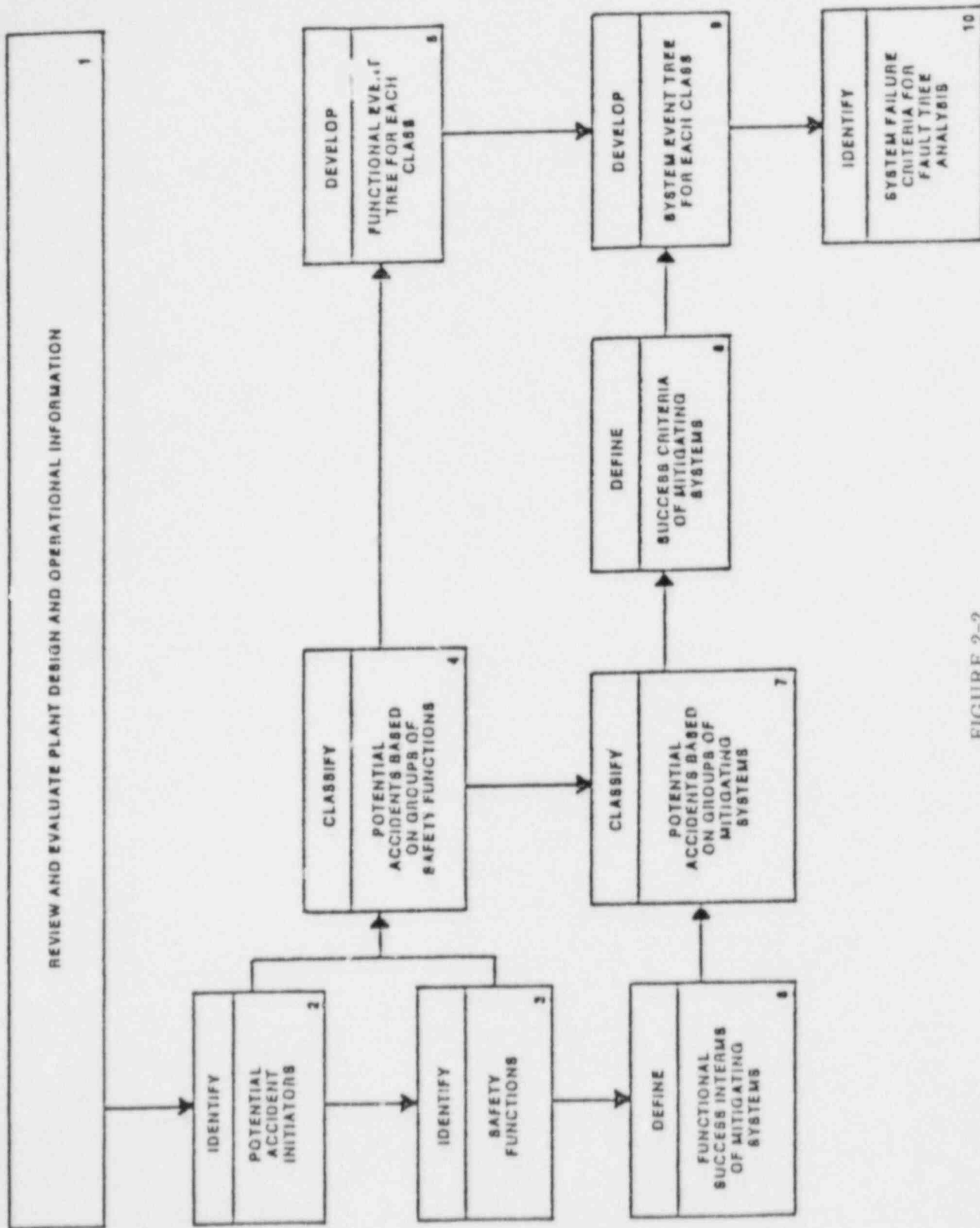


FIGURE 2-2
GENERAL PROCESS FOR EVENT TREE DEVELOPMENT

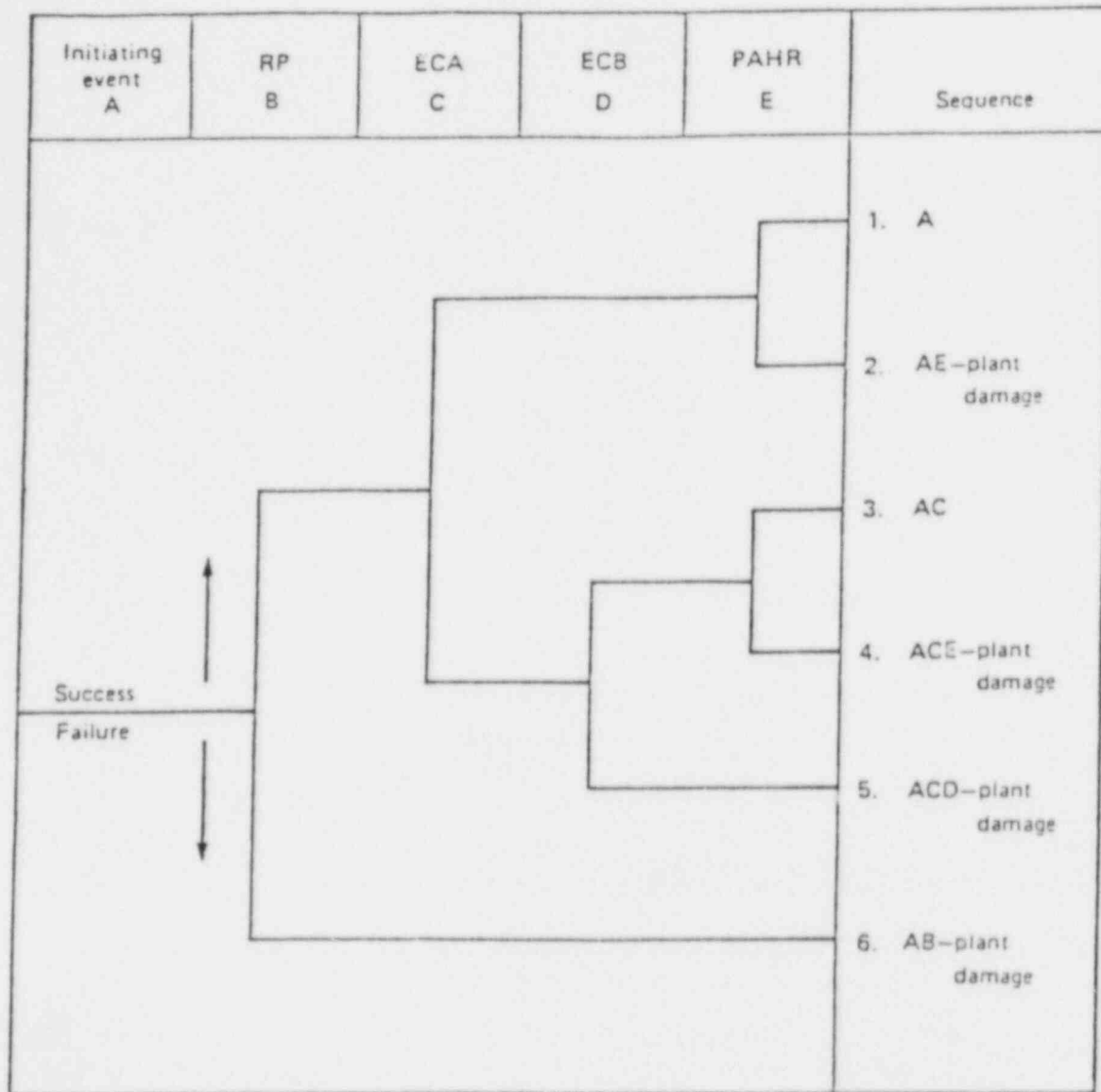


FIGURE 2-3
SIMPLE EVENT TREE MODEL

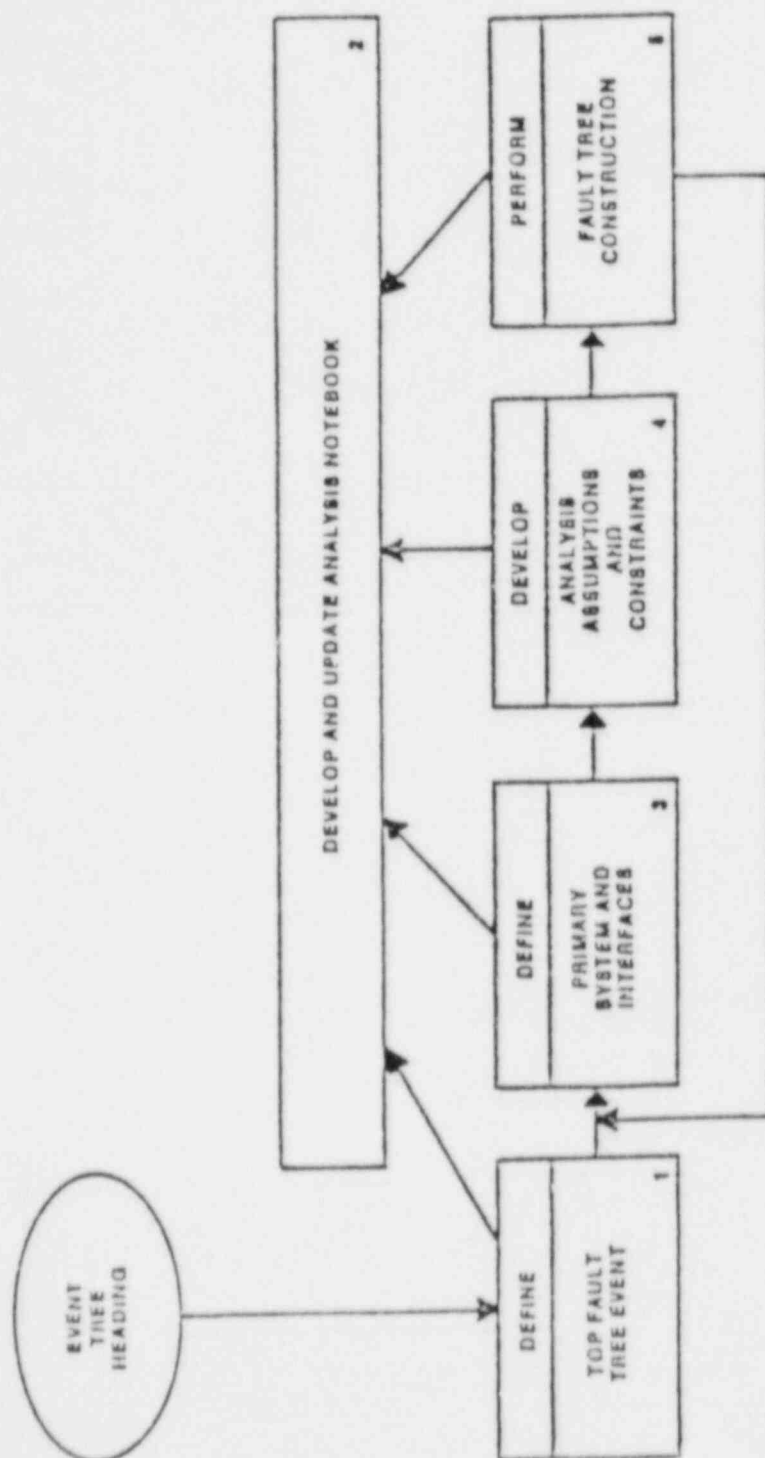


FIGURE 2-4
FAULT TREE DEVELOPMENT PROCESS

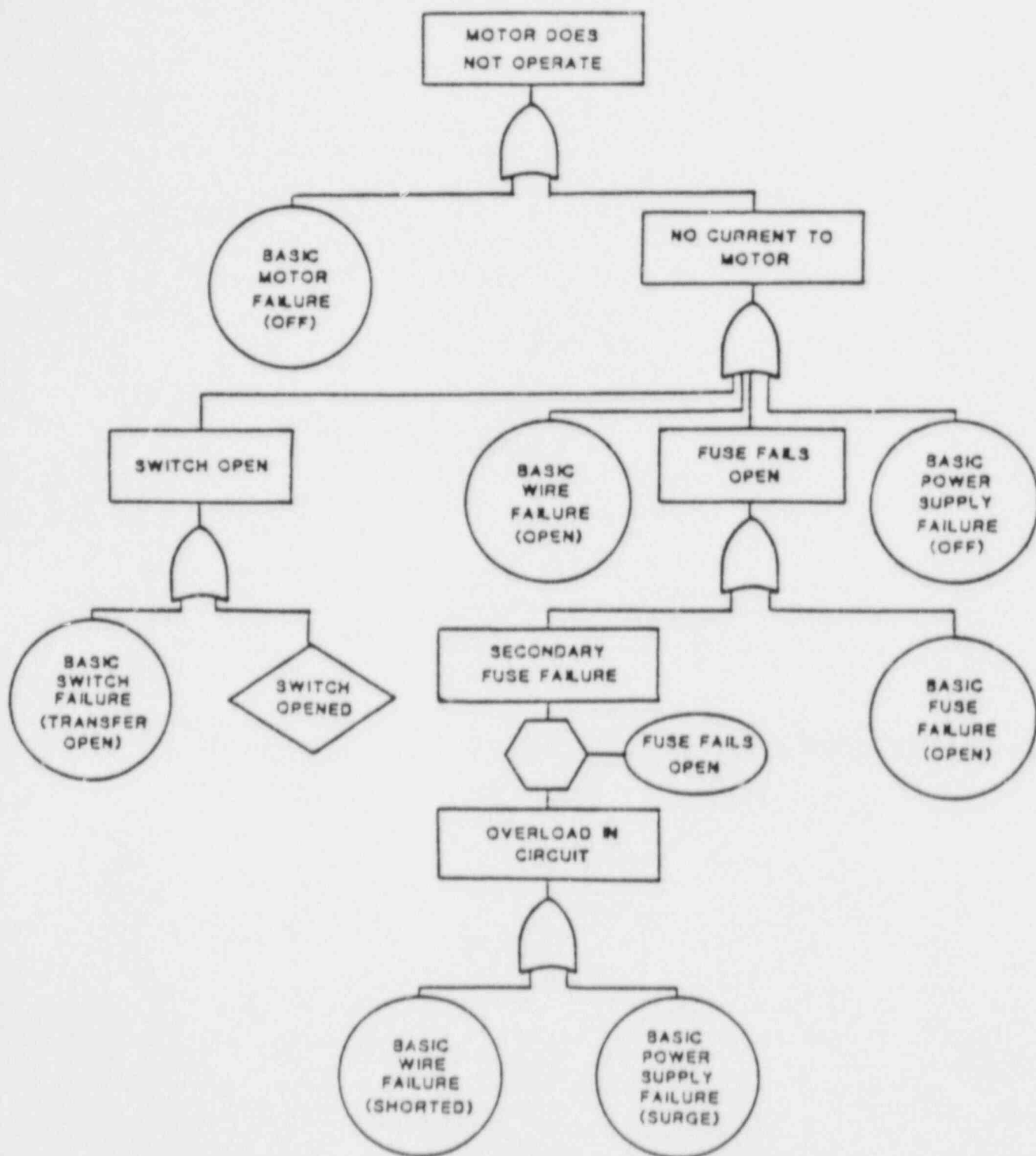


FIGURE 2-5
SIMPLE FAULT TREE MODEL

Although event tree analysis and fault tree analysis are almost always used in nuclear plant PRA, other methods may occasionally be used to supplement these primary system modeling techniques. Two of these supplementary techniques are the reliability block diagram and the failure modes and effects analysis (FMEA). A simple example of a reliability block diagram is shown in Figure 2-6. The structure of a reliability block diagram essentially matches the structure of the system which is being modeled. Blocks which represent system components are placed on the diagram using the appropriate parallel and series logic. By assigning reliability values to each of the components represented on the reliability block diagram, and combining those reliability values in accordance with the appropriate combinational logic, a system reliability value can be calculated. This modeling technique is occasionally used as a preliminary step to fault tree analysis because it provides a convenient way to identify the relationships between system components. It is not required, however, and is not in widespread use in nuclear power plant PRA.

Like the reliability block diagram, the FMEA is sometimes used as a supplement to fault tree analysis. The FMEA is used to compile basic component reliability data and to display it in tabular form. This modeling tool essentially provides a listing of system components and indicates their applicable failure modes. In addition, the effects of those component failures in terms of system operability are listed. An example of an FMEA is shown in Table 2-1.

2.1.2 Accident Process Analysis

The plant damage states which are identified in the system modeling task are used as the starting points for accident process analysis. This PRA task assesses the reactor core behavior and containment response under accident conditions. The degrees of core damage which may result from a particular accident are identified through structural analysis. In addition, the behavior of radionuclides as they migrate throughout the containment from their point of release is examined. Finally, the containment response is delineated using a containment event tree. A task flow chart for the containment and degraded core analysis activity is shown in Figure 2-7. The outcome of the accident process analysis task is the identification of potential releases to the environment in terms of their energies, magnitudes, and timing. Accident process analysis is discussed in more detail in Topics 11 and 12.

2.1.3 Accident Consequence Analysis

The radiological release information which is developed in the accident process analysis task serves as a direct input to the accident consequence analysis task. Beginning with an understanding of the magnitudes, energies, and timing of radiological releases which result from various accident sequences, the environmental transport, dosimetry, and health and property damage aspects of the accidents are assessed. Using local weather data, the probable radiological dispersion and depletion mechanisms are determined. Based on this information, estimates of population radiological doses and environmental contamination can be developed. Finally, the health effects and property damage which result can be estimated. Figure 2-8 shows the task flow of the various aspects of environmental transport and consequence analysis. Accident consequence analysis is discussed in Topic 13.

2.2 Levels of PRA

A PRA may be performed on any of three levels of resolution. The level which is chosen for a particular study depends on the nature of results which are desired. For this

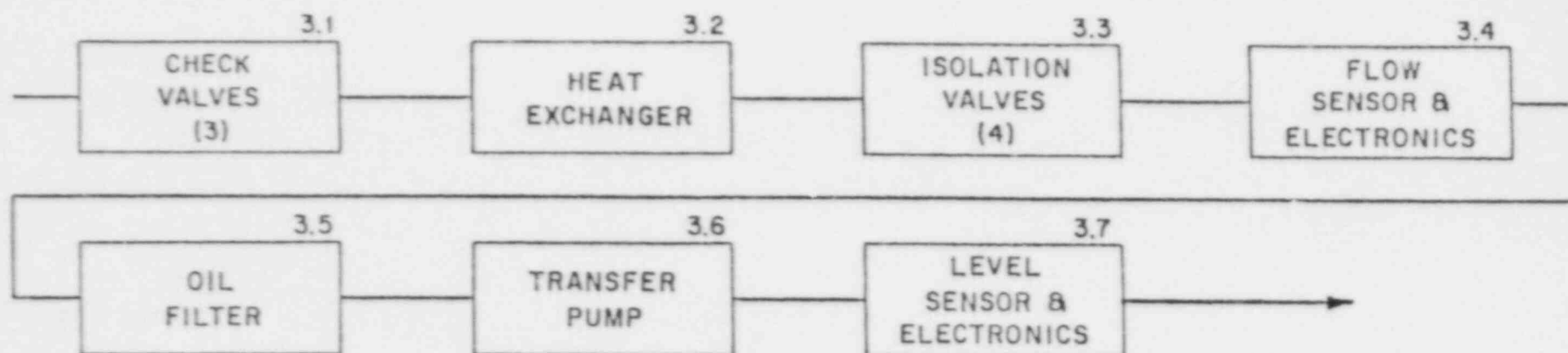


FIGURE 2-6
EXAMPLE RELIABILITY BLOCK DIAGRAM

TABLE 2-1
TYPICAL FORMAT FOR A FAILURE MODE AND EFFECTS ANALYSIS

Component Identification	Function	Failure mode	Failure mechanism	Effect on system	Method of failure detection	Remarks
1. Circuit breaker S2/RTA, RTB, BYA, BYB	Trip	Fail closed	Mechanism jammed	Makes trip 1/1	Monthly test	
			UV trip attachment mechanism stuck	"	"	
		Fail open	Main contacts fused	"	"	
			Loss of dc control power	Spurious trip	Spurious trip	Immediate detection
2. DC control relay	Break circuit to trip breaker UV coil on trip (de-energize to trip)	Fail closed	UV coil failure	"	"	
			Worn trip latch	"	"	
			Contacts shorted or fused	Makes trip 1/1	Monthly test	
		Fail open	Armature jammed	"	"	
			Wiring fault	"	"	
			Loss of dc control power	Spurious trip	Spurious trip	Immediate detection
3. AC control relay X1A, B, X2A, B, X3A, B	Break circuit to dc relays on trip (de-energize to trip)	Fail closed	Coil failure	Spurious trip if 2/2 fail	"	
			Broken contacts	"	"	
			Broken wire or loose connection	"	"	
		Fail open	Contacts shorted or fused	Makes 1 train 2/2 vice 2/3	Monthly test	
			Armature jammed	"	"	
			Wiring fault	"	"	
			Loss of ac power (instrument bus)	Spurious trip if 2/3	Spurious trip	
			Coil failure	"	"	
4. Alarm unit PC-1,2,3	Remove ac power to relays for $F_M > P$ set	Fail off	Broken contacts	"	"	
			Broken wire or loose connection	"	"	
			Transformer failure	Makes both trains 1/2	Spurious trip if 2/3 fail	Partial trip alarm
		Fail on	Open circuit in output section	"	"	
			Setpoint drift	"	"	
			Short in output section	Makes both trains 2/2	Monthly test	
5. DC power supply PQ-1,2,3	Provide power for analog current loop	Fail low or off	Setpoint drift	"	"	
			Transformer failure	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm
		Fail high	Diode failure	"	"	
			Heat effects	Makes both trains 2/2	Monthly test	
6. Pressure transmitter PT-1,2,3	Convert pressure to analog current	Fail low	Misadjustment	"	"	
			Corrosion	Makes both trains 2/2	Monthly test and comparison with redundant channel indicators	Possible immediate detection
			Wear	"	"	
			Mechanical damage	"	"	
		Fail high	Heat effects	"	"	
			Misadjustment	Makes both trains 1/2	Spurious trip if 2 fail	Partial trip alarm

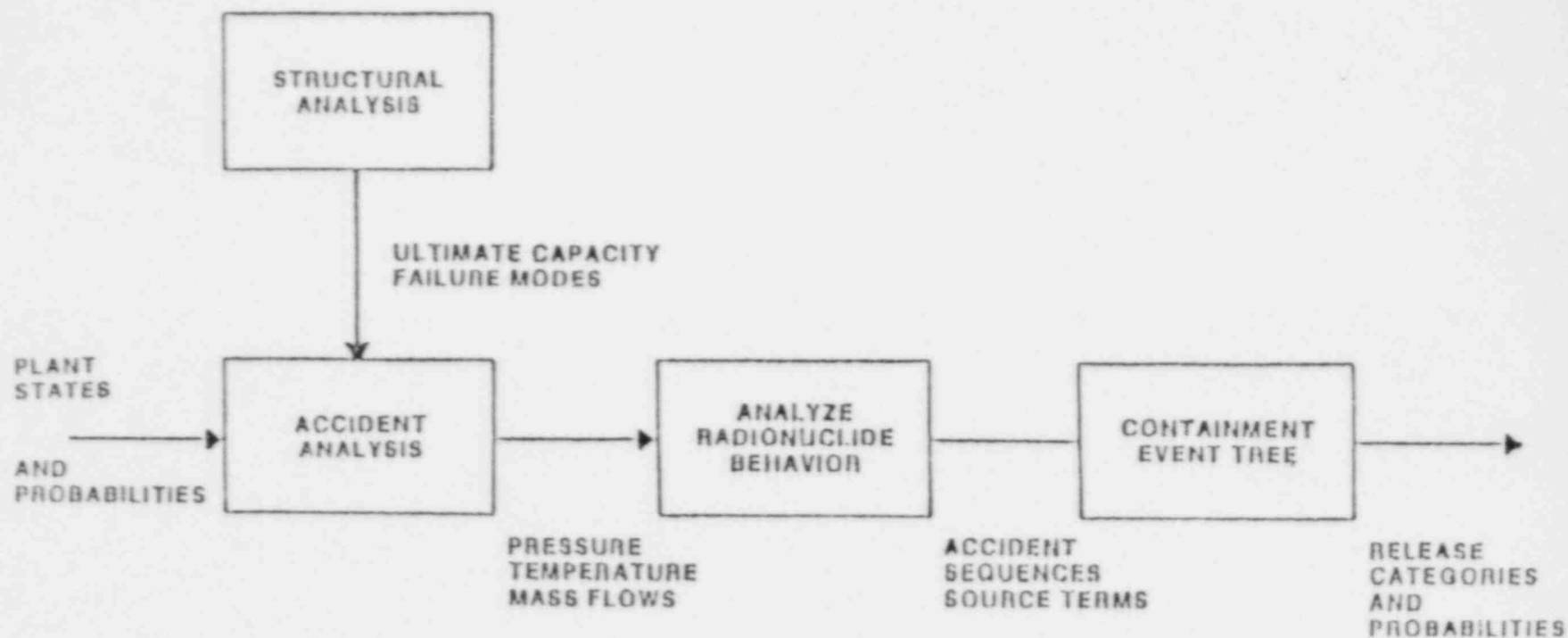


FIGURE 2-7
CONTAINMENT AND DEGRADED CORE ANALYSIS FLOW CHART

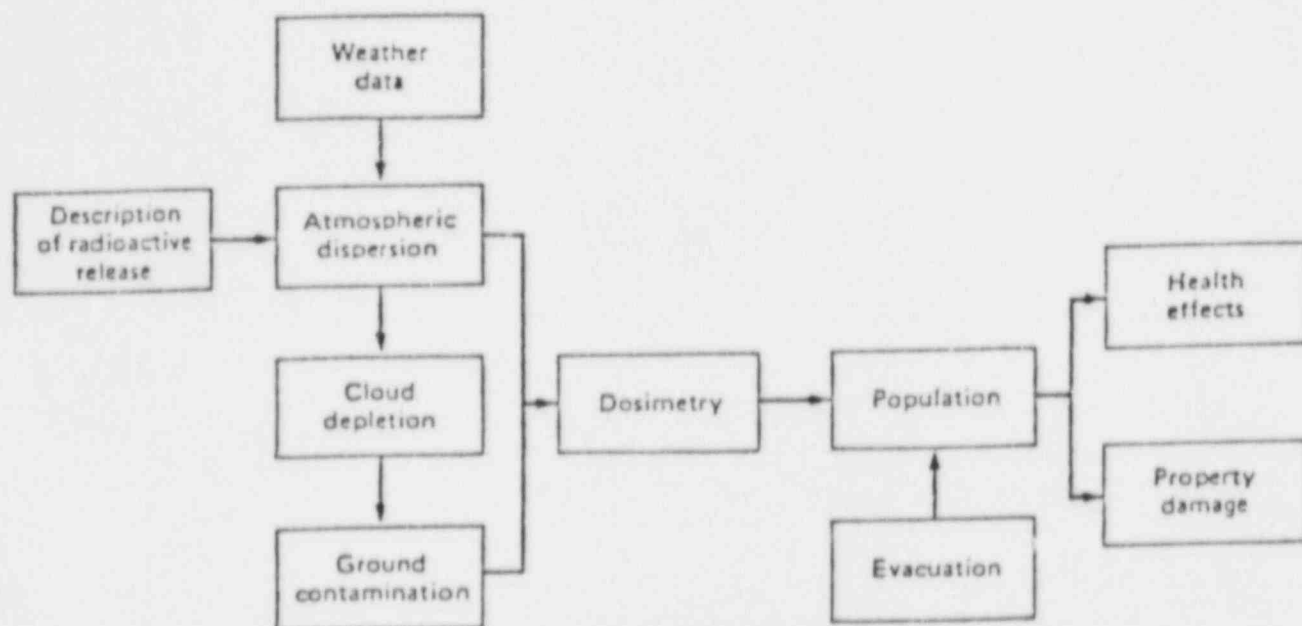


FIGURE 2-8
ENVIRONMENTAL TRANSPORT AND CONSEQUENCE ANALYSIS

reason, it is very important that the goals of the PRA study are carefully defined and explicitly stated prior to the beginning of work.

A Level 1 PRA is one in which only system modeling is performed. No accident process analysis or consequence analysis is included in a Level 1 PRA. A Level 1 PRA may be performed when the primary goals of the study are to assess only accident initiators, safety system response, and the resultant plant damage states. The advantage of a Level 1 PRA over more extensive studies is that a study of this limited scope can be accomplished relatively quickly and at less cost.

A Level 2 PRA is one which includes both system modeling and accident process analysis. By extending the scope of the study to include accident process analysis, the study results include not only the identification of plant damage states, but also insights into the core and containment behavior which accompany those plant damage states. These insights into core and containment behavior may include the timing and extent of core damage, intra-containment fission product transport, fission product inventory, and identification of the magnitude, energy, and timing of radiological release to the environment. These types of insights are both useful in their own right, and may be used as the basis for an informal assessment of accident consequences. It has been argued that a characterization of radiological releases to the environment provides at least an indirect indication of the potential offsite consequences. For a more detailed assessment of offsite consequences, however, the PRA must include accident consequence analysis.

A Level 3 PRA includes all three elements of risk assessment - system modeling, accident process analysis, and accident consequence analysis. A Level 3 PRA is performed when the most accurate and detailed assessment of risk is desired. By combining all three elements of PRA, a Level 3 study examines potential reactor accidents from the identification of initiating events through the ultimate long-term health and property damage effects of those accidents.

Each of the three levels of PRA may or may not include consideration of external events. External events include such phenomena as fires, floods, and earthquakes. External events are defined as events which are external to the plant systems that can act as accident initiators and/or contribute to the unavailability of plant systems. Depending on the goals of the analysis, a PRA may include an examination of any, all, or none of the external events which may apply to a given plant. For example, potential seismic events may be of great concern with respect to nuclear plants in the western United States. A PRA for these plants is likely to include consideration of seismic events. However, a plant located in Kansas, where earthquakes occur far less frequently, may not be assessed with respect to seismic events. External events are discussed in Topic 10.

2.3 PRA Element Quality Assurance

A PRA of a nuclear power plant is an extremely complex activity. Although the techniques of PRA are rigorous and disciplined, there are many opportunities for errors or omissions to enter into the study. For this reason, many recent PRAs have included formal quality assurance programs. These quality assurance efforts have focused primarily on five aspects of the PRA. These aspects are listed and briefly discussed below:

Completeness - Treatment of the full range of tasks, analyses, and model construction and evaluation should be assured. The completeness issue is most significant in any probabilistic assessment. It includes such diverse

concerns as identification of initiating events, determination of plant and operator responses, specification of system or component failure modes, physical processes analysis, and application of numerical input data.

Comprehensiveness - A probabilistic assessment is unlikely to identify every possible initiator and accident sequence. The aim is to ensure that the significant contributors to risk are identified and addressed. Assurance must be provided that comprehensive treatment is given to all phases of the study in a manner which provides confidence that all items of significance have been considered.

Consistency - Consistency in planning, scope, goals, methods and data within the study are essential to a credible assessment. Equally important is an attempt to achieve consistency from one study to another, especially in methodologies and the application of data to allow comparison between system or plant design. In many cases, the acceptability of an activity is based on its comparability (risk) with other similar activities. The use of standardized methods and procedures enhances comparability.

Traceability - The ability to retrace the steps taken, i.e., reconstruct the thought process to reproduce an answer, is important not only to the reviewer and regulator but also to the study team.

Documentation - The documentation associated with a PRA is substantial. Large amounts of information are generated during the analysis, and many assumptions are made. The information must be well documented to permit an adequate technical review of the work, to ensure reproducible results, to ensure that the final document is understandable, and to permit informed interpretation of the study results.

2.4 Summary

The field of PRA includes the three general elements of system modeling, accident process analysis, and accident consequence analysis. Depending on the specific aims of a particular study, a PRA can consist of only system modeling (Level 1), system modeling and accident process analysis (Level 2), or all three elements (Level 3).

In performing a PRA of any of the three levels, a number of different techniques and approaches may be used. Their applications are discussed in subsequent topics.

TOPIC 3
APPLICATIONS OF PRA

3. APPLICATIONS OF PRA

As discussed briefly in Topics 1 and 2, PRA techniques can be used to address a wide variety of safety and reliability issues. Just as the specific complement of techniques which are used depends largely on the aims of the study, PRA techniques have evolved, in large part, in response to specific needs and for specific applications. This topic describes the evaluation of PRA in a general sense, and discusses how PRA applications have varied. The topic concludes with a discussion of some unresolved issues in PRA.

3.1 Programmatic Advancements in PRA

As stated earlier, there is little new about the concept of risk assessment. Informal risk assessments have been performed since the beginning of time as people have decided how they can best meet their needs without subjecting themselves to injury or loss. Although the concept of risk assessment is not new, the development of formal, disciplined techniques with which to evaluate risk and reliability is very new. The fault tree methodology, for example, was developed by Bell Laboratories and was applied by the Boeing Company in the early 1960's to the Minuteman missile program. This application of methodology represented the first step toward disciplining, codifying, and documenting an analysis technique that addressed itself to systems analysis. For the nuclear power industry, the formal risk assessment activity began in the mid-1950's. In 1956, WASH-740 was published and was a sort of "primitive" risk assessment for the operation of nuclear power plants. This risk assessment was utilized to help determine the level of indemnification that needed to be provided for the operation of nuclear power plants in the utility environment. No systematic methods for the systems analysis or for risk assessment had been developed at the time of WASH-740 and therefore the analyses that were used were deterministic analyses of the sort that one normally sees in a Safety Analysis Report (SAR).

3.1.1 WASH-1400

Over several years, between the beginning of the activities within the nuclear power industry until the emergence of WASH-1400 report, systems analysis was applied in isolated cases, including the evaluation of probabilities of certain events. The efforts relative to the WASH-1400 activity were actually begun in about 1972 and the report was completed and published in 1975. WASH-1400 was a landmark in the nuclear power industry and was the first major, relatively complete probabilistic assessment ever made for the nuclear industry. Its publication brought confidence and support from the nuclear industry because most felt that it identified the fact that the deployment of nuclear power plants in our society did not represent a major risk. However, to intervenors and opponents, the same document was used to show that the risk associated with nuclear power plants was unacceptable. It was pointed out that this was a new technology, that many mistakes could have been made, that assumptions were likely to have been incorrect, that uncertainties in the data were probably not properly accounted for. As a result of these comments, a committee to evaluate the WASH-1400 document was convened under the leadership of Dr. Harold Lewis. After considerable discussion, study, and testimony, the Lewis Committee finally published a report. Generally the report indicated that the WASH-1400 effort was very well done, it was comprehensive, and it was a very excellent first attempt at a very difficult methodology for evaluating risk from such a complex facility. The Lewis Report made several comments and recommendations. The most important recommendation was that the methodology used in WASH-1400 should be used more extensively in the licensing process to evaluate the severity and importance of safety questions. The criticism was made that the

uncertainty bounds on the data were unjustifiably narrow. This might have led some to conclude that the risks shown were considerably understated.

A number of insights were developed as a result of the WASH-1400 study, and subsequent studies, which have generally been incorporated into subsequent PRAs. These insights included the following conclusions: small LOCAs and transients are larger risk contributors than the very large LOCAs. This is somewhat different from the position that is taken in SARs which look carefully at very large events but do not look at small events that are encompassed by the larger events. Human error turns out to be a major contributor to risk according to several risk assessments that have been performed. Dominant accident sequences vary from one plant to another, primarily because of differences in design and operational practices. System unavailability varies up to two orders of magnitude from one plant to another. For example, an auxiliary feedwater system for one plant which appears to be similar to another might have a very significant variation in its availability. Plant design differences can affect the risk as greatly as population differences near the plant. Overpressure failure of the containment is the containment failure mode which makes the greatest contribution to risk for LWRs.

Not long after the Lewis Report was completed, the TMI-2 incident occurred. Since this involved the auxiliary feedwater system for that plant, several studies similar to WASH-1400 were made throughout the industry to evaluate the likelihood that auxiliary feedwater systems would be unavailable to perform their function. This program demonstrated the value of performing PRA activities of very narrow scope to address specific, system-level issues.

3.1.2 Reactor Safety Study Methods Application Program (RSSMAP)

Shortly after the publication of the RSS, the Nuclear Regulatory Commission (NRC) established the Reactor Safety Study Methods Application Program (RSSMAP). This study was a two-year effort to apply the RSS techniques to four nuclear power plants (Sequoyah-1, Oconee-3, Calvert Cliffs-2, and Grand Gulf-1) of design significantly different from the two RSS plants (Surry and Peach Bottom). The goals of this program were to:

- Identify risk dominating sequences for a broader spectrum of plant designs than was covered in the RSS.
- Compare the results with the RSS.
- Identify design differences between plants which significantly affect risk.

The scope of the program was fairly limited. A minimum level of effort was expended in achieving the goals. The method chosen was to develop plant-specific event trees for each plant, similar to what was done for the RSS. However, fault trees were not developed for the safety systems and support systems. Instead, RSS results were used as much as possible. Also, the release categories, human error modeling, and data base were obtained from the RSS. No consequence analysis was performed, and no external events (seismic, fire, flood, missile, etc.) were considered. This program, thus, demonstrated that abbreviated PRA efforts which borrow from previous, more complete studies could be performed.

Even with the limited scope, the RSSMAP studies resulted in several improvements to the state of the art. The transient event trees were expanded and improved. Complementary events (success events) were extensively used in the quantification of

dominant accident sequences. Loss of coolant accident (LOCA) and transient event trees were interconnected to account for situations in which events in the transient event trees led to LOCAs (e.g., stuck open relief valves). Finally, the use of the MARCH and CORRAL codes for the modeling of core melt and fission product release was an improvement over the RSS techniques.

Results from the RSSMAP studies indicated that the list of dominant accident sequences relative to risk varied considerably among the plants. For example, a dominant sequence for the Sequoyah-1 plant involved the failure of core cooling and containment spray in the recirculation mode due to plugged drains connecting the upper and lower containments. Also, the likelihood of an interfacing system LOCA was judged to be higher at Oconee-3 than for other plants.

3.1.3 Interim Reliability Evaluation Program (IREP)

In 1979, the NRC initiated another program to further broaden the base of PRA applications to nuclear power plants. Entitled the Interim Reliability Evaluation Program (IREP), the objects of this program were to:

- Identify the dominant accident sequences relative to public risk from the operation of nuclear power plants.
- Develop a base for more detailed and more widespread application of PRA to nuclear power plants.
- Expand the number of people experienced in PRA methods, both in NRC and in the nuclear power industry.
- Develop procedures for the competent use of PRA techniques in the possible extension of the IREP study of all U.S. light water reactors (LWRs).

The IREP study was divided into two phases. The first phase was a study of the Crystal River-3 plant and the subsequent preparation of a preliminary set of procedures to be used for other IREP studies. The second phase included analysis of four nuclear power plants: Browns Ferry-1, Arkansas Nuclear One-1, Calvert Cliffs-1, and Millstone-1.

The scope of the PRA studies was limited in several ways:

- No consequence analysis.
- No external events.
- Limited uncertainty and sensitivity analysis.

Despite these limitations, however, significant advances to the state-of-the-art were made in the development and standardization of system fault trees, in the inclusion of human error in both the fault and event trees, and in the identification of initiating events.

The results of the individual IREP studies indicated specific potential deficiencies within each plant analyzed. General results included a better understanding of the role of support systems as both accident initiators and mitigators, and the determination that repair times for support system failures can be very long. Also, the significance of reactor coolant pump seal ruptures relative to risk was better established.

3.1.4 Integrated Safety Assessment Program (ISAP)

In a project to utilize PRA in the safety review process, the NRC has established the Integrated Safety Assessment Program (ISAP). This pilot program would require systematic PRAs to be conducted for two operating nuclear power plants to test the procedures for and effectiveness of the approach.

As a preliminary effort, the NRC has co-sponsored the development of the procedures guide addressing all aspects of PRA for LWRs. This guide, NUREG/CR-2815 has recently been published.

3.1.5 Utility Studies

Parallel with the NRC-sponsored studies relating to PRA methods and applications, utility-sponsored studies have also been conducted. Several of these studies will be discussed. The first major utility-funded PRA was the Oyster Creek PRA. This study improved upon the methods established in the RSS by:

- Conducting a site-specific consequence analysis
- Providing more detail in the event trees
- Improving the data base
- Conducting a more detailed seismic analysis
- Providing a more conservative treatment of uncertainty and uncertainty propagation.

The unpublished results (1979) of the Oyster Creek study were in general agreement with the RSS results.

The Limerick Generation Station PRA was performed at the request of the NRC in 1981 because of the high population density near the plant. In this study, external events were not considered. However, improvements to the RSS methodology included:

- Revised list of accident initiators specific to the Limerick plant
- More detailed modeling of the accident sequences
- Site-specific consequence analysis
- Success criteria closer to best-estimate compared with the conservative RSS criteria.

Results from this study indicated that the frequency of core melt and the public risk (early and latent fatalities) were lower for the Limerick plant than those from the RSS.

A monumental study, both in terms of cost and effort, was the Zion Station Probabilistic Safety Study. This utility study was initiated in response to an NRC study of the Zion plant which incorporated RSS (Surry) plant models rather than Zion-specific models. This utility-sponsored study was a major advance in RSS methodologies. The external events analyses were much more detailed, especially for seismic and fire events. The data base for initiating events, systems, and components was expanded considerably, and was made

for initiating events, systems, and components was expanded considerably, and was made plant-specific. Analyses of the degraded core accident progression and the containment response were much more detailed. The effects of particle bed cooling in the lower plenum and on the concrete basemat were considered, and credit was taken where possible for these effects to terminate the molten core accident progression. The results of these efforts were detailed core melt and containment response event trees which indicated that many core melt accidents would not result in serious releases of radioactivity to the atmosphere. Finally, the consequence modeling included site-specific terrain, meteorology, and evacuation routes. Results of the Zion Station study indicated that even though the frequency of core melt was similar to the RSS results, the risk was much less, due to more credit being taken for the potential termination of degraded core accident progression and for containment integrity being preserved.

3.2 Current and Future PRA Applications

The foregoing discussion has focused on the ways in which past programs have contributed to the development of PRA techniques. Some of these developments are summarized in Table 3-1. As an engineering tool, PRA can be used in a variety of different ways. In addition, it seems likely that with continued refinement and further acceptance, the applications of PRA will expand in the future.

One recommendation of the Lewis Committee, which reviewed the WASH-1400, was that risk assessment methodology should be used in the regulatory process. A productive area for application would be the ranking of generic safety issues. A number of generic safety issues have been identified but not all are equally important. Risk assessment techniques can be used to rank these issues in order of priority so that the most important ones to safety can be resolved on the earliest schedule.

Occasionally, regulatory requirements are imposed without comprehensively evaluating their contribution to safety or their cost. PRA can be used as a cost/benefit tool to evaluate proposed regulations. The assessment of design or operational adequacy is an obvious application of the risk assessment technology. There are a myriad of other applications that can be made including prioritizing those things that should be inspected on a routine basis or that should be tested and maintained on a routine basis. A number of examples of applications of PRA and PRA type methodology are provided in Table 3-2.

Figure 3-1 presents a comparison of core melt frequencies predicted by a variety of PRAs. These frequencies, with two exceptions, fall in the range between 10^{-4} per year and 10^{-5} per year for core damage. The two exceptions are Big Rock Point and Crystal River 3. Some explanation of these two is justified. It should be pointed out that Big Rock Point is a relatively small reactor capable of producing about 70 megawatts of electricity. It was put into commercial operation in 1965, so not only is it small but it is a fairly old design (a BWR). Because of the relatively high core damage frequency for Big Rock Point, the full risk analysis approach was useful. Using the risk assessment, it could be shown that even with a high core melt frequency compared with other nuclear plants, the risk from the operation of Big Rock Point was well within the line compared to the other plants. This is because of two major considerations. First, the plant is fairly small and has a smaller fission product inventory and second, it is very remotely sited in the northern portion of Michigan such that the population concentrations within several miles of the plant are quite small and they are sparse. The other PRA showing higher than comparable core damage frequencies is the Crystal River 3 plant. In this case, investigators drew on the experience of the Three Mile Island accident to identify extensive systems interactions which increased the core melt frequency. No consequence analysis was performed for the Crystal River study.

TABLE 3-1
PRA METHODOLOGICAL AND EXPERIMENTAL ADVANCE

1962	Development of Fault Tree Analysis
1969	Development of KITT Codes
1974	Conference on Reliability and Fault Tree Analysis
1975	Reactor Safety Study
1975	Development of CRAC Code
1975	Core Meltdown Experimental Review
1978	Data Summary Licensee Event Reports
1978	ANS Topical Meeting on Probabilistic Analysis
1979	Fault Tree Handbook
1980	Development of MARCH Code
1980	Handbook on Human Reliability
1981	Steam Explosion Experiments and Analysis
1981	Zion PSS Seismic Analysis
1982	Industry/NRC PRA Procedures Guide

TABLE 3-2
EXAMPLES OF APPLICATIONS

- Operator Training and Simulator Design
 - Present list of severe accident sequences with rough assessments of likelihood, severity, and root causes
 - Examine symptom profile vs. operator response
 - Assess instrumentation and status monitoring
- Emergency Planning
 - Develop guides for declaration of site and general emergencies
 - Help in diagnosis and prognosis of accidents
 - Use dominant sequences to train emergency response personnel on what to expect
- Procedure Adequacy
 - Explore risk impact associated with individual procedures
 - Identify procedures which need strengthening
- Limiting Conditions of Operation
 - Optimize allowable outage times and surveillance intervals
- Systems Integration Studies
 - Identify "weak link" auxiliary systems
 - Evaluate cross-system human interactions
- Significance of Component Reliability
 - Develop importance measures of components trains and systems for use in cost-benefit analyses of reliability improvements. Discriminate need for qualification tests and in-service inspection
- System Reliability
 - Assess repair possibilities in more likely accidents
 - Train in fault diagnosis
 - Assess surveillance practices
- Accident Sequences - Explore Value of Risk Reduction Modifications
 - Evaluate attendant risks associated with changes
- Evaluation of operating experience
 - Evaluate importance of precursors
 - Evaluate trends in plant-specific data which varies from generic data base
- Validate Models
 - Evaluate and improve models based on operational experience
- Design Errors and Generic Safety Issues
 - Estimate severity level where issue becomes important
 - Permit bounding analyses to be used for resolution
 - Place concerns in perspective

COMPARISON OF PRA CORE MELT FREQUENCIES

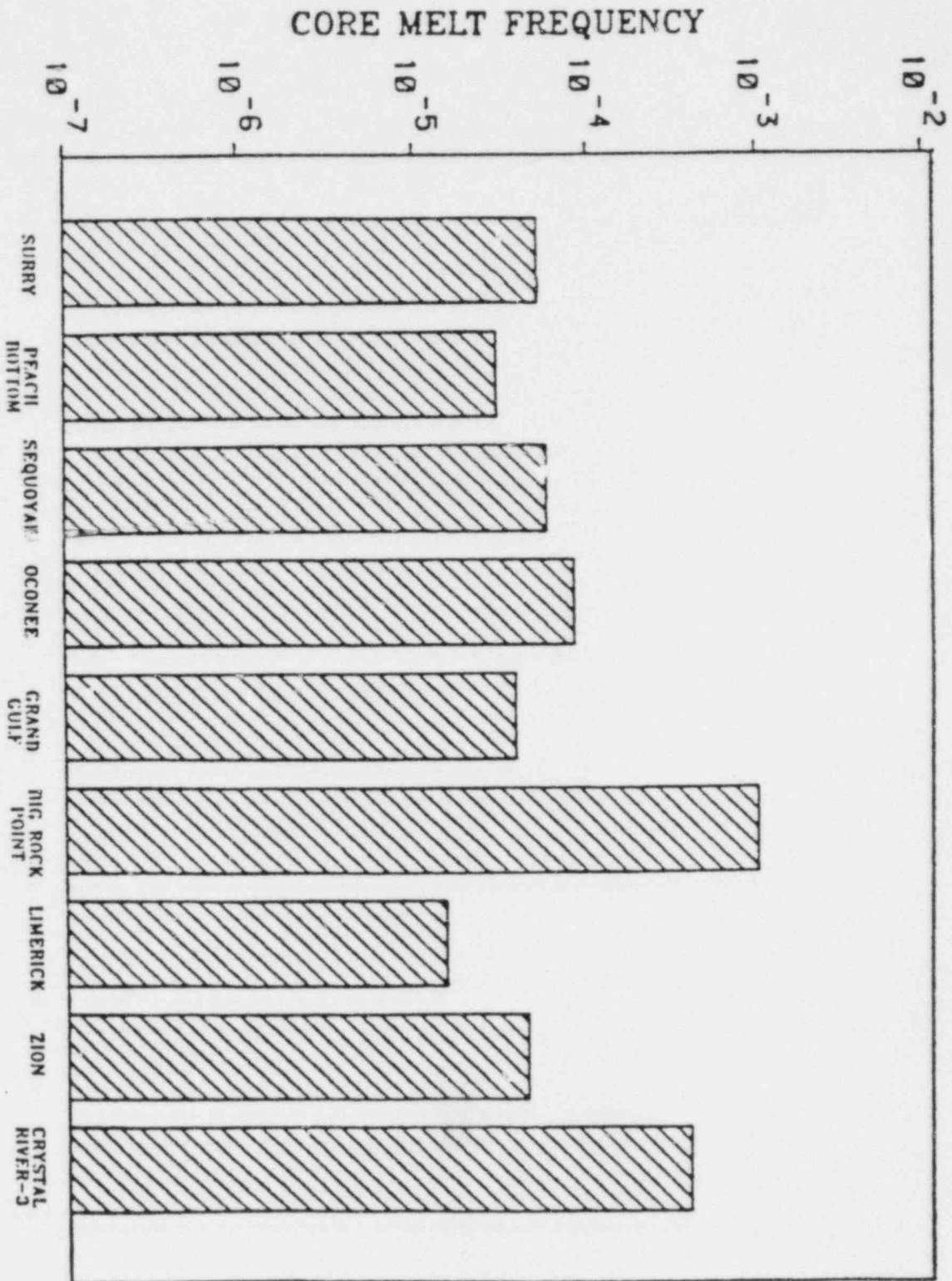


FIGURE 3-1
PROBABILISTIC RISK ASSESSMENT

3.3 Unresolved Issues

A number of PRA issues are the subject of discussion at the present time. Should PRAs be used in the absolute sense or should they be used only for comparative analysis? In the absolute sense, the uncertainties tend to limit one's ability to state absolute conclusions. However, because similar models and similar data are used from plant to plant, comparisons can be made. As the technology advances and as data accumulation increases, absolute evaluations may become more rational. The NRC has been working on a quantitative safety goal for nuclear power plants through the use of PRA for several years. Presently there is a revised document available to the public for comment regarding the safety goals. Traditionally, there have been two safety goals. First, an overall goal regarding the consequences of nuclear power plant accidents in the probabilistic sense, dealing with immediate deaths and with latent cancer fatalities. A second goal has been to identify an acceptable probability of core damage. Without core damage, consequences of significance do not occur since core damage is the precursor of consequences to the public.

Several specific aspects of PRA must also be included in a discussion of unresolved issues. These are identified below.

Dependencies - The treatment of dependencies in a PRA has been a difficult area to resolve since the beginning. It has been shown that common mode and common cause failures may dominate the sequences that lead to high consequences. Therefore, treatment of the dependencies is an issue that needs to be resolved.

Completeness - Completeness is an area of special concern. It should not be the goal of a risk assessment activity to identify every initiator and every sequence of events that could conceivably lead to the release of radioactivity because such would be an impossible task to complete. However, a comprehensive treatment of the initiators in the event sequences is necessary and the case must be made that the study is comprehensive in its treatment of events and sequences leading to consequences to the public. The aim of the risk assessment should be to provide assurance that the dominant contributors to risk are identified and that any event or sequence that may contribute to risk that is not included will make a very small contribution compared to the overall risk evaluated.

Human Reliability - The subject of human reliability has been addressed since the WASH-1400 study was performed. The variability of human behavior presents a special problem for analysts. Methods of evaluating the effects of human reliability on the risk associated with a nuclear power plant have been implemented and are constantly being examined and updated.

Uncertainties - Uncertainties in the plant model, the core damage model, the containment model, and the risk model are another area of special concern. Several research and development programs are presently underway to help us better understand the uncertainties in these models. As the uncertainties are reduced, the level of confidence in the analytical results will be increased.

Role of PRA - The initial PRAs were performed to evaluate the level of plant risk due to operating nuclear power plants. The opinion that a PRA can only be performed in an as-built operating plant, leads one to believe that a PRA would only be effective in the licensing process or as a tool to evaluate backfit or regulatory requirements. This may not be the case. The successful PRA performed for the Clinch River Breeder was done

during the design process, and was of considerable value for providing input to the design of the plant. The issue remains unresolved however, as to how PRAs can best be used.

3.4 Role of PRA

PRAs play a beneficial part in the evaluation, understanding and safety of nuclear power plants. The performance of a PRA provides a comprehensive decision making tool which is a framework by which safety can be measured and modifications can be evaluated regarding their contribution to safety. The PRA methodology provides an excellent method by which safety issues may be ranked in order according to their significance. Design weaknesses have been located in plants through the use of the PRA even though these plants met the traditional licensing requirements. The PRA plays a unique function in linking the design, operation, maintenance, testing, and safety of the plant. In addition, the PRA activity can not only enhance safety but provides the basis for increasing plant productivity. Of course, plant productivity is not necessarily a subject that would be of concern to the regulator. To a regulator, however, it certainly is of concern when considering the long-term viability of the nuclear industry.

There are significant limitations to the performance of a PRA as well. PRA is not expected to replace the traditional licensing approach but is expected rather to support and complement that activity. Although a useful, and in the opinion of some, a necessary tool to the design and operation of a nuclear plant, the PRA is not a panacea. It will not solve all problems. The PRA will not yield the type of results that are desirable unless it is properly scoped at the beginning and managed throughout the performance of the work. Full documentation of the PRA is required so that it can be understood, it can be traceable, and it can be more useful to the regulator and the utility. The limitations of data and models are significant. They are significant but they are not insurmountable. There are uncertainties in the data and the uncertainties can be properly dealt with, primarily through the use of the sensitivity analyses, to determine whether or not the uncertain data that is used is in an area that contributes significantly to the results of the work. Model uncertainties are significant in a number of areas. The modeling of the plant and the plant response are less uncertain than the modeling of, for example, the degradation of the core. However, this indicates that the uncertainty related to the core damage frequency is smaller than the uncertainty related to the behavior of the degraded core, containment, and fission products that are released to the environment. Therefore, the evaluations up to the core degradation; that is, the result of a Level I PRA, are less uncertain than the remaining portions of an overall risk assessment. This indicates that the core damage frequency can be taken as a reasonable point for a goal as far as plant design is concerned.

There has been increasing emphasis on PRA ever since the WASH-1400 was completed. Several review commissions have offered the recommendation that PRA techniques should be used in more varied applications to enhance the safety of nuclear power plants. Many of those have already been mentioned, including the prioritization of unresolved safety issues. The methods being used in PRA are becoming more standardized. As they do so, and as procedures to assist in achieving standardization are developed, the consistency between one PRA and another will be greater and the job of the peer reviewer and the regulator will be made easier. It is expected that this trend toward standardization will continue and that the PRA methodology will become ever more useful in the nuclear industry. Currently, PRA is being used for a number of purposes to evaluate the worth of backfit or design changes. It would appear that the methodology can be used very effectively in design and cost optimization studies and it is expected that this will become a major use of PRA in the future.

TOPIC 4

RELIABILITY AND RISK ANALYSIS

4. RELIABILITY AND RISK ANALYSIS

4.1 Introduction

The common thread that runs through a discussion of the parameters of availability and reliability is the fact that they are both expressed in terms of a probability. Availability has already been defined as "the probability that a system or equipment will perform satisfactorily at any point in time when used under stated conditions, where the total time considered includes operating time, active repair time, administrative time, and logistical time." The related concept of reliability was defined as "the probability that a system or equipment will perform satisfactorily for at least a given period of time when used under stated conditions." A number of parameters are considered in a calculation of system or component reliability or availability. These parameters are the subject of this section.

4.2 Probability

In the context of PRA, the concept of probability is often thought of in three ways. Each has its own applications, and collectively, then provide a good feel for what is specifically meant by the term "probability".

The classical probability concept is based on the relationship between the number of times some event (E) occurs and the number of opportunities for that event to occur. This probability concept is akin to what is thought of as "chance". To illustrate the concept, consider a box filled with ten marbles, seven of the marbles are black, three are white. Based on the classical definition of probability, there is a probability of .30 of drawing a white marble on the first try (3 chances in 10 equals .30). If, in fact, a white marble is drawn on the first try, the population of marbles has been changed (2 white, 7 black) and so has the probability of drawing a white marble on the second try. This probability is now 2 chances in 9 equals .22. This probability concept is expressed as:

$$PR(E) = \frac{n}{N}$$

(Equation 4-1)

where: n has characteristic E
and N represents equally likely outcomes.

The second concept of probability that is considered in PRA is the frequentist concept. This concept is also based on the relationship between the number of occurrences of an event and the number of opportunities for that event to occur. This concept, however, regards the total number of opportunities as being ever increasing and not predefined (as was the marble population in the example above). This view of probability can be expressed as:

$$PR(E) = \lim_{N \rightarrow \infty} \frac{n}{N} \quad \text{(Equation 4-2)}$$

The third definition of probability is the subjective concept and really represents the degree of belief that a given event may occur. This subjective view of probability represents part of the basis for Bayesian inference which is discussed briefly in Topic 8.6. Given these definitions of probability, basic availability concepts are described below. Much of the following material is drawn from WASH-1400, Appendix II.

4.3 Unavailability

Component unavailability is defined in general as the probability of being in a failed state when required (i.e., the probability of the component being "unavailable"). Point unavailability is associated with a requirement of the component at a particular time. The point unavailability is the probability that the component is down at that time. Interval unavailability is associated with some interval and is the fraction of time that the component is down. Interval unavailability is that computed by the ratio of downtime to some cycle time (the base time interval).

When testing is performed periodically and failures repaired, and when the requirement or demand of the component occurs at random, the average point unavailability will be equal to the interval unavailability. In other words, the two types of unavailability are equivalent and either can be used in the calculations. Any transient type of deviations will in general be minor compared to the data error spreads.

The unavailability will in general be denoted by the symbol Q . The standard forms for Q are:

$$Q = \lambda t, \quad (\text{Equation 4-3})$$

or

$$Q = \frac{t_D}{t_T} \quad (\text{Equation 4-4})$$

In the first equation λ is the component failure rate and t the average fault duration time (detection plus repair time). The value for t is the value impacting on the system availability or safety (for example, the interval during which the reactor is not shut down). In the second equation, t_D is the average downtime and t_T is the total cycle time (such as the interval between periodic tests). The first equation is of the point type and the second of the interval type.

In addition to the above, unavailabilities can also be treated as basic data. Examples are cyclic failure rates and demand probability data (given the component has been required or demanded). More detailed contributions to Q will be discussed in subsequent sections.

4.3.1 Failure Probability

The failure probability is defined in general as the probability of failure in some time interval. The time interval is a required operation time or mission time, but can also be a standby time interval. The failure probability is sometimes called the unreliability (one minus the reliability). Reliability is often associated with system efficiency (e.g., success from all types of failures, whether safety related or not); hence, the term failure probability is instead used here.

The failure probability will in general be denoted by P . The standard form for P when the component is nonrepairable, is

$$P = 1 - e^{-\lambda t} \approx \lambda t \quad (\text{Equation 4-5})$$

As for the unavailability, a constant failure rate is employed in the equation. The failure rate λ can be operating or standby failure rate. The approximation $P \approx \lambda t$ is conservative and accurate to within approximately 5% if P is less than 0.1. For higher

probabilities the exponential must be calculated. Subsequent discussions cover more detailed forms for P, when the component is repairable or when combinations are considered.

There are numerous additional terms which can be defined and which are used in reliability theory. However, P and Q represent the basic quantitative characteristics of a component. The various other defined terms can be recast into these two basic characteristics.

4.3.2 Unavailability Contributions

The particular contributions to component unavailability which arise in the analyses are broken down below.

Failure-Upon-Demand

Contributions from failure upon demand arise from failure of components to start, e.g., a pump failing to start. In addition to actual component failure (given the correct demand), contributions result from failure of the demand itself. An example is failure of a control signal to be transmitted to the component. The demands (signals) can be automatically initiated or manually initiated by the operator. In the operator case, the demand failure is failure of the operator, i.e., a human error of omission.

These failure-upon-demand contributions are the standard cyclic and demand failures treated in reliability theory. In PRA they are treated as unavailability contributions since they are all related to a failed state existing (the component, for example, may have been in failed state before the actual demand and the failure simply realized at the demand).

The failure-upon-demand contributions Q are given directly by the demand data in the data base:

$$Q = Q_d \quad (\text{Equation 4-6})$$

where Q_d is the component demand probability or a human error for an act. These numbers are time independent because they represent probabilities per act.

Unrepaired Failure Contributions

The unavailability contribution for unrepaired failures is given by the formula:

$$Q = \lambda t \quad (\text{Equation 4-3})$$

where λ is the failure rate and t the average fault duration time.

If the component is monitored, the t is the average downtime for which the failure can exist after detection, given for example by specifications and operating procedures. If the component is not monitored but periodically tested, then t is one-half the test interval. If the component is not tested or the tests are not able to detect the particular mode of failure, then t is taken as the median time for which the calculations can be extrapolated (maximum prediction time), i.e., it is treated as nonrepairable for the maximum time considered in the calculation.

Test Outages

If the component is disabled in on-line periodic testing (i.e., effectively placed in a failed state), then the unavailability contribution is the standard interval unavailability:

$$Q = \frac{t_D}{t_T} \quad (\text{Equation 4-7})$$

where t_D is the average test downtime and t_T the average interval between tests. If the component is not disabled during testing or if there is an override backup capability (enabling the component to be placed on-line if required) then Q is negligible.

In cases of component disablement, the average downtime t_D and average test interval are data parameters. For actual calculations, specific values are obtained from the data base and system specifications.

An additional contribution from testing arises when the second leg of a redundancy is tested after detection of failure of the first leg. This arises, for example, when for a redundant pair of valves, one valve is tested when the other is detected to have failed. In the operations where this is performed, the unavailability is of the point value form:

$$Q = \lambda t_D \quad (\text{Equation 4-8})$$

where λ is the failure rate of the initiating leg failure and t_D is the average test time for the redundant leg test.

For multiple testing, as is the standard technique when several components are simultaneously disabled in a test, the effective test downtime is the maximum of the individual component downtimes. When the two legs of a redundancy cannot both be under test, due to specification restrictions, then individual leg test unavailabilities are not multiplied together. (This intersection event is not allowed and is therefore not existent on the fault tree.)

Maintenance Outages

The treatment of the unavailability contribution from maintenance outages is comparable to the test outage treatment. If the on-line maintenance is performed periodically, then

$$Q = t_D/t_M \quad (\text{Equation 4-9})$$

where t_D is the downtime associated with the maintenance and t_M is the cyclic time interval between maintenance.

The on-line maintenance is often unscheduled maintenance performed at non-periodic intervals, i.e., when needed. For this case, the above formula becomes slightly modified as follows:

$$Q = \frac{t_D}{t} \quad (\text{Equation 4-7})$$

In this case, t is the average time between maintenance acts of the maintenance distribution (the probability distribution associated with the maintenance occurring at a particular time).

As for multiple testing, maximum downtime is used for simultaneous maintenances and the summed downtime for sequential maintenances. Where concurrent maintenances are disallowed, maintenance unavailability contributions are not multiplied.

4.3.3 Cumulative Failure Probability

The cumulative failure probability, or simply failure probability, is the probability that the component will not operate successfully for a required time period t . In this definition, the component is given to have started successfully; and hence, the failure probability is associated only with the failure to run mode. In other words, the component fails to run (operate) after it has started.

For a single component, the failure probability P is given by:

$$P = 1 - e^{-\lambda t} \approx \lambda t \quad (\text{Equation 4-10})$$

where the approximation $P \approx \lambda t$ is that used since it is valid to several significant figures for probabilities less than 0.1. In all cases, the approximation is slightly conservative. When probabilities can be extremely high (greater than 0.1), the exponential is used. The above formula (and approximation) is the standard unreliability expression given in texts.

For a combination (intersection) of two or more components which are all non-repairable, the failure probability for the combination is simply the product of the individual component failure probabilities. For example, for two parallel components, denoted, say, as component 1 and component 2, the failure probability for both failing is:

$$P = \lambda_1 t \lambda_2 t \quad (\text{Equation 4-11})$$

when λ_1 and λ_2 are the individual component operating failure rates and t is the operating time.

If the combination consists of two repairable components, then the failure probability for the parallel combination can be expressed as:

$$P = Q_1 \lambda_2 t + Q_2 \lambda_1 t \quad (\text{Equation 4-12})$$

where Q_1 is the unavailability of component 1 and Q_2 the unavailability for component 2. The unavailabilities are the total component unavailabilities consisting of all relevant contributions.

The above formula simply says that for both components to fail in time t , one component has to be down and the other has to fail. The first term on the right-hand side gives the contribution from component 1 being down and component 2 then failing, thus causing the combination to fail. The second term gives the alternative contribution from component 2 being down and component 1 failing while 2 is down.

The above equation is the standard repairable form which is sometimes called the (cumulative) hazard function. The formula is the first order form which is accurate to several significant figures. Any slight error made, in all cases, is on the conservative side.

The formula can be generalized to any number of repairable components in the combination (in parallel):

$$P = Q_2 Q_3 \dots Q_n \lambda_1 t + Q_1 Q_3 \dots \lambda_2 t + \dots Q_1 Q_2 \dots Q_{n-1} \lambda_n t \quad (\text{Equation 4-13})$$

In this equation, each term on the right-hand side represents the contribution from all components but one being down (being unavailable), and the other component then failing, thus causing the entire combination to fail.

If certain components are nonrepairable, then in the above equation appropriate failure probabilities are used instead of Q 's for the nonrepairable components. An extra proportionality factor must multiply each nonrepairable combination to account for the

ordering sequence of the nonrepairable components. For example, consider the particular contribution P_i where:

$$P_i = Q_2 Q_3 Q_4 \lambda_1 t$$

If components 1, 3, and 4 are nonrepairable, then $\lambda_3 t$ is substituted for Q_3 , $\lambda_4 t$ for Q_4 and a factor of $2!/3! = 1/3$ included to incorporate the number of ways in which 3 and 4 can fail before 1 (there are two sequences, or permutations, i.e., 341 and 431 out of a total of $3!$ permutations of 134 thus giving $2!/3!$). The final expression for P_i is then:

$$P_i = 1/3 Q_2 \lambda_3 t \lambda_4 t \lambda_1 t$$

For the above sequence considerations, the repairable components are not considered, since they fail any number of times and are repaired; the only requirement on the repairable components is that they be down at the particular time the combination fails. Each general contribution term is considered, analogously. These considerations are the standard ordering and permutation analyses performed for nonrepairable situations.

Finally, with regard to failure probability calculations, situations occur in which a failure only occurs if the component or combination is down for a time greater than some maximum allowed outage time. If the component can be repaired in short enough time when it fails, then no resulting system failure will occur. If the repair takes longer than the maximum allowed outage, system failure will then occur. Analogous considerations apply to a combination where the downtime and maximum allowed outage time now refer to the combination.

The maximum allowed outage considerations have applications to long-term safety system operation after the initiating event, such as a pipe rupture. An example is the long-term cooling function. If the safety systems are down for a sufficient time, then failure results. If they fail but are brought up in time, no severe consequences result.

For these maximum allowed outage cases, the repair times and repair probabilities are modified and incorporate the likelihood of being down and remaining down for a time greater than some specified allowed outage time. Only when the component remains

down longer than this specified time does a defined failure occur. The modification is straightforward and includes multiplication by an extra factor, i.e., an extra probability, to account for the extra condition of being down greater than the specified time.

If t_{\max} is then the maximum allowed outage time, then for each component with this condition, the factor f is consequently:

$$f = P(t_R > t_{\max}) \quad (\text{Equation 4-14})$$

where $P(t_R > t_{\max})$ is the probability that the repair time (fault duration time) is greater than t_{\max} . The value for this probability is derived from the data base repair distributions and parameters. An adequate and standardly used distribution is exponential repair for which:

$$f = \exp(-t_{\max}/t) \quad (\text{Equation 4-15})$$

where t is the average repair, or fault duration, time for the component.

For exponential repair, the factors f then simply multiply each affected component term in the previous failure probability operations. For example, for a single component P becomes:

$$P = \lambda tf. \quad (\text{Equation 4-16})$$

For the two repairable components, the failure probability becomes:

$$P = Q_1 f_1 \lambda_2 t f_2 + Q_2 f_2 \lambda_1 t f_1 \quad (\text{Equation 4-17})$$

The other equations are handled in a similar manner. The above equations can also be obtained by the usual approach of integration of repair distributions.

4.4 Range Propagation and Bounding Techniques

The system characteristics as computed by the techniques described in the previous section are referred to as "point values" because fixed values were used for the failure rates and other data parameters. In a probabilistic approach, because of the variations and uncertainties in the failure rates and data parameters, these quantities are treated as random variables. Since the system characteristic, the unavailability, is a function of these random variables, it is itself then a random variable. The process of determining the system distribution in terms of the individual parameter distributions is referred to here as error or probabilistic range propagation. The following discussion describes the range-propagation techniques commonly used in PRA.

The probability concepts associated with random variables are discussed in any statistical text. In essence, a random variable can be viewed as having a range of values which are possible. A probability distribution is assigned to this range, which gives the probability associated with particular assumed values. The probability distribution is sometimes termed, as in this course, the a priori distribution.

In terms of classical modeling, the data are treated as random variables because of the data variability from component to component and from plant to plant. The models are constructed to be applicable not only to one specific condition but to a population of conditions, which vary because of differing applicable environments and differing individual component characteristics (e.g., from plant to plant). The population includes different conditions existing among various reactors. Data variability, therefore, exists among similar components in different plants. The population also incorporates differing conditions that one individual component may be subjected to, for example, due to varying maintenance or different operational demands.

The treatment of data as random variables furthermore serves as a means to describe the uncertainty of the data. With regard to the uncertainty, the random variable, representing a range of values, gives the possible values that the data may assume in various applications. The probability distribution associated with the random variable gives the likelihood that the data value will actually be any one given value in this range. The distribution can be simply interpreted as arising because one sample, that is, one reactor or one component, is selected from a variable population of reactors or components.

Since the distribution is a probability and the system unavailability itself is a probability, the distribution is in a sense a "probability of a probability". As stated, the distribution does give the probability that the system unavailability will be any given value or lie in any given range. Nevertheless, these probabilities cannot necessarily be lumped together to obtain one system unavailability and avoid all the extra calculations. The system unavailability as treated here is a random variable and is a system characteristic. Furthermore, a particular unavailability value is an estimate based on data values. The distribution shows the variation in the system characteristic which can arise due to uncertainties and population variations.

4.5 Reliability and Availability Analysis Tools

The major systems analysis techniques used in PRA are fault tree analysis and event tree analysis. These techniques are discussed in detail in Topics 6 and 7, respectively. In addition to these system modeling techniques, a number of other analysis tools are available and may be appropriate for certain applications. These techniques are described briefly below.

4.5.1 Failure Modes and Effects Analysis

The failure modes and effects analysis (FMEA) is performed by considering the ways in which system components can fail and what the effects of those failures are in terms of system operability. The product of an FMEA is a table which lists system components, component failure modes, and the effects of those component failures. The FMEA may also contain an indication of the severity of those failures. For some types of systems, the FMEA may be the only analysis tool required. A major limitation of this tool, however, is that it is limited to an examination of single failures only and does not permit consideration of multiple failures. In some cases, the FMEA may be used as a preliminary step in fault tree analysis because it provides a convenient framework in which to consider various component failure modes. The FMEA may also be useful in identifying plant-specific initiating events.

4.5.2 Reliability Block Diagram

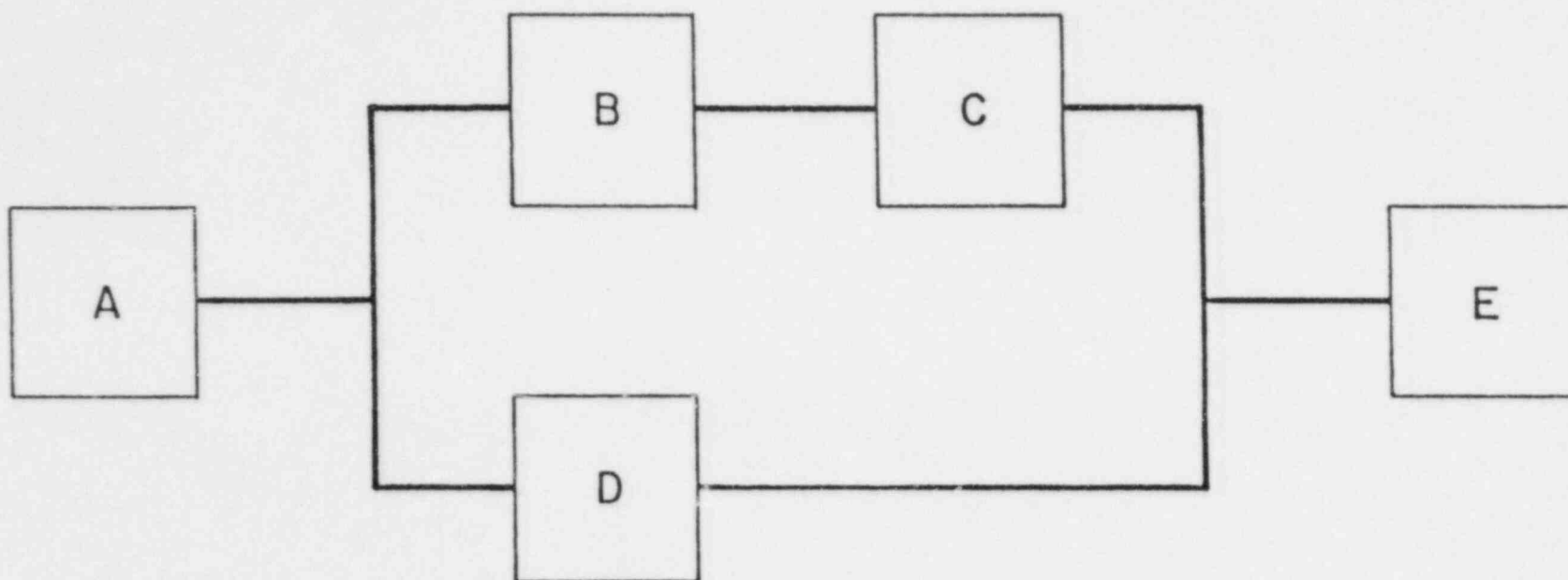
Like the FMEA, the reliability block diagram is occasionally used as an adjunct to fault tree analysis. This technique results in a success-oriented model which can be quantified to calculate system reliability values. The reliability block diagram model is a simple reflection of the parallel and series relationship between system components. By assigning component reliability values to the model blocks which represent system components, the model can be evaluated to obtain a reliability value for the system. An example of a very simple reliability block diagram is shown in Figure 4-1.

4.5.3 Parts Count Approach

This system evaluation tool is perhaps the simplest and most conservative technique used in systems analysis. As a practical matter, its applications in nuclear power plant risk assessment are few. The parts count approach is useful in those situations in which a rough upper bound on the probability of system failure is desired. The technique is predicated on the assumption that any component failure results in system failure. The parts count technique simply lists all of the system components and their estimated probabilities of failure. These probabilities are then added and the resulting sum is taken to represent the upper bound system failure probability.

4.5.4 Other Techniques

In addition to the techniques described above, there are a number of other systems analysis approaches available. These include failure mode effect and criticality analysis (FMECA), preliminary hazard analysis (PHA), fault hazard analysis (FHA), double failure matrix (DFM), management oversight risk tree (MORT), GO modeling, and so forth. While each of these techniques may be useful for specific applications, they have not been used in nuclear power plant PRA.



$$R_S = 1 - [Q_A + (Q_B + Q_C)(Q_D) + Q_E]$$

R_S = SYSTEM RELIABILITY

Q_A = UNRELIABILITY OF A

Q_B = UNRELIABILITY OF B

Q_C = UNRELIABILITY OF C

Q_D = UNRELIABILITY OF D

Q_E = UNRELIABILITY OF E

FIGURE 4-1
BLOCK DIAGRAM EXAMPLE

TOPIC 5
ACCIDENT INITIATORS

5. ACCIDENT INITIATORS

The first technical step in a PRA, performed at the beginning of the system modeling activity, is the identification of potential accident initiators. Accident initiators, sometimes called initiating events, are undesired events which present a challenge to the plant in that if they are not successfully responded to, core damage may result. All of the system modeling, and ultimately, all PRA activities, are based on the identification of initiating events. This topic discusses the nature of initiating events and the ways in which potential initiators are identified. Additional information is available in Section 3.4.2 of the PRA Procedures Guide (NUREG/CR-2300) from which some of this material is drawn.

5.1 Nature of Accident Initiators

Before proceeding to the identification of initiating events, the PRA analysts involved should have acquired an understanding of the plant design and operation. This familiarity should extend down to the system level, including the requisite support systems. Analysts should also review PRAs for similar plants and note the types of initiators utilized in those studies. Initiating events are typically divided into two broad groups: transients and loss-of-coolant accidents (LOCAs). These groups are then subdivided in terms of the systems required to respond to the initiator. The division into transient and LOCA initiators has been carried over from the design basis accident approach used in plant licensing. Some accidents do not fit well in either category, such as a sequence of events initiated by a transient in which a safety/relief valve sticks open.

The subdivision of the LOCAs is fairly straightforward and depends upon the size and location of the break. Sometimes different pipe size categories are established depending upon whether the flow from the break is expected to be steam or liquid. The size of the break is important because different systems must compensate for the loss of reactor coolant depending upon the rate of coolant loss and the pressure in the reactor vessel. Generally, reactors are designed with high and low pressure emergency core coolant injection (ECCI) systems. The low pressure system(s) deliver a great deal of water to keep the core covered in case of a large LOCA where the loss of coolant is rapid and the reactor vessel is quickly depressurized. The high pressure systems deliver more modest amounts of water to compensate for small breaks where the fluid loss is not enough to depressurize the reactor coolant system. The small LOCAs are usually subdivided based upon the number of ECCI systems or trains required to provide the necessary flow. Figure 5-1 illustrates this type of subdivision.

The reactor coolant system and interfacing systems should be surveyed to determine all the possible breaks that could result in loss of reactor coolant. Event V for PWRs is an example of a break in an interfacing system that could lead to a severe accident. While a complete spectrum of break sizes must be considered, the number of LOCAs to be considered can usually be reduced to three or four, depending upon the capabilities of the ECCI systems. Traditionally, the breaks of the very largest lines have been denoted as Event A, and the smaller breaks by the letter S (S1, S2, etc.). As might be expected from the diversity of commercial reactors, there is no standard set of break sizes, largely due to the differing capabilities of the ECCI systems. There is not even complete agreement on the event designators. Table 5-1 shows that in the Arkansas Nuclear One IREP study all LOCAs were designated by letter B. Transient initiators comprise a more complex and extensive set of initiating events. Table 5-1 illustrates the groups of transient initiators selected for ANO-1, and Table 5-2 illustrates an exhaustive list for BWRs from EPRI NP-2230.

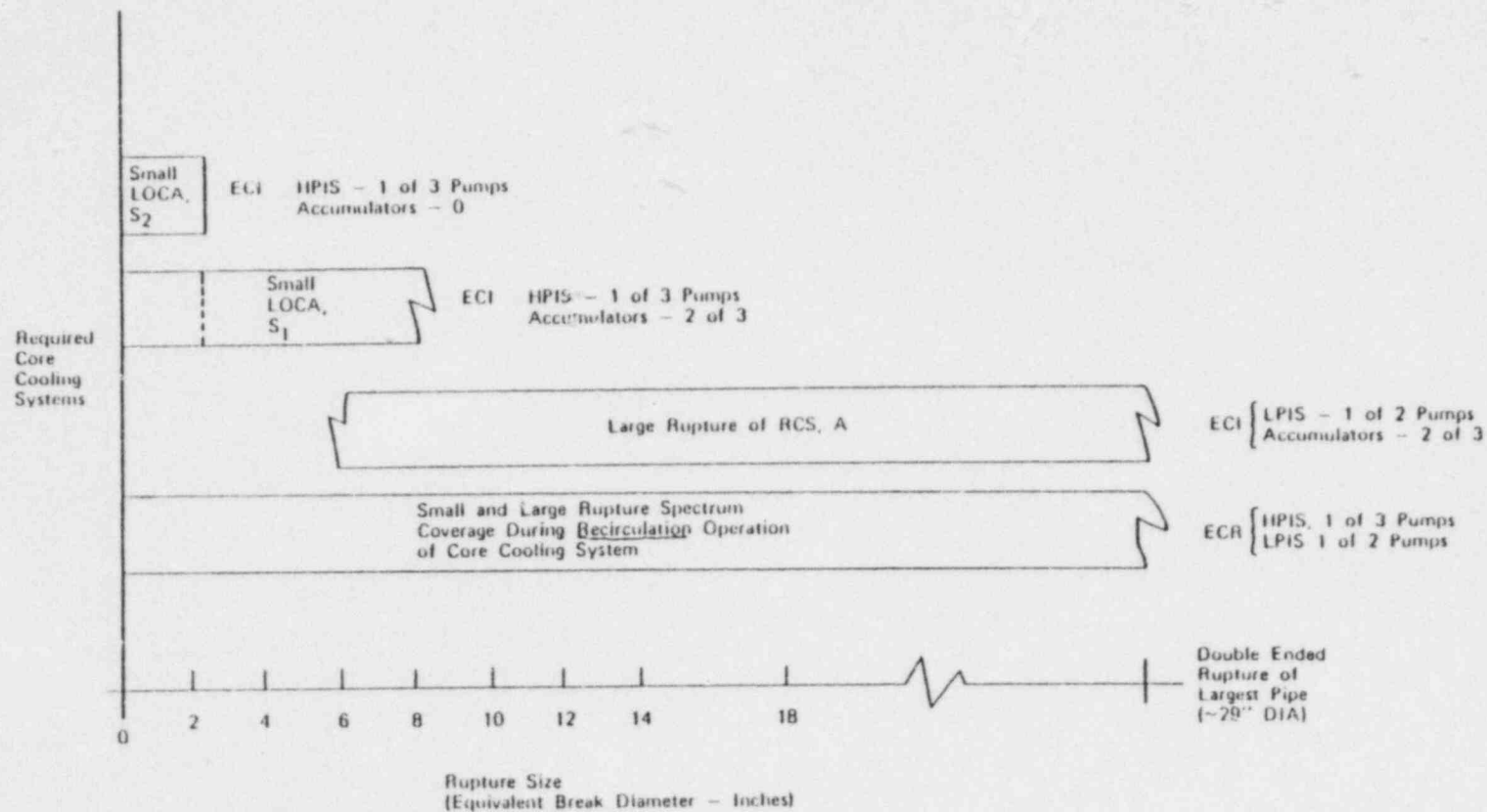


FIGURE 5-1
CORE COOLING SUCCESS CRITERIA FOR VARIOUS LOCA's

TABLE 5-1
INITIATING EVENTS USED IN THE ANO-1 ANALYSIS

<u>Designator</u>	<u>Initiating Event Description</u>	<u>Frequency Per Reactor Year</u>
B(1.2)	LOCA with a .38 to 1.2 inch equivalent diameter break	2.0×10^{-2}
B(1.66)	LOCA with a 1.2 to 1.66 inch equivalent diameter break	3.1×10^{-4}
B(4)	LOCA with a 1.66 to 4 inch equivalent diameter break	3.8×10^{-4}
B(10)	LOCA with a 4 to 10 inch equivalent diameter break	1.6×10^{-4}
B(13.5)	LOCA with a 10 to 13.5 inch equivalent diameter break	1.2×10^{-5}
B(> 13.5)	LOCA with an equivalent diameter break greater than 13.5 inches	7.5×10^{-5}
T(LOP)	Loss of offsite power transient	3.2×10^{-1}
T(PCS)	Transient initiated by a total interruption of main feedwater	1.0
T(FIA)	All other transients which do not affect frontline systems significantly	7.1
T(A3)	Transient initiated by a failure of AC power bus A3	3.5×10^{-2}
T(B5)	Transient initiated by a failure of AC power bus B5	3.5×10^{-2}
T(D01)	Transient initiated by a failure of DC power bus D01	1.8×10^{-2}
T(D02)	Transient initiated by a failure of DC power bus D02	1.8×10^{-2}
T(LOSW)	Transient initiated by failure of	2.6×10^{-3}

TABLE 5-2
BWR TRANSIENT INITIATORS

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 Closure
6. Inadvertent Closure of One MSIV (Rest Open)
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 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 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
37. Cause Unknown

SUPPORT SYSTEMS INITIATORS

1. Loss of Turbine Building Secondary Closed Cooling Water (TBSCCW)
2. Loss of Service Water
3. Loss of Circulating Water
4. Loss of Plant Air Compressors

SOURCE: EPRI NP-801/2230

5.2 Grouping and Quantification of Accident Initiators

It is not feasible to construct event trees for thirty or forty transient initiators, so some sort of grouping and consolidation must be employed. The LOCAs are grouped according to the systems required to respond to the initiating event. Since the power conversion system (PCS) provides a means of heat removal (the condenser) and a means of water supply to the core (the feedwater systems) transients are often divided into groups depending on whether the PCS is available or not. Transients in which offsite electrical power is lost are also usually singled out for explicit consideration. Comprehensive lists such as that in Table 5-2 often contain complex events which include failures that occurred after the reactor trip. Transient initiators chosen from a generic list such as this must be examined for applicability to the specific plant in question. If the plant is currently in operation, its history should be examined for transient event information to supplement the generic data. The grouping of transients should take into account the nature and extent of the specific mitigating systems of the plant to be analyzed.

For most transients, the flow of coolant from the core is uninterrupted so that emergency injection is required only to replace coolant that may be released by the safety/relief valves to limit the reactor coolant system pressure. If one of these valves sticks open, however, the transient event is transformed into an event that is very similar to a small LOCA. In some PRAs these types of accidents have been treated by special transient event trees while in others they have been grouped with the LOCAs of the appropriate size.

The development of event trees is very much an iterative process. The grouping of the initiating events will be modified in the course of the analysis as more extensive information from subsequent tasks becomes available. New event trees may have to be developed for certain initiators if all the initiating events placed in a certain group cannot at first be considered together in one event tree.

Data on the frequency of initiating events is generally obtained from three or four sources. The largest body of data is generic: recent compilations are available in several EPRI documents. Operating data from the plant should be analyzed, but may be scanty or nonexistent if the plant has not been operating for several years. Finally, data from similar plants, and the information from recent PRAs on the same types of reactors can be used. The most specific data available should be used if possible. Table 5-3 illustrates three types of transients; it shows the different transients which comprise each type, and the frequency and source of data for each.

To guide the selection and grouping of accident initiators, a master logic diagram or summary fault tree can be constructed. The top event is usually a significant release of radioactive materials from the site or the occurrence of severe core damage. The various levels in such a diagram help to order and locate events and to ensure completeness. The master logic diagram groups initiating events by the safety function with which they are most closely associated. This is not a sufficient grouping for initiators because all the safety functions required to mitigate the accident must be considered. However, this grouping does provide a useful starting point.

TABLE 5-3
TRANSIENT CLASSES AND FREQUENCIES

<u>Class</u>	<u>Transient</u>	<u>Frequency (per year)</u>	<u>Source of Frequency</u>
T ₃	LOSS OF FEEDWATER	.18	---
	Loss of All Feedwater Flow	.06	Plant Data
	Loss of Turbine Building Closed Cooling Water System	.06	Plant Data
	Loss of Service Water System	.06	Plant Data
T ₄	LOSS OF NORMAL AC POWER	.20	---
	Loss of Offsite Power	.16	NP-801
	Loss of Auxiliary Power	.04	NP-801
T ₅	SAFETY/RELIEF VALVE TRANSIENT	.20	---
	Inadvertent Opening of a S/R Valve	.20	NP-801

TOPIC 6
EVENT TREE ANALYSIS

6. EVENT TREE ANALYSIS

The event tree is an analytical tool which organizes and characterizes potential accidents in a methodical manner. Event tree analysis is a general and flexible approach which can be used for a wide variety of purposes. This method has been used in some form in all recent risk assessments of commercial nuclear power reactors. It is suitable for modeling complex sequences of events and allows for their efficient evaluation. Event trees are discussed in some detail in the PRA Procedures Guide (NUREG/CR-2300), particularly Section 3.4, from which much of the material presented here is taken.

6.1 Event Tree Analysis Process

The tasks involved in event tree analysis are illustrated in Figure 6-1, which depicts the development of the event tree in general terms. Potential accident initiating events are first identified based upon plant design as discussed in Topic 5. Groups of initiators are defined to encompass all physically possible accidents which could degrade the reactor core. This provides reasonable assurance that all significant causal factors have been included in the analysis and that the results will provide a realistic bounding of potential accidents.

Once the initiating events have been described, functional event trees are developed for each initiator group. These event trees display the functional relationships among the relevant safety systems. Generic trees for the type of reactor involved may suffice since these trees are often rather general. Even if very detailed functional event trees are desired, the generic trees offer a good starting point for their development.

When the functional relationships have been established, the events are expanded to depict the response in terms of the systems which perform the mitigating functions. That is, the functional event trees are developed into systemic event trees. The systemic event trees define specific system responses and requirements which are then used as top events for the system fault tree analyses. The use of fault trees to determine the probability of individual system failure will be discussed in Topic 7.

The system event trees may include only the frontline systems, those that directly perform the safety functions, or the trees may show the support systems in addition. If the support systems are shown, the interdependencies among them must be clearly shown. Upon completion of the initial systemic event trees, they should be compared with those of a similar plant and operating experience. This comparison may identify omissions and oversights.

These analytical activities represent an interactive process. Information from each task is fed back to the preceding tasks, which are then modified to reflect the new understanding and information developed in the course of the project.

The sources of the data required for a complete event tree analysis of a nuclear power plant are many and varied. Table 6-1 lists the types of data required and some of the sources from which this information may be obtained. The plant Final Safety Analysis Report (FSAR) is a good source of basic information about the safety systems, but more detailed information will be needed in many areas. This information can be obtained from the utility and/or the architect/engineer. The data requirements should not be underestimated. If the plant familiarization step is carried out thoroughly, the bulk of the needed data should be on hand when the event tree construction task commences.

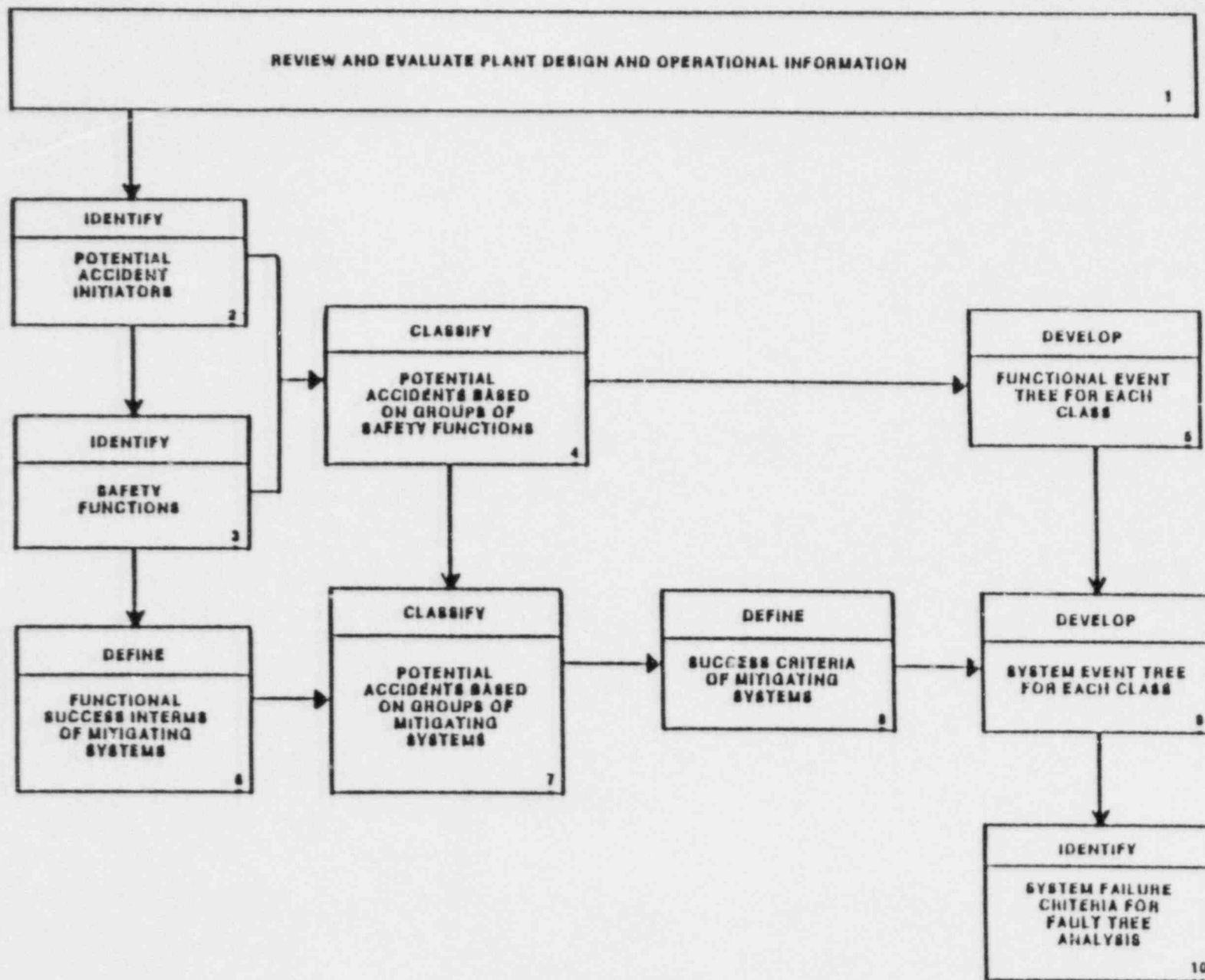


FIGURE 6-1
GENERAL PROCESS FOR EVENT TREE DEVELOPMENT

TABLE 6-1
SPECIFICATIONS OF DESIRED DATA FOR EVENT TREE ANALYSIS

<u>Analysis Task</u>	<u>Desired Data</u>
(1) Initiator Selection	
(a) Plant accident review	Final Safety Analysis Report (FSAR) for the selected plant Preliminary Design Report (PDR) FSARs for similar plants WASH-1400 Appendix I Current accident analysis studies
(b) LOCA pipe rupture classification	FSAR RCS system description RCS flow diagram Emergency Safeguard Features (ESFs) design requirements
(c) Identification of transient events	FSAR WASH-1400 Appendices I & V ATWS - NUREG-0460 Current EPRI studies
(d) Identification of minimum ESF requirements	FSAR ESF system descriptions ESF operating procedures ESF emergency procedures
(2) Potential Accident Evaluation	
(a) Core melt phenomena	Thermal-hydraulic analyses WASH-1400 - Appendix VIII Current literature on core melt experimentation
(b) Steam explosion potential	WASH-1400 - Appendix VIII Current experiments on metal-water reactions at Sandia Laboratories
(c) Containment base mat melt-through	Drawings on basemat thickness and composition Reactor cavity drawings Recirculation sump drawings
(d) Containment analysis	FSAR Containment support system description Pressure-time histories Containment integrity (minimum leak size studies)

TABLE 6-1 (cont'd.)

<u>Analysis Task</u>	<u>Desired Data</u>
(3) Event Tree Development (a) System operation review	System descriptions System flow diagrams Operating instructions Emergency procedures
(b) Accident sequence timing	FSAR Blowdown analyses Emergency operating instructions
(c) System/function interrelationships	System logic diagrams System flow diagrams Functional block diagrams Overall schematics and functional drawings showing interface areas Plant layout drawings

6.2 Functional Event Trees

The functional event trees order the plant safety functions and depict their relationship for each group of initiating events. The functions that must be performed to prevent core damage and a release of radioactivity from the containment are denoted "safety functions". These functions form the basis for grouping the initiators and delineating the plant response. The safety functions will be taken up in more detail later. Frequently, the relationships between safety functions are such that if a particular function is successfully performed, it is not necessary that certain others are performed. For example, containment integrity will not be challenged if scram and core heat removal are successful. The more important safety functions appear at the left side of the event tree. These functions are generally the ones that are performed first if the accident is successfully mitigated.

A separate functional event tree is developed for each group of initiating events because each group requires a distinct functional response. The functional event tree is an intermediate step which provides baseline information and organizes the complex relationships between accident initiators and the plant response. It is the initial step in determining which of the plant safety features are required to mitigate different types of accidents.

Figure 6-2 shows a fairly simple functional event tree. The initiating event forms the first event heading, and the required safety functions comprise the rest. Each path through the tree defines a specific accident sequence. The sequence is denoted by symbols indicating which functions have not been performed as required. The iterative nature of the interaction between event tree development and accident process analysis is clear. Figure 6-2 also illustrates how the number of possible sequences to be analyzed can be reduced. The total possible number of sequences is $2^7 = 128$ since there are seven safety functions listed, each of which may succeed or fail. However, only 17 meaningful sequences have been identified. For example, it has been assumed that if no electrical power is available, core melt and containment failure will inevitably follow since there is no power to the pumps needed to perform the other functions. Similarly, if emergency coolant injection fails, the success of emergency coolant recirculation need not be considered. For a LOCA initiator, an example is that if the reactor coolant system inventory cannot be maintained, there is no chance of removing heat from the core.

Each safety function identified as an event tree heading is performed by a collection of systems. Some systems perform more than one function or portions of several functions, depending on plant design. To define headings for the system event tree, the analyst must identify those systems required to successfully perform each safety function.

Some functions will be performed by different systems, depending on the nature of 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 safety function of reactor coolant makeup 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 backup mitigating actions. For example, the power conversion system could contribute toward accomplishment of the heat rejection function for transients and very small LOCAs, and therefore would be included in the definition of systems that perform this safety function.

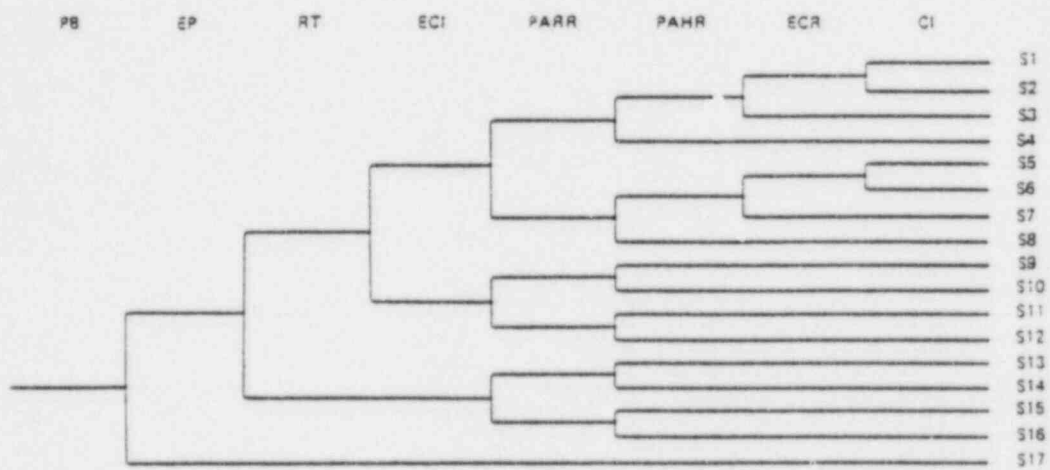


FIGURE 6-2
FUNCTIONAL LOCA EVENT TREE

Systems that provide support functions, such as component cooling water and electric power, and that do not directly perform the necessary safety functions, are not included in this definition. However, it is necessary to treat these systems in the systems analysis because they can significantly contribute to the probability of failure of a system or group of systems that perform safety functions. Therefore, it is also necessary to define the set of systems that provide necessary support functions to those systems that directly perform the safety functions.

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

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

6.3 Systemic Event Tree Analysis

For the systemic event trees, the classes of accidents, classified according to safety functions, will serve as the starting point for classification according to mitigating systems. However, two main factors associated with system design and accident initiation will usually result in more classes being defined on a system basis than were identified for accidents when considering safety functions alone. These factors are:

- **Design capacity of systems:** It may be necessary to divide a group of initiators because different systems may be employed to perform the same function due to the nature of the initiating events. For example, a distinction will be made between different size LOCAs if they require a different complement of systems for coolant makeup.
- **Initiating event/system interaction:** Some initiating events will occur in such a way to impact either the function or the availability of potential mitigating systems. Therefore, the mitigating systems available in these events will be different from the systems available for initiators that do not have interactions. An obvious example of this is the situation at many plants where a loss of offsite power transient results in a loss of the power conversion system so it is not available to perform the core/containment heat rejection function. In addition, this initiator impacts the availability of the remaining systems because emergency power is the only source of electrical power for the mitigating systems.

A systemic event tree will be developed for each class of accidents identified. Each event tree will identify the potential accident sequences that may follow the accident initiator. Each sequence is a unique combination of system success and failure states in response to the initiating event.

Although the systemic event trees utilize the information in the functional event trees, the sequences that result from the systemic event trees will differ somewhat from the sequences derived from the functional event trees. There are many reasons for this. One system may perform several functions, so its failure will affect multiple safety functions. Or several systems may be available to perform the same function, so that loss of only one system does not necessarily lead to a functional failure. Or the operation of a certain system may be of interest due to its impact on consequences even though it may not be able to perform its primary safety function due to other system failures.

Each systemic event tree will have a specific system or group of systems as the event tree 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 selection of the order of the headings: temporal, functional, and hardware relationships. However, only by performing the event tree analysis activity can the analyst determine the "best" order. Temporal considerations are a good starting point for ordering the headings. Systems are placed on the event tree in the order in which they are expected to respond to an accident. Those systems responding immediately (for example, reactor protection system) are placed first and those responding later are listed in order of response (for example, high pressure injection then high pressure recirculation). However, timing alone is not a sufficient consideration.

Functional and hardware relationships between systems should also be considered when selecting the order of the 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 successful containment spray and thus may be listed after containment spray on the event tree. Hardware dependencies also may determine order, such as in the case of a system that has multiple modes of operation. Since failure of one mode may imply failure of 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 previous system states. Only those unique combinations of success/failure states which 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/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 those system success/failure states which have potential significance in terms of accident sequence outcome or subsequent system operation and physical reality are postulated.

Success/failure choices in the event tree can be made based on a positive response to any of the following questions after first asking: Can the system hardware operate in this context? If yes,

- (1) Does the success or failure of the system impact the outcome (for example, core melt, fission product release, containment response)?
- (2) Does operation of this system contribute to a safety function in this context?

- (3) Does operation of this system at this point impact the need for or operation of other systems?

If any of the response are positive for these three questions, the particular system success/failure state should be explicitly included in the event tree. Because the importance of a particular system success or failure depends, in part, on the status of other systems, each of these question must be examined in the context of a particular accident sequence.

6.4 Summary

Event tree analysis is used to identify and depict the various functional and systemic success/failure states as they combine to form accident sequences. Unique event tree models are developed for each identifiable category of accident initiators. This topic has described the general task flow of event tree analysis as well as the specific analytical guidelines which are employed by an event tree analyst.

To provide some practice in the application of the principles discussed in this topic, students are asked to work the sample problem which follows.

EVENT TREE ANALYSIS
SAMPLE PROBLEM

SAMPLE PROBLEM

INSTRUCTIONS

Based upon the system information contained in the package entitled "Sample Problem" and a knowledge of the thermal-hydraulics of PWR accidents, develop a systemic event tree for a hypothetical LOCA. The development will be based on identification of the functions to be performed in response to a LOCA, the systems which perform those functions, and the major assumptions made in development of the event tree itself.

In performing the event tree analysis, consider the three major emergency functions of emergency coolant makeup, containment pressure reduction, and containment heat rejection. Although other functions such as core reactivity control may be necessary, the development will be restricted to the three functions identified in the sample problem material. In addition, start the event tree analysis by assuming that each of these functions must be performed for successful mitigation of the initiating event, a hypothetical LOCA.

Next define each function in system terms to identify the systems that will be addressed in the systemic event tree. This results in a table which identifies the success of each function in terms of the system or systems required to perform that function. For example, successful emergency coolant makeup requires both the coolant injection and coolant recirculation systems. Sometimes, system operation may be required for more than one function. This is the case of the coolant recirculation system which is necessary for successful emergency coolant makeup and containment heat rejection.

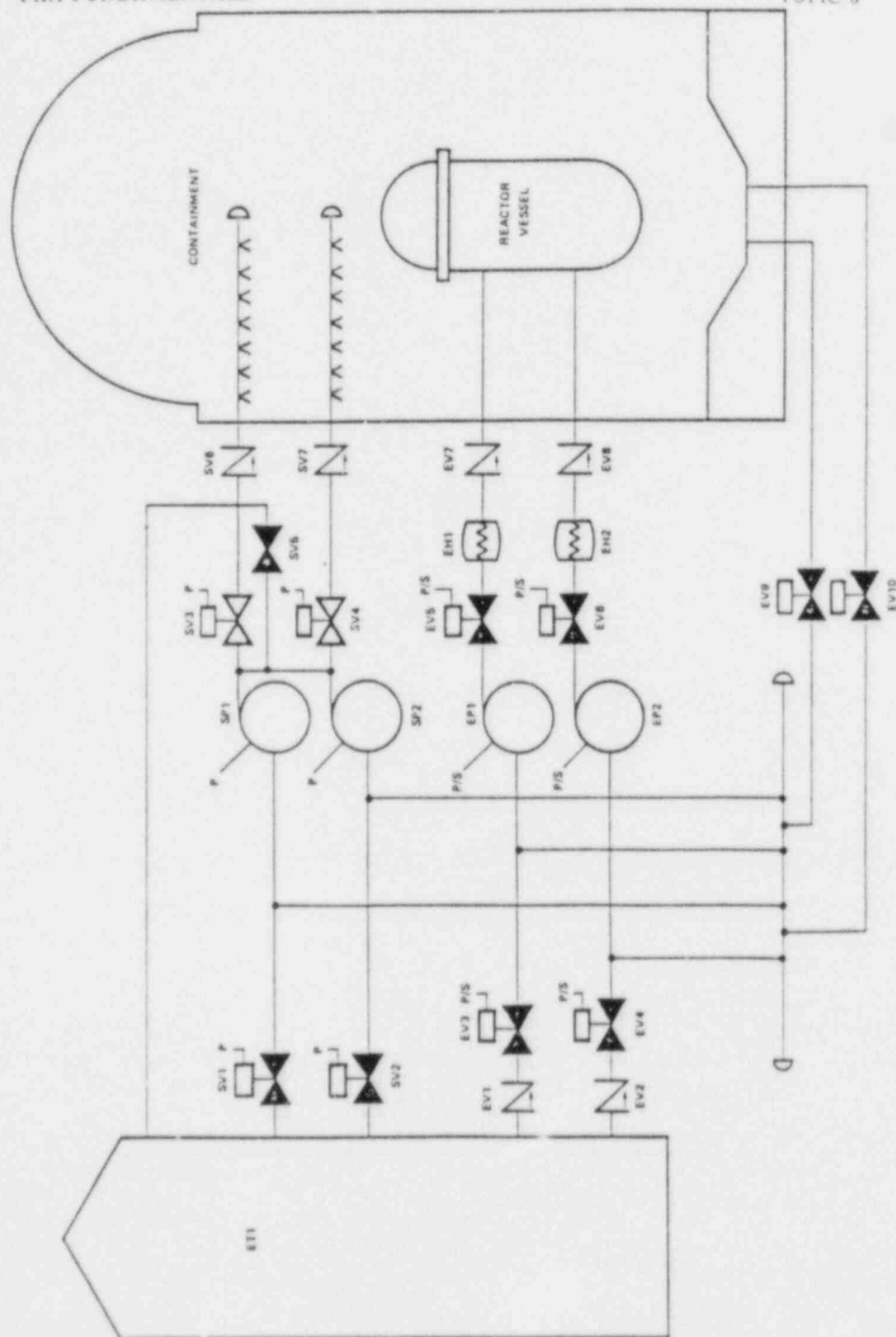
After identifying all the systems for consideration in the systemic event tree, determine the order in which they are listed as event tree headings. Two considerations previously mentioned will be included when determining heading order: response timing and system functional dependencies. Therefore, the system listed first should be the one expected to respond to the initiating event first. However, some compromise to timing may be necessary to accommodate system dependency and in some cases, the ordering decision must be arbitrary.

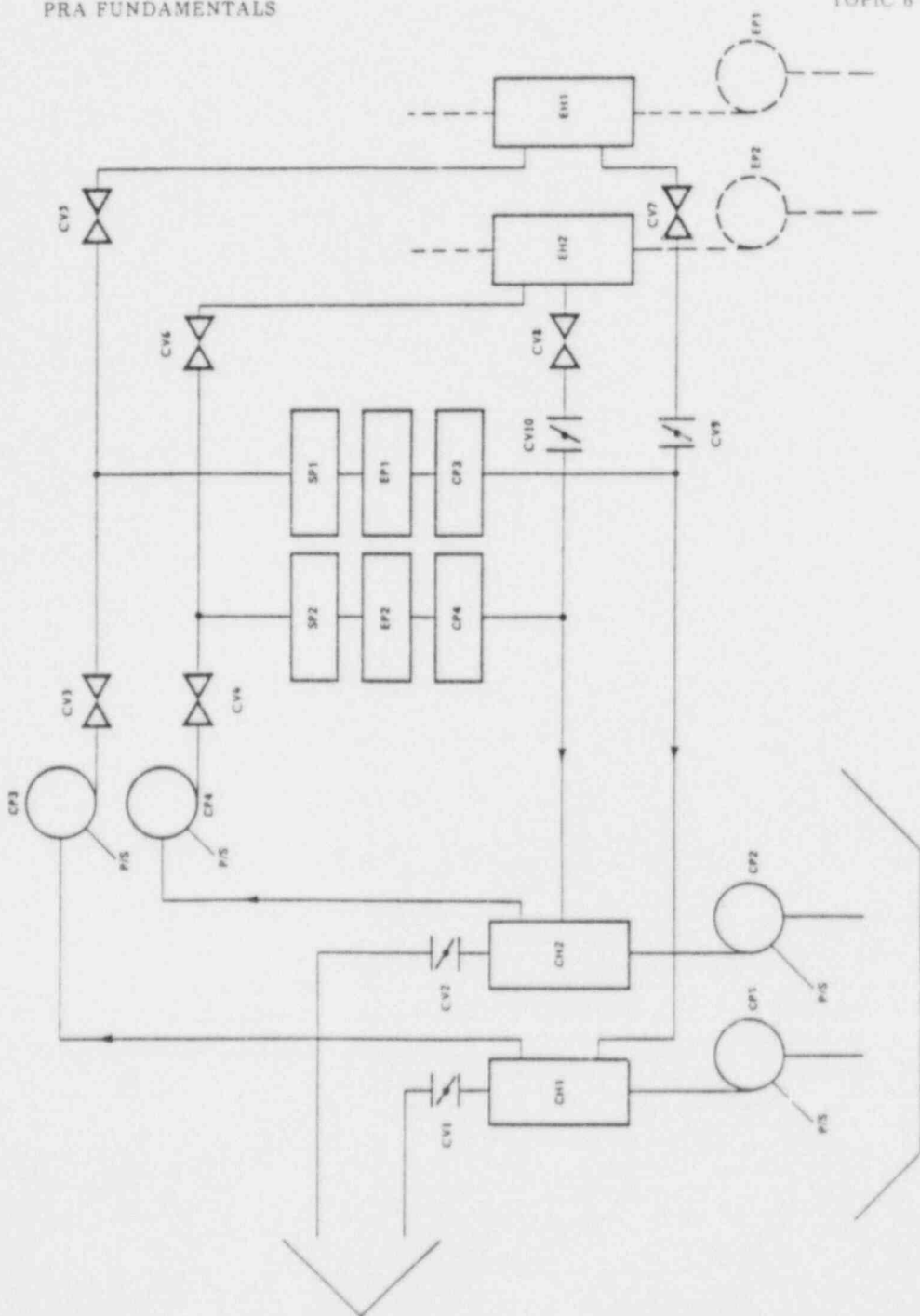
Once the systems have been listed as event tree headings, they must be dealt within the context of two important factors. First, each time a success or failure of a system is postulated, it must be considered in terms of the function the system is performing. For example, even though the post-accident heat removal system performs a pump cooling function in addition to containment heat rejection, this systemic event tree only considers the latter function. In fact, this iteration of the event tree included only frontline systems. Additional iterations of the sample problem may be made considering both the frontline and support aspects of the post-accident heat removal system.

The second important context to consider is the outcome of concern for the event tree analysis. The postulation of system successes or failures is only of concern when they may impact the outcome of an accident sequence in relation to the outcome of concern. For this sample problem, two potential outcomes should be considered. The first (and most important) shall be the status of the core. That is, does the core melt, yes or no? The second outcome considered shall be the status of the containment in relation to failure due to overpressure, yes or no? In some cases, the outcome may not be clear. In that case, a success/failure decision will be made and some indication given that identification of the particular outcome requires more information.



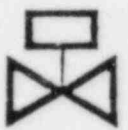





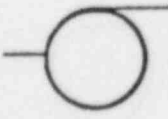

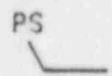

Two assumptions should be made initially when developing the systemic event tree. First, if a system fails in one mode of operation, it remains failed in all subsequent modes. If this assumption becomes important to the result, it may be adjusted later. Secondly, assume that spray system operation is necessary for containment overpressure protection even with containment heat rejection function success. This assumption may also be examined if it becomes important to the result.

The development of the event tree should be based on a systematic examination of each success failure possibility in accordance with the list of four questions utilized for event tree development. The answer to the questions depends upon the success/failure states prior to the point at which the question is being asked and the level of knowledge available. (The event tree does not answer questions but merely provides a simplified display of the information available as answers.)





KEY

	VALVE (NORMALLY OPEN) LOCALLY OPERATED
	VALVE (NORMALLY CLOSED) LOCALLY OPERATED
	VALVE (NORMALLY OPEN) MOTOR OPERATED
	VALVE, CHECK
	VALVE, DAMPER
	TANK
	SPRAY NOZZLES
	PIPE CAP
	PUMP
	HEAT EXCHANGER
	AUTOMATIC SIGNAL (P = PRESSURE, S = INJECTION)
	SUMP OR INTAKE STRUCTURE

SAMPLE PROBLEM

Systems

- Spray System (S)
- Emergency Coolant System (E)
- Component Cooling System

Emergency Functions

- Emergency Coolant Makeup
- Containment Pressure Reduction
- Containment Heat Rejection

System Operating Modes

- Spray Injection
- Spray Recirculation
- Coolant Injection
- Coolant Recirculation
- Post-Accident Heat Removal

System Success

- One-out-of-two pump operation for all systems

Emergency Condition

- Loss-of-Coolant Accident

Results in low coolant level in reactor vessel (S-Signal) and high pressure in containment (P-Signal) which automatically starts all the pumps and opens the appropriate valves.

Injection Phase

Water is taken from the Emergency Tank (ET1) and injected into the reactor vessel by the Emergency Coolant System. Water is also taken from ET1 and sprayed into the containment atmosphere by the spray system. The Component Cooling System provides cooling for both the spray and emergency coolant pumps during the injection phase.

Recirculation Phase

When the ET1 water level reaches the low level, the containment sump valves EV9 and EV10 are opened by the operators. This begins the recirculation phase. After the sump valves are opened, the ET1 discharge valves to both the spray and emergency coolant system pumps are closed by the operators. The Component Cooling System provides cooling for both the spray and emergency coolant pumps and heat removal from containment (e.g., the core) via heat exchanger EH1 and/or EH2 during the recirculation phase.

Technical Specifications

- (A) Each spray and emergency coolant flow path must be verified operable once every 30 days.
- (B) The reactor may remain critical for a maximum of 72 hours with any one spray flow path inoperable. The reactor must be shut down within one hour with both spray flow paths inoperable.
- (C) The reactor may remain critical for a maximum of 72 hours with anyone emergency coolant flow path inoperable. The reactor must be shut down within one hour with both spray flow paths inoperable.
- (D) The emergency tank level shall be verified once every 24 hours. The reactor may remain critical for a maximum of four hours with insufficient water in ET1.
- (E) Each spray pump shall be verified operable once very 30 days.
- (F) Each emergency coolant pump shall be verified operable every 30 days.
- (G) Automatic actuation of emergency coolant, spray and component cooling systems shall be verified by test once every 12 months during refueling.

Test Operations

- (A) Flow path operability test is accomplished by opening remote-controlled valves from the control room and verifying their position by check-list from the control room.
- (B) Pump operability test for the spray pumps is accomplished by operating the pump for one hour taking suction from ET1 and discharging through SV5 back to ET1. Both spray pump discharge valves (SV3 and SV4) are closed during test of either pump.
- (C) Pump operability test for the emergency coolant pumps is accomplished by opening the pump suction valve (EV3 or EV4) and operating the pump for 15 minutes.
- (D) The appropriate component cooling system loop must be operated for each pump test.
- (E) The ET1 level is verified by reading local redundant indicators. If the indicator values vary by more than 5% of specified level, a dipstick test is used.

Emergency Operational Conditions

- (A) The injection phase of emergency operation is 30 minutes long.
- (B) The recirculation phase of emergency operation is 24 hours long.
- (C) Pumps can operate for 15 minures without cooling water.
- (D) During the injection phase, sufficient cooling water is available to each spray and emergency coolant pump if coolant pumps CP3 and/or CP4 are operating. Coolant pumps CP1 and/or CP2 are necessary for adequate cooling during recirculation.

- (E) Successful emergency coolant and spray pump operation during recirculation requires closure of pump suction valves from the emergency tank (SV1, SV2, EV3, EV4).
- (F) Operators may not impact injection operations.
- (G) Operators may start pumps and change valve positions to achieve successful recirculation operation.

L	CI		SI		CR		PAIR		SR		SEQUENCE	CORE MELT	CONTAINMENT FAILURE (OP)
	A		B		C		D		E				
											L	N	N
											LE	?	?
											LD	Y	Y
											LC	Y	Y
											LB	?	?
											LBD	Y	Y
											LBC	Y	Y
											LA	Y	Y
											LAB	Y	Y

SAMPLE PROBLEM FRONT LINE SYSTEM SOLUTION

TOPIC 7
FAULT TREE ANALYSIS

7. FAULT TREE ANALYSIS

7.1 Introduction

One of the general goals of probabilistic risk assessment (PRA) is to assess the susceptibility of a system or set of systems to the occurrence of events which could lead to the failure of those systems. Various system modeling techniques can be used to accomplish this assessment of susceptibility to system failure. The "PRA Procedures Guide (NUREG/CR-2300)" states on page 3-38, that the system modeling techniques which are used in PRA should possess 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 impacts reduced.

No system modeling technique exists which is capable of completely fulfilling all of the above criteria. Fault tree analysis, however, is the technique which most fully satisfies the criteria and is the most frequently used tool for determining how nuclear power plant systems work and how they might fail. Other techniques such as reliability block diagrams or failure modes and effects analysis (FMEA) are sometimes used to supplement fault tree analysis by guiding the analytical process. Event tree analysis is another modeling technique which is often used in conjunction with fault tree analysis. The combination of event tree analysis and fault tree analysis, however, extends the scope of a systems analysis from an examination of only how a single system might fail to an examination of how systems might work or fail in concert with one another in response to postulated accident initiators.

Fault tree analysis provides a disciplined, rigorous approach to the identification and quantification of system failures. A discussion of the nature, purpose, and mechanics of fault tree analysis is included in this section.

7.2 Definition and Nature of Fault Tree Analysis

Fault tree analysis has been defined as "An analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur" (NUREG-0492). Although this definition, by itself, does not promote a full understanding of the nature and purpose of fault tree analysis, it is certainly accurate and provides a good starting point for a discussion of this system analysis technique. There are several aspects of this definition

which are important for a basic understanding of fault tree analysis and require further explanations. These important aspects are presented below.

The technique specifies an undesired state of the system. This undesired state of the system is stated in terms of an operability state of the system and this statement of the undesired system operability state constitutes the top event of the fault tree. The entire course of the analysis is directed at identifying the events or combinations of events which result in the occurrence of the top event.

Fault tree analysis evaluates the system in the context of its environment and operation. In assessing the ways in which the undesired system operability state might come to exist, the system's operating environment, and its potential effects on system performance are considered. In this way, fault tree analysis can account for the fact that compartment flooding may produce pump failures which in turn fails an emergency core cooling system or that the especially high level of stress which might exist under some accident conditions might increase the probability of certain operator errors which could produce or contribute to system failures. The degree to which these environmental considerations can be incorporated into the fault tree is limited only by the analyst's understanding of what those environmental considerations might be.

The technique is directed at finding all of the credible ways in which the undesired event can occur. A fault tree model cannot be used to identify all of the ways a system can fail, only those which are most credible as assessed by the analyst. The analyst's skill in identifying credible system faults is derived in part from a thorough knowledge of how the system functions, a familiarity with component failure rate data bases, experience with similar systems, and sometimes, a subjective combination of logic and intuition.

In addition to the aspects of fault tree analysis described above, there are a number of features of the technique which serve to further define it. One of the most basic of these features is the fact that fault tree analysis is a deductive technique. It considers system failures from effect to cause; from the general to the specific. Using a deductive approach, we first postulate that the system has failed in some way, and then attempt to identify all of the events which could produce or contribute to this failure. This deductive approach stands in contrast to the inductive techniques which start with a particular fault or initiating condition and attempt to determine the effects of that fault or condition on system operation. Examples of inductive methods include failure modes and effects analysis (FMEA), preliminary hazard analysis (PHA), fault hazard analysis (FHA), and event tree analysis. Although both of these general approaches to system analysis have appropriate applications, the deductive fault tree approach has been found to be most useful in nuclear power plant PRA system modeling. In general, it can be said that inductive approaches are applied to determine what system states are possible, deductive methods are applied to determine how a given system state (usually a failed state) can occur. It is this identification of how undesired system states can come to exist that is of interest most often in PRA.

Another feature of fault tree analysis is the fact that it actually results in re-definition of the undesired event by depicting the logical interrelationships between system fault events as they contribute to the occurrence of the top event. This depiction of fault interrelationships serves as a kind of a "roadmap" of system fault paths. This pictorial representation of fault logic may be presented at any of various levels of analytical resolution depending on the specific goals of the analysis and on the level of detail associated with available data. One very important point which must be made in describing the nature of fault tree analysis is that the technique allows the examination of multiple failures. Many other system modeling techniques consider the occurrence

and effects of only single failures. Fault tree analysis, on the other hand, allows the postulation of multiple faults which might occur or exist simultaneously or sequentially, and is not limited to an examination of single faults only. This capability to systematically identify fault combinations which would result in system failure is one of the features that make fault tree analysis such a powerful tool.

7.3 Purposes of Fault Tree Analysis

Given the fact that fault tree analysis is a rigorous, detailed, disciplined approach to systems analysis, what is the product of the technique and how does it justify the often sizable commitment of resources required to perform a "good" fault tree analysis? The product of fault tree analysis, the fault tree model, was described above as a graphical representation of the logical interrelationships between postulated fault events as they contribute to the occurrence of the top event. This system model gives visibility to the answer to one of the most basic questions asked in a PRA - "In what ways can this system fail?".

In addition, fault tree analysis often develops some unique insights into the nature of the interrelationships between component faults and system failures, support systems and frontline systems, and so forth. Some of these insights result in understandings of system successes and failures which either would not or could not be identified without the benefit of this structured approach to system analysis. In general, fault tree analysis is a powerful analytical tool which is capable of conveying a great deal of information about the interrelationships between system model elements.

Although fault tree analysis is not, in itself, a quantitative technique, it does lend itself very conveniently to quantitative evaluation. Thus, when combined with quantitative techniques, fault tree analysis provides a means of calculating the probabilities of system failures. Another way of thinking about the purpose of fault tree analysis is to recognize that it results in the identification of system "weaknesses." As used here, the term "weaknesses" is not intended to connote aspects of system design which necessarily constitute a "bad system." Rather, the "weaknesses" referred to here are those ways in which the system is particularly vulnerable to the occurrence of the top event. Obviously, the first step in improving those aspects of system design and operation which may contribute most significantly to the system's unavailability is the identification of those contributors. Fault tree analysis is uniquely suited to this purpose.

The common thread that runs through this discussion of the purpose of fault tree analysis is that this technique provides some genuinely unique insights into the ways in which a system might fail. These insights have application not only in the assessment of system unavailability, but throughout the PRA process.

7.4 The Fault Tree Development Process

The PRA Procedures Guide (NUREG/CR-2300) identifies and describes five essential tasks which comprise the fault tree analysis process. Although this paradigm tends to oversimplify what can be highly complex and iterative process, it does describe the essential elements of fault tree analysis. Figure 7-1 illustrates the process as it is outlined in NUREG/CR-2300. Each of the elements of the process is explained below.

7.4.1 Define Fault Tree Top Event

As will be more fully discussed in the session on event tree analysis, the fault tree's top event is a direct input from the event tree heading. The top event is an explicit, specific

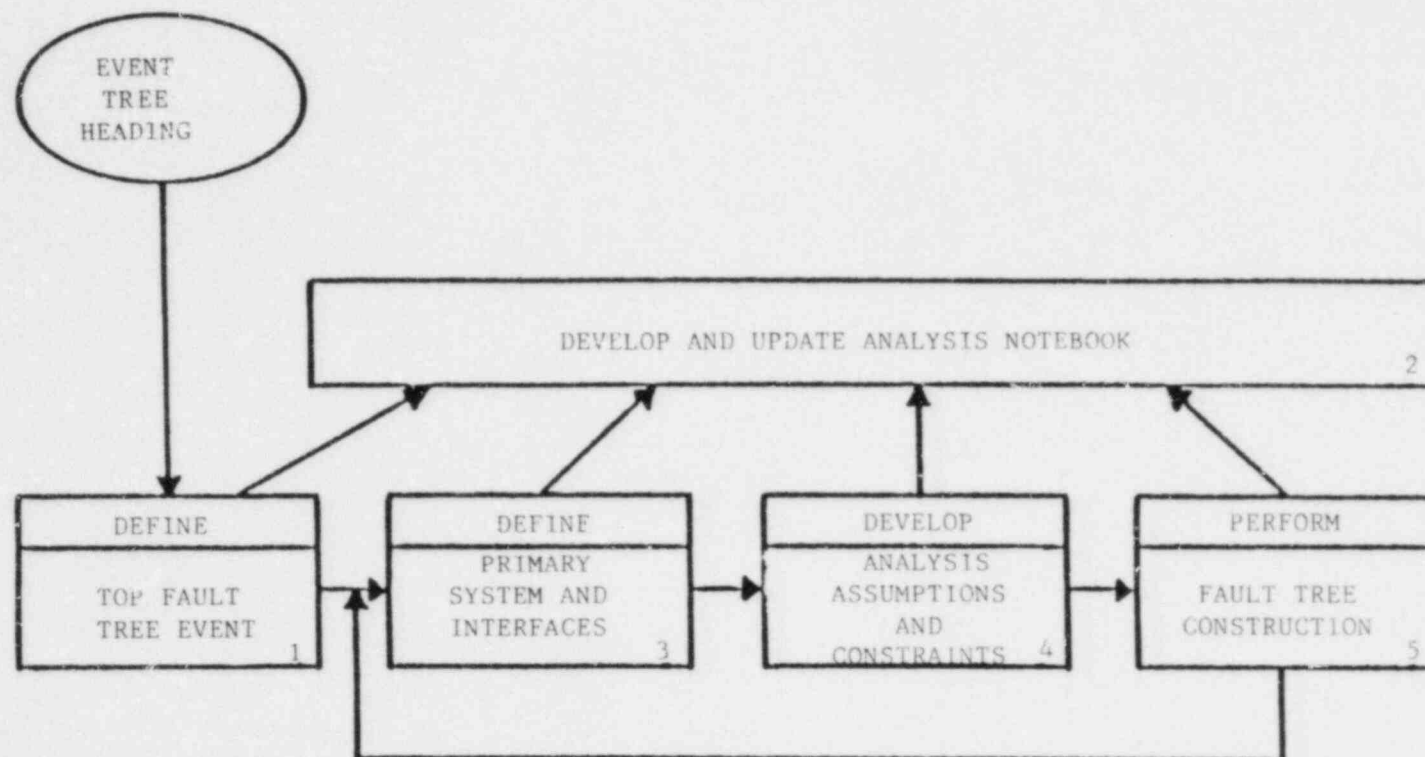


FIGURE 7-1
FAULT TREE DEVELOPMENT PROCESS

statement which describes the undesired state of the system or undesired event for a system or interest. The entire fault tree analysis will be specifically directed at identifying all of the events or combinations of events which could lead to the occurrence of the top event. Achieving the appropriate level of specificity in the statement of the top event is essential to the accuracy and comprehensiveness of the analysis. As there may be a number of different kinds of accidents to which a system would have to respond in different ways, the fault tree analyst may be tempted to formulate a very general statement of the top event, thereby setting the stage for the construction of a "general purpose" fault tree. While this approach to top event definition would be highly convenient, it is also wrong. It is often necessary to construct several different fault trees, each with a different top event, when a system must respond in different ways to different initiating events. For example, a low pressure coolant injection system might be required to deliver rated flow via only one out of four system pumps in response to a small LOCA, but might be required to deliver flow via three out of four pumps in response to a large LOCA. One would certainly expect the fault tree model for low pressure coolant injection system failure in response to a small LOCA to look quite different from that for a large LOCA. Accordingly, there should be two fault tree analyses performed for these two distinct initiating events. Each fault tree will have a different top event.

Because the entire fault tree analysis is tailored to the top event, an accurate, complete, and specific statement of the top event is essential. Proper statement of the top event will contain a description of both the postulated physical aspects of the occurrence and any temporal considerations. For example, an undesired state of a system might be stated as "more than two out of four LPCI pumps fail to start within five minutes and deliver rated flow for at least two hours following an intermediate LOCA." This top event statement specifies both what constitutes failure in physical terms (more than two pumps fail to deliver flow) and stipulates the temporal considerations (must actuate within five minutes and run for two hours) associated with LPCI failure in the context of an intermediate LOCA.

A top event which is stated too generally leads to a fault tree analysis which is not sufficiently bounded and which becomes unmanageable. Conversely, a top event which is stated too specifically sacrifices the comprehensiveness of the analysis and may result in the inadvertent exclusion of essential information.

7.4.2 Develop and Update Analysis Notebook

At the beginning of the system analysis activity, an analysis notebook should be developed for every system which is to be analyzed. This analysis notebook will contain all of the system design and operating data which is to be considered in the course of the analysis. In addition, all analytical assumptions and constraints which are formulated are fully documented in the notebook. A tremendous amount of system information must be assembled in order to perform a detailed fault tree analysis. Without having this information assembled and logically organized in one place, it is very difficult for the analyst to perform and interpret the fault tree analysis without losing essential information.

Although the amount nature of the data which is required to perform a fault tree analysis will vary with the scope of the analysis, several general types of data will almost always be included in the analysis notebook. Hardware design data is, of course, essential. For typical nuclear plant fluid delivery systems, piping and instrumentation drawings depict the system hardware components and illustrate the pathways by which fluid must or may be delivered. These piping and instrumentation drawings are very basic to the system

analysis and for very simple system analyses, may be the only required system diagrams. For more detailed analyses, location drawings (planview and elevation) contain information which allows the analyst to evaluate the system's susceptibility to such potential occurrences as compartment flooding, pipe whip, fire, or other environmental failure mechanisms. These drawings also help the analyst to determine the degree of separation which exists between redundant system components. Such a determination is important with respect to common cause failure considerations. Hardware design information should also include written system descriptions which explain the function of the system and how the system accomplishes this function. The description should also include an explanation of how the system is initiated, various modes of operation (if applicable), and associated rates, capacities, etc. Electrical one-line drawings, elementary wiring diagrams, and the like help to identify essential interfaces with electric power.

Typical analysis notebooks for nuclear systems should also generally include system operating procedures and technical specifications. It has been found that operator errors, as a class, can constitute a significant contributor to system unavailability. By examining normal and emergency operating procedures, analysts can make judgments about the likelihood of postulated operator errors and whether or not these postulated errors should be included in the system fault tree. Ideally, such determinations should be made by, or with the assistance of, a specialist in the field of human reliability analysis. System Technical Specifications, among other things, define limiting conditions for operation, system testing procedures, and scheduled test and maintenance frequencies. Such information is important in quantifying system unavailability and in determining how test and maintenance acts might produce so-called "latent faults", which exist prior to a demand for system operation.

Another general class of information which should be included in the analysis notebook is the collection of quantitative data which will be used in calculating the system's unavailability. Among this quantitative data will be both plant-specific and generic data for unscheduled acts of test and maintenance as well as a data base of applicable component failure rates. When available in a usable form, unscheduled test and maintenance data gathered from plant logs can be very valuable. Such information can often be used to determine the durations as well as the frequencies of these unscheduled acts. Because unscheduled test and maintenance acts often are identified as significant system unavailability contributors, this data should be collected whenever possible.

7.4.3 Define Primary System and Interfaces

In view of the fact that fault tree analysis is a system analysis technique, it is not surprising that one of the most basic tasks of this technique is the definition of the system of interest and its interfaces. Although this task is very basic to fault tree analysis, it is not trivial and frequently requires analysis in its own right.

Ideally, it would be desirable to define the system of interest in such a way that a "closed" system is being analyzed. In practice, however, no system is truly closed. It is therefore necessary to explicitly define the boundaries of the system of interest. This bounding can be surprisingly complex and there is, unfortunately, no one correct way to define a specific system. Consider, for example, a telephone sitting on a desk. If we were to analyze this "system," is it sufficient to define the system as the instrument itself (earpiece, cord, and cradle), or should the line running to the wall jack be included? Should the jack itself be included? What about the external lines to the telephone pole? What about the vast network of lines, switching equipment, etc. that comprise the telephone system in the local area, the nation, the world? For this

example, there is an obvious need to define some external system boundary. The decision regarding the system boundary definition will depend, at least in part, on the aspect of system performance that is of concern.

When formulating system boundary definitions, it is important that those definitions are compatible with one another and that they be compatible with the top event. Failure to ensure this consistency results in a disjointed, sloppy analysis. It is also possible that a lack of consistency in establishing system boundaries may result in a failure to examine all of the essential plant elements. Past experience in probabilistic risk assessment has shown that the interfaces between systems, particularly between frontline systems (those systems which directly perform an essential safety function) and support systems (systems which support front-line system operability), are frequently very important to system analyses. Although there is no step-by-step procedure to follow in defining a system for analysis, in the end, the analysis team must be able to satisfy itself that all essential components have been evaluated.

As is true of the other tasks of fault tree analysis, clean, complete documentation serves to reduce the likelihood of misinterpretation of the analytical results. The analysis notebook must include a detailed definition of the system of interest as well as a listing of the interfaces with that system.

7.4.4 Develop Analytical Assumptions and Constraints

Because it is not possible to assemble or develop all of the items of information which are required to perform a fault tree analysis, it is necessary to formulate a number of analytical assumptions and to place some constraints on the analysis. The analytical assumptions serve to supplement the body of system data which is used in the system modeling effort. The analytical constraints define the comprehensiveness of the analysis and explicitly define what will, and will not, be considered as the fault tree model is developed. Together, these assumptions and constraints address such items as the postulation of passive failures, how operator reliability is influenced by prevailing stress levels, postulation of secondary failures, time periods required for certain acts, the quality of component operating environments, and so forth. In practice, any time that an analyst requires information which is not available or cannot be developed, an assumption must be formulated.

Given that a great many assumptions underlie most fault tree models, it is natural to wonder about the "accuracy" of the assumptions and the resultant fault trees. This issue of the accuracy of analytical assumptions is addressed by supporting the assumptions with deterministic analysis whenever possible. Thermal-hydraulic analyses, for example, can be used to make determinations regarding the operating environment in which components might have to operate following an accident. Assumptions about how an operator would behave under various conditions might be based on psychological studies. When directly related deterministic data does not exist, extrapolation from similar deterministic data may be possible. Whatever the assumptions might be based on, it is necessary that these assumptions be objectively derived and that they be fully documented.

The task of developing analytical assumptions and constraints is not a task which can be done in one self-contained step near the start of the analysis. Fault tree analysis as a whole is a highly iterative process and its tasks cannot be completed in a simple sequential fashion. Often, information discovered in later stages of the analysis may force a re-examination of earlier work. For this reason, the development of analytical assumptions and constraints is a task which actually is performed throughout the fault tree analysis process.

7.4.5 Fault Tree Construction

The last step in fault tree analysis, which interactively makes use of the preceding steps, is the actual construction of the fault tree model. The fault tree technique employs a standard notation and symbology which allows fault tree analysts and interpreters to understand one another. The standard notation and symbology of fault tree analysis, as well as the basic concepts and groundrules of the technique, are presented in the pages which follow.

7.5 Fault Tree Symbology

The fault tree model consists of a collection of postulated fault events which are logically interrelated in a particular way. The symbols which are used to represent these fault events and relative logic are called "event symbols" and "logic gates" respectively. These symbols are shown and described in Figure 7-2.

In addition to the event symbols and logic gates, "transfer symbols" are often used as a convenience to the analyst in order to avoid unnecessary duplication of portions of the fault tree. These transfer symbols also provide for ease in continuing the fault tree model on additional sheets of paper when required. The basic symbol for the transfer function is a triangle. A line extending from the apex of the triangle is called a "transfer in" and a line from the side of the triangle is called a "transfer out." Every "transfer in" will have a corresponding "transfer out" which will be identified with precisely the same alpha-numeric identifier wherever the transfer is made.

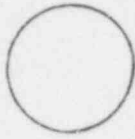
Almost without exception, the symbols described above are sufficient to model any system fault logic. However, several additional symbols are occasionally used to model very rare situations. Because the use of these infrequently applied symbols can be avoided through judicious use of the basic symbols described above, these very unusual symbols will not be discussed here. Interested students can find descriptions of these infrequently used symbols in section IV of The Fault Tree Handbook, NUREG-0492.

7.6 Ground Rules of Fault Tree Analysis

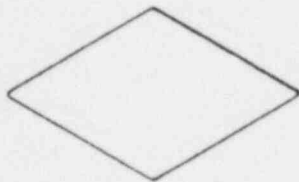
The ground rules which underlie fault tree analysis are deceptively simple. Although the rules themselves are very simple, many analysts have a difficult time adhering to them. Much of this difficulty seems to stem from an inability to grasp two very basic tenets of this analytical technique:

- Fault tree analysis is a step-by-step process in which the analyst must think small.
- The postulation of fault events must be consistent with the resolution of available data and with all analytical assumptions and constraints which have been formulated.

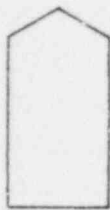
The fact that fault tree analysis is a step-by-step process is what gives the technique the discipline and rigor which make it so useful. There is a tendency among inexperienced analysts, especially, to attempt to find the "answer" without really doing the analysis. To avoid overlooking essential information, the analyst must resist this tendency and perform a step-by-step analysis in accordance with the "immediate cause concept." Beginning with the fault tree's top event, the immediate cause concept dictates that the analyst "look first for the immediate, necessary, and sufficient causes" of the top event.



BASIC EVENT - The circle is used to represent a basic fault event which requires no further development. This symbol indicates that the limit of resolution has been reached and that further definition of the event cannot be achieved.



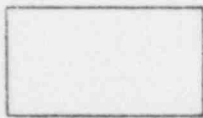
UNDEVELOPED EVENT - The diamond is used to represent a fault event which is not further developed, either because the event is not of sufficient consequence, or because sufficient information pertaining to the event is not available.



EXTERNAL EVENT - The "house" is used to represent events which are normally expected to occur and are external to the component of interest. The house might be used to indicate such events as the success of some interfacing system, the compliance with prescribed environmental parameters, etc. The house represents events which are not, by themselves, faults.



CONDITIONING EVENT - The ellipse is used to represent specific conditions or restrictions which apply to a particular logic gate. This symbol is used almost exclusively in conjunction with the "INHIBIT" gate.



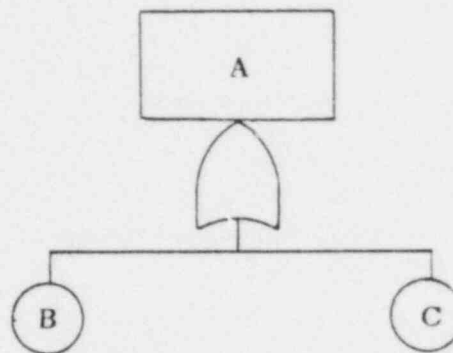
INTERMEDIATE EVENT - The rectangle is used to represent a fault event which occurs due to one or more constituent faults. A complete fault tree model will contain no unresolved intermediate events.

FIGURE 7-2

FAULT TREE SYMBOLS



OR GATE - The OR gate indicates that the output event occurs if any, or all, of the input events occur. For example, the following logic represents the condition in which the output "A" occurs only if input "B" occurs, input "C" occurs, or if both inputs "B" and "C" occur.



AND GATE - The AND gate indicates that the output event occurs only if all of the input events occur. For example, the following logic represents a case in which the output "A" occurs only if both inputs "B" and "C" occur.

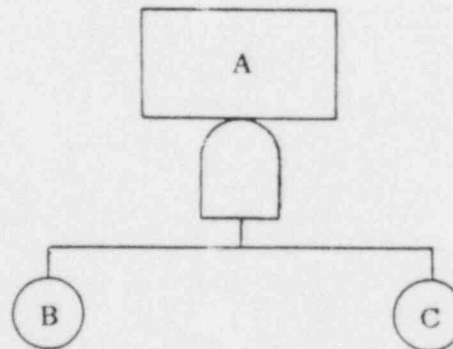
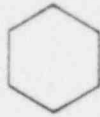


FIGURE 7-2 (cont'd)



INHIBIT GATE - The INHIBIT gate, which is represented with a hexagon, is used to indicate a situation in which the output is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The nature of this condition is described in an ellipse (see description of "conditioning event") to the right of the INHIBIT gate. For example, the following logic represents a situation in which the output "A" occurs only if the input "B" occurs and if the condition described in the ellipse is satisfied. In this way, the use of the INHIBIT gate actually constitutes a specialized "AND" gate.

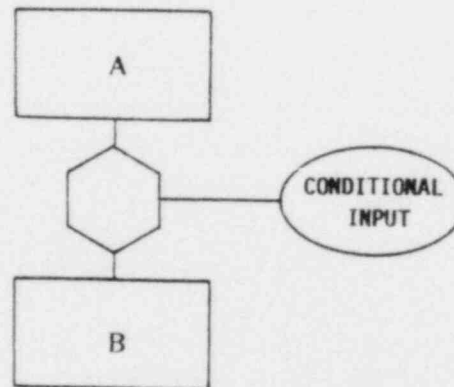


FIGURE 7-2 (cont'd)

After identifying these causes, the analytical process continues in this fashion until all faults have been resolved into their basic constituent failures. In general, a fault tree analysis should begin at the system output end. For a fluid delivery system, for example, the analysis should initially focus on the point to which fluid is to be delivered. The analyst then works back through the system to the fluid source.

In identifying the immediate, necessary, and sufficient causes of every intermediate event, the analyst must ask the question, "Can this event consist entirely of a failure of the component?" If the answer is yes, the event is termed a "state of the component fault." The analyst places an OR gate beneath the intermediate event and proceeds to postulate the applicable, immediate, necessary, and sufficient faults and failures. At least one of these will be the primary failure of the component. If the answer to the question is no, the event is called a "state of the system fault." The logic gate beneath such an event may be an OR gate, AND gate, INHIBIT gate, or possibly, no gate at all. The use of this question at every intermediate fault on the fault tree helps to guide the analyst's approach to the analysis and provides a useful tool to aid in the fault tree construction process.

Another ground rule of fault tree analysis requires that analysts write entries in event boxes in a way that fully describes the postulated fault event. A complete description of a postulated fault event must include not only a statement of "what" is postulated to occur, but a statement of "when" it occurs as well. Although the "when" associated with a fault event may frequently be implicit in the fault statement, if it is not completely clear, it should be explicitly stated. A complete and accurate statement of postulated fault events enhances the quality of the analysis in two distinct ways. It first helps to focus the analyst's attention on the actual event of interest, thereby improving the accuracy of the analysis. Secondly, it assists someone who must interpret the fault tree, but who has not had the benefit of actually having performed the analysis. Good conclusions regarding the results of the fault tree analysis can only be formulated if the person who draws those conclusions has a complete understanding of the nature of the faults postulated in the model.

The third basic ground rule of fault tree analysis is often termed the "no miracles" rule. This rule states that if normal component function is a part of some fault sequence, normal function is assumed to occur. For example, if a postulated human error would result in the closure of a valve which must be open for successful system operation, the analyst does not postulate a simultaneous failure of the valve's actuation relay which would keep the valve open, thereby preserving system success. Although it may be true that there is a small probability that the actuation relay may indeed fail, the conservative nature of fault tree analysis precludes the identification of such an event as part of the system fault model. In addition, the fault tree is, by definition, a failure oriented model. Success logic is not a part of the fault tree technique.

The fourth ground rule, which requires little explanation, is the "complete the gate rule." This rule directs the analyst to completely define all inputs to a given gate before the analysis of any other gates is begun. This rule is a means of ensuring accuracy and completeness as well as a means of preserving the analyst's train of thought.

The last basic ground rule of fault tree analysis prohibits "gate to gate" fault tree construction. Gate to gate construction occurs when two or more logic gates are linked directly together without the benefit of an intermediate event (rectangle) between them. An example of this is shown in Figure 7-3. In this example, logic gate 1 is directly linked to logic gates 2 and 3 without any intermediate events between. This careless practice detracts from the discipline of the technique, does not provide visibility on the

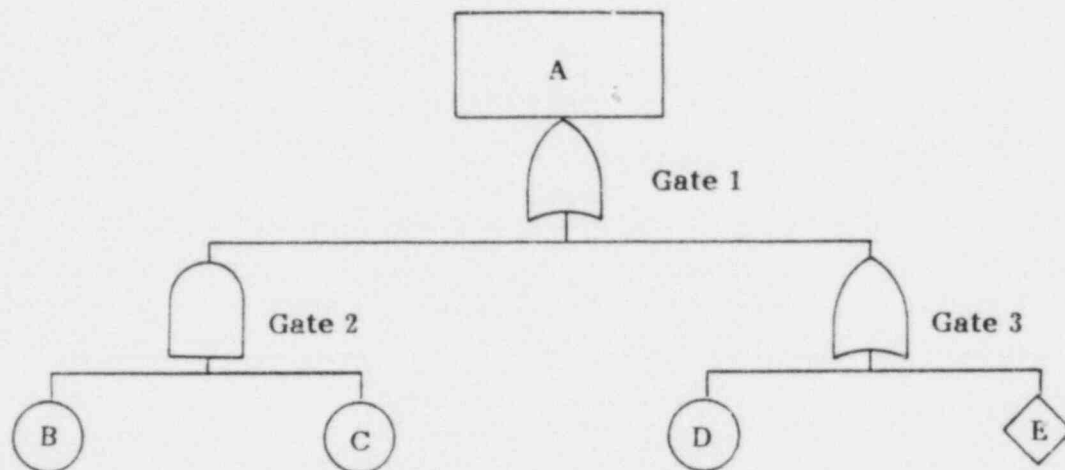


FIGURE 7-3
EXAMPLE OF IMPROPER GATE-TO-GATE CONSTRUCTION

intermediate events, and invites errors in the interpretation of the fault tree model. The correct development of the above faulty fault tree is shown in Figure 7-4.

The basic groundrules of fault tree construction are summarized in Table 7-1.

7.7 Faults and Failures - Definitions

Although the terms "faults" and "failures" are often casually used quite interchangeably, in the context of fault tree analysis, these terms have more distinct meanings. In general, it can be said that all failures are faults, but not all faults are failures. Put another way, failures constitute a subset of the larger set of faults. For our purposes, failures can be regarded as basic abnormal (and undesired) events which render a component, subsystem, or system incapable of performing its intended function. Faults, on the other hand, are higher order events. A fault may be defined as the occurrence or existence of an undesired state of a component or set of components. In the context of fault tree analysis, an event which represents a basic fault tree input and is not analyzed further (circle or diamond), is referred to as a "failure". Events which are analyzed further, and ultimately resolved into their constituent failures are called "faults".

In addition to recognizing the distinction between faults and failures, fault tree analysts also recognize three distinct categories of faults. These fault categories are listed and defined below:

- Primary Fault - A basic fault which occurs in an environment for which the component is qualified. Examples include broken pipes, pumps failing to start, valves failing to open, and similar events which occur when those components' design environments have not been exceeded.
- Secondary Fault - A fault which occurs in an environment for which the component is not qualified. These faults occur when a component must operate in a situation in which it was not intended to operate. Examples include pumps failing to continue to run because lube oil cooling has failed, pipe breaks which occur because they are overpressured, and motor-operated valves which will not open because electric power is not available to them.
- Command Faults - A common fault occurs when a component does not receive a command to operate when it should, or when a spurious command to operate is received. In this case, the component actually performs as it should, but the command which actuates the component is either absent or premature.

7.8 Fault Tree Reduction

Many system fault trees can become very large, sometimes covering 50 pages or more. Such fault trees are very difficult to evaluate and interpret. Fault tree reduction provides a means of simplifying fault tree models, thereby facilitating their evaluation. The most basic step in fault tree reduction, and one in which absolutely no information is lost, is a Boolean reduction process. Boolean algebra is an algebraic system in which the logical operators are OR, AND, and NOT. Fault tree analysis, of course, employs this same logic system, making it possible to express fault tree models as Boolean equations. By applying the basics of Boolean algebra, these equations can be simplified and reduced. A reduced fault tree model can be produced by translating the simplified Boolean equation into a new fault tree.

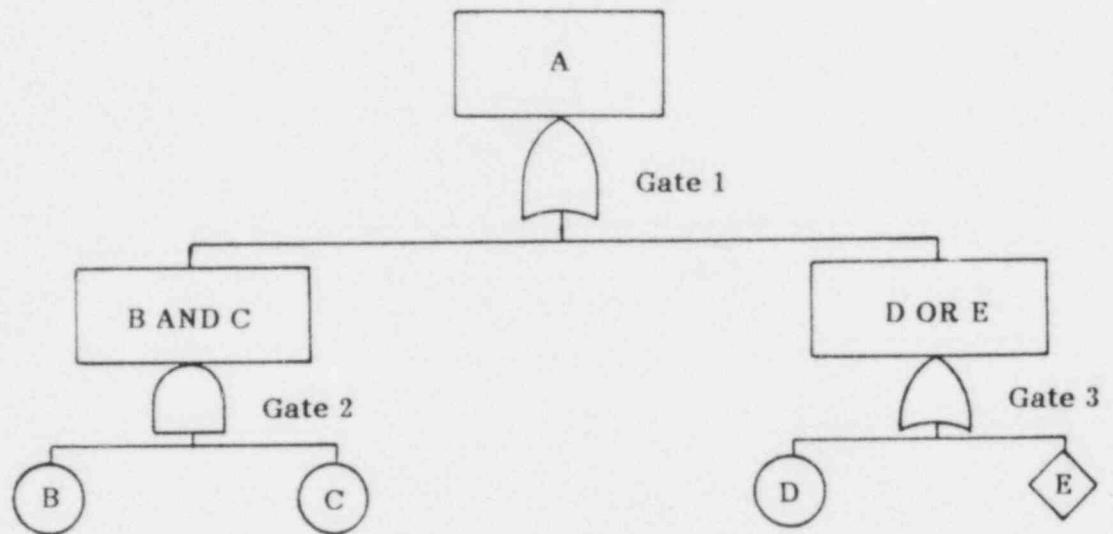


FIGURE 7-4
CORRECTED EXAMPLE OF GATE-TO-GATE CONSTRUCTION

TABLE 7-1
RULES FOR FAULT TREE CONSTRUCTION

1. Step-by-step development.
2. Pose the question, "Can this fault consist entirely of a component failure?" If yes, classify fault as "state of component." If no, classify as "state of system."
3. Write entries in event boxes as faults, stating "what" and "when".
4. No miracles. If normal component function leads to fault sequence, normal function is assumed.
5. Complete the gate. All gate inputs should be defined before further analysis of any input is begun.
6. No gate to gate construction. Logic gates should not be directly connected to other logic gates.

A discussion of the properties of Boolean algebra is not within the scope of this course and will not be presented here. However, in order to aid in the understanding of the example problems at the end of this section, the basic rules of Boolean algebra are presented in Table 7-2.

The first step in Boolean fault tree reduction is to label all logic gates and basic events with unique alpha-numeric identifiers. With that complete, the fault tree model can be re-expressed as a series of Boolean equations. The equations are very easy to formulate by remembering that the fault tree OR gates and AND gates correspond to the Boolean logic operators $+$ and $*$, respectively, as in the example shown in Figure 7-5.

See the sample problem at the end of this section for a more complex example of Boolean fault tree reduction.

Once the detailed fault tree model has been simplified by Boolean reduction, it may be desirable to further reduce the model. A reduced fault tree model gives a more concise presentation of the results of the system analysis and allows an easier identification of the significant contributors to system failure. Any fault tree reduction beyond the Boolean simplification, however, actually results in a reduction in the amount of information contained in the model, and thus must be done with great care. When properly performed, however, only superfluous or insignificant information is eliminated. This reduction must be made in a structured manner and is based on the lessons learned through the fault tree analysis of the system.

The paring of nonessential information is based, at least implicitly, on probabilistic criteria. Common guidelines for fault tree reduction might include the elimination of all double passive failures or all three-input AND gates. In some cases, numerical probability values may be used as reduction criteria. For example, all faults with probabilities of less than $1.0\text{E}-06$ might be eliminated from the tree. Naturally, such numerical reduction criteria must depend somewhat on the specific nature of the detailed fault tree. Such fault tree reduction must be performed in a relativistic manner. It is, for example, not reasonable to discard all faults with probabilities of less than $1.0\text{E}-06$ if no single fault has a probability greater than $1.0\text{E}-05$. Whatever reduction criteria is decided upon, as in all aspects of fault tree analysis, full documentation is essential.

As a final caution, special care must be taken that potential dependent failures are not discarded in the reduction process. Some system faults may have the potential of failing more than one system, or by themselves, of failing more than one train of an otherwise redundant system. Because of the significance of these dependent failures, they must not be eliminated from the fault tree model.

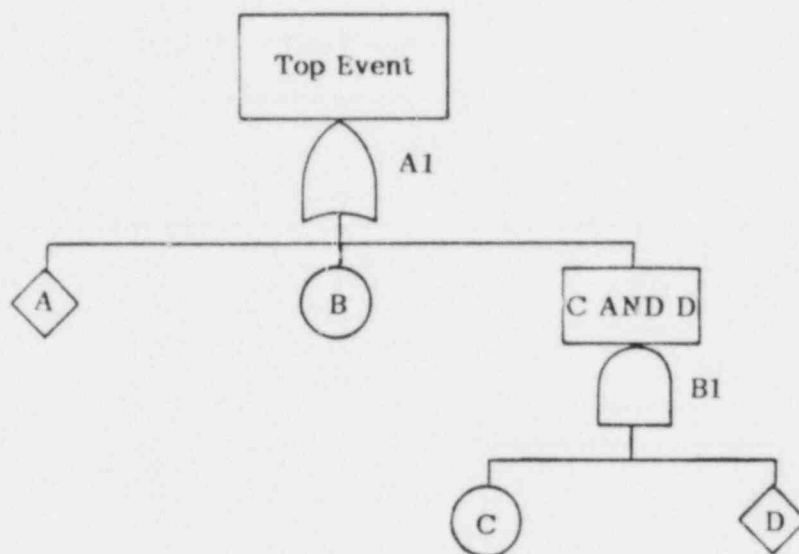
7.9 Summary

Fault tree analysis is a disciplined, rigorous system analysis tool which can be used to model the unavailability of nuclear plant systems. This topic has introduced the symbology and terminology of the fault tree technique and has presented the ground rules of fault tree construction.

The fault tree technique is a very powerful tool which has a rather simple logical basis. Despite this simple logical basis, however, good fault tree models can be deceptively difficult to develop. The best means of developing proficiency with the fault tree technique is to actually attempt to construct some fault tree models. The fault tree sample problem at the conclusion of this topic provides an opportunity to gain some "hands-on" experience in the application of the fault tree technique.

TABLE 7-2
RULES OF BOOLEAN ALGEBRA

<u>MATHEMATICAL SYMBOLISM</u>	<u>ENGINEERING SYMBOLISM</u>	<u>DESIGNATION</u>
(1a) $X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$	Commutative Law
(1b) $X \cup Y = Y \cup X$	$X + Y = Y + X$	
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$	Associative Law
(2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X(YZ) = (XY)Z$	
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$	Distributive Law
(3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X(Y + Z) = XY + XZ$	
(4a) $X \cap X = X$	$X \cdot X = X$	Idempotent Law
(4b) $X \cup X = X$	$X + X = X$	
(5a) $X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$	Law of Absorption
(5b) $X \cup (X \cap Y) = X$	$X + X \cdot Y = X$	
(6a) $X \cap X' = \phi$	$X \cdot X' = \phi$	Complementation
(6b) $X \cup X' = \Omega = I$	$X + X' = \Omega = I$	
(6c) $(X')' = X$	$(X')' = X$	De Morgan's Theorem
(7a) $(X \cap Y)' = X' \cup Y'$	$(X \cdot Y)' = X' + Y'$	
(7b) $(X \cup Y)' = X' \cap Y'$	$(X + Y)' = X' \cdot Y'$	



$$A1 = A + B + B1$$

$$B1 = C \cdot D$$

FIGURE 7-5

LOGIC GATE/BOOLEAN CORRELATION

FAULT TREE ANALYSIS
SAMPLE PROBLEM

FAULT TREE SAMPLE PROBLEM

SYSTEM DESCRIPTION

The "simple injection system," shown on the following page, is designed to deliver fluid from a fluid source at the pump to the arrow head on the exit side of valve D. In order to deliver fluid through valve D, valve D must open, valves B or C must open, valve A must open, valve E must close, and the pump must start and continue to run for some defined mission time. The line diameters are such that flow through either valves B or C is adequate for success and that undesired flow through valve E represents a fluid diversion path which precludes system success.

A common safety injection signal, shown as "SIS" actuates all components. Specifically, the SIS is intended to open valves A, B, C, and D and to close valve E. In addition, the SIS starts the pump.

OBJECTIVE

The objective of this exercise is to construct a fault tree model for the simple injection system. The top event of the fault tree model is to be, "Failure to deliver sufficient flow through valve D."

In developing the model you are to use the ground rules of fault tree analysis presented in this topic and the analysis assumptions listed below. After developing the fault tree model of the simple injection system, the laws of Boolean algebra will be used to reduce the model.

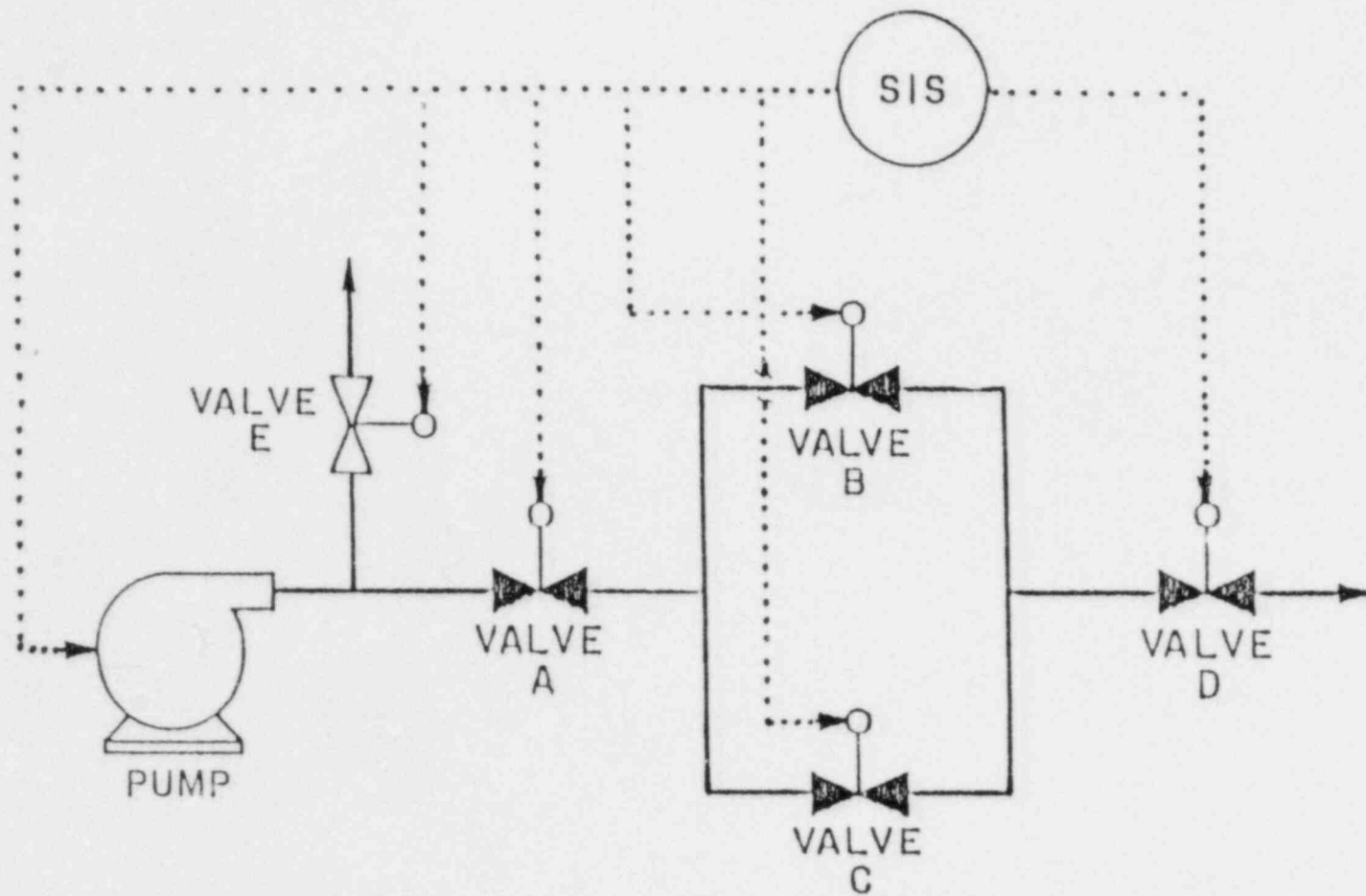
Although solutions are provided for both the fault tree model and the Boolean reduction portions of the sample problem, students are encouraged to attempt the problem before looking at the solutions.

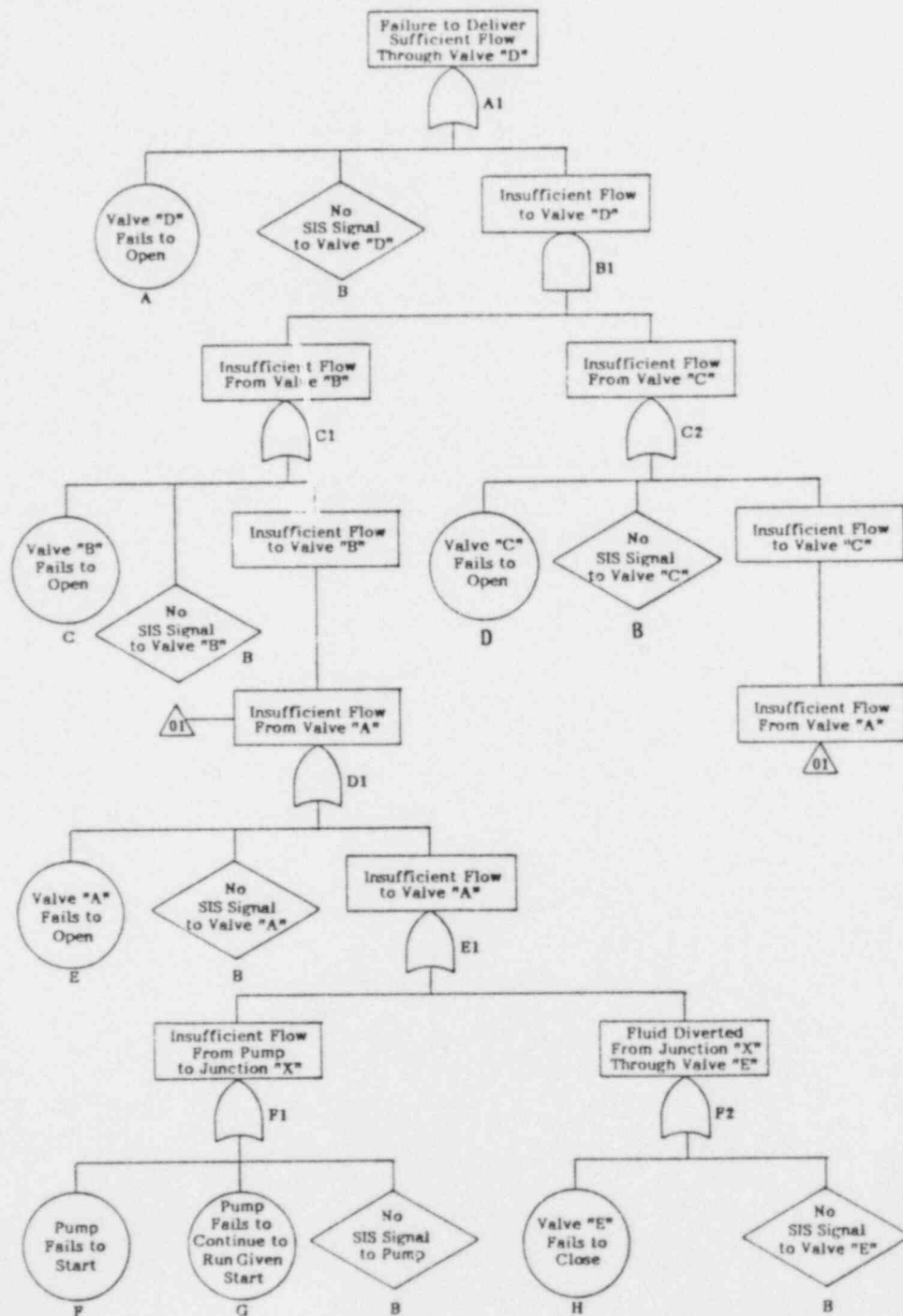
ANALYSIS ASSUMPTIONS AND CONSTRAINTS

Several analysis assumptions and constraints should be applied in working through the sample problem. These are:

- (1) No passive failures such as pipe breaks, open wires, etc., are to be considered in the fault tree analysis.
- (2) No secondary failures such as loss of power, overheating, etc., are to be considered.
- (3) Components are aligned prior to system actuation as shown in the system schematic.
- (4) An inexhaustible fluid supply is available to the pump.

SIMPLE INJECTION SYSTEM





DETAILED "FAILURE TO INJECT" FAULT TREE -
LABELLED FOR BOOLEAN REDUCTION

BOOLEAN REDUCTION
"FAILURE TO INJECT" FAULT TREE

$$A1 = A + B + B1$$

$$B1 = C1 \cdot C2$$

$$C1 = C + B + D1$$

$$C2 = D + B + D1$$

$$D1 = E + B + E1$$

$$E1 = F1 + F2$$

$$F1 = F + G + B$$

$$F2 = H + B$$

By Substitution,

$$E1 = (F + G + B) + (H + B)$$

$$D1 = E + B + (F + G + B) + (H + B)$$

$$C2 = D + B + (E + B + ((F + G + B) + (H + B)))$$

$$C1 = C + B + (E + B + ((F + G + B) + (H + B)))$$

$$B1 = (C + B + (E + B + ((F + G + B) + (H + B)))) \cdot (D + B + (E + B + ((F + G + B) + (H + B))))$$

$$A1 = A + B + (C + B + (E + B + ((F + G + B) + (H + B)))) \cdot (D + B + (E + B + ((F + G + B) + (H + B))))$$

Simplifying,

$$\begin{aligned} A1 &= A + B + (C + B + E + B + F + G + H + B) \cdot (D + B + E + B + F + G + B + H + B) \\ &= A + B + (C + B + E + F + G + H) \cdot (D + B + E + F + G + H) \end{aligned}$$

Multiplying,

$$\begin{aligned} A1 &= A + B + CD + CB + CE + CF + CG + CH + BD + BB + BE + BF + BG + BH + ED + EB + \\ &\quad EE + EF + EG + EH + FD + FB + FE + FF + FG + FH + GD + GB + GE + GF + GG + GH + \\ &\quad HD + HB + HE + HF + HG + HH \end{aligned}$$

Using Identity "X·X=X",

$$\begin{aligned} A1 &= A + B + CD + CB + CE + CF + CG + CH + BD + B + BE + 3F + BG + BH + ED + EB + \\ &\quad E + EF + EG + EH + FD + FB + FE + F + FG + FH + GD + GB + GE + GF + G + GH + \\ &\quad HD + HB + HE + HF + HG + H \end{aligned}$$

Using Identity "X+(X·Y)=X",

$$A1 = A + B + E + F + G + H + CD$$

TOPIC 8

FAULT TREE/EVENT TREE QUANTIFICATION

8. FAULT TREE AND EVENT TREE QUANTIFICATION

Quantification of the fault tree and event tree models is required to obtain numerical frequencies for the accident sequences of interest. Without quantification, the PRA remains a qualitative exercise which can produce only general results.

Accident sequences are developed by the event tree procedure, described in the previous chapters, that considers both initiating events and the success or failure of the relevant systems (or functions) in succession. The quantification may consider individual sequences or groups of sequences, denoted "plant damage bins" (PDBs), formed by combining sequences with certain similarities. The quantification should usually include an estimate of the uncertainty in the analysis resulting from uncertainties in the frequencies of initiating events and the probabilities of primary events. Quantification is discussed in Chapter 6 of the Procedures Guide (NUREG/CR-2300), from which much of this material is drawn.

8.1 Preparation for Quantification

Each accident sequence contains an initiating event and the subsequent failure of one or more safety systems. The quantification process determines the frequency of accident sequences from the initiating event, fault tree models of the systems, and event tree descriptions of the system failures making up that sequence. The system failures can represent combinations of faults undetected before the initiating event, failures of components or the operator to act on demand, failure of components to operate throughout a specified interval, or component unavailabilities due to testing or maintenance. In each case the component is functionally ineffective and unable or unavailable to carry out its mission. The probability of any of these faults is termed "failure probability." Thus, as used here, "failure probability" incorporates failure to start and/or failure to operate.

The results of the accident-sequence quantification task may or may not be the last task of the PRA study. In a PRA where the objective is the quantification of core-melt sequences, the final product is the estimated frequency of the accident sequences, and there may be no need to distinguish these sequences in more detail than by the occurrence of core melt. In the more general case, in which containment failure, radionuclide release, or offsite consequences are to be analyzed (Levels 2 or 3 PRA), the results of the accident sequence quantification are used as input to the containment analysis described.

Besides the results generated for use in the risk assessment, the fault trees, event trees, and logic models can provide great insight into design and operation. They can be used to derive reliability parameters and importance measures to determine the minimal cut sets, and to analyze common cause events.

The plant logic model consists of the event trees and fault trees. It is composed of various primary events which may be initiating events, component failures, unavailabilities due to testing or maintenance, recovery failures, dependent failures, human errors, or external events. All primary event values are expressed as probabilities except for the values of initiating events, which are frequencies, and the values of external events, which can be frequencies or probabilities. Solution of the plant logic model yields combinations of initiating events and system failures that are evaluated to yield accident sequence frequencies.

Before quantification begins, event trees and the fault tree models, required by their top events (headings), are developed. These logic models must be consistent with one another regardless of which method of quantification is utilized. The fault tree models should identify the primary events in sufficient detail for their quantification, including unavailabilities and frequencies, and their distribution parameters if uncertainty is to be propagated. The event trees for each initiating event define the accident sequences to be evaluated, including the definition of the set of system faults that are included in each. The fault tree models indicate the primary event faults and fault combinations that cause these system faults to occur.

However, because of similarities among certain accident sequences and the amount of work involved in their analysis, the accident sequences are usually grouped into PDBs. A PDB may contain one accident sequence or many accident sequences. The binning process reduces the total number of sequences in quantification, but is not required for quantification. The PDBs may be quite different if the PRA continues on to consider the containment response and/or the offsite consequences as opposed to terminating with the core damage frequencies. Further grouping of the PDBs for the offsite consequence analysis is common.

3.2 General Procedure

Accident sequence analysis begins with the identification of the accident sequences to be analyzed, usually followed by a grouping of accident sequences into PDBs. Sequences that cause similar physical responses in the plant are grouped into the same bin. If a PDB contains numerous sequences, the sequences in each bin may be screened to eliminate those that will not contribute significantly to the total frequency of the bin. Then a probability expression for each sequence is created from the solution of the plant logic model and then used to combine the estimated values for initiating and primary events. The two methods commonly used for quantification, fault tree linking and event trees with boundary conditions, differ in this part of the process.

In fault tree linking, the accident sequence is represented by a fault tree whose top event is an AND gate with inputs representing the top gates of the system fault trees for each system depicted in the accident sequence. System dependencies are explicitly treated in the fault tree logic. The resultant sequence fault tree can then be analyzed by one of the available fault tree reduction techniques resulting in a set of minimal cut sets which are then used to develop a probability expression for determining the sequence or bin frequency. These minimal cut sets represent the smallest sets of primary events that must exist simultaneously for the system failure (or sequence) to occur. A probability expression for the top event of the system failure or sequence can be determined from the minimal cut sets and used to quantify the probability of the top event.

Using the other quantification method, event trees with boundary conditions, each branch of the event tree is evaluated. The appropriate boundary conditions reflect the various states of the support systems appearing in the path of the accident sequence. Thus, these support dependencies are treated within the event tree. Once all branch point probabilities have been determined, the sequence frequency is obtained by simply multiplying the probabilities of the branch points in the accident sequence. If uncertainty calculations are to be made, the uncertainty for each branch point is derived and propagated through the accident sequence.

Using either fault tree linking or event trees with boundary conditions, when rigorously applied, will result in equivalent solutions. However, since both methods apply some approximations and assumptions in practice, the final results for any given solution may vary if the assumptions used are not carefully examined.

One further distinction between the two quantification approaches that should be pointed out. The fault tree linking method, also called the small event tree/large fault tree method combines systems and component failures that are not necessarily independent. It automatically accounts for intersystem dependencies within a sequence. The other method, which utilizes event trees with boundary conditions, also called the large event tree/small fault tree approach, requires the development of more complex and detailed event trees since each event in the tree must be independent of the others. In this method each event in the tree is quantified, and the sequence frequency is obtained by multiplying the probabilities of these events.

Both approaches to accident sequence quantification make use of event trees in conjunction with fault trees and both require some assumptions and approximations to be practical. In the fault tree linking technique, the event trees have been constructed at a high level so they display only the frontline functions or systems. The dependencies on support systems and subsystems are included entirely within the fault trees. The resultant linked fault trees are thus large and complex, but the existence of efficient computer reduction techniques makes analysis by this approach possible in spite of the many cut sets that can be generated for quantification.

In the other quantification method, which uses event trees with boundary conditions, the more elaborate event trees explicitly display the significant dependencies. The resultant fault trees for the top events are thus simpler and independent, and can be analyzed by hand. Heavy reliance is placed on the analyst to identify and separate the dependencies in the event tree modeling. Considerable care must therefore be taken to ensure that the significant dependencies in a sequence have either been identified and included as top events in the event tree or otherwise accounted for in generating the split fractions along a sequence path.

The use of detailed event trees generally yields many more sequences because of its evaluation for the various mutually exclusive support system states. Several such sequences would combine to result in the same frontline system configuration as the identified fault tree linking.

Overall, the basic conceptual difference between the methods is the point in which the quantification (conversion from symbolic representation to numerical results) takes place. That is, whether it is done stepwise throughout the process (for event trees with boundary conditions) or as a single step near the end (for fault tree linking). Both methods can be successfully employed and have been used in major studies performed to date. An advantage of stepwise quantification is a reduction in the need to carry through algebraic terms, so that quantification can be performed manually. An advantage of quantification as the last step is that the symbolic representation allows computer searches for dependencies as the last step before quantification and the presentation of results in terms of cut sets for dominant accident sequences.

8.2.1 Fault Tree Linking Method

This approach involves constructing sequence fault trees, solving these fault trees for dominant cut sets, generating a probability expression from dominant cut sets, and combining the probability expressions for each accident sequence into an expression for the PDB.

The fault trees for each event or system heading in the event tree are combined or linked with an AND gate to form a new top event that is the accident sequence. Furthermore,

if accident sequences with the same initiating event are combined in the same plant PDB, an OR gate may be used to combine the sequence fault trees into a single model. Since initiating events are treated as being mutually exclusive, the estimated frequencies for sequences with different initiating events can be summed to produce an estimated frequency of the PDB. A fault tree reduction code is then used to find the minimal cut sets of this new top event. Any dependencies in the way of shared components or support systems are thus automatically accounted for in the Boolean reduction process, if and only if the same identifiers have been assigned to these components in every constituent fault tree. With this process, the quantification takes place on the overall sequence cut sets as opposed to the individual systems or subsystems.

The first step is the identification of the accident sequences to be quantified. The number of sequences quantified may be reduced by grouping consideration of the PDBs. When a PDB contains more than one sequence, the probabilities of the accident sequences can be summed to yield a total PDB frequency. If the mutual exclusivity of the accident sequences has been lost (that is, success states were not modeled in the accident logic), a conservative result may be obtained when the algebraic sum is used. This potential problem can be reduced by using a logical OR to combine accident sequences that are not mutually exclusive, thereby eliminating cut sets or sequences that subsume others within the PDB.

Valuable information can be gained by examining the magnitude of the fission product release for each PDB. This information can be used to establish the relative effects of each PDB on the analysis results and determine which ones will have the greatest effect on the results of the consequence analysis. This will ensure that low-probability/high-consequence sequences will not be left out of the analysis. If accident sequences are chosen without regard to PDBs, a small probability cutoff is used to eliminate sequences from consideration. If that cutoff results in the elimination of all sequences from the more severe PDBs, the truncation value is lowered until sequences in the most severe PDBs appear. All significant contributions to bin frequency, including the contributions by large numbers of low frequency sequences, must be carefully considered.

If PDBs are used to group sequences, a number of approaches for coalescing accident sequences or PDBs for further analysis are available. If the outcome of a particular PDB is not significantly different from another, the two PDBs can be combined.

Within a particular PDB chosen for quantification, some sequences can be discarded for any one of several reasons. It may be possible to estimate the frequency of some of the sequences and to eliminate those that do not significantly contribute to the PDB frequency. Finally, sequences within a PDB that are identical except for their initiating events can be modeled as one sequence, with a single initiating event frequency representing the combined frequencies of the initiating events if there are no differences in the interactions between each initiating event and the subsequent system failures. The sequence fault tree has an AND gate as its top gate. The inputs to the top gate are:

- the initiating event
- the system fault trees for the system failures of the accident sequence.

When a number of fault trees are linked together, certain types of dependencies can result in a situation where the failure of system A causes the failure of system B and the failure of system B causes the failure of system A. This is called a circular-logic loop. Any attempt to combine the two fault trees for these systems will be difficult unless one branch of the circular logic is artificially cut off. Such problems should be revealed by the fault tree process code.

The number of events in the system fault trees can be substantially reduced by defining an equivalent system fault tree in which independent subtrees (modules) are replaced by developed events. The independent subtrees must be independent with respect to all of the systems represented in the accident sequence, including the initiating event. While subtrees may be developed that are independent only for one or two sequences, subtrees should be used that are independent for all the sequences. Then the independent subtrees will be independent for any sequence of system failures and system successes and they can be used for any event tree sequence. The quantification and evaluation of the independent subtrees must be done only once and will apply to all event tree sequences.

The sequence minimal cut sets may represent the solution to a very large fault tree because the sequence fault tree is formed by combining, under an AND gate, several system fault trees. Consequently, there may be millions or even billions of minimal cut sets for a particular accident sequence. To reduce the number of minimal cut sets, a truncation value can be used to eliminate cut sets that make a negligible contribution to the total sequence probability.

Because the truncation process eliminates minimal cut sets from the set of minimal cut sets for the accident sequence, it is non-conservative. If a suitably low truncation value is used, the effect on the total accident sequence probability is slight. Since this process is non-conservative, an appropriate truncation value must be carefully selected.

In some sequences, characterized by explicit definitions of system success, cutsets which result in failing those systems required to operate must be eliminated. Not eliminating these cutsets results in an overly conservative prediction of sequence frequency. These cutsets are eliminated by essentially removing from the list of cutsets for the sequence those faults which would result in failure of the systems identified as successfully operating. This process is referred to as including consideration of "complemented events" (system successes) in the sequence evaluation.

The cut sets that survive the truncation must then be examined and modified to remove overly conservative assumptions about primary event data. Cut sets that are inconsistent with the sequence definition, either because they violate the system success states or contain mutually exclusive primary events, must be eliminated. This may be done manually or by computer codes.

If conservative assumptions have been made about component recovery from failure or conservative probability estimates have been used in screening cut sets, it may be desirable to treat these conservatisms in a more realistic manner. If conservatism in the screening process has been excessive, then a relaxation of the conservatisms may lower cut set probabilities drastically. As a result, additional fault tree quantification may be required since cut sets previously excluded in the truncation process may become relatively significant.

The quantification of accident sequence cut sets begins with the generation of a probability expression for the sequence minimal cut sets. This expression is then used to quantify the accident sequence by using the estimated values for primary event probabilities and estimated initiating event frequencies. Together, these values yield a best-estimate value for the frequency of the event sequence. This probability expression is also used as the basis for the uncertainty analysis.

A number of techniques are available to generate probability expressions for the minimal cut set representation of accident sequences. An upper bound may be generated by

means of the sum-of-products approximation for rare events which is often adequate in nuclear plant risk analysis because of the small numerical magnitude of the core melt risk frequencies. A bounding technique that generates both upper and lower bounds may be used, or the exact probability expression for the top event can be calculated. Where the sum-of-products method yields an overconservative expression for the sequence frequency, one of the bounding techniques or an approximation of the exact expression can be used.

When an approximation other than the sum of products is used, it is usually done by eliminating cut set intersections that do not contribute to the final result. Generation of the probability expressions can be extremely difficult: most computer codes that generate an exact probability expression are generally unable to handle more than a few hundred minimal cut sets. Two techniques that are used to generate Boolean expressions for accident sequences that can be more efficiently quantified are the creation of independent subtrees (modularization) and the creation of mutually exclusive sets of cut sets.

Fault tree linking provides a structure that can be used to perform the common cause analysis. The approach taken depends primarily on the number of minimal cut sets generated by the accident sequence fault tree since the solution and enumeration of large numbers of cut sets is impractical.

If the dependent failure approach is to be used for quantifying common cause events, two distinct methods are used. Typically, with small fault tree models generating hundreds of cut sets, the beta-factor method can be applied on a cut set basis. This approach requires that all the minimal cut sets for the fault tree be generated (i.e., no probability truncation) and that each cut set be individually examined to determine whether a dependent failure probability should be applied to increase the cut set frequency or probability. Since all the cut sets must be generated and examined, there is a limitation on the total number of cut sets that can be analyzed. While it may prove to be impractical to apply dependent failure probabilities to all the cut sets of the accident sequence, it may be possible to apply them to the cut sets of independent subtrees within the accident sequence fault tree, since the independent subtrees are quantified individually and replaced by primary events within the accident sequence fault tree. If the fault tree has been modularized, care must be taken that dependencies between modules are calculated and included.

For accident sequence fault trees that generate too many minimal cut sets for using dependent failure probabilities on an individual basis, dependent failure probabilities may be introduced as primary events in the system fault trees. This method uses solutions at intermediate gates of the sequence fault tree to analyze portions of systems and derive dependent failure probabilities from those solutions. The accident sequence fault tree is then modified, to include new primary events representing the dependent failure probabilities, at the appropriate places. The modified fault trees are then solved in a normal fashion (including truncation) to yield a result with dependent failure probabilities included.

Similarly, qualitative searches can be made from common cause events on the accident sequence cut sets but if any cut sets are eliminated during the fault tree solution, the common cause analysis is not complete, and the results of common cause searches may not include all significant common cause events. One way around this problem is to break the accident sequence fault tree into subtrees for which all the cut sets can be searched for common cause events.

8.2.2 Event Trees With Boundary Conditions

In this approach, dependencies like those between a support system and two or more frontline systems are explicitly displayed in the event tree. A frontline system is a system that directly performs a safety function, an example being the high pressure injection system. A support system is a system that is needed for a frontline system to perform its safety function. An example is the AC electric power system. Each system is quantified for every set of boundary conditions that have a unique effect on system failure probability, where the boundary conditions are a given set of component and system states that affect the system being quantified. The quantification involves the calculation of conditional probabilities since specific component and system states are assumed. Events are combined within the event tree by multiplication to obtain estimated frequencies or approximate frequency distributions for each sequence. The estimated sequence frequencies within each PDB are then summed to obtain a total estimated frequency for each bin.

When the method of event trees with boundary conditions is used, algebraic expressions are (usually) implicitly developed for each PDB. This development process is implicit because, unlike the fault tree linking method, no single Boolean expression at the component level is defined for each bin. However, after an optional initial screening for dominant sequences, either method can be used to combine distributions in an identical way. The key differences between the methods lie in how the dominant sequences are defined and how the frequencies for the PDBs are obtained.

The method of event trees with boundary conditions uses more detailed event trees and therefore simpler fault trees than does the fault tree linking approach. In particular, the support systems found to be important are included explicitly as top events in the event trees. In this approach, then, "systems" or "top events" are narrowly defined. Thus, important dependencies between top events are shown explicitly in the event tree rather than being contained in the fault trees underlying the top events. In this approach, separate fault trees or system models are, in effect, also written for each branch point of the event tree. These fault trees then explicitly recognize the states of the systems or top events upstream on the path leading to that branch point. (This recognition can also be thought of as boundary conditions on the system fault tree; hence, the term "event trees with boundary conditions.") When such a fault tree is quantified, it yields the split fractions, that is, the frequencies of the events that make up the sequence for that specific branch point. To be more specific, it yields the split fraction for that top event conditional upon the path through the event tree by which that top event is reached. Each path through this event tree (i.e., each accident sequence) is characterized by the particular initiating event and by the failed and partially failed systems in the path.

The first step is to develop event trees displaying all the significant intersystem dependencies between the frontline systems whose performance is pertinent for the initiating event of interest. These result from common support systems and other dependencies such as human error. The event trees include these support systems and any dependencies between support systems must be identified and displayed in the event tree. Multiple branches reflecting partial success may be used where this more appropriately describes the support system state and facilitates the quantification of the frontline system. For example, for the electric power heading of the event tree with two buses supplying the safety systems, four branches could be used in the event tree to describe the availability of electric power. These branches would represent "both buses working," "Bus 1 working and Bus 2 failed," "Bus 1 failed and Bus 2 working," and "both buses failed."

When the event trees have been completed, the split fractions in the event trees are determined from logic models for the system or top event under the conditions represented by the particular branch point or node in question. The system logic models are usually in the form of fault trees, but they can be reliability block diagrams, GO models, subevent trees, FMEA models, or some other kind of model. If fault trees are used to relate the state of the top event system to the states of its components, the minimal cut sets of these trees describe the system failure in terms of sets of component failures.

8.3 Simultaneous Test and Maintenance Contribution

Before quantification, cut sets are screened to eliminate those that are inconsistent with the accident sequence definition. Cut sets containing two or more test and maintenance primary events may be eliminated if testing schedules do not coincide or if technical specifications prevent both from being out-of-service for maintenance at the same time. For the remaining cut sets that contain test and maintenance primary events, these events are assumed to be random and independent. If a cut set contains two or more test and maintenance primary events, however, the probability that these primary events occur simultaneously will often be greater than the value calculated by treating them as random and independent. In this case, the cut set frequency can significantly increase because of the simultaneous occurrence of these primary events.

Simultaneous testing and maintenance can occur for any of several reasons. Components in separate systems may unknowingly be tested at the same time because of coincident testing schedules. For example, a pump in system A tested every 8,000 hours and a pump in system B tested every 6,000 hours might be simultaneously tested every 24,000 hours after the first simultaneous test. Human error that results in simultaneous testing and maintenance in violation of technical specifications is another cause. These and any other causes of simultaneous testing and maintenance must be accounted for to avoid underestimating the frequency of an accident sequence.

To illustrate the significance of simultaneous testing and maintenance, suppose a cut set contains two test primary events for two diesel generators. If testing is monthly and requires an hour, then the estimated testing unavailability contribution of the pair, assuming random and independent testing, is 1.9×10^{-6} . If, however, the two diesel generators are simultaneously tested once every 10 years in violation of technical specifications, then the simultaneous testing unavailability of the pair is 1.1×10^{-5} .

To account for the effect of simultaneous testing and maintenance, it is first necessary to identify the cut sets in a PDB that contain two or more test and maintenance primary events. For each of these cut sets, the test and maintenance primary events are then replaced with a single new test and maintenance primary event that represents the unavailability due to simultaneous testing and maintenance.

The probability to be used for the new simultaneous test and maintenance primary event is the fraction of time the replaced test and maintenance primary events occur simultaneously. If the simultaneous testing and maintenance results are in violation of technical specifications, then the probability for this new primary event is given by the product of the probability of violating technical specifications through simultaneous testing and maintenance and the probability of the replaced primary event with the shortest average test and maintenance time. For example, if the probability of violating technical specifications is .01 and the probabilities of three replaced test and maintenance primary events are .001, .0001, and .00001, then the probability for the single new test and maintenance primary event is 10^{-6} .

8.4 Human Error

Because the nuclear power plant is designed, constructed, maintained, and operated by people, a PRA must consider human error. There will be considerable and continuing interaction between those responsible for the human reliability analysis (HRA) and those working in fault tree and system reliability analysis. Further information on human error may be found in Chapter 4 of the PRA Procedures Guide (NUREG/CR-2300) and the Handbook of Human Reliability Analysis (NUREG/CR-1278).

The analyst must consider the human tasks that are performed under normal operating conditions and those performed after accidents or abnormal occurrences. In the former situation, errors might be made during or after maintenance, calibration, testing, or in the normal operation of the plant. These errors may occur in or out of the control room. In the post-accident situation, most safety-related errors occur in the control room.

In either situation, most of the errors identified and analyzed are those made in following plant procedures. Only occasionally are extraneous acts considered. That is, in most cases, the analyst determines whether a given procedure is followed correctly and does not attempt to determine which uncalled-for elements are manipulated. The analyst assumes that only human errors are dealt with, i.e., mistakes made in the performance of assigned tasks. Malevolent behavior such as deliberate acts of sabotage are not considered. It is assumed that all plant personnel act in a manner they believe to be in the best interests of the plant.

The major source of uncertainty in HRA is the dearth of data on human error probabilities (HEPs). For the most part, the Handbook (NUREG/CR-1278) presents the best available data on human performance in carrying out the tasks performed in nuclear power plants. Most of these estimates of HEPs represent extrapolations from human error data based on tasks similar to those performed in nuclear power plants. Nearly all of the tabled HEPs relate to routine human actions. For some operations, cognitive errors are critical (for example, errors in evaluating display indications). Very little information on errors of interpretation or decision making is available.

There are several sources of uncertainty in the generic HEP values. The variability of human performance is reflected in the differences among plant personnel as well as in differences in skill, experience, and other personal characteristics. There can be wide variation in specific environmental situations and in other physical aspects of the tasks to be performed or in the response requirements under which the operator must act. The data can account for only some of this variation in such performance shaping factors (PSF). The width of the uncertainty bounds surrounding each estimated nominal probability represents an attempt to account for the residual uncertainty.

Most probability estimates are based on a set of common assumptions that limit or restrict the use of the data. Exceptions to these assumptions should be clearly indicated. Typically, the assumptions are that the plant is operating under normal conditions, and that the operator does not need to wear protective clothing, and so on.

The HRA is usually divided into four phases: familiarization, qualitative assessment, quantitative assessment, and incorporation. The order of the various activities is not fixed; the entire process is highly iterative and its parts recursive.

A critical task in the HRA is to ensure that all human actions are analyzed in the context of actual performance. Human actions in a nuclear power plant should not be treated as isolated entities, unaffected by other factors. Some interactions will affect the

assessment of performance on individual tasks and others will have a global effect on the performance of all tasks in a given procedure. In some cases, a single plant procedure will cover several sets of tasks involving critical components. For example, in restoring items of equipment after maintenance, the operators may follow a general plant procedure governing the application and removal of tags.

Potential errors must be identified for each step of a task, which should be considered in order of performance. For any given step, the consideration of an error of omission or the various errors of commission (selection, reversal, sequence, etc.) must be made based on the relevant PSFs and the task analysis. For example, if an operator is directed by a set of written procedures to manipulate a valve which is well isolated and labeled on the panel and differs in shape from other valves on the same panel, errors of selection may not have to be considered for this particular step.

Extreme care should be exercised in deciding which errors, if any, are to be completely discounted. In comparison with tasks in other industries, most of the tasks performed in nuclear power plants have very low HEPs, on the order of 10^{-3} . Although one error in a thousand opportunities seems quite low, a HEP of 10^{-3} may contribute substantially to the frequency of system failure.

For example, if something is to be done at the discretion of the shift supervisor, the supervisor's remembering to order the task will determine whether the task is performed by the operator. These extraneous factors that affect the probability of human error usually involve some sort of failure in the plant's administrative control system. Events other than human actions that affect subsequent performance must also be taken into account. If an operator's cue to initiate a task involves some signal from the equipment or an order from a supervisor, the probability of that signal's being generated or that order's being given must be considered.

In making a probabilistic statement as to the likelihood of HEPs, each error defined as likely in the task analysis is entered as the right limb in a binary branch of the HRA event tree. Chronologically, in the order of their potential occurrence, these binary branches form the limbs of the HRA event tree, with the first potential error starting from the highest point on the tree at the top of the page. An example of an HRA event tree is shown in Figure 8-1.

Any given task appears as a two-limb branch, with each left representing the probability of success and each right limb representing the probability of failure. Once a task is diagrammed as having been completed successfully or unsuccessfully, another task is considered. The binary branch describing the probability of the success (or the failure) of the second event extends from the left (or the right) limb of the first branch. Thus, every limb following the initial branching depicts a conditional probability. The initial branching also represents a conditional probability in that the probabilities for that branch are based on the existence of a given situation. Since failure of the initial actions is often assumed to lead to failure of the entire task, the right-hand branches are often not developed further.

A primary consideration in conducting an HRA analysis is the variability of human performance. This variability is exhibited by any given individual in the performance of tasks over time and is affected by PSFs acting within the individual or in the environment in which the task is performed. Variability also results from the performances of different personnel. Because of this variability, the reliability of human performance usually is not predicted solely as a point-estimate but is determined to lie within a range of uncertainty. A point value can be estimated by considering the effects

of relevant PSFs for the task in question. If the plant situation is worse in terms of the PSFs or the response requirements than the one described in the data source, the HEP for that task should be higher than the nominal value. Likewise, if a plant's situation is judged to be less likely to result in a human error, an HEP that is closer to the lower bound may be used. In any event, the objective is to realistically reflect the actual operating environment of the plant.

For errors of omission, for example, the analysis should consider cues or reminders that would make forgetting any item less likely or for poorly written procedures that would make forgetting an item more likely. For errors of commission, it is necessary to identify the elements of the performance situation that might affect the actions themselves or the operator as he performs them. For example, if the face of a display is such that reading it is unusually difficult, an HEP higher than the nominal value for reading errors for such a display should be assigned. The analysis should consider the influence of PSFs that affect the probability of error for all or most of the events in the analysis, such as stress or the operator's level of experience.

Complete human error analyses are performed for the dominant sequences identified by the event tree and fault tree analyses. To save time and effort in the HRA, the effects of recovery factors are not considered until it is determined that a given analysis is part of a potentially dominant sequence. The probability of system failure due to human error will certainly be higher when recovery factors are ignored than when they are included. If the situation being analyzed does not appear as a potentially dominant sequence when this inflated system failure probability is used, there is no need to analyze it further. In fault tree terms, the frequency of an accident sequence can only be decreased by considering recovery factors.

To decrease the actual number of HRAs that must be performed for each plant, recovery factors should not be included in the preliminary analyses. Once potentially dominant sequences have been identified, recovery factors for each can be added to see whether a complete representation of the system as it operates will eliminate the potential dominance. The incorporation of recovery factors can be done in stages, the purpose being to decrease the amount of time required for each analysis. If there are five recovery factors for a given scenario, the human reliability analyst may choose to model only two of them at first. If the inclusion of these results in that sequence ceases to be potentially dominant, no more work need be done at this time. If this scenario still shows up as one of the system's potentially dominant sequences, the other three recovery factors should be analyzed.

8.4.1 Sources of Uncertainty In Human Error Estimation

There are five major sources of uncertainty in estimating the probabilities of human errors in operation of nuclear power plants:

1. Dearth of data on human performance in nuclear power plants
2. Inexactness of models of human performance that purport to describe how people act in various situations
3. Identification of all relevant PSFs and their interactions and effects
4. Skill and knowledge of those performing the HRA
5. Variability in the performance of a given individual and among different individuals.

The first source, the shortage of human performance data specific to nuclear power plants, is the most critical. Historically, such data have not been collected on a scale large enough to establish a data base for operations in nuclear power plants. The licensee event reports include descriptions of incidents involving human error, but no information on human error rates or probabilities is given. Furthermore, the determination of what constitutes human error in these reports is frequently questionable. Although programs to collect data useful for HRA are underway, there is at present no single source of data collected from the measurement of human performance in nuclear power plants. Therefore, most estimates of HEPs must involve extrapolation from other sources. In those cases for which data from operationally similar situations or even derived data are not available, various methods for the use of expert judgment can be applied.

The second source of uncertainty is the modeling of human performance. The state of the art of HRA is such that the modeling of human behavior can qualitatively account for its variability and for discrepancies in response situations; quantifying such models has definite limitations. There are many models of human performance, but they only partially represent the situations they simulate. In some cases, experimental data have provided strong support for the general form of the models, but in other cases the forms are still speculative although based on sound psychological concepts.

The third source of uncertainty, the identification of the PSFs associated with a task, also involves some abstraction and is subject to some interpretation on the part of the analyst. This is probably the biggest source of error in extrapolating data from other sources to the nuclear power plant. Unless the tasks required in both situations are analyzed in sufficient detail, data from other sources may be misapplied to the tasks performed in a nuclear power plant.

The above difficulties will be exacerbated if there is little interaction between the human reliability analyst and other members of the PRA team. Unless the human reliability analyst is a real working member of the team, his identification of relevant PSFs and estimates of the effects of these factors in the HRA may ignore important influences of certain plant-specific factors. His estimates of nominal HEP values may be too low or too high. In such cases, the assignment of large uncertainty bounds will not compensate for his lack of knowledge.

The analysis team itself is the fourth source of uncertainty; that is, the PRA team may include an HRA analyst who is not fully qualified. The less the PRA team knows about the operation and human activities in a given plant, and about the underlying psychology, physiology, and sociology of human behavior in general, the less accurate their estimates of HEPs will be.

Finally, in the prediction of human behavior, there is an uncertainty that results from the inherent variability of human performance due to individual differences, both within and between the people whose performances are being assessed in the HRA. Even if one had a large amount of excellent quality human performance data collected for years on all nuclear power plants tasks, this variability would contribute to the uncertainty in HRA. The amount of uncertainty resulting from intra- and inter-individual differences is judged to be considerably less than that resulting from the combination of all the other sources of uncertainty.

8.5 Data Base

Two types of events identified during accident sequence definition and system modeling must be quantified in order to estimate frequencies of occurrence for accident sequences: (1) initiating events and (2) component failures or primary events. Their quantification for event and fault tree evaluation involves two separate activities. First, the reliability model for each event must be established, and then the parameters of the model must be estimated. This involves data analysis, the use of generic and specific data, and, in some cases, the collection and use of subjective data. The necessary data include component failure rates, repair times, test frequencies, test downtimes, common cause probabilities, and uncertainty characterizations. Also involved is the quantification of human errors. This data is used to estimate the frequencies of the initiating events and the probability of the primary events. The data must be consistent with the general approach chosen and the tools to be used in sequence quantification. The tools or codes used in sequence quantification will also affect the data analysis, in that the data must be in a compatible form.

The development of a data base for accident sequence quantification is a multi-step process involving the collection of data, the analysis of data, and the evaluation of appropriate reliability models. It produces tables that specify the quantity to be used for each event in the fault and event trees. It is most likely to be accomplished largely in parallel with accident sequence development. Time constraints, budget constraints, or study goals will dictate the extent and detail of new, plant-specific data developed. For example, instead of collecting and analyzing raw data, it may be sufficient to use data from a previous PRA study in certain areas, thus saving considerable time and cost.

Early in the PRA project, the analyst should begin gathering all information that may be pertinent to events usually included in PRA studies. At this point, the development of accident sequences will not have been completed, and hence, this early information gathering must rely on previous data. The information should include published data reports, data from other PRA studies, and available information about the specific plant that is being analyzed.

The primary events in the fault and event trees can be analyzed with four types of models: component failure models, test contribution models, maintenance contribution models, and initiating event models. The first three models provide estimates of the probability that a plant element cannot accomplish its design function because it has failed, is being tested, or is being maintained. Component failure models can be divided into two general types: time-related models and demand models. The model for initiating events provides the estimated frequency of the specific event of interest.

Most data used in a PRA these days is generic data or if it is data specific to the Nuclear Steam Supply System vendor, it has been updated as required with specific information from the plant being analyzed. The Reactor Safety Study, of course, had to develop its own data base almost entirely from basic data collected in the course of the study. Since that time, data base development has proceeded apace, and many sources are available. For example, EPRI has recently produced some useful compendia on transient frequencies (NP-2230) and loss of electrical power (NP-2301 and NP-2433). Other often-used sources are the NRC's summaries of Licensee Event Reports, reports of the Nuclear Plant Reliability Data System, and the National Electric Reliability Council. These and other sources are discussed in Chapter 5 of the PRA Procedures Guide.

If the generic data available is insufficient or if plant-specific data is required, additional data will have to be gathered and analyzed in the course of the PRA in order to constitute an acceptable data base.

The objective of the data gathering task is to obtain the raw information needed for estimating the event model parameters:

- Number of failures in time or number of demands for reliability models
- Frequency and duration of tests for systems or components
- Frequency and duration of maintenance on components
- Frequency of initiating events.

Representative existing data sources should be examined to determine the type of data needed before beginning the collection of plant data.

8.5.1 Existing Data Sources

As the data analyst proceeds to determine the appropriate reliability data, he finds a spectrum of available resources. In some cases a clearly appropriate source is available. In other instances, however, few sources of data have content and format that allow unambiguous selection. The parameters of the logic models can be estimated by the classical or the Bayesian method. Reliability and availability models involve a variety of parameters, such as component failure rates and expected repair times. Such parameters must be estimated in order to estimate the probability of specific accident sequences. In a classical analysis, knowledge and expertise generally serve as aids in choosing probability models and relevant data. For example, data obtained under normal operating conditions may or may not be applicable to accident conditions. An understanding of the situation is needed to resolve this question. Once such questions are resolved, a classical analysis produces the required estimates in a straightforward manner. A Bayesian analysis allows for the augmentation of available data by qualified personal opinion or by plant-specific data.

Classical point estimates are single parameter representations of a body of data. The point estimates are well established for the models commonly used in risk analysis, such as the binomial, Poisson, and log-normal distributions. Because the point estimators summarize the data, information is necessarily lost. The loss is serious in the case of point estimation because the amount of data going into the estimates is lost. For example, one failure in 10,000 hours yields the same point estimate of a failure rate as do ten failures in 100,000 hours, but clearly more information is present in the latter case. If this information is ignored or not communicated, an incomplete analysis results. Two classical methods by which the amount of information pertaining to parameters of interest can be conveyed are standard errors and statistical confidence intervals.

Physically caused random variations in a parameter like a failure rate may stem from plant and/or system effects, operational differences, maintenance effects, environmental differences, and the like. This physically caused random variation in the parameter is sometimes referred to as the "population variability". Such random variation can be modeled by classical methods, using compound distributions. However, if the distribution embodies subjective probability notions regarding the analyst's degree of belief about the parameter, the Bayesian method is the appropriate framework for making parameter estimates.

The Bayesian approach is similar to the classical approach in that it yields "best" estimates and estimates of the intervals or range in which the parameter lies. It differs in that the Bayesian approach starts from an old or prior data distribution and uses judgment or additional data to produce a final or posterior distribution. Section 5.5 of the PRA Procedures Guide and the references given therein may be consulted for a more detailed description of the Bayesian technique.

The data base for nuclear power plants is such that there is often a substantial amount of information available about the components in general, but very little about the specific items in the plant in question. Similarly, the plant being analyzed may contain a new piece of equipment which is widely believed to be more reliable than the former models, but for which no experience has been accumulated. The Bayesian approach provides a formal method for combining this large body of general information with more directly applicable but sparse information or with expert opinion.

8.6 Treatment of Uncertainty

The probability or frequency estimates that are obtained by analyzing fault trees or event trees are generally associated with considerable uncertainty. It is important to have a good measure of the accuracy of the quantitative results of a PRA. Therefore, in most PRAs an uncertainty analysis is performed.

Uncertainty comes about primarily because the models used are incorrect, the analysis is incomplete, or the input data is inexactly known. Basic assumptions about the accident sequences, system interactions, failure modes, etc., may be incorrect or certain interactions may have not been found. Perhaps the scope of the study precluded the inclusion of certain types of events. The data base available has known limitations.

In theory it may be possible to quantify the contribution to total uncertainty made by each of these sources, but in practice it is very difficult to develop credible quantitative measures for all the sources of uncertainty in the analysis. It is usually more practical to perform additional analyses to ensure that the modeling is correct than to try estimating a particular quantitative uncertainty.

In addition, there are sources of uncertainty that are directly related to the sequence quantification. Truncation schemes that eliminate accident sequences and the elimination of cut sets that are determined to be insignificant produce non-conservative errors. Another source of error in quantification is the rare-event approximation used to develop a probability expression for the accident sequences; it produces conservative errors. Accident-sequence quantification provides the opportunity for assessing the effect of these as well as uncertainties in the input data on the calculated frequencies of accident sequences.

The uncertainty introduced through Boolean manipulations, truncations, and screenings should be small in comparison with that in the accident-sequence logic models and the data base. However, significant uncertainty can be introduced through the elimination of large numbers of low-frequency cut sets or accident sequences whose sum contributes significantly to the PDB frequency. In order to quantify this contribution, the cut sets must be generated and quantified. Unfortunately, most truncation schemes used in fault tree analysis have no capability for estimating this contribution.

One way to estimate the total contribution of many low frequency events is to use a direct quantification code (e.g., WAM-BAM), which is very efficient and can use a low truncation value because it does not have to perform cut set manipulations. Some of

these codes have the capability to estimate an upper bound on the sum total of the truncated terms.

When trying to evaluate the contribution to system-failure probability from variations in input parameters, the analyst can either perform a probabilistic importance analysis to get a qualitative feel for the effect of input parameters on the results or derive probability distributions or interval estimates for the result.

Probabilistic importance measures are a means of estimating the contribution of a primary event to the accident sequence frequency. The two most commonly used are the Barlow-Proshan and the Fussell-Vesely measures, which compute the probability that a primary event is contributing to the failure of a system. They therefore provide information on which primary events, if made more failure resistant through improved quality or redundancy, will most decrease the probability of a system failure.

A consideration in the propagation of primary event uncertainty through a top event probability expression is the method of treating the uncertainty distribution or interval estimates of two primary event probabilities derived from components assumed to be identical. Their uncertainty parameters are considered to be correlated. In evaluating the probability expression, only one distribution should be used to represent uncertainty for every primary event whose probability is derived from components assumed to be identical. Consider, for example, the probability expression:

$$\begin{aligned} P(\text{top}) = & P(\text{pump A}) * P(\text{pump B}) \\ & + P(\text{pump A}) * P(\text{control B}) \\ & + P(\text{pump B}) * P(\text{control A}) \\ & + P(\text{control B}) * P(\text{control A}) \end{aligned}$$

If pumps A and B along with controls A and B are assumed to have identical failure rates, the probability expression should be changed to the form

$$P(\text{top}) = P(\text{pump})^2 + 2 P(\text{pump}) P(\text{control}) + P(\text{control})^2$$

In this way the assumption that the primary events are identical can be correctly evaluated. With independent primary events and distributions, the sums or products of the means of the distributions for the individual primary events will yield the correct mean for the top event. In practice, the propagation of uncertainty in primary event probability may be very difficult to perform by methods other than Monte Carlo for large numbers of independent modules containing similar components.

8.7 Computer Codes

A great many codes or code packages are available to assist in both qualitative and quantitative evaluation of system or plant logic models. Tables 8-1 and 8-2 list some of these codes, primarily those which are not proprietary and possess adequate documentation. Each was developed for a specific purpose, so it is difficult to recommend any of them for general use. GO, for example, requires the use of specific GO logic models. SETS and the WAM series have received widespread use and have general applicability. Further information about computer codes may be found in Section 6.6 of the Procedures Guide or The Fault Tree Handbook.

8.3 Summary

The qualitative evaluation of the event tree and fault tree system models is the means by which numerical frequencies are obtained for selected accident sequences. The quantification element of a PRA also deals with the issue of uncertainty.

Depending on the selected level of the PRA, quantification may or may not be the final study task. A Level 1 PRA is essentially complete following quantification of the system models. Level 2 and 3 PRAs use the quantification results in subsequent analytical tasks.

Although there are a number of quantification tools and approaches available, they all yield substantially equivalent results when properly applied.

TABLE 8-1
COMPUTER CODES FOR QUANTITATIVE ANALYSIS

<u>Code</u>	<u>Comments and Relative Utility</u>
ARMM (1965)	First direct evaluation code, models a reliability block diagram using a success path approach.
SAFTE (1968)	Computes probability of system failure using either direct or importance sampling techniques.
GO (1978)	Models system without fault tree process; different approach to system evaluation; different logic process.
KITT 1 (1969) KITT 2 (1970)	Evaluates time-dependent availability, reliability, and expected number of failures from component failure rates and repair times; can be expensive to run on large fault trees; KITT 2 is an update of KITT 1; not as efficient as other codes available.
ALMONA (1977)	Both qualitative and quantitative; success or failure notation uses logical networks; finds and evaluates minimal cut sets for time-dependent unavailability, including complex testing and failure and repair models.
RELY4 (1972)	Uses Monte Carlo importance sampling to determine minimal cut sets.
PATREC (1974)	Uses a pattern-recognition algorithm to evaluate fault trees directly; can evaluate time-dependent system unavailability; limited to machines with PL/I programming language.
WAM-BAM (1976)	Code package using concepts from GO and fault tree analysis; generates input to SPASM; may be difficult to convert to new computer system (from CDC 6600).
FAUNET (1977)	For use on minicomputer; uses top-down pruning and bottom-up modularization.
PL-MOD (1977)	Performs both qualitative and quantitative analysis; has Monte Carlo option for use in uncertainty analysis; limited to machines with PL/I programming language.
FRANTIC (1977) FRANTIC (1981)	Evaluates time-dependent and average unavailability; NRC code to be used in optimizing surveillance testing; FRANTIC II extends analysis over total in-service life of components and system.

SOURCE: PRA Procedures Guide, NUREG/CR-2300.

TABLE 8-1 (cont'd.)

<u>Code</u>	<u>Comments and Relative Utility</u>
IMPORTANCE (1977)	Calculates various measures of component importance and other quantitative information.
SUPERPOCUS (1977)	Similar to KITT using boundary approximation on methods.
RAS (1977)	Code package to evaluate all phases of fault tree evaluation; some of the individual codes are efficient; all codes have not been used extensively.
EXCON (1978)	Determines risk through cause-consequence diagrams.
PREP (1970)	Simple to use; output straightforward; for analysis of large fault trees, output is lengthy and difficult to evaluate.
ELRAFT (1971)	Uses unique factorization property of natural numbers; capable of finding minimal cut sets of up to six basic events; not recommended for large trees.
MOCUS (1972)	Update of PREP; uses top-down Boolean substitution method; user may place upper limit on cut set length.
TREEL and MISCUP (1975)	MISCUP uses bottom-up algorithm using Boolean substitution; TREEL is a preprocessor.
ALLCUTS (1975)	Similar to MOCUS.
SETS (1977)	Uses Boolean manipulation to determine prime implicants, allows tree reduction on both cut set order and cut set probability.
MFAULT (1977)	Uses bottom-up algorithm and calculates approximate values of top event probabilities.
FAULTRAN (1977)	Tree reduction based on binary coding of events and bit manipulation.
FATRAM (1978)	Similar to MOCUS with refinements for efficiency.
FTAP (1978)	Determines prime implicants; offers considerable flexibility over processing and output.
WAM-CUT (1978)	Uses a Boolean manipulation and minimization algorithm.
PRANK (1978)	Modification of PREP/KITT.

SOURCE: PRA Procedures Guide, NUREG/CR-2300.

TABLE 8-2
COMPUTER CODES FOR DEPENDENT FAILURE ANALYSIS

<u>Code</u>	<u>Comments and Relative Utility</u>
COMCAN (1976)	Determines possible dependent failure candidates; difficult to use; results not comprehensive.
COMCAN II (1978)	Uses reduced fault tree approach to determine minimal cut sets with failure potential due to common causes.
BACFIRE (1977)	Similar to COMCAN.
SETS (1977)	Similar to results to COMCAN and BACFIRE.

SOURCE: PRA Procedures Guide, NUREG/CR-2300.

TOPIC 9
COMMON CAUSE FAILURES

9. COMMON CAUSE FAILURES

Dependent failures are extremely important in risk quantification and must be given appropriate treatment to avoid gross underestimation of risk. Risk estimates can err by orders of magnitude if the possibilities for common cause failures and system interactions are overlooked. Dependent failures must be taken into account in several PRA tasks. More detail is available in Section 3.7 of the Procedures Guide, from which much of this material is drawn.

In risk analysis, the treatment of dependencies in the identification and quantification of accident sequences is called "dependent-failure analysis." Dependencies tend to increase the frequency of multiple, concurrent failures. Since most important accident sequences for nuclear reactor systems involve the hypothesized failure of multiple components, systems, and containment barriers, dependent failure analysis is extremely important. The failure events A and B are said to be dependent if the frequency of concurrent failure events A and B cannot be expressed simply as the product of the unconditional failure event frequencies.

9.1 Definition of Dependencies

Several types of dependencies must be defined for clarity. Common mode failures are multiple, concurrent, and dependent failures of identical equipment that fails in the same mode. An example of a common mode failure is when a loss of electrical power causes a number of identical valves to fail in the closed position. This is also a common cause failure, but since they all fail closed, their failure mode is common also. Propagating 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. As an example of a propagating failure, consider the case where a bearing overheats on a service water pump, which causes the pump to seize, which stops service water to a recirculation pump room cooler which in turn causes the recirculation pump to trip on high temperature. Common cause failures are failures of multiple equipment items occurring from some single cause that is common to all of them. If, in an earthquake, a wall fell on a low pressure emergency core coolant injection (ECCI) pump and a high pressure ECCI pump, they would have been disabled by a common cause. 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, which has resulted in much confusion. The terms "dependent-failure" or "systems interaction" are often used to describe all multiple, concurrent, and dependent failures.

The following simplified classification scheme for dependent failures is taken from Section 3.7.2 of the Procedures Guide.

Type 1 - Common cause initiating events (external events) are external and internal events that have the potential for initiating a plant transient and that 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 dependencies are events or failure causes that create interdependencies among the probabilities of failure for multiple systems. Stated another way, intersystem dependencies 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. Several subtypes are of interest in risk analysis.

Type 2A - Functional dependencies are dependencies 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 dependencies are dependencies 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 are 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 dependencies are dependencies 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 of this nature happened during the Three Mile Island accident when an operator turned off the emergency core cooling system.

Type 3 - Intercomponent dependencies are 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.

Dependent failures must be taken into account in the selection of the initiating events, including external events, the definition of accident sequences (event tree construction), system modeling (fault tree construction), and quantification. The analysis of dependent failures is therefore performed using a combination of separate methods.

9.2 Analysis of Dependencies

The available methods for dependent failure analysis can be categorized as either explicit, parametric, or computer aided. Explicit methods involve the quantification of specific causes of dependent failures in the event tree and fault tree logic. Included in this category are the event-specific models which treat event frequencies and impacts (fragilities) in terms uniquely appropriate to each event. Examples are earthquakes, fires, and floods.

The second category of methods, termed parametric, includes the models known as the beta-factor and the binomial failure rate. 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.

Computer aided techniques for dependent failure analysis comprise the third category of method, which includes the codes SETS, WAMCOM, BACFIRE, COMCAN and GO. 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, can also be used to analyze intersystem dependencies in the construction and quantification of event trees.

The dependencies associated with common cause initiating events are usually handled with event-specific models, and with the methods of event tree and fault tree analysis. Intersystem functional dependencies are normally identified in the construction of event trees. Shared equipment dependencies can be treated with a combination of event tree and fault tree methods. Physical interactions resulting in multiple failures are treated with event-specific models and are identified in event trees and cause tables. All the methods except event tree analysis are useful in the analysis of intercomponent dependencies. The parametric methods were developed and have been applied especially for the subset of intercomponent dependencies known as common cause failures.

Dependent failures due to common cause initiating events will be discussed in the next section and are covered in Chapter 10 of the Procedures Guide. The treatment of intersystem dependencies in the event trees is presented in Section 3.7.3.3 of the Procedures Guide.

An alternative to treating intersystem dependencies in the event tree is to link the system fault trees together to create a single large fault tree for the entire accident sequence. This tree would be synthesized from the respective system fault trees by linking them together with an AND gate. During the Boolean reduction of the fault tree, the shared equipment dependencies as well as the effect of success states are properly taken into account. It can be shown that the methods of fault tree linking and event trees with boundary conditions give equally correct results if each is implemented correctly. One drawback to expressing the intersystem dependencies in the event tree is that they must be fully known by the person constructing the event tree. A weak point in analyzing these dependencies by linking the fault trees is that the resultant tree may be so large that manipulation and reduction of the tree may be impossible or extremely costly.

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.

An alternative approach, 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. 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.

When rigorously followed, both fault tree linking and event trees with boundary conditions correctly model the shared equipment dependencies and both entail comparable levels of data processing. There is a trade-off between the level of detail in the event trees and that in the fault trees. In the method of fault tree linking, the event trees can be kept rather small, on the order of those used in the Reactor Safety Study, 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. Some ways to do this are discussed in Section 3.7.3.3 of the Procedures Guide.

Once the intersystem dependencies are accounted for, the plant logic has been developed to a level of detail corresponding to the basic component failure modes. Before the quantification of the event and fault trees can be completed, the possibilities for dependencies among the basic component failures must be analyzed. A common cause failure is the occurrence of multiple component failures induced by a single, shared cause.

The significance of common cause failures, should they exist, is that they could greatly increase the probability of system unavailability over what it would be if the component failures were independent. These common causes show up as dependencies in that the conditional component unavailabilities are different from, and often significantly greater than, the respective unconditional unavailabilities; in other words, $P(B/A) > P(B)$. It is well known 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 sensitivity of reliability predictions to the assumption that component failures are independent is 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 the error resulting from the assumption of independence certainly be 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 induced by human actions. Design errors and other human acts during manufacture, installation, operation, and maintenance are among the chief causes of multiple as well as single component failures. A substantial number of human errors and shortcomings affect the entire system, or at least multiple components, as opposed to individual components. 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.

The limitations and uncertainties associated with attempts to analyze common cause failures can be largely attributed to a lack 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 common 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, the currently available data sources are quite limited for common cause analysis.

Three approaches may be used to analyze and quantify 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 common cause failure experience data.

To model common cause failures directly in a system fault tree or as specific entries in a cause table, the experience data is applied at the finest level of detail. Specific details of the system failure modes are compared with the common cause failures experienced in similar systems to determine their applicability. Judgment must be exercised 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, 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 dependencies 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 common cause failure 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. Computer-aided procedures are useful in carrying out such systematic searches for common cause failures. 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 most important common cause failure events were accounted for. It is extremely difficult to establish that any redundant system is not susceptible to common cause failures.

The beta-factor method can be used to model dependencies 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 and human interactions.

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

$$\lambda = \lambda_i + \lambda_c \quad (\text{Equation 9-1})$$

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

For convenience, a parameter, β , is defined as the fraction of the total failure rate attributable to dependent failures, $\beta = \lambda_c / \lambda$ so that $\lambda_c = \beta\lambda$ where $0 \leq \beta \leq 1$.

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. Markov models can be used in conjunction with the above definitions to develop expressions for the unavailability and reliability of repairable systems.

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, it may be necessary to consider dependent failures of two or three units out of a total system of n units. Note that, in general, the beta-factor for the failure to continue running (β) is not necessarily equal to the beta-factor for the failure to start on demand (β_d).

The strength of the beta-factor 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.

The beta-factor method can also be used at the component level, rather than at the system or train level. 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, less failure data is available 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 a single dependence between trains, the analyst must consider dependencies between the valves, the pumps, and the strainers, as well as cross-component dependencies 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 binomial failure rate model is somewhat more involved than the beta-factor method and is not treated here in this overview course. Explanations may be found in Section 3.7.3.7 of the Procedures Guide and the literature cited therein.

Both the beta-factor method and the binomial failure rate model 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 estimates one extra parameter, β , while the binomial failure rate method estimates two extra parameters, μ and p . 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 binomial failure rate model with the parameter p set equal to 1. The beta-factor method is 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 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 binomial failure rate method, this may be a real difficulty. With either method, complex reality is being modeled with fairly simple methods. The amount of data available should be considered when choosing a method. When only a little data is available, only simple methods can be justified.

Automated search procedures have been developed to search large logic models for common cause failures, which are usually the most likely type of dependent failures. These computer codes are designed to identify these failures qualitatively and make no attempt to quantify the system failure probability. Section 3.7.3.9 of the Procedures Guide discusses some specific computer codes.

9.3 Summary

In summary, there is at least one method for each type of dependent failure. The Procedures Guide presents a recommended procedure for dependent failure analysis in a plant-specific risk analysis (see Section 3.7.4). This 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. Risk analysis in general and dependent failure analysis in particular are rapidly evolving in both methods and practical application and improvements in dependent failure analysis are both necessary and inevitable.

TOPIC 10
EXTERNAL EVENTS

10. EXTERNAL EVENTS

10.1 Introduction and Overview

External events are included in a complete PRA because they can initiate a core melt. The term "external events" is something of a misnomer because the loss of offsite power is not considered an external event. The distinction between internal events like LOCAs, failure to scram, and stuck open relief valves, and external events is somewhat arbitrary. The term external events has come to mean all those initiators which were excluded from the Reactor Safety Study (RSS, WASH-1400). Generally they are external to the normal operating systems and to the safety systems. Some external events such as fires in the wiring and floods due to a ruptured service water pipe occur inside the plant. Others such as earthquakes and tornadoes are truly external to the plant. These initiators introduce complications in that they often negate the mitigation measures or cause additional failures. For example, severe offsite flooding or an earthquake could make evacuation of the nearby populace impossible. These multiple effects call for special handling for these initiators.

Table 10-1 lists some possible external events. It is obvious that some of these, such as avalanche, hurricane, and landslide, can only be treated on a site-specific basis. Others, such as aircraft impact, can be considered more generically. Note that war and sabotage are specifically excluded. It is generally felt that these initiators are impossible to address in a probabilistic manner consistent with the treatment of the other initiators.

Some of the terms in Table 10-1 for types of external flooding may not be familiar to the reader. A seiche is a resonant oscillation in a body of water, usually set off by an unusual meteorological event. Substantial damage from seiches is rather rare. A storm surge is an exceptionally high sea level caused by atmospheric pressure differences, high winds, and the tide. Extreme pressure differences and high winds often accompany large-scale storms such as typhoons or hurricanes. The storm surge, however, can occur hundreds of miles from the area of peak winds. In Bangladesh (then East Pakistan) in 1970, a surge associated with a cyclonic disturbance was 12 feet above normal high tide and flooded a huge low-lying area on the shore of the Bay of Bengal, killing 300,000 people. Hurricane Camille in 1969 caused a surge on the Gulf Coast that raised the water 20 feet above normal high tide, killing 200 people and causing \$500,000,000 in damage. A tsunami is a solitary sea wave caused by an earthquake. The earthquake may be underwater so that no damage on land is observable. Tsunamis are often called tidal waves, but this is misleading since no tidal forces are involved.

Even when a certain external event is possible at a site, the analyst may be able to eliminate it from further consideration by doing a simple, conservative bounding calculation. For example, consider aircraft impact: if the site being considered is not near a major airport, some simple calculations along the lines of those outlined in SRP 3.5.16 using appropriate data from NUREG-0533 often suffices to show that severe accidents due to aircraft impact are so infrequent that no further consideration is warranted. Other transportation accidents, occurrences on nearby industrial sites and military bases, and pipeline ruptures can often be treated in a similar fashion. Section 10.3.1 of the Procedures Guide discusses this in more detail. As is pointed out there, the external hazard is usually dismissed if the maximum possible event is less severe than that for which the plant was designed.

Since the plant is designed to resist all normal levels of external hazards, only the most extreme events must be considered. For example, because the design basis and safe

TABLE 10-1
POSSIBLE EXTERNAL EVENTS

<u>Event</u>	<u>Usual Cause for Exclusion</u>
Aircraft	----
Avalanche	Physically impossible for most sites
Earthquake	----
Fire in Plant	----
Fire Outside Plant but on site	----
Fire Offsite	No means to propagate to plant
Flammable Fluid Release	Considered under fire (onsite) <u>or</u> pipeline accident (offsite)
Fog	Included in aircraft or ship impact
Flooding, External (including seiche, storm surge dam failure, and Tsunami)	----
Flooding, Internal	----
High Winds (including tornadoes)	----
Hurricane	Wind damage covered under high winds; water damage covered under flooding, external
Ice	Ice formation on aircraft covered under aircraft impact; ice formation on transmission lines covered under loss of offsite power; ice blockage of river or lake covered in plant design - loss of cooling
Industrial or Military Accident Offsite	----
Landslide	Physically impossible for most sites
Lightning	Included in plant design
Meteorite Impact	Frequency less than earthquake or tornado
Pipeline Accident	---
Sabotage	Outside Scope - Impossible to assess
Ship Impact	Impossible to damage more than water intake
Toxic Gas Release	----
Transportation Accident	----
Turbine Missile	----
Volcanic Activity	Geologic setting of most sites makes this extremely remote
War	Outside scope - Impossible to assess

shutdown earthquakes are taken into account in the structural and piping design, the rare seismic events that are larger than these earthquakes are generally included in a PRA. Thus, the assumption is that the failure probability at levels below the design level is negligible. This may not be the case, but considering the safety margins designed into the plant, it is not an unreasonable assumption.

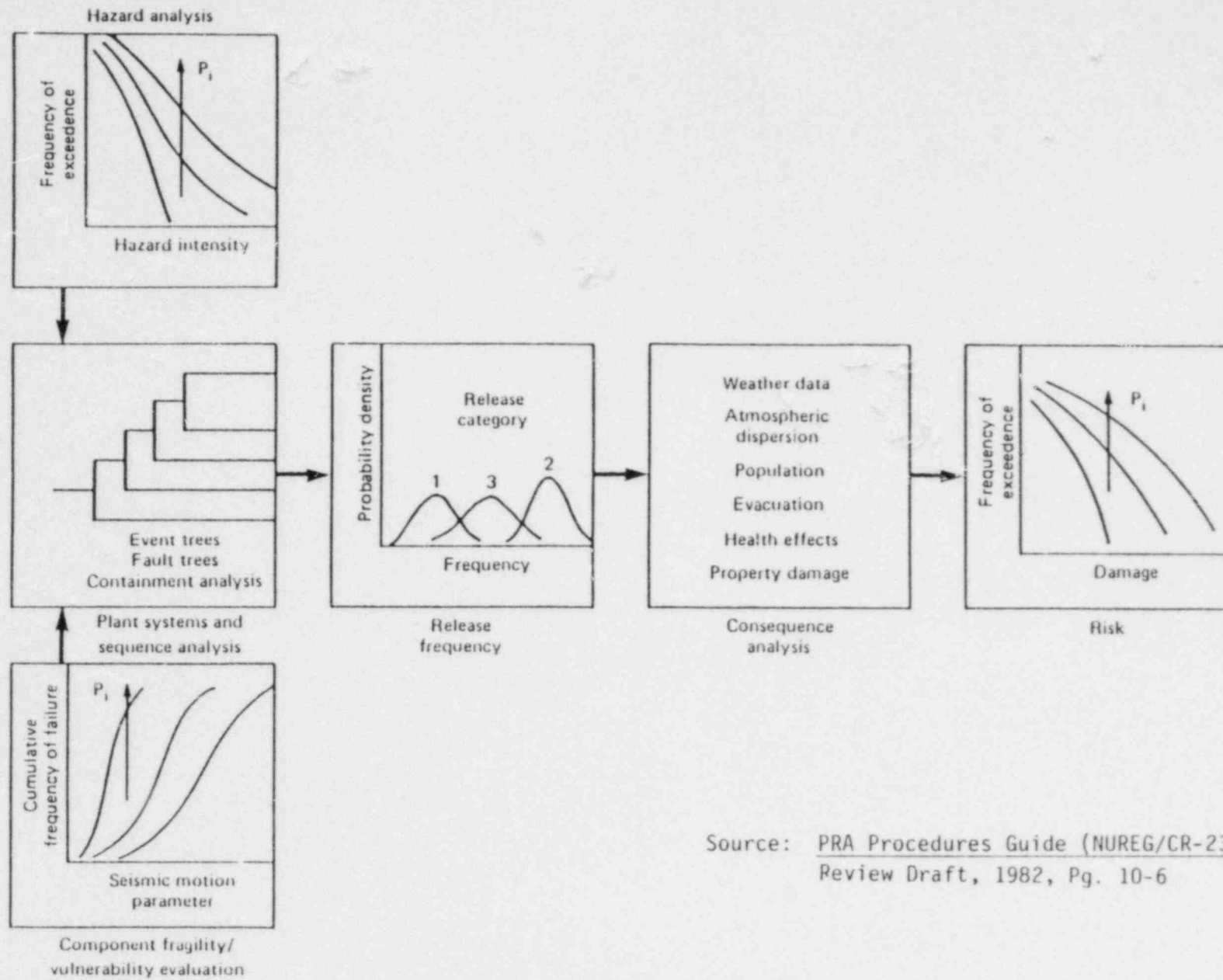
Another assumption is that of complete failure at the specified hazard level. That is, it is assumed that the component, system, or structure functions as designed up to the failure level of the hazard. For initiators that exceed the failure level, the system fails completely. For some systems or components, it would be more realistic to consider partially degraded performance at one level, more degraded performance at another level and so on. This introduces significant complications into the PRA process and so has not been attempted.

The analysis of external events is similar to that for internal events as shown in Figure 10-1. Data regarding the magnitude and frequency of the external event is input to the system modeling activity. The system models are then manipulated to obtain release frequencies. Finally, following consequence analysis, a measure of risk obtained. Take the case where the rupture of a certain pipe causes a core melt accident. For the internal event analysis all that is required is to look up the frequency with which pipes of that size rupture due to normal operations, vibratory and static loads, etc. For the rupture of the same pipe due to an earthquake, first the frequency of earthquakes of various intensities in the vicinity of the plant must be estimated, then the attenuation from the possible sites computed to get the ground acceleration at the plant, and then a structural analysis must be done to determine the stresses placed on the pipe by the earthquake, taking the response of the building and the equipment connected to the pipe into account. After all this considerations, an estimate of the pipe failure frequency due to earthquakes may be obtained.

The estimation of the earthquake frequency and the location and attenuation in the above example is called the hazard analysis. The hazard analysis determines the magnitude and frequency of the initiating event. Figure 10-2 shows the results of a hazard analysis for high winds as an example. (Note that P in this figure is the NON-exceedance probability.) The response of the plant, its structures and systems, to the hazard is denoted the fragility analysis. In this step, the effect of the hazard is evaluated. As an example, the results of a fragility analysis for high winds are shown in Figure 10-3. (Once again, P is the NON-exceedance probability.)

The external events analysis is usually started somewhat later than the analysis of the internal events so that a basic knowledge of the plant systems and their interaction is available when it is time to perform the fragility analyses. Much time and effort can be saved by knowing which systems are crucial to plant safety so that fragility analyses for the less important systems can be avoided.

Figure 10-4 illustrates that the external events analysis can be integrated into the analysis of internal events at several places in the course of the complete PRA. If the external event results are integrated right away, before the systems and sequence analysis, time and money are saved and a consistent treatment of all initiating events is assured. The results of the PRA will show the total risk. However, the risk due to external events may not be identifiable separately later on, and unless the external events are dominant, they may not receive a thorough treatment due to their low frequency, even though concomitant events may cause the externally initiated accidents to have very large consequences.



Source: PRA Procedures Guide (NUREG/CR-2300),
Review Draft, 1982, Pg. 10-6

FIGURE 10-1

RISK-ASSESSMENT METHODOLOGY FOR EXTERNAL EVENTS

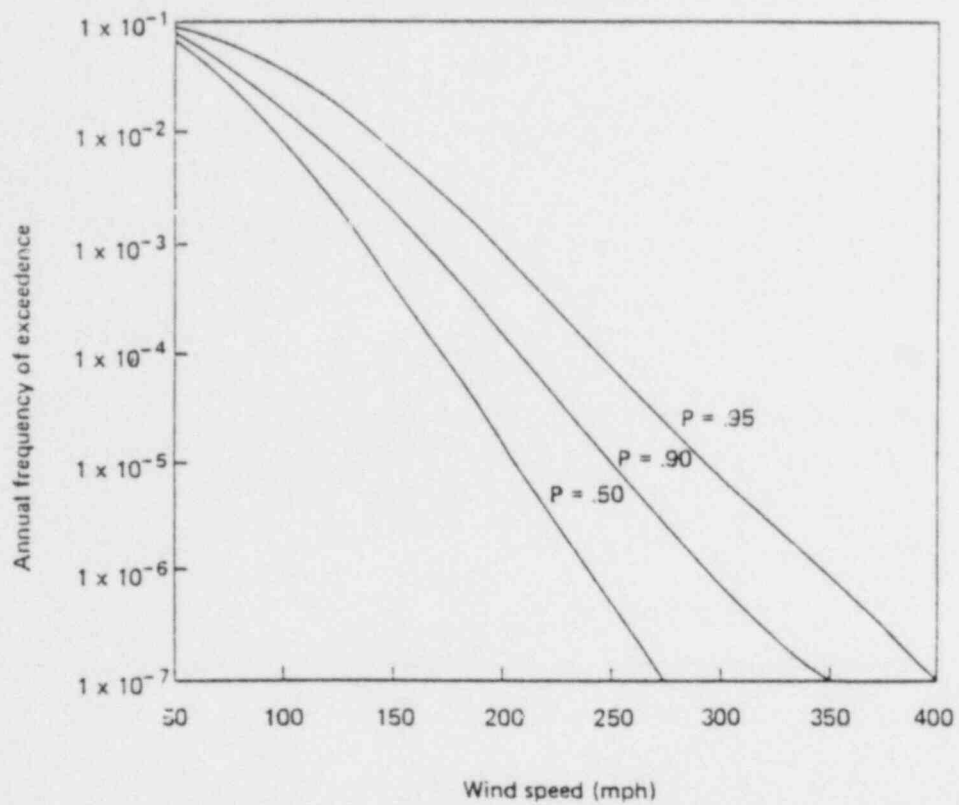


FIGURE 10-2
FAMILY OF HAZARD CURVES

Source: PRA Procedures Guide (NUREG/CR-2300),
Review Draft. 1982, Pg. 10-11

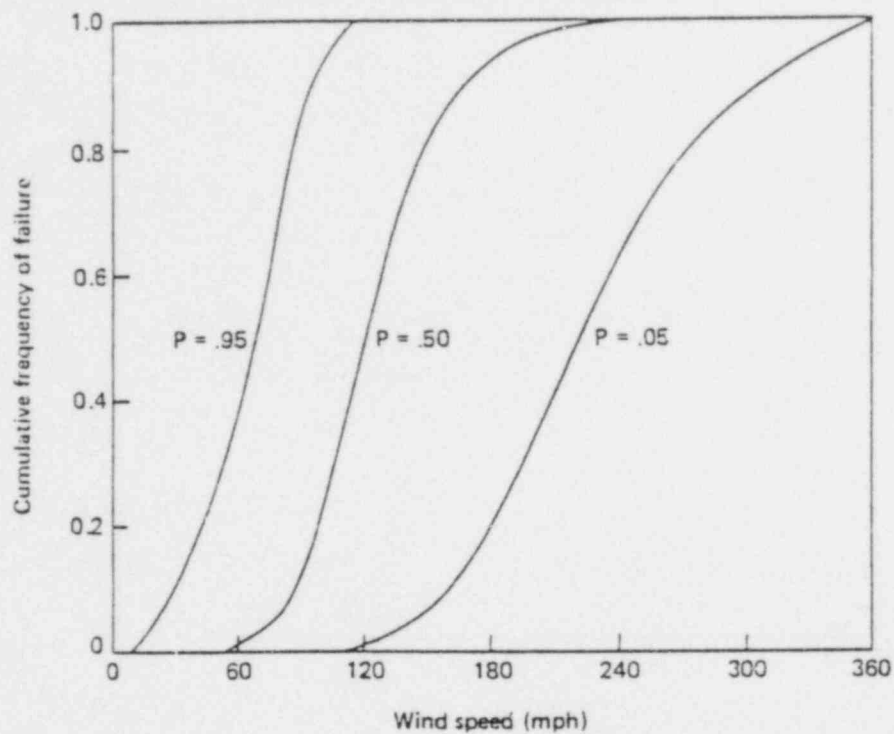


FIGURE 10-3
FRAGILITY CURVES FOR WIND LOADING

Source: PRA Procedures Guide (NUREG/CR-2300),
Review Draft. 1982, Pg. 10-14

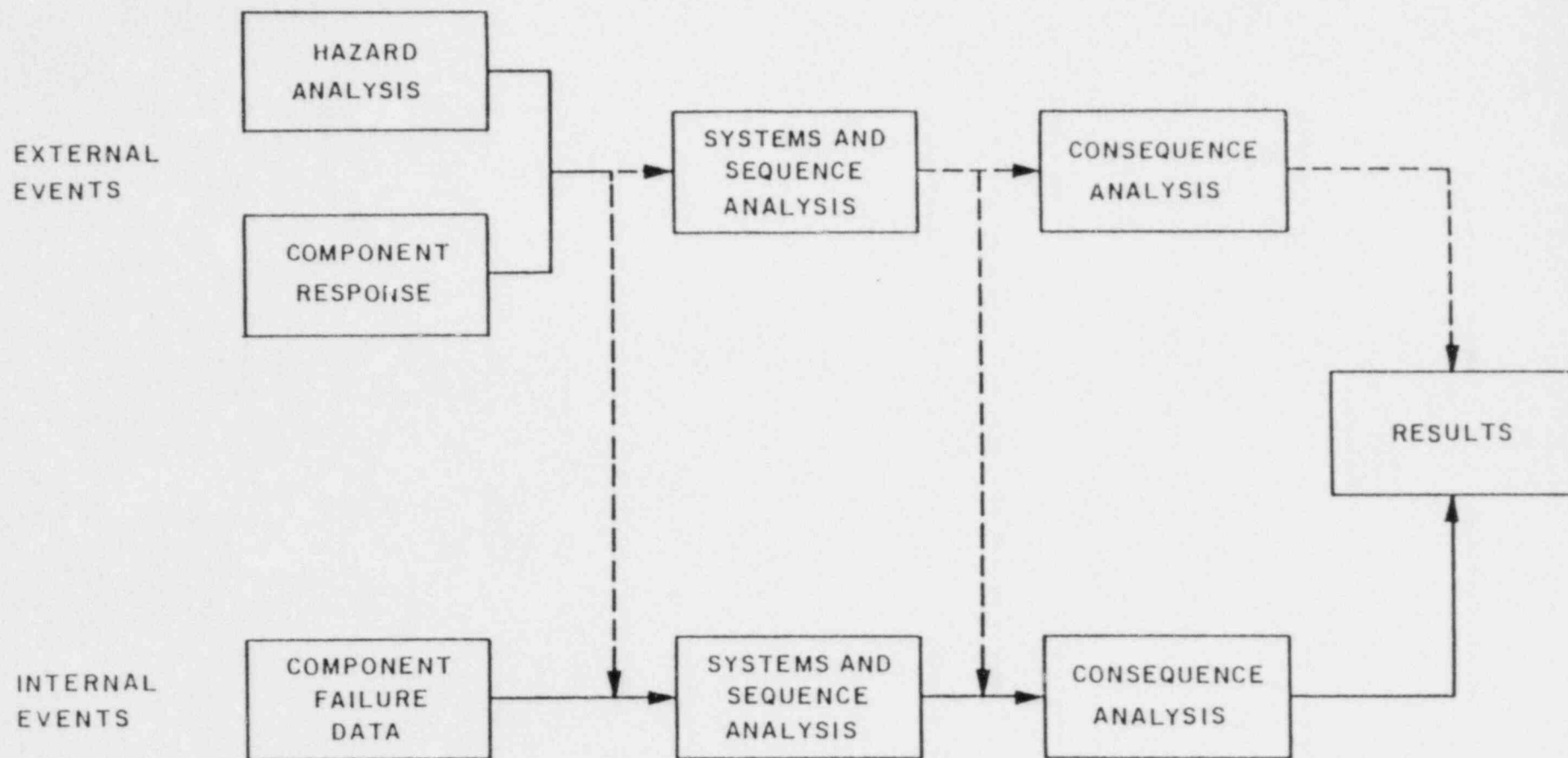


FIGURE 10-4
COMBINATION OF RISK FROM EXTERNAL EVENTS WITH THE
RISK FROM INTERNAL EVENTS

Another means of incorporating external event analysis into the PRA process is to treat these events separately through the system and sequence analysis and combine the results of these activities prior to the consequence analysis. Although this approach may be more costly and time consuming than integrating the external events prior to the system analysis, it can provide enhanced visibility in terms of the identification of core damage and release category frequencies for each external event.

10.2 Earthquakes

An earthquake or seismic event occurs when two portions of the earth's crust move a short distance relative to each other. While infrequent, especially in the eastern two-thirds of the country, the amount of energy released in a large earthquake is immense. If such a seismic event occurs in an area where few structures are designed to modern standards for a high seismic risk zone and in which the population density is high, the devastation is overwhelming. While movement on a fault is the usual cause of earthquakes, large volcanic eruptions also cause earthquakes.

10.2.1 General Discussion

Earthquakes occur when stresses in the earth's crust accumulate to the point where they can no longer be resisted and movement takes place. This movement is almost always along a plane on which movement has occurred before. These planes are called faults. This sudden release of stored strain energy causes longitudinal and transverse vibratory waves to propagate away from the source. Figure 10-5 illustrates this and defines the focus and epicenter of the quake. The types of movement along a fault are defined in Figure 10-6. Most of the earthquakes in the world are related to the movements of large rigid blocks of the crust relative to each other. The boundaries of these blocks are known; indeed, they were first defined by plotting the frequencies of earthquakes, so the distribution of earthquakes is far from being random.

The fault on which the seismic motion occurs may not be visible at the surface. Even if it is, there is often little or no evidence of movement along the fault at the surface. When there is this type of evidence at the surface, it is often dramatic.

Active faults are not randomly distributed around the surface of the earth, but tend to be grouped in fault zones. Mapping these zones showed that they divided the earth's surface into about a dozen or more large stable areas or plates. In the center of these plates, seismic events are rare. It was later determined that these plates are in motion, albeit very slow motion in human terms, with respect to one another.

Figure 10-7 shows the location of the San Andreas fault zone. Although there is a San Andreas fault per se, the fault zone consists of hundreds of separate identifiable faults, all involved to one extent or another in the motion of the two plates. The zone marks the boundary between the North American and Pacific plates. The southwestern part of California is moving northwest with respect to the rest of North America at an average rate of about 1 cm per year. This is not rapid in the human time frame but is very significant in the geologic time scale.

When the two sides of a fault move relative to one another, an earthquake or seism occurs. Thousands of quakes, all too small to be felt, occur in this country every year. These small seisms, as well as the large ones that can be felt, can be measured by instruments called seismographs. A seismograph essentially consists of a large mass suspended so that it remains motionless when the ground shakes. The rest of the instrument measures and records the relative motion of the ground and the suspended

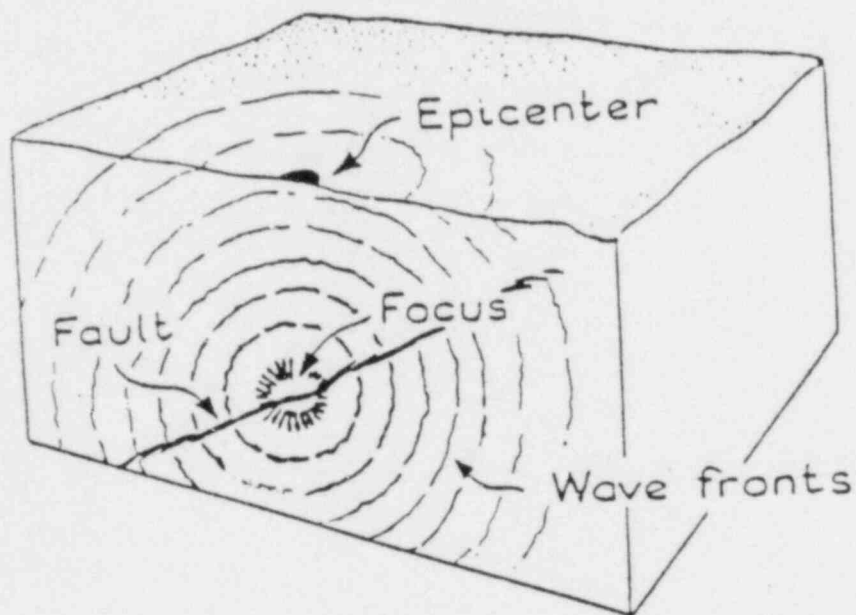


FIGURE 10-5

THE FOCUS AND EPICENTER OF AN EARTHQUAKE

SOURCE: Gilluly, J. et al. Principles of Geology San Francisco: W. H. Freeman, 1951. Pg. 485. Used with permission.

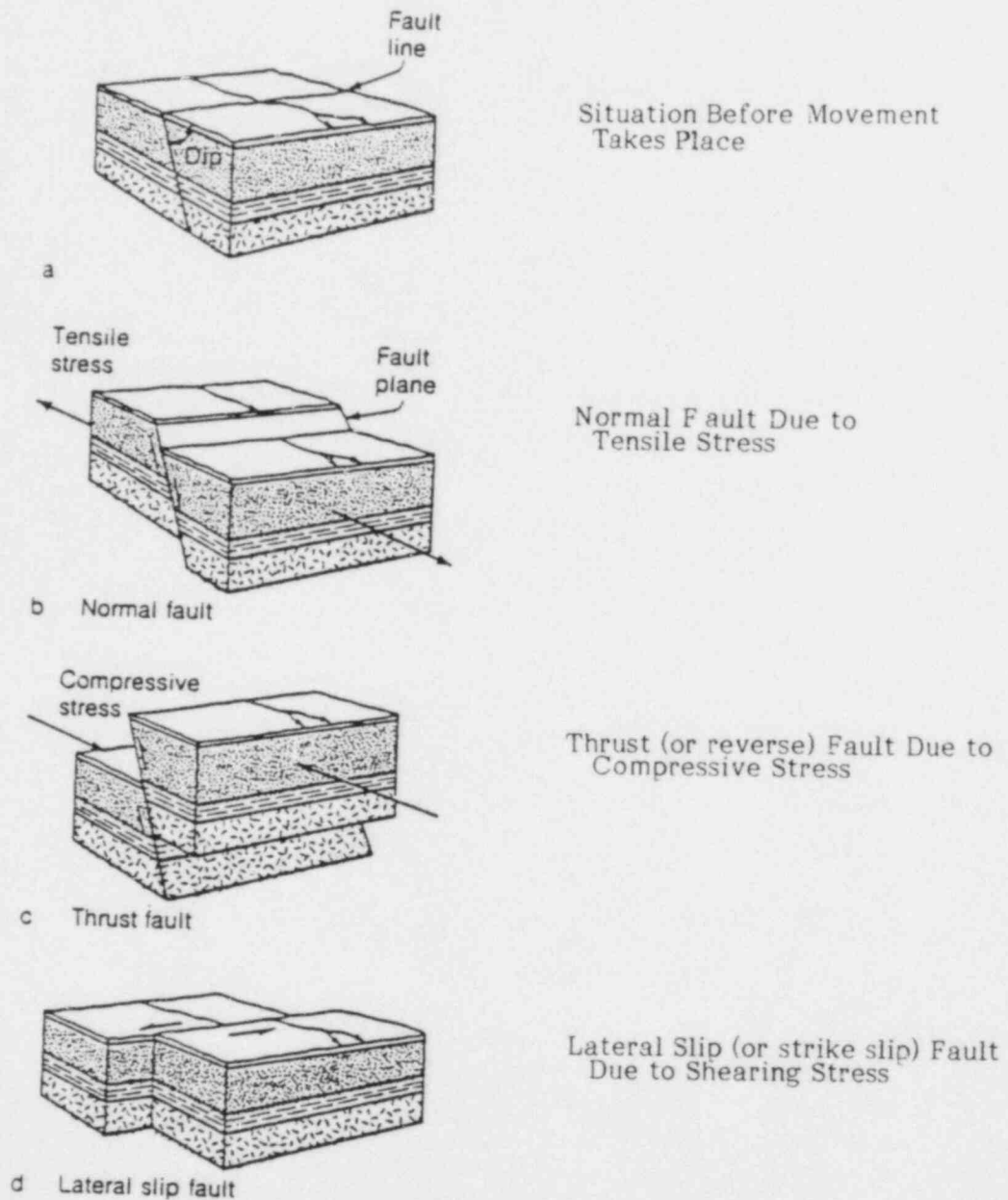


FIGURE 10-6
SUMMARY OF TYPES OF FAULT MOVEMENT

SOURCE: Press, F. and Siever, R. Earth. San Francisco: W.H. Freeman, 1974. Pg. 415. Used with permission.

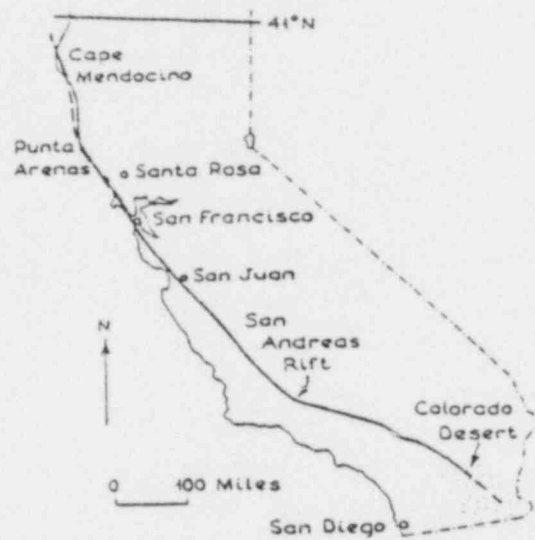


FIGURE 10-7

THE SAN ANDREAS FAULT ZONE, CALIFORNIA

SOURCE: Gilluly, J. et al. Principles of Geology. San Francisco: W.H. Freeman, 1951. Pg. 473. Used with permission.

mass. Another similar instrument, the accelerograph, measures relative acceleration instead of relative displacement.

Figure 10-8 shows the accelerations of the Parkfield seism of 1966. This earthquake was rather brief, but did have a fairly large peak acceleration. The velocity and ground displacement, obtained by integrating this record, demonstrate that although the peak acceleration was large, the net ground displacement was quite small. In spite of the relatively high accelerations in the Parkfield earthquake (Richter magnitude = 5.5), destruction was limited due to its very short duration. Quakes such as the El Centro, California earthquake of 1940 and the Alaska event of 1964 caused much more damage because they lasted so much longer even though their peak accelerations were lower.

The map in Figure 10-9 shows the seismic hazard for the 48 contiguous states. The hazards are highest on the west coast and in certain areas of the Rocky Mountains, as most people would expect from common knowledge. The areas of elevated seismic hazard east of the Rockies are based on a few large earthquakes that have occurred at those locations in the 350 years for which we have records. While hundreds of active faults and fault zones are known in the west, only around New Madrid, Missouri have active faults been identified in the east and midwest. Many old faults have been identified east of the Rockies, but seismic motion in this region generally takes place on faults that cannot be located at the surface.

The strength of earthquakes are measured in two ways: the Modified Mercalli (MM) scale shown in Table 10-2 and the Richter scale shown in Table 10-3. The Mercalli scale is a measure of perceived intensity; that is, of seismic strength as observed by humans from its effects. The MM intensity is not directly related to the amount of energy released since local effects with no dependence upon the amount of energy released may largely determine the amount of damage. The MM scale is the only one that can be used for earthquakes that occurred before the modern seismograph was invented. Since so few earthquakes occur east of the Rockies, seismic events in this region are usually considered using the MM scale. Late in 1982, the NRC, on the advice of the Geological Survey, decided to place more emphasis on the resistance of nuclear plants to earthquakes in the east and midwest. Although large earthquakes in this region are much less frequent than in the west, they cannot be ruled out entirely.

In the west, earthquakes are more common and enough data has been accumulated in the last 50 to 100 years or so to allow use of the more precise Richter scale. The Richter magnitude is based on the logarithm of the amplitude of motion of a standard seismograph corrected for attenuation to a distance of 100 km from the epicenter. Thus, the peak ground motion goes as the exponential of the Richter magnitude. An increase of one unit on the Richter scale corresponds to an increase in released energy of about 250.

The few significant earthquakes in the east all occurred before 1900. This is believed to be merely chance since it appears that the seismic activity of a region changes only on the geologic time scale. A reanalysis of the seismographs in use over the last century or so has indicated that the magnitude of the great San Francisco earthquake was probably only 7.9 instead of the 8.3 given in most sources. The 1964 Alaska quake, on the other hand, has been upgraded to 9.2. The greatest magnitude seism recorded so far was the southern Chile event of 1960. It is now believed to have had a Richter magnitude of 9.5, which may be about the maximum possible.

Station 2

June 27, 1966 Parkfield Earthquake

Accelerograph Record

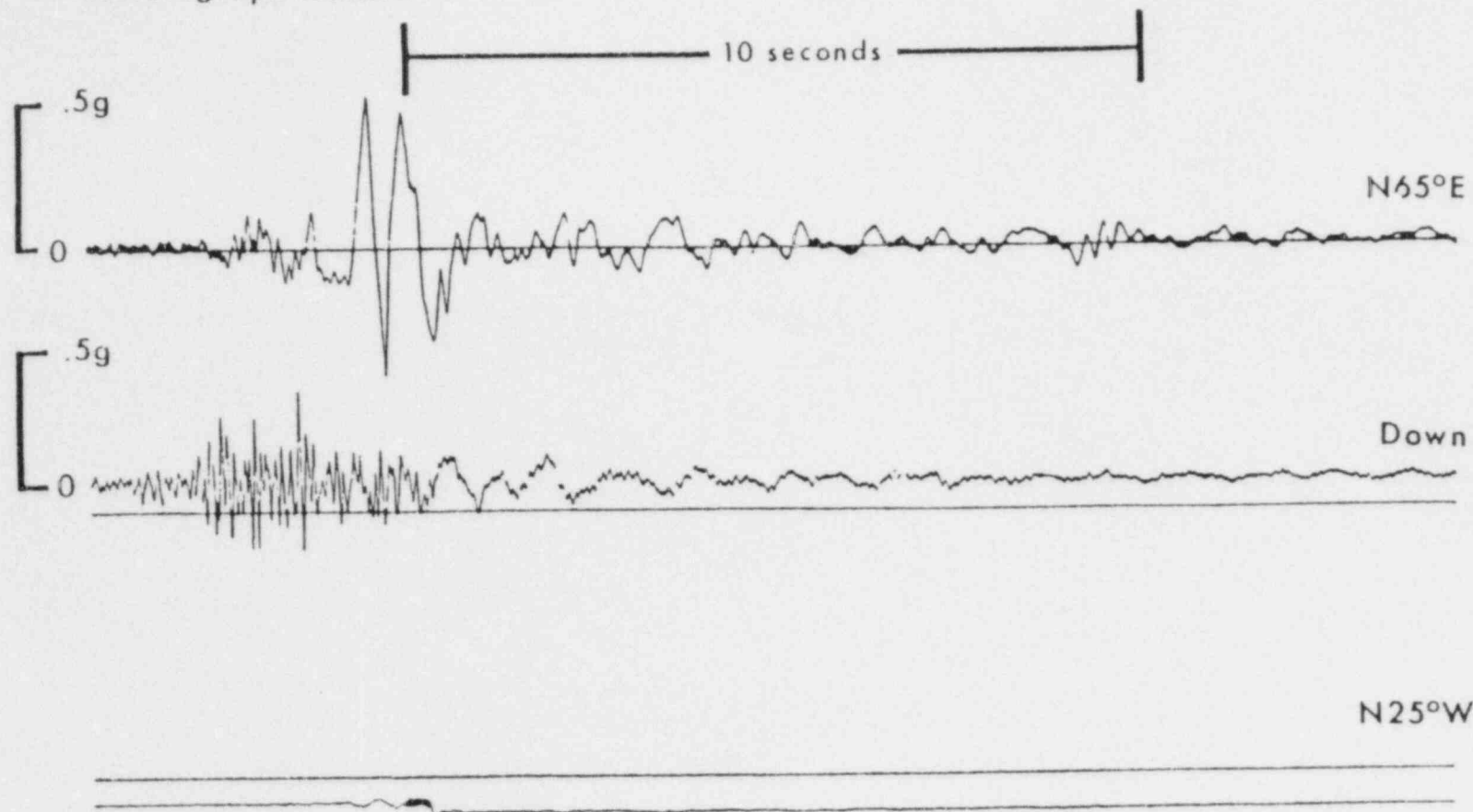


FIGURE 10-8

ACCELEROGRAPH RECORD OF THE 1966 PARKFIELD, CALIFORNIA EARTHQUAKE

SOURCE: Aki, K. Seismic Design for Nuclear Power Plants. MIT Press, 1970, pg. 108, Figure 4. Used with permission.



FIGURE 10-9
EXPECTED LEVEL OF EARTHQUAKE HAZARDS

SOURCE: Press, F. and Siever, R. Earth. San Francisco: W.H. Freeman, 1974. Pg. 420. Used with permission.

TABLE 10-2
MODIFIED MERCALI SCALE
(Wood-Neumann Scale)
PERCEIVED INTENSITY

- I. Not felt except by very few, favorably situated.
- II. Felt only on upper floors, by a few people at rest. Swinging of some suspended objects.
- III. Quite noticeable indoors, especially on upper floors, but many people fail to recognize it as an earthquake. Standing automobiles may sway. Feels like passing truck.
- IV. Felt indoors by many during day, outdoors by few. If at night, wakens some. Dishes, windows and doors rattle, walls creak. Standing cars may rock noticeably. Sensation like heavy truck striking building.
- V. Felt by nearly all. Many wakened. Some fragile objects broken and unstable objects overturned. A little cracked plaster. Trees and poles notably disturbed. Pendulum clocks may stop.
- VI. Felt by all. Many run outdoors. Slight damage. Heavy furniture moved. Some fallen plaster.
- VII. Everyone runs outdoors. Slight damage to moderately well-built structures, but considerable to poorly built. Some chimneys broken. Noticed by automobile drivers.
- VIII. Damage slight in well-built structures, considerable in ordinary substantial buildings with some collapse. Great damage in poor structures. Panels thrown out of frame structures. Chimneys, monuments, factory stacks thrown down. Heavy furniture overturned. Some sand and mud ejected, wells disturbed. Automobile drivers disturbed.
- IX. Damage considerable even in well-designed buildings. Frame structures thrown out of plumb. Substantial buildings greatly damaged, shifted off foundations, partial collapse. Conspicuous ground cracks, buried pipes broken.
- X. Some well-built wooden structures destroyed. Most masonry and frame structures destroyed, with their foundations. Rails bent, ground cracked. Landslides on steep slopes and river banks. Water slopped over from tanks and rivers.
- XI. Few, if any, masonry structures left standing. Bridges destroyed. Underground pipes completely out of service. Rails bent greatly. Broad cracks in ground and earth slumps and landslides in soft ground.
- XII. Damage total. Waves left in ground surface and lines of sight disturbed. Objects thrown upward into the air.

SOURCE: Gilluly, J., et al, Principles of Geology. San Francisco: W.H. Freeman, 1951. pg. 485. Used with permission.

TABLE 10-3
EARTHQUAKE MAGNITUDES, ENERGIES, EFFECTS, AND FREQUENCIES

<u>Characteristic Effects of Shallow Shocks In Populated Areas</u>	<u>Approximate Magnitude</u>	<u>Number of Earthquakes Per Year</u>	<u>Energy (ergs)</u>
Damage nearly total	8.0	0.0 - 0.2	10^{25}
Great damage	7.4	4	4×10^{24}
Serious damage, rails bent	7.0-7.3	15	$0.04-0.2 \times 10^{24}$
Considerable damage to buildings	6.2-6.9	100	$0.5-23 \times 10^{21}$
Slight damage to buildings	5.5-6.1	500	$1-27 \times 10^{19}$
Felt by all	4.9-5.4	1,400	$3.6-57 \times 10^{17}$
Felt by many	4.3-4.8	4,800	$1.3-27 \times 10^{16}$
Felt by some	3.5-4.2	30,000	$1.6-76 \times 10^{15}$
Not felt but recorded	2.0-3.4	800,000	$4 \times 10^{10}-9 \times 10^{13}$

SOURCE: Press, F. and Siever, R. Earth. San Francisco: W.H. Freeman, 1974. pg. 411.
Used with permission.

Although residential and light commercial buildings are quite susceptible to seismic damage, the resistance of heavy industrial structures to ground motion loadings is surprisingly high. The day before the magnitude 9.5 quake in Chile, a magnitude 7.5 event rocked the Huachipato Steel Mill. Although this facility had been designed to minimal seismic standards, it survived with relatively little damage. Similarly, the ESSO refinery in Managua, Nicaragua suffered almost no damage in the 1972 quake which registered 6.2 on the Richter scale even though it was only three miles from the fault. It was back in operation in only a few days. This earthquake had a maximum ground acceleration of 0.39 g, killed 10,000 people in Managua, and it was estimated to have caused \$800,000,000 worth of damage.

The causes of seismic destruction are ground motion, unstable ground (liquefaction), mud slides, rock slides and avalanches, fires, and tsunamis. Ground motion is what usually comes immediately to mind when an earthquake is envisaged, but the accompanying events often cause significantly more damage. Many people are aware, for example, that much of the damage in the San Francisco earthquake was due to the accompanying fire. Much of the death and damage from the 1755 Lisbon, Portugal earthquake was due to the accompanying seismic sea wave or tsunami. The 1970 earthquake in Peru was not particularly large in itself, but it set off an avalanche which in turn triggered a mudslide which buried several entire towns. The bulk of the damage in the Turnagain Heights area near Fairbanks in the 1964 earthquake was due to liquefaction of the ground. The ground consisted of layers of sand and clay with a high water table. The shaking caused the clay particles, which are highly aspherical, to pack closer together, thus, causing an excess of water several layers below the surface. The surface of the ground in the affected area just appeared to turn to liquid mud, houses slid away downhill and turned over.

Reactors are carefully located with extensive foundation investigations, so ground motion itself is the principal hazard for reactors. The ground motion can be characterized in several ways. The simplest is to give the maximum acceleration at the site of interest and the duration of accelerations that reach some fraction of the maximum. Since any structure responds more strongly to some frequencies than to others, a more complete description consists of a spectral or harmonic analysis in which the strength of all the frequencies present are given. The soil between bedrock and the structure of interest can alter the frequency content considerably. Usually a soil layer decreases the intensity of the seismic wave, but certain frequencies have been shown to be amplified under uncommon conditions. The frequencies which cause the greatest damage are those between 0.1 and 5 cycles per second.

The maximum acceleration of the ground likely to occur appears to be about 1.0 to 1.2 g, no matter how large the earthquake. The reason for this is that a large earthquake releases more energy because movement occurs along a longer section of the fault than it does for a small earthquake. Near the fault, where the ground acceleration will be the highest, only the closest portion of the fault contributes effectively to the ground motion. Thus, after a certain point, the total length of the fault involved becomes irrelevant insofar as the maximum local acceleration is concerned. However, an extremely large earthquake will cause a much larger area to experience these maximum accelerations than will a lower magnitude earthquake.

10.2.2 Characterization of the Seismic Hazard

The seismic hazard analysis is carried out in four steps as illustrated in Figure 10-10. First the sources are identified; these will be active faults in the west and general seismic areas or regions in the rest of the country. For each source, a recurrence

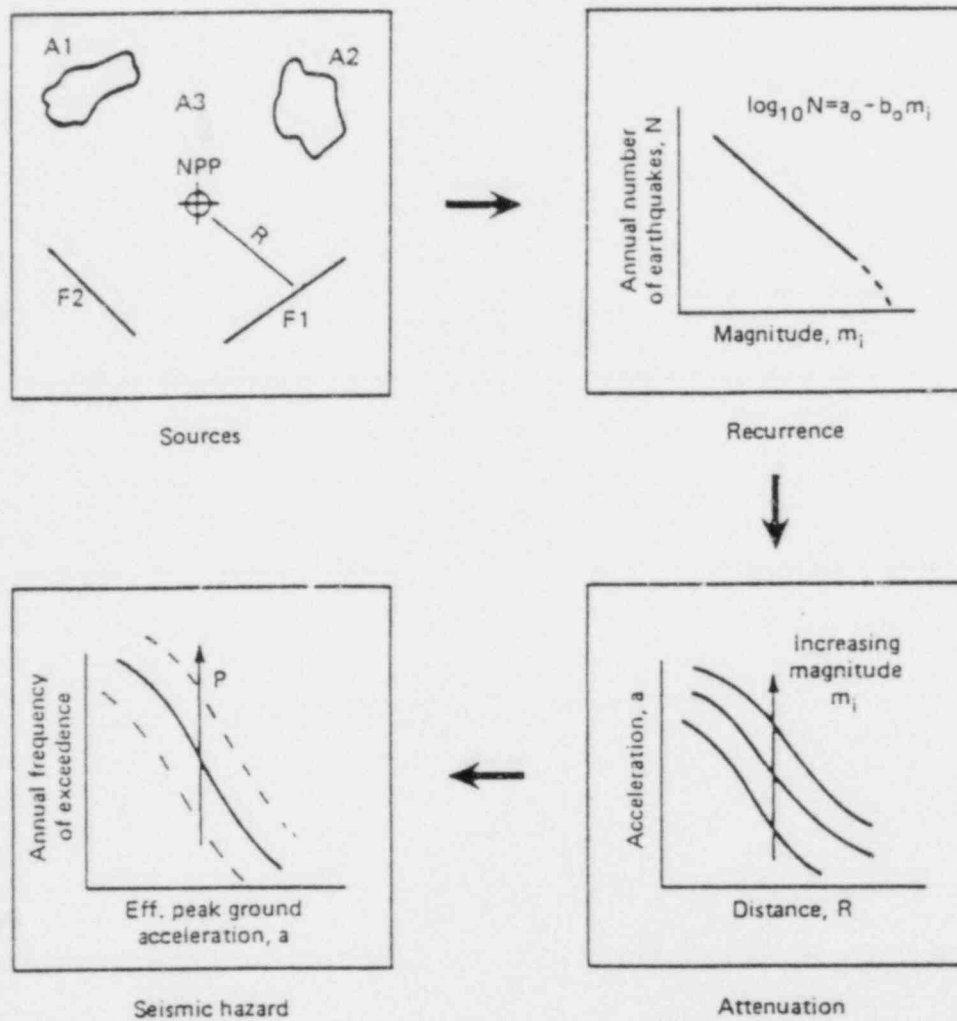


FIGURE 10-10
MODEL OF SEISMIC HAZARD ANALYSIS

SOURCE: PRA Procedures Guide (NUREG/CR-2300), Review Draft.1982.
Pg. 11-13

relationship is derived. In the west, this can be based upon the historical record of the fault or the records of other faults in the area which appear similar. In the east and midwest, even for the known seismic areas, the records are so sparse that more judgment is involved.

The recurrence rate is expressed as the annual frequency of events exceeding a given magnitude. Historical rates are considerably stable since changes usually take centuries or millenia. Fortunately, the frequency of large earthquakes can be predicted from smaller ones. Since the relationship used predicts a non-zero frequency for any magnitude no matter how large, an upper bound is chosen for each fault.

Once the source is characterized, its effect at the reactor site is needed. This will depend upon the site's distance from the source and the type of rock between the focus and the plant. The decrease in the strength of the seismic wave with distance from the epicenter is termed attenuation. Good data is available for attenuation in the west, but for the rest of the country the data is sparse. The attenuation is greater in the west than it is in the east and midwest. That is, an earthquake will be felt further away from the epicenter in the east than in the west. The scatter in attenuation data is large, so the values to be used should be carefully chosen by a seismologist who is thoroughly familiar with the area under consideration.

Numerous computer programs are available to perform the attenuation calculations. Bayesian techniques may be used to augment sparse data. Sensitivity studies show that the strength of the seismic hazard is more strongly influenced by the variability of the attenuation than it is by the uncertainty of the frequency content.

The hazard due to a particular source is described by giving either the effective peak ground acceleration as a function of frequency of occurrence, or by specifying the amplitude of all frequencies present, also as a function of frequency of occurrence. The results for all the sources are combined to give the end result: some measure of the magnitude of the ground motion vs. frequency of occurrence.

10.2.3 Structural and System Response

Knowing the motion of the ground under the reactor building, the final task is to determine how the structure and the systems it contains react to this seismic acceleration. All the systems and components whose failure might lead to core damage should be considered. Component fragilities are combined to give the system response if the system is not analyzed as a whole. Uncertainties are tracked throughout the process so that a confidence level can be stated for the result. The correlation between failures of different components must be treated in detail. Typical interactions are:

- failure of one component caused by failure of another,
- two components are manufactured by the same vendor and therefore may be expected to fail at the same stress level, and
- two components have the same location and orientation, so they would both be impacted by a gross structural failure at that location.

Related common cause failures must also be dealt with. For example, the earthquake may cause a loss of offsite power as well as failing several pumps due to vibration.

From the PRA viewpoint, failure is the inability of the component to perform its intended function, not just a departure from the design specifications. This should be kept in mind throughout the fragility analysis. A pipe that is bent but not broken is still intact and is not failed. Also, note that several failure modes are possible for any piece of equipment. As an example, a fan might fail in any of the following ways:

- Short or open circuit in wires conveying power,
- Short or open circuit in wires conveying control information,
- Motor failure,
- Housing shifted so it contacts the fan blades, and
- Housing ruptured so air is not confined to duct.

There are several methods available for the seismic fragility analysis, depending upon the level of effort involved. At the low-effort end is the limited analysis or Delphi method which is largely based upon available data and test results and a lot of engineering judgment. At the other extreme is the sort of analysis done by Lawrence Livermore for the Seismic Safety Margins Research Program (SSMRP). In this program, very extensive models of systems and components were constructed and detailed responses to seismic inputs were calculated. Other methods of fragility analysis fall in between these two extremes.

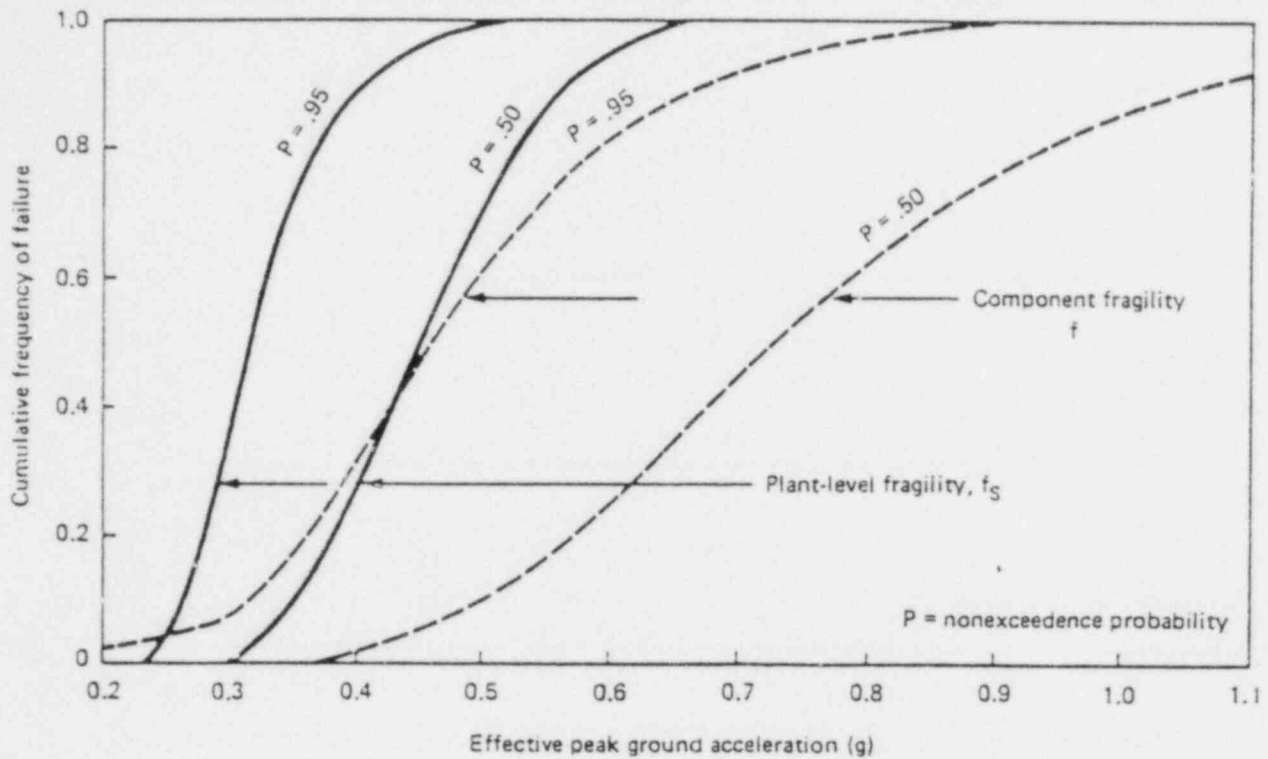
In the limited analysis method, a factor of safety for the response of each structure or system is derived from a linear dynamic analysis. This is usually done by estimates based on the design analyses done for the earthquake accelerations for the design basis and the safe shutdown earthquakes. The effects of soil-structure interactions and the damping of the structure are usually included, as is inelastic energy absorption. The resultant fragility is expressed probabilistically using three parameters:

- Best-estimate of the median required for failure,
- Random variable representing the inherent variation in the component, and
- Random variable expressing the uncertainty in the best-estimate value.

The overall approach is to identify seismically induced component or system failures which could initiate a core melt accident. Event trees are then constructed for each initiator, and fault trees are constructed for key systems that could prevent the accident from proceeding on to core melt or mitigate the effects. The fragility of the components of these systems are estimated and a Boolean expression is developed for each sequence.

The SSMRP analysis is somewhat more involved. The fragilities of systems or components are expressed in terms of local response parameters to the amplitude (magnitude) and frequency of the vibration. A value for the failure occurrence is obtained by convolving the amplitude expression (as a function of frequency) with the response curve. The major emphasis is on the computation of component and structural responses. Actual or simulated ground motion records are used for input and a detailed analysis is made of the bedrock-soil-reactor building interaction. Subsystems are modeled as a whole. Uncertainties are included by means of the Latin-hypercube technique.

No matter which method is used for the fragility analysis, after the sequences have been evaluated, they are assigned to release categories and the total frequencies for each category are determined. Figure 10-11 illustrates the results of this process.



COMPONENT AND PLANT-LEVEL FRAGILITY CURVES

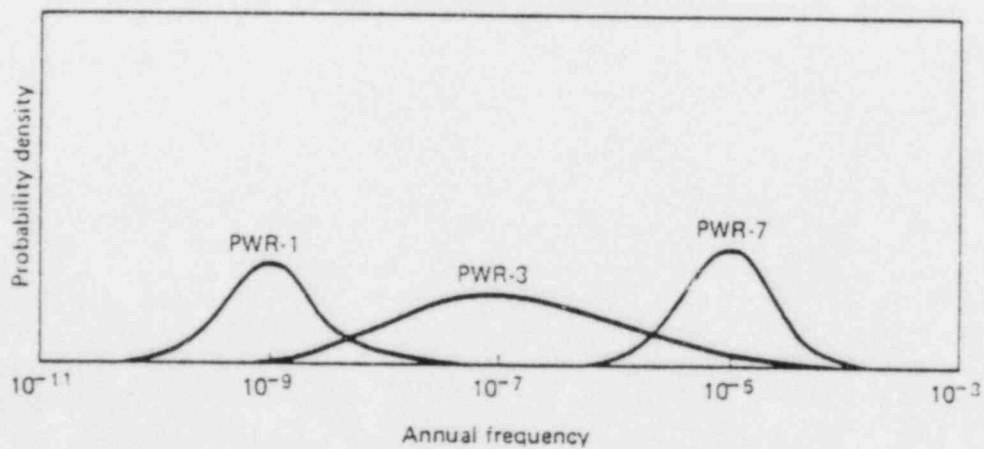


FIGURE 10-11

PROBABILITY DENSITY FUNCTIONS OF RELEASE FREQUENCIES
FROM SEISMIC EVENTS

SOURCE: PRA Procedures Guide (NUREG/CR-2300), Review Draft. 1982. Pg. 11-35.

As might be expected for an initiating event which is so variable in size, location, and occurrence, the uncertainties associated with determining its frequency are very large. It is very important to have a measure of the total uncertainties at the end of the seismic analysis so that confidence levels can be assigned. These uncertainties include, but are not limited to, source, frequency, duration, magnitude, attenuation, soil response, structural response, and component response.

10.3 Fires

At the start of the RSS, fires were excluded from consideration on the grounds that there was little if anything to burn in an operating reactor and no significant fires had been observed to date. Toward the end of the study, the Browns Ferry fire occurred and caused some rethinking on this subject.

The fire occurred when workers were plugging air leaks in the cable spreading room under the control room, using foam to plug holes where cables left the room. A candle was used to test for air movement. The draft drew the flame into the foam which ignited and in turn ignited the PVC insulation of some non-IE cables. (The IE wiring used polyfluoroethylene (PFE) insulation, which is more fire-resistant. Cross-linked PFE insulation is now specified, which is even more fire-resistant.) The fire spread in the cable trays into the reactor building and was not put out for some hours. There was no core damage or unusual release of radioactivity, but control of all ECCS was lost and control of some redundant systems was lost. The fire was finally extinguished with water. Firefighting was hampered by the location of the fire (in cable trays near the ceiling of a high-ceiling room) and dense smoke requiring the use of respirators.

In its general form, the fire analysis proceeds in much the same way as the seismic analysis so the discussion here will be abbreviated. Details are contained in the Procedures Guide.

The first step in a fire hazard analysis consists of location screening. Three methods of selecting the most important locations for more detailed consideration are:

- By location and contents, any safety equipment, FMEA to select significant locations.
- By loss of contents, which causes LOCA or transient. Most significant locations also cause loss of ability to remove decay heat and/or monitor and control reactor coolant system.
- By ranking on basis of contents, fuel available, and means of suppression available. Spread from/to adjacent locations considered.

Reactor experience to date indicates that one significant fire may be expected at a given reactor for every 6 to 10 years of operation. It is important to distinguish between operation and construction because fires are much more common during construction.

Table 10-4 contains two tables which illustrate the method of Apostolakis and Kazarians, which is described in more detail in the Procedures Guide. The values in the lower table are the coefficients for the equation:

$$\pi(\lambda) = \frac{\beta\alpha}{\tau(\alpha)} \exp(-\beta\lambda) \quad (\text{Equation 10-1})$$

TABLE 10-4
STATISTICAL EVIDENCE OF FIRES IN LIGHT-WATER REACTORS

<u>Area</u>	<u>Number of Fires, r</u>	<u>Number of Relevant Years, T</u>
Control Room	1	288.5
Cable-Spreading Room	2	301.3
Diesel-Generator Room	10	543.0
Containment	5	337
Turbine Building	9	295.3
Auxiliary Building	10	303.3

As of May 1, 1978.

DISTRIBUTION OF THE FREQUENCY OF FIRES
(Events Per Room Year)

<u>Area</u>	<u>α</u>	<u>β</u>	<u>λ_{05}</u>	<u>λ_{50}</u>	<u>λ_{95}</u>	<u>$\langle \lambda \rangle$</u>
Control Room						
Prior	0.182	0.96	5×10^{-8}	0.015	1.0	0.21
Posterior	1.182	289.46	3.1×10^{-4}	0.003	0.012	0.0041
Cable-Spreading Room						
Prior	0.182	0.96	5×10^{-8}	0.015	1.0	0.21
Posterior	2.182	302.26	1.4×10^{-3}	0.062	0.017	0.0072
Diesel-Generator Room						
Prior	0.32	0.29	2.1×10^{-4}	0.30	5.0	1.11
Posterior	10.32	543.29	1.1×10^{-2}	0.018	0.03	0.019
Containment						
Prior	0.32	0.29	2.1×10^{-4}	0.30	5.0	1.11
Posterior	5.32	337.29	6.2×10^{-3}	0.014	0.028	0.016
Turbine Building						
Prior	0.32	0.29	2.1×10^{-4}	0.30	5.0	1.11
Posterior	9.32	295.59	1.7×10^{-2}	0.03	0.05	0.032
Auxiliary Building						
Prior	0.32	0.29	2.1×10^{-4}	0.30	5.0	1.11
Posterior	10.32	303.59	1.9×10^{-2}	0.033	0.053	0.034

SOURCE: PRA Procedures Guide (NUREG/CR-2300), Review Draft, 1982, pg. 12-11.

The coefficients have been derived from the data in the upper table by applying Bayes theorem.

Once the important locations for the start of a fire have been selected, an analysis must be undertaken to determine the extent and spread of the fire. Table 10-5 shows three ways of systematizing this analysis. The difficulty with detailed physical models for propagation is that they must be coupled with very crude models for detection and suppression. The suppression efforts depend largely on human interaction; there is very little experience and data in this area so it is largely based on expert opinion.

The plant systems analysis for fires proceeds much the same as it does for the seismic or any other external event. There is more emphasis on the quantification of human actions in the fire analysis because of the need to consider detection, suppression efforts, and the manual operation of equipment that is usually operated automatically. This would be needed when a fire had destroyed part of the control system. If fire renders certain equipment inoperable or specific locations uninhabitable, the possibility of the operators devising alternate methods of operation should be considered also. The side effects of smoke and flooding from water used to fight the fire must be taken into account, as must the dependencies between different systems. And, of course, the uncertainties must be quantified.

10.4 Floods

Because the seismic event was considered in some detail, floods will be only briefly presented. A more comprehensive discussion may be found in the Procedures Guide. Table 10-6 lists some of the causes of flooding. Obviously, some of these can be ruled out for any specific site. For example, a tsunami would be impossible for an inland site not on a large lake. Some of the external causes would be expected to have sufficient warning time that the reactor could be shut down before the flood occurred or precautions taken to avert it. For the internal floods and external floods, like the failure of a nearby dam, there would be essentially no warning.

The main damage mechanism is submergence, primarily of pumps, motors, and electrical equipment. Other mechanisms for external flooding are listed below:

- Submergence
- Undermining of foundations
- Mudslides
- Battering by waves and debris
- Seepage and leakage
- Blockage of cooling water intakes

External floods are often accompanied by complicating factors such as the disruption of evacuation routes or damage to electrical power transmission facilities. For internal floods, in addition to submergence, problems may also be caused by the spray from a ruptured pipe onto pumps, motors, or other electrical equipment.

As might be expected from the care with which reactors are sited, most serious floods to date have been internal. The most notable flood was in 1972 at Quad Cities 1, when a ruptured pipe in the circulating water system rapidly flooded a pump room. The equipment damaged was quite extensive. Changes were made so a similar flood could not damage so much equipment. Current design practice is to separate equipment and restrict the number of components at any one location.

TABLE 10-5
PROPAGATION ANALYSIS

1. Equations Derived (based on record) for Distance Spread as $f(t)$
Dependency on Fuel Included
Not Plant-Specific
Assumes Ignition Uniformly in Location
2. Event Tree Analysis
Ignition
Propagation
Detection
Suppression
3. Simple Physical Model
Takes Physical Arrangement Into Account
Heat Transfer and Distribution of Combustible Material Modeled
Suppression Information Required - Usually Based On Historical Data

TABLE 10-6
POTENTIAL CAUSES OF FLOODING

- EXTERNAL
 - Dam Failure
 - Dike/Levee Failure
 - Tsunamis
 - Storm Surges and Seiches
 - Heavy Precipitation
 - High Winds and Hurricanes
 - Rapid Snow Melt

- INTERNAL
 - Pipe Rupture
 - Tank Rupture
 - Overfilling of Tanks
 - Sump Pump Failure
 - Drain Blockage

There have been some threats of external flooding. Sandbags were placed along the Susquehanna River at Peach Bottom once because high water was expected. It was found that a specific sequence of inadvertent operations at Oconee could cause the lake, used as the ultimate heat sink, to siphon into the plant. Several computer codes are available to compute flood routing, heights, and arrival time for hypothetical dam failures. The NRC has sponsored the development of NOAH, a code which computes the failure frequency of equipment given flood height.

In the past, floods have been excluded from PRAs because it was argued that most external floods can be predicted far enough in advance to shut the plant down in an orderly fashion and because plant design takes historic high water levels into account. While it is true that siting and design criteria ensure that only an extremely rare natural flood could cause problems, the arguments against including floods are now considered outweighed by several factors. First, some dam or dike failures may allow very little warning time. Secondly, the great uncertainty in the recurrence interval of very large floods should be taken into account. Finally, it now appears that internal floods pose a greater risk than external floods.

The methods of analysis for floods are of the same general nature as those for other external events. Although the damage mechanism, submergence in water, is the same for both external and internal floods, the hazards analyses are quite different. The external flood hazard analysis is similar to the seismic analysis in that information about the local and regional environment is collected and analyzed to determine the frequencies with which various flood heights may be expected. The routes by which water would enter the plant are then determined and fragility curves constructed for the equipment affected.

The internal flood hazard analysis starts, as does the fire analysis, with a screening by location to determine where vulnerable equipment is located. Another screening is then performed to determine what sources could conceivably cause flooding at those locations. Historical data for pipe and tank rupture, valve failure, etc., is then used to determine flooding depths and frequencies for each location.

Once frequencies of water depths at the important locations have been determined, the fragility and sequence analyses follow in a straightforward manner.

10.5 Summary

Table 10-7 lists some of the external events which should be considered for every plant. The decision of which are worthy of attention can only be made on a site-specific basis. Aircraft impacts and tornadoes can often be eliminated because the plant design has taken these factors into account. For example, part of the design consideration in determining the thickness of the containment shell is protection from the missiles generated by tornadoes. Some external events are potential threats to any plant. These include fires, internal floods, and turbine missiles. Others, such as earthquakes, external floods, and accidents at nearby industrial or transportation facilities can only be assessed on a local basis. Usually a relatively simple analysis can determine which of the external events are important enough to warrant detailed consideration.

The above presentation has touched on only some of the external events, but they are the ones most likely to require investigation in depth.

TABLE 10-7
EXTERNAL EVENTS

1. Aircraft Impacts
2. Earthquakes
3. Fire
4. Flooding, External
5. Flooding, Internal
6. Industrial and Military Facility Accidents
7. Missiles from Turbine
8. Release of Toxic Chemicals Onsite
9. Tornadoes and High Winds
10. Transportation (rail, highway, pipeline)

TOPIC 11
ACCIDENT PROCESS ANALYSIS

11. ACCIDENT PROCESS ANALYSIS

This section discusses the progression of events from the initiating event until containment failure. The subject will be introduced by discussing very basic considerations of accident phenomenology, and a brief history of degraded core treatment. The progression of the accident can be divided into four stages:

1. Degradation or melting of the core,
2. Reactor vessel failure,
3. Behavior of core material after vessel failure, and
4. Response of containment to the stresses placed upon it.

Each of these areas is presented in some detail below. There is also a discussion of the relationship between the systems analysis and the accident process analysis and a short review of the computer programs employed to model these accident processes.

11.1 Introduction and General Discussion

The analyses of system failures which could challenge the containment or lead to the release of radioactivity have been the basis for the licensing process. In the design basis accident approach, these analyses have been deterministic and degraded core accidents have not been considered. Over the years another method of analysis has been developed. PRA determines the probabilities of numerous sequences of events leading to core degradation and the behavior of the core under degraded conditions. An understanding of the likelihood and results of such sequences provides an index of risk. The preceding topics have concentrated on the methods for determining the failure probability for a system, and how the various sequences of system failures may be analyzed. This topic will briefly discuss the physical processes which will take place if these sequences actually occur. It is only by considering these processes in some detail that a reasonable estimate of the onsite consequence and the amount of radioactivity released can be made.

The first general risk study, WASH-740 (1957), did not consider the accident processes in detail, but merely assumed that a certain fraction of the radioactive fission product would be released. There was virtually no study of LWR core damage events until the Reactor Safety Study (RSS) (WASH-1400, 1975). Since that time, it has been recognized that core damage accidents, although very improbable, are the major contributors to the offsite risk. Therefore, since the RSS, analyses and experiments on degraded core phenomena have proceeded steadily. Sandia National Laboratories has had a major role in this work. Research has also been going on in Germany for some time.

For Liquid Metal Fast Breeder Reactors (LMFBRs), the EBR-I incident in 1955 and the Fermi incident in 1965 were early indicators that degraded core conditions should be considered for LMFBRs. Thus, there has been slow but continuous progress in understanding degraded core problems in LMFBRs. Since this course is concerned with commercial power reactors, degraded core processes in the LMFBR will not be discussed further.

In a nuclear facility, the source of potential hazard is the fission product inventory that is contained in the fuel after some level of burnup has been achieved. The public is protected from this material by numerous safety and systems and four physical barriers. First, the fuel matrix itself is an effective retention system for fission product activity. Even when the fuel is subjected to significant stress such as inordinately high

temperatures, many of the fission products remain in the uranium dioxide lattice of the fuel pellet. Gaseous and volatile fission products are driven from the fuel to various extents by the temperatures encountered in normal operations. The non-volatile fission products would escape from the fuel matrix only if the core was severely degraded.

The second barrier to fission product release is the fuel cladding. Depending on the type of reactor, this may be stainless steel or an alloy of zirconium. The cladding is a long cylinder about 1/2 inch in diameter into which the fuel pellets are loaded. Once the fuel is placed into the cladding, the fuel pin is pre-pressurized with helium to enhance internal heat transfer between the fuel and the cladding and the ends of the cladding are sealed by welding. The gaseous and volatile fission products that escape from the fuel matrix during power generation are retained within the clad in the gas space or gap.

The third barrier to release is the reactor coolant system, including the reactor vessel and piping. This system can be compromised by events such as a seal failure, a stuck-open valve, or a pipe break. The fourth barrier is the reactor containment system, which is designed to prevent the release to the environment of fission product activity in the event of considerable core and primary system damage. In addition, most reactor sites are in fairly remote areas, thus providing another protective feature.

Long-term safe shutdown of the reactor requires that the chain reaction be stopped and decay heat removed from the core. The previous portions of this course have dealt with the assessment of how frequently, and in what fashion, the systems which perform one or both of these functions may fail. Failures of these systems imply that damage to the core and possibly a significant radioactive release from the containment may follow. If a mismatch between power generation and heat removal occurs, core damage may result, depending upon how severe the mismatch is and how long it persists. In such a sequence, if mitigation is prompt, core damage will be minimal or nonexistent. If the sequence is not terminated promptly, damage to the core and core structures may occur.

The relationship of the accident process analysis to other portions of the PRA are illustrated in Figure 11-1. The event tree analysis delineates the combinations of available and failed systems that define each plant state. The failure probability of each individual system is derived from quantification of the system fault trees and these probabilities are combined in the event tree to produce a probability for each plant state. For each plant state, the accident will proceed in a different way because of the different systems available. Also feeding into the accident process analysis is the structural analysis of the containment which determines the pressure at which the containment will fail. This piece of information is crucial in determining the relative frequency of the various containment failure modes.

The results of the accident process analysis include the pressures, temperatures, and flow rates in the reactor coolant system before the pressure vessel is breached, and the pressure and temperature in the containment from the beginning of the accident until the ultimate failure pressure of the containment is exceeded. If the containment pressure never exceeds the failure pressure, the simulation is continued until the pressure has decreased significantly from its peak value. In these cases, the release of radioactivity to the environment will be very small unless an isolation failure has occurred.

The output of the accident process analysis is used to determine how the fission products will behave during the course of the accident. The next topic covers this portion of the analysis. When the results of this analysis are available, enough information is on hand to allow construction of the containment event tree and the formation of release categories.

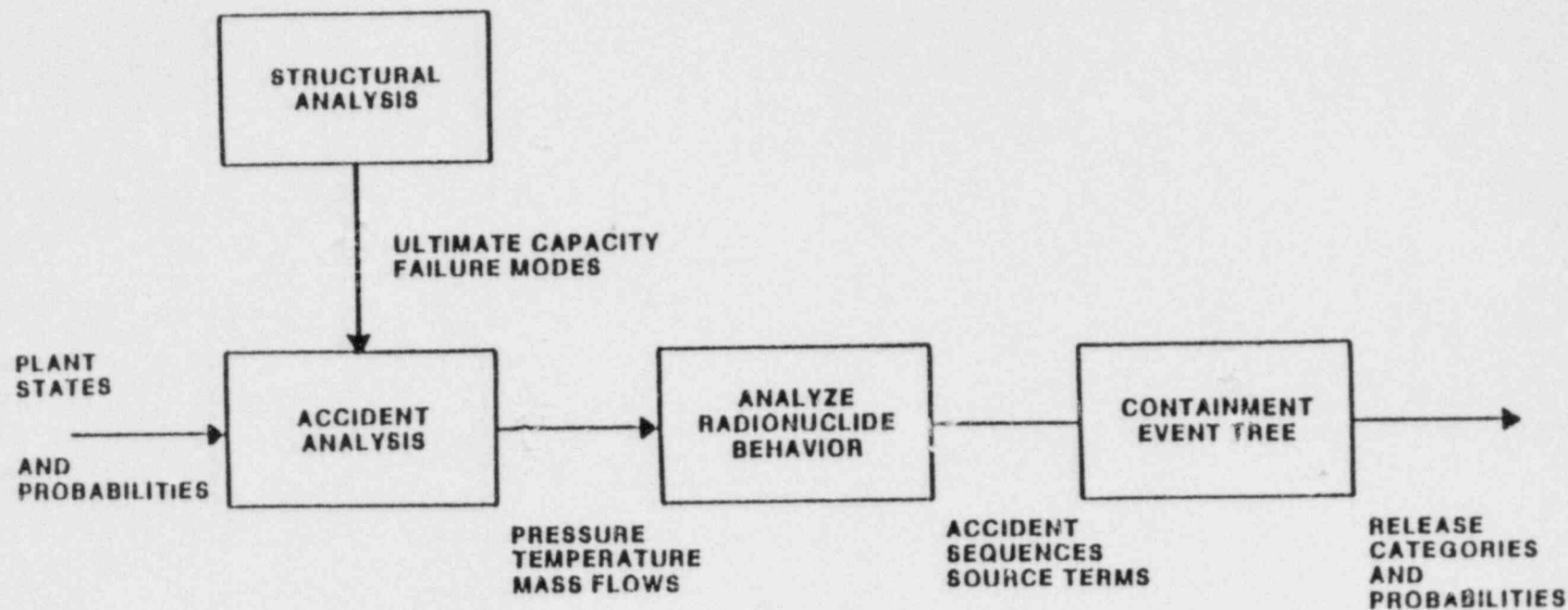


FIGURE 11-1

CONTAINMENT AND DEGRADED CORE ANALYSIS FLOW CHART

The accident process analysis itself is divided into stages since different tools are often utilized within analysis of different stages. Table 11-1 lists the stages of the accident that follow if scram, decay heat removal, or both are accomplished. Through automatic functioning of certain emergency systems or positive actions on the part of an operator, there is a possibility of arresting the accident in some degraded but coolable state. TMI is a well-known example of an accident where such recovery occurred. Accidents such as these are not the focus of the accident process analysis because the offsite consequences are small compared to those accidents where the core melts and the containment fails. Nonetheless, the possibility of recovery affects the probability that the sequence will proceed to a complete melt and must be considered.

In considering how the four barriers fail, their past history as well as their static and dynamic loadings following the accident must be considered. Radiation embrittlement, the effect of zirconium-water reactions, and thermal shock may have altered the materials considerably since their manufacture so that test results based on new material are inappropriate. The cycling of temperature and pressure over the life of the reactor may have introduced considerable fatigue in addition.

Table 11-2 lists the phenomena that must be taken into account before and after reactor vessel meltthrough in order to describe the progression of the accident completely. It is obvious from this list that many of these phenomena are such that full-scale experiments would be difficult and extremely expensive to carry out. TMI has been our only full-scale experiment to date. Thus, analysis must depend upon extrapolations from the TMI experiences (when fully known), small laboratory experiments, and theoretical analysis in many areas.

11.2 Core Degradation and Melting Within the Reactor Vessel

This discussion will assume that the nuclear reaction has been brought under control by the insertion of the control rods. (The progression of events in failure to scram accidents is similar, only much faster.) Figure 11-2 illustrates the basic consideration leading to core melt: radioactive decay of fission products continues to produce power after the fission reaction has been terminated. There is no way to shut off this decay heat production, so the heat must be removed from the core. Further, the heat must be removed as fast as it is produced or the temperature of the core will increase, eventually leading to degradation. Adequate cooling generally means keeping the core covered with liquid water; however, cooling by steam flow can be adequate in certain conditions.

The first stage in a LOCA is the blowdown phase; the breach in the reactor coolant system pressure boundary causes a rapid loss of coolant. Depending on the size of the hole, a considerable portion of the core may be uncovered. This uncover period will be brief if the injection systems function as designed. If the core is never recovered with liquid water, degradation may follow quickly. If the reactor vessel is filled promptly, water must continue to be supplied to the reactor vessel to make up for the losses out the break. In less than one hour, the emergency core cooling systems must switch from the injection mode to the recirculation mode as the sources of injection water are depleted.

For many transients, a blowdown also takes place due to the release of steam through the safety/relief valves. As in a LOCA, this lost water must be replaced by an injection system. Following the reflooding of the core, water must continue to be circulated through the core to remove decay heat. If a safety/relief valve sticks open, then the accident may behave much like a small LOCA.

TABLE 11-1
ACCIDENT SEQUENCE STAGES

1. Initiation (until core uncover)
2. Core Uncovery and Meltdown
3. In-Vessel Recovery
4. Melt Interactions in Lower Head
5. Melt Interactions in Reactor Cavity
6. Containment Response
7. Radiological Consequence Evaluation

TABLE 11-2
CORE PHENOMENOLOGY

- In-Vessel
 - decay heat
 - pre-core melt phenomena
 - degradation and melting
 - hydrogen production
 - steam explosions
 - vessel failure
 - core coolability in degraded state

- Ex-Vessel
 - entry into reactor cavity
 - steam explosion
 - core attack of concrete
 - noncondensable gas production
 - coolability

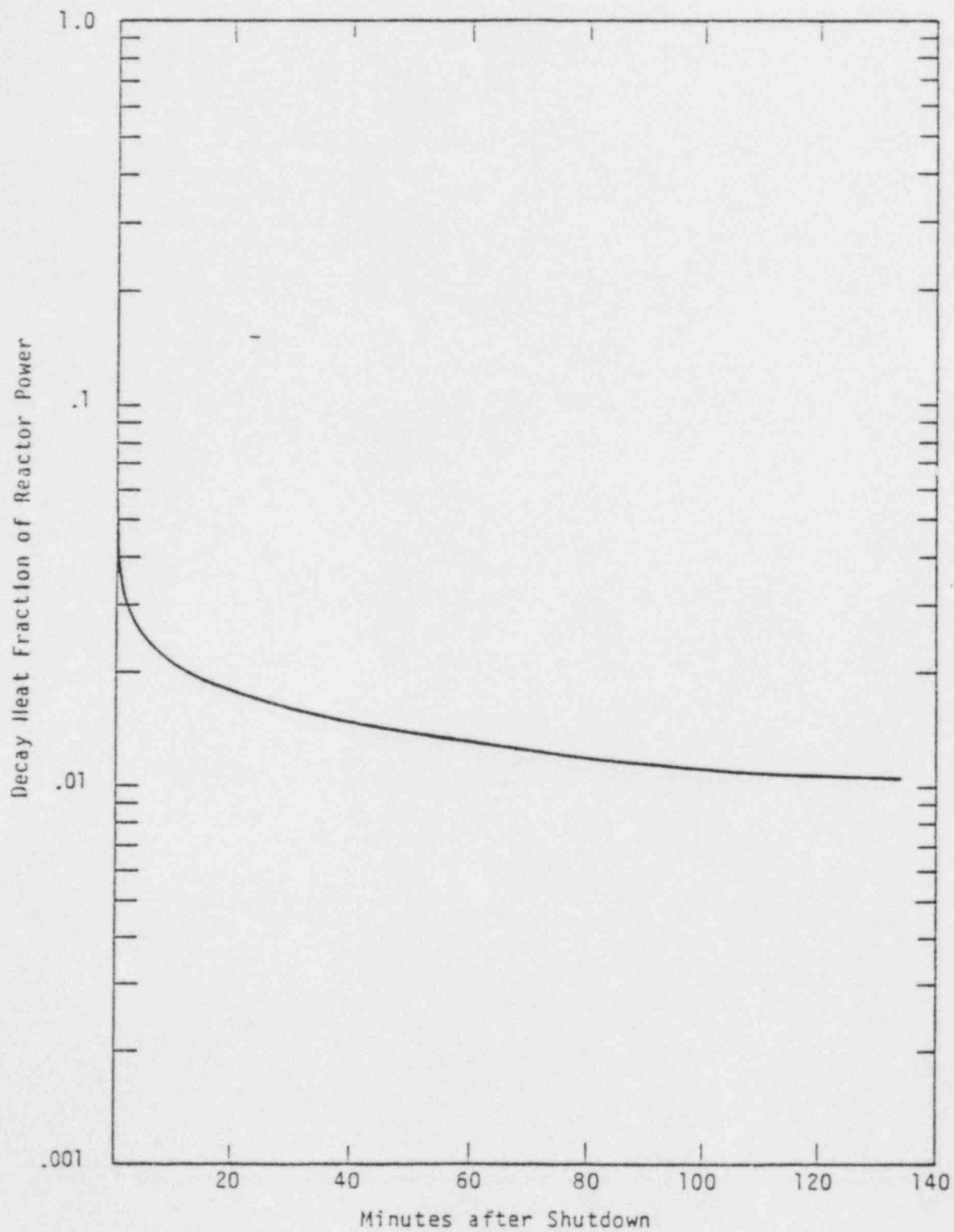


FIGURE 11-2
DECAY HEAT REDUCTION OVER TIME

If the core cooling is insufficient, the water level will fall until the top of the core is uncovered. When enough of the active part of the fuel rods is uncovered, steam cooling will be inadequate to prevent core degradation. The first event in this process is the reaction of zirconium and steam (water) to form zirconium oxide and liberate hydrogen. This reaction destroys the structural properties of the cladding, converting a malleable metal into a brittle, ceramic-like oxide.

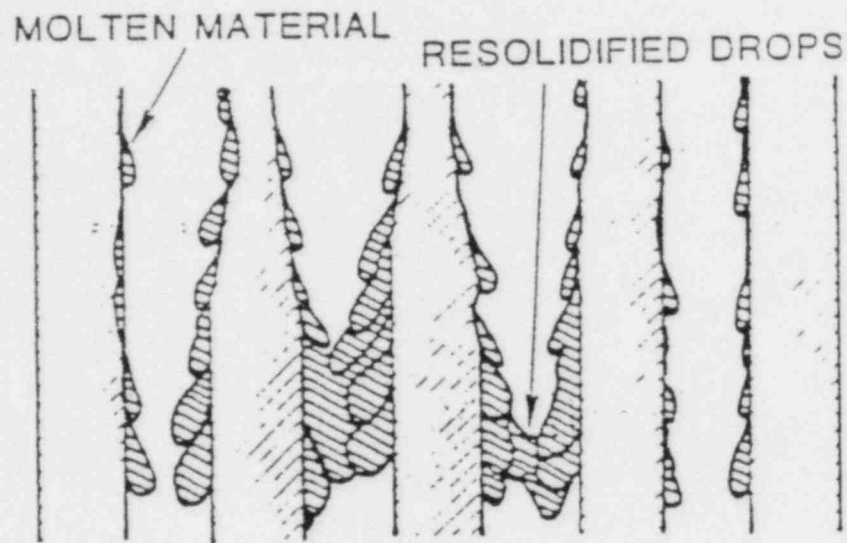
If the core temperature continues to increase, the clad and the control rods will be the first to melt since they have the lowest melting points. The clad is the barrier to the release of the gaseous fission products. The degradation of the control rods is not of immediate concern since liquid water is necessary as a moderator to sustain the neutron reaction in an LWR. If the core temperatures are high enough to melt the control rods, there is certainly no liquid water present. Figure 11-3 shows two steps in the progression toward a partially molten core. First, the clad will start to melt and will begin to deform. The rate of clad melting will increase once the flow passages between the fuel rods are blocked and the steam flow is impeded. If the core is reflooded at this point, the sudden quenching of the unmelted but oxidized zircaloy may cause it to shatter. The core at TMI apparently was uncovered and recovered twice. The top portion of the core now resembles a "rubble bed" due to the destruction of the cladding due to melting and embrittlement.

If the cooling remains deficient, the fuel pellets will eventually melt and the situation will resemble Figure 11-3(b). In part because downfacing heat transfer is less effective than upfacing heat transfer, and in part because steam generated by any remaining water inventory will help cool the lower portion of the melt, a solidified crust of sintered rubble below the molten mass will be created. This is expected to support the rubble mass on top of the still intact portion of the fuel rods. The molten portion of the core will progress slowly downward as the water in the lower portion of the reactor vessel boils away.

This molten core material will slowly gain in mass as it progresses downward through the core. Figures 11-4, 11-5, and 11-6 show one conception of how the accident might progress as it nears the bottom of a PWR reactor vessel. The progress in a BWR might be similar except that the lower plenum is of much greater height and contains all the control rod drive mechanisms.

The first obstruction to the downward motion of the molten portion of the core will be the lower core support plate which marks the lower end of the fuel rods. Figure 11-5 shows the situation when the molten mass has sunk far enough that the lower core support structure is beginning to weaken. At this point, there are two possibilities: the core can continue to move on downward through the diffuser plate and the support plate; or the core barrel can give way as shown in Figure 11-6. The latter is considered more likely. In either case, vigorous boiling is expected at some point when a structural failure drops hot material into the remaining water in the lower plenum. If the boiling is vigorous enough, it was postulated in the RSS that a reactor vessel steam explosion could occur, which would fail not only the reactor vessel but the containment as well. The scenario envisaged was: rapid steam generation in the lower plenum would propel the core and any above-core structures up into the reactor head, tearing the head off the vessel, and the head would then become a missile with sufficient momentum to breach the containment. Of this event, the RSS states, "Although such a release is predicted to be very unlikely, it cannot be ruled out completely on the basis of present evidence."

a. FORMATION OF LOCAL BLOCKAGE



b. GROWTH OF THE MOLTEN POOL

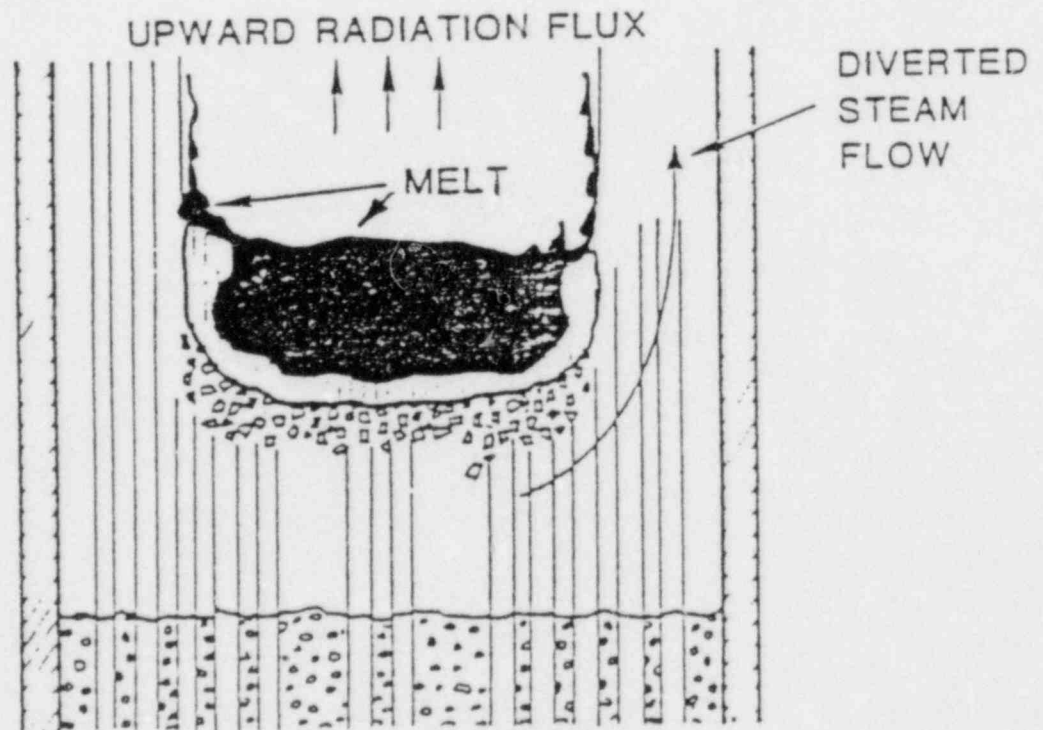


FIGURE 11-3
EARLY CORE MELT PROGRESSION

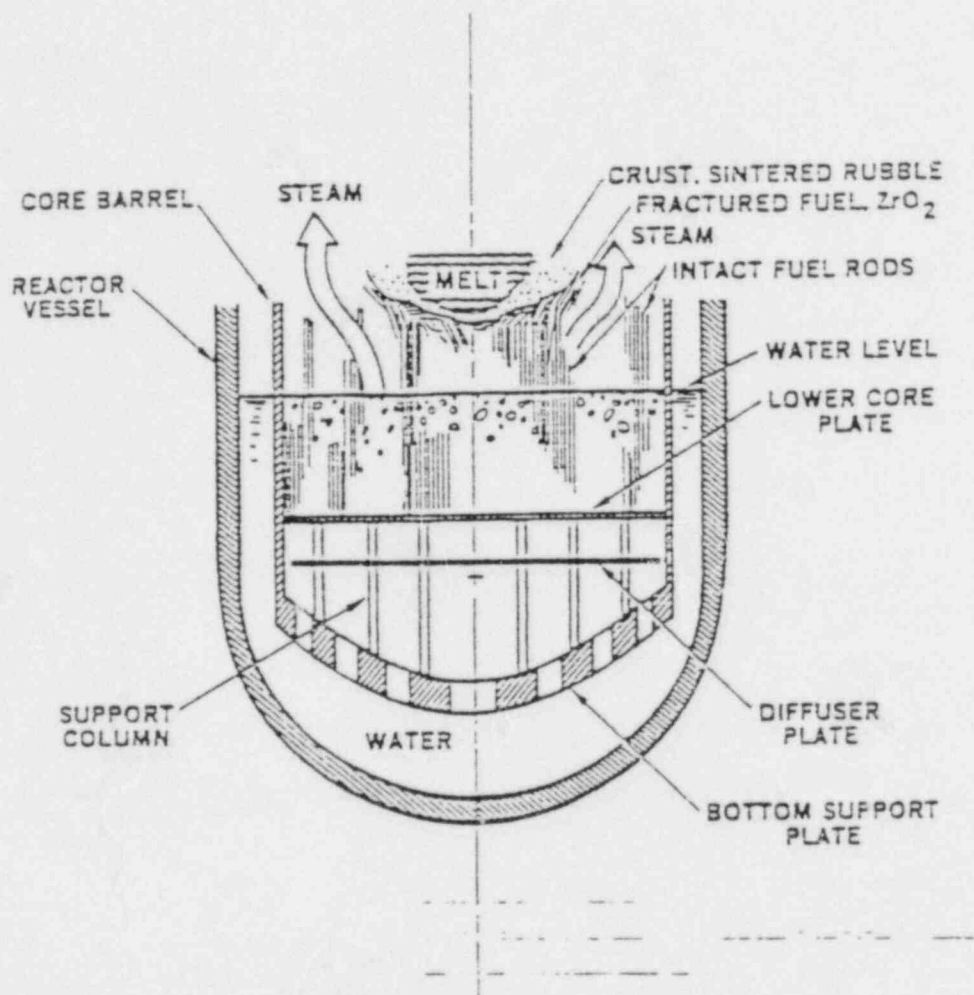


FIGURE 11-4

GENERAL STRUCTURE AND FEATURES
OF MELTDOWN IN A REACTOR VESSEL

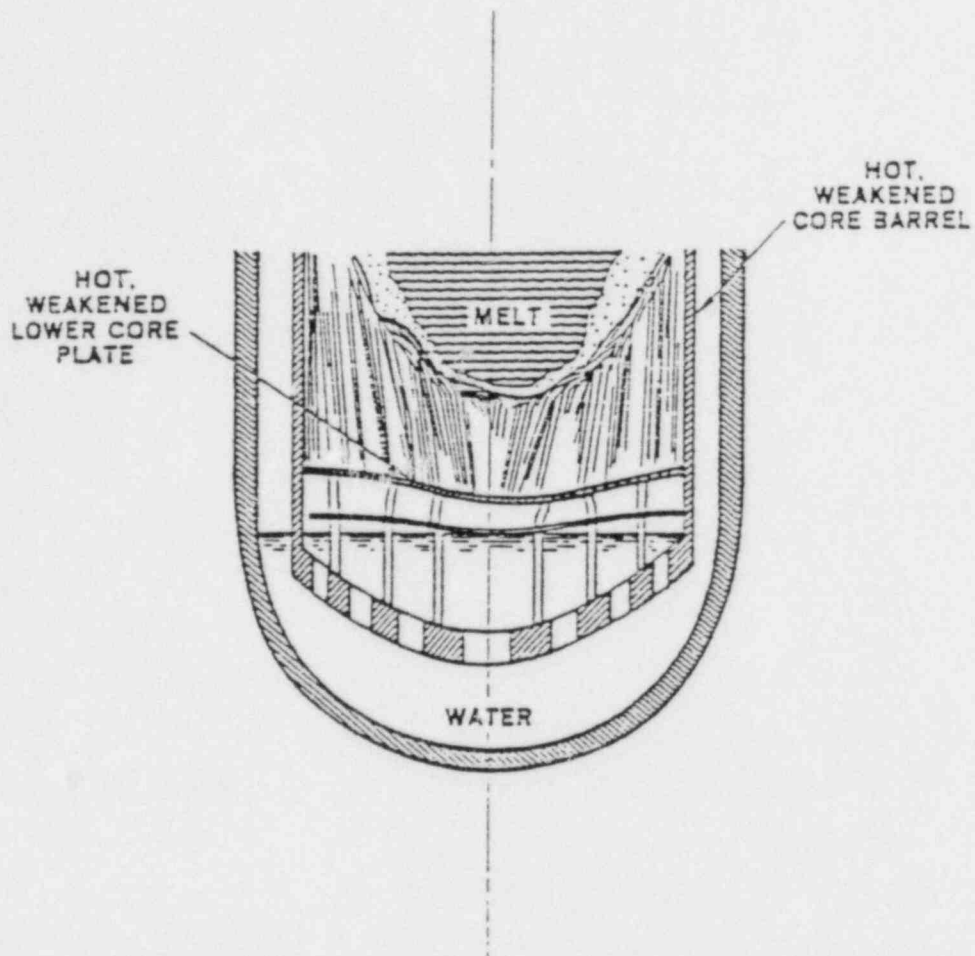


FIGURE 11-5

VISUALIZATION OF THE DOWNWARD PROGRESS OF A COHERENT
MOLTEN MASS AS THE BELOW-CORE STRUCTURE WEAKENS

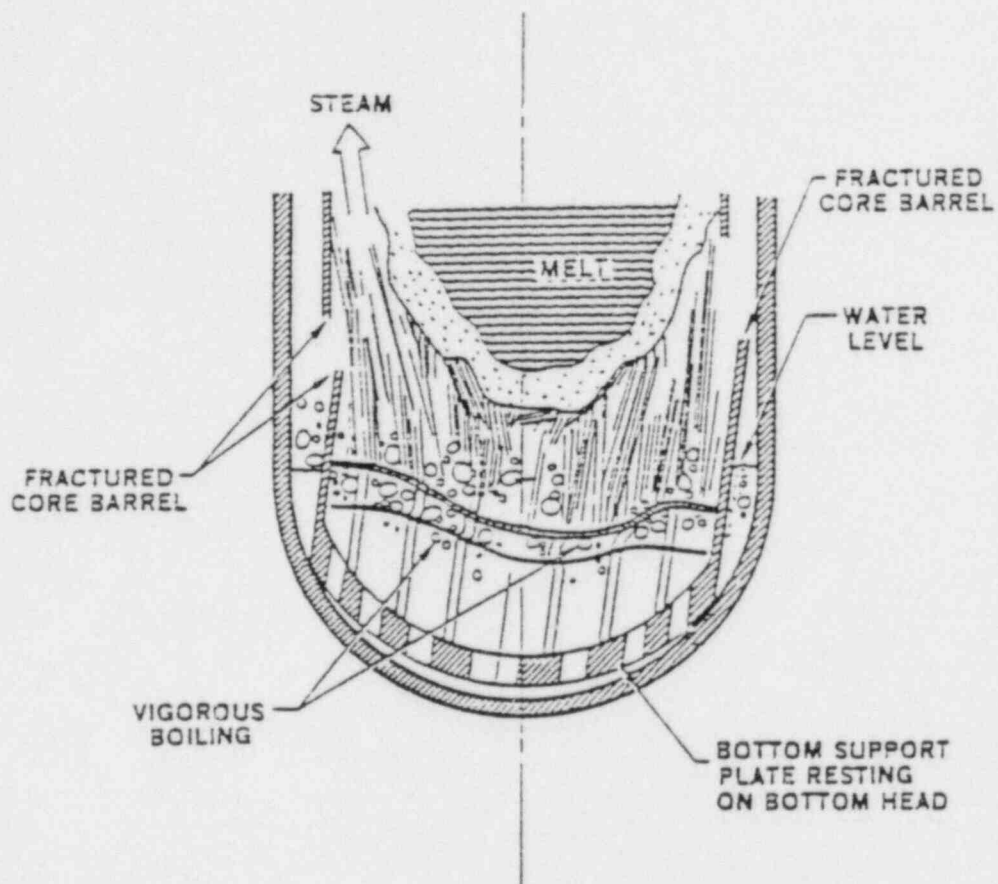


FIGURE 11-6

VISUALIZATION OF THE STATE RESULTING FROM FAILURE
OF THE CORE BARREL PRIOR TO PENETRATION OF A
COHERENT MOLTEN MASS THROUGH THE
BELOW-CORE STRUCTURE

Even with the stated low likelihood of this event, this scenario has met with considerable technical criticism, primarily because of a number of mechanisms and conditions that were not fully considered during the RSS. In the first place, the core would have to fragment as it contacted the liquid water in order to generate a large enough surface area for rapid heat transfer and explosive steam generation. Secondly, the molten core would have to hit the head as a compact, coherent mass in order to transmit sufficient momentum to it. It is difficult to imagine a set of conditions that would satisfy the requirements of both the finely divided material necessary for rapid steam generation and the coherent mass to act as a projectile.

Finally, the effects of structures in the region above the core must be considered. The upper plenum of the BWR contains steam separators and steam dryers. The upper plenum of the PWR is occupied by the control rod drive mechanisms. The energy required to dislodge and deform the structures in the upper plenum was not considered in the RSS. If a slug of core material is accelerated upward by a steam explosion, these upper plenum structures are likely to destroy any coherency this mass may have originally possessed. Current thinking is that while the core might be accelerated upward by rapid steam generation in the lower plenum, it is most unlikely to have enough momentum to dislodge the head. The possibility of the head gaining sufficient momentum to fail the containment appears to be physically impossible. Therefore, this containment failure mechanism has not been considered in most recent PRAs.

The description just given is a very simplified overview of the beginning of the core melt; many factors are expected to influence the progress of core degradation. While it is not possible to predict all the details of the core degradation at this time, there are gross thermal considerations which allow us to predict, with fair accuracy, the timing of important events such as the beginning of core melt and the failure of the reactor vessel. The major sources and sinks of thermal energy are shown in Figure 11-7. The heat input comes from the radioactive decay of fission products and can be computed with considerable accuracy. The masses of fuel and the metallic structures within the core are also well known. The time needed to boil off all the water in the vessel can be calculated from thermodynamic constraints. The rate of heat-up of the vessel and its contents, as a whole, can be conservatively calculated since the heat loss mechanisms may be limited to steam production (until the water is all gone), and radiation and convection from the outside of the vessel. In this manner, overall thermal limitations on the timing of core melting and vessel failure may be determined. The effects of various assumptions about temperature and mass distributions inside the vessel do not have profound effects upon the timing of the important events. Thus, although we cannot predict internal conditions in detail, the times given for important events are considered to be roughly correct. Note that this means correct based on the underlying assumptions, such as termination of all water delivery to the core at some specified time, and so on.

11.3 Molten Core Phenomena Outside the Reactor Vessel

The mode and location of the reactor vessel failure are important in determining the future course of the accident. The most important factors are the size of the initial hole and whether or not the vessel is at high pressure. At the time of the RSS, it was considered quite likely that the vessel would remain at high pressure until vessel failure in certain sequences. Lately, this has been questioned by analysts who postulate that portions of the reactor coolant system boundary such as pump seals will degrade, thus depressurizing the system before the vessel fails.

Figure 11-8 illustrates three possible failure modes of the reactor vessel. The center and right sketches illustrate the results of ruptures which are initially small, but could

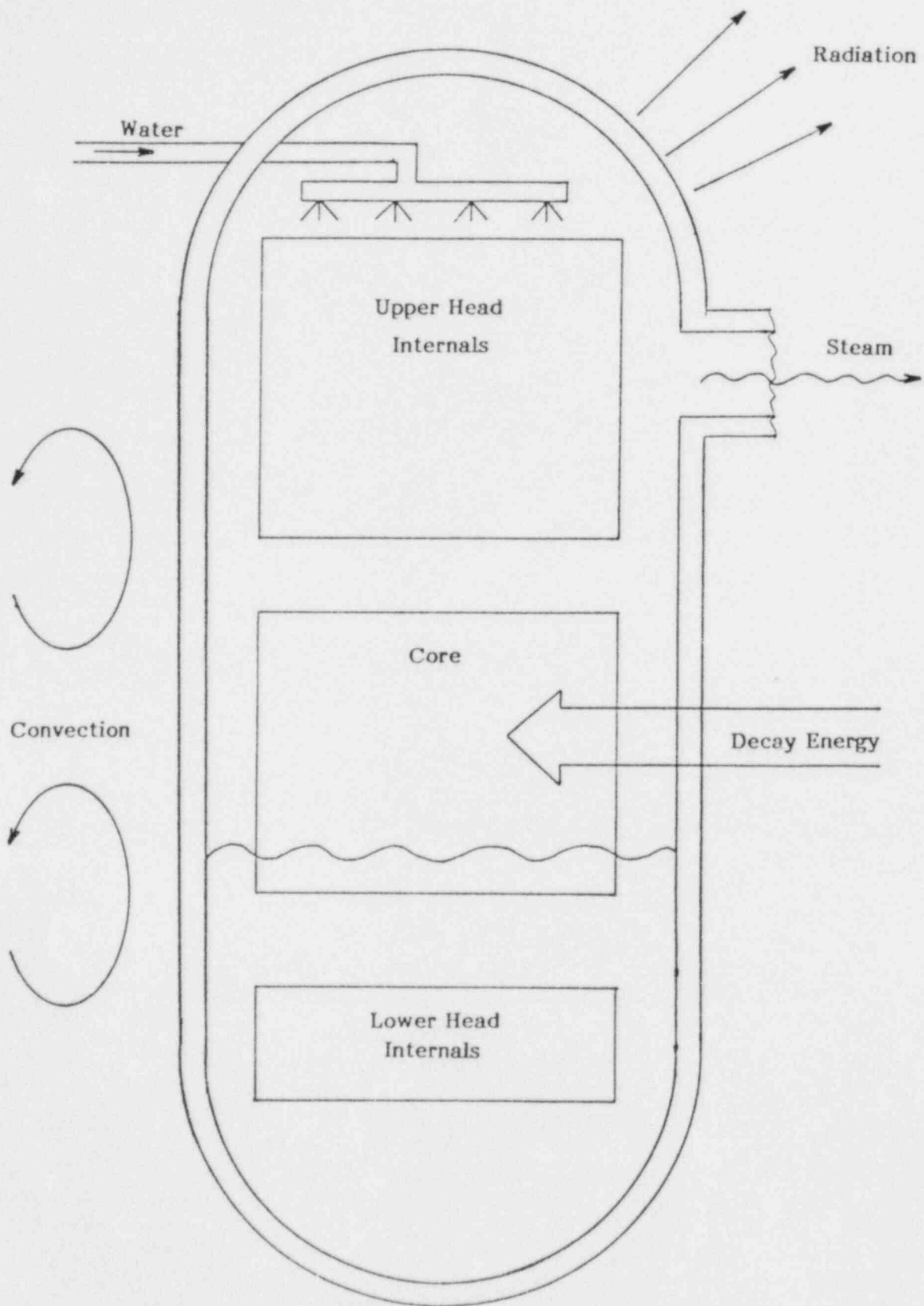


FIGURE 11-7
MAJOR SOURCES AND SINKS OF THERMAL ENERGY

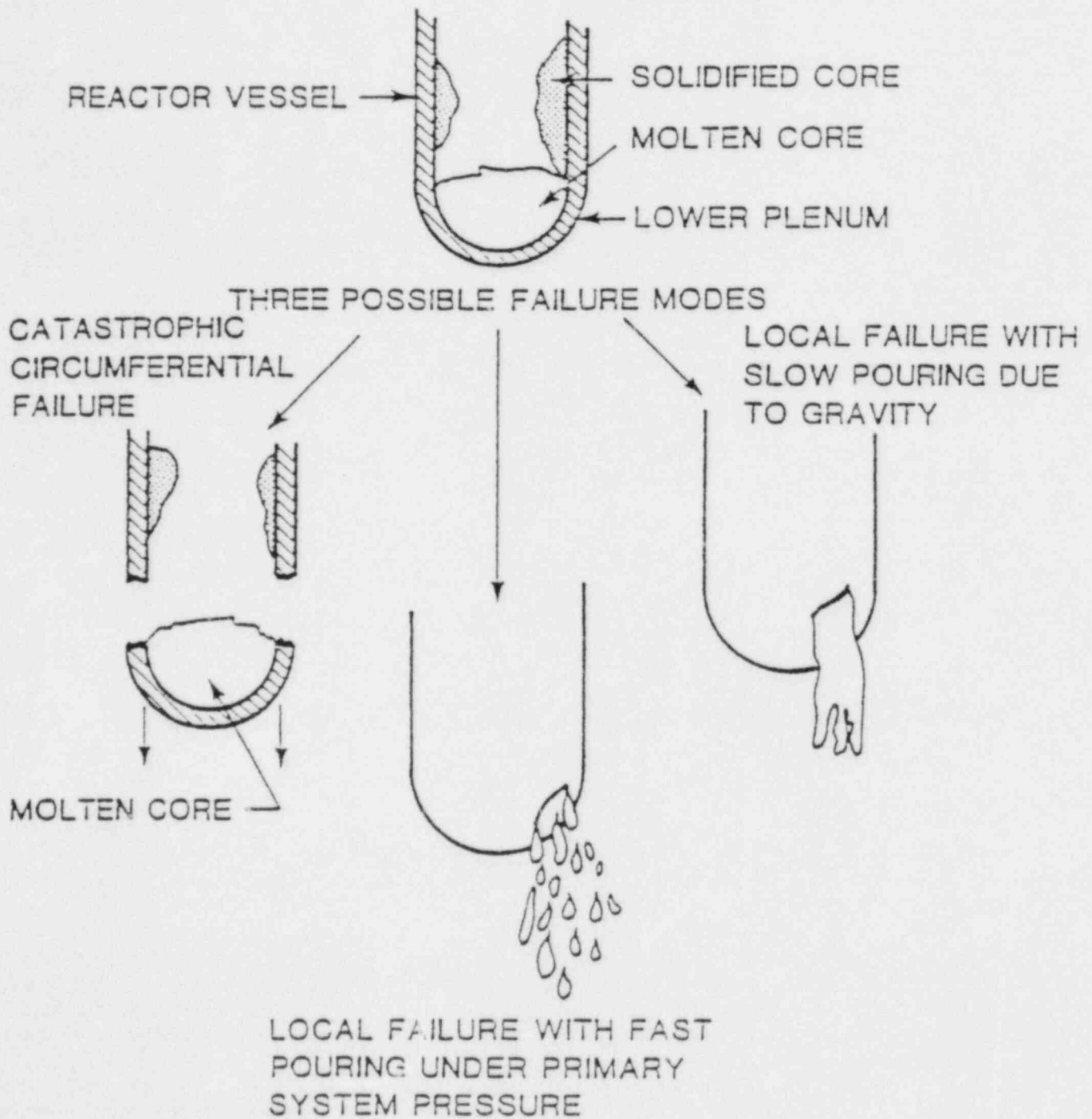


FIGURE 11-8

VARIOUS POSSIBLE MODES OF LOWER PLENUM FAILURE

increase rapidly in size. Such failures might be expected at penetrations in the bottom of the reactor vessel. The PWR reactor vessel has several such penetrations for instrumentation purposes. The BWR reactor vessel has many penetrations in the bottom for the control rod drives. The pressure driving the molten material through a small hole will determine the form the melt upon the cavity floor and the extent of its spread. The possibility that the entire bottom of the vessel will separate from the rest is shown in the left sketch. In this case, the melt would fall into the reactor cavity "en masse".

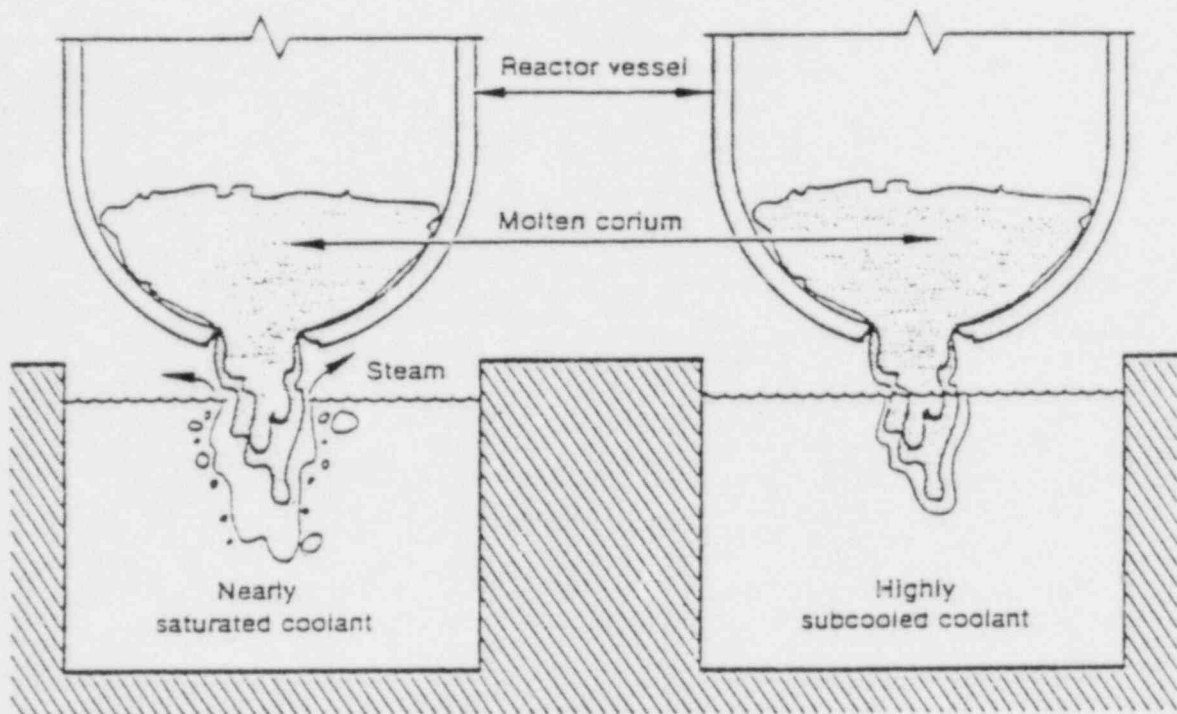
Given that core material enters the reactor cavity, several phenomena must be considered. Interaction with water to produce steam or with concrete to produce a number of reaction products complicates the situation. The core material may move out of the reactor cavity into the main part of the containment. If the core remains within the cavity, it will begin to attack the concrete cavity floor by melting or erosion, generating considerable amounts of noncondensable gases. Coolability and bed leveling will have to be considered, as well as short-term and long-term disengagement of fission products from the mass of material in the cavity.

If there is water in the reactor cavity when the vessel fails, the temperature of this water may be significant as shown in Figure 11-9. Although it may seem paradoxical at first, recent research indicates that a steam explosion is more likely if the water in the reactor cavity is not at or near the saturation temperature. The basis for this conclusion is the need to get a great deal of finely fragmented core material mixed into the water volume in order to produce the large surface area needed to generate steam fast enough to produce a shock wave. (To be considered an explosion, a shock wave must be present. A rapid rise in pressure due to steam generation without a shock wave is denoted a steam pressure spike.) If the cavity water is at saturation temperature, significant amounts of steam will be generated as soon as the first bits of molten core contact the water. This steam will "blanket" the following core material, preventing its contact with liquid water. If the water in the cavity is considerably subcooled, it will take some time to produce steam by the first portion of the core to contact the water. By the time this steam is produced, enough corium may have penetrated the water to provide the required surface area in contact with water.

In the RSS, the probability of containment failure due to a steam explosion upon reactor vessel failure, denoted the containment steam explosion, was estimated to be 0.01. It was admitted that the uncertainty in this value was large. The probability of a containment steam explosion is now considered to be much less than 0.01. Some authorities hold that it is physically impossible. (There is no question as to whether or not steam explosions occur when hot metal falls into water: the existence of such explosions is well documented by experiment. The question is whether an explosion large enough to fail the containment is attainable.)

Whether a steam pressure spike (no shock wave, just a rapid pressure increase) that is generated when the molten core material falls into the reactor cavity will fail the containment depends upon the existing containment pressure and whether sprays or other pressure suppression means are available. There is one scenario where a steam pressure spike is possible even though the reactor cavity is dry when the vessel fails. If the primary system in a PWR remains at high pressure until the vessel fails and if the reactor has accumulators which then discharge, the core and the accumulator water could enter the cavity together.

If the reactor cavity is dry when the vessel fails and remains so, rapid concrete attack by the molten core material is expected. The reactions between corium (uranium dioxide, zirconium, steel, control rod materials, etc.) and concrete are very complex and



Case A:

For nearly saturated coolant, initial molten corium entry will cause rapid, extensive steam formation

Subsequent molten corium entry is effectively vapor blanketed

Intimate liquid-liquid, fuel-coolant contact is avoided

MFCi explosion hazard reduced

Case B:

For highly subcooled coolant, initial molten corium entry results in limited steam production

Subsequent molten corium entry can mix with liquid coolant

Large-scale liquid-liquid, fuel-coolant contact possible

Enhanced MFCi explosion potential

FIGURE 11-9
CONDITION FOR POTENTIAL STEAM EXPLOSIONS

Source: Reilly, Cox, Polkinghorne, et. al. Conceptual Design of a Core Melt Mitigation System for a PWR with an Ice Condenser Containment. DOE, EGG PR-5633.

are poorly understood. While some limited experiments have been carried out, they are difficult to perform and many possible chemical reactions are involved. In view of this, detailed explanation of the processes is not now possible. It is clear that non-condensable gases (hydrogen, carbon monoxide, carbon dioxide) are generated in large quantities from the thermal decomposition of the concrete and the chemical reactions that ensue. In addition to the possibility of hydrogen combustion, the non-condensable gases could eventually fail the containment due to overpressure. The core-concrete reactions are exothermic, which adds to the heat source within the containment.

Hydrogen is of more interest than the other non-condensable gases generated because of its flammability. Hydrogen generated from the core-concrete reaction will add to that generated by the zirconium-water reaction. Hydrogen will also be generated by the radiolysis of water (caused by the gamma radiation due to the decay of fission products), by steam reactions with stainless steel, and by chemical reactions with galvanized (zinc) surfaces and certain coating materials. These sources are small compared to the zirconium-water and core-concrete reactions. In most core melt accident scenarios the amount of hydrogen generated by clad oxidation is not enough to reach the lower flammability limit in large containments assuming homogeneous mixing. (At TMI, more hydrogen was generated than would have been expected in a straightforward core melt because the top of the core was uncovered and reflooded twice.) After the corium has been attacking the basemat for a few hours, however, combustible conditions may occur.

It is evident that the length of time that the hot core material attacks the concrete of the basemat will have a strong effect on the outcome of the accident. It has been postulated that the attack could continue until the basemat is penetrated. However, the reactor originally contained a great deal of water and more would have been added in most sequences by various engineered safety functions. Therefore, it can be argued that sufficient water should be available to cool the core. How much of this water can be contained in the sump and other locations where it is not available to cool the molten core depends upon the specific geometry of the plant in question. Even if water is available in substantial quantities, whether the core can be cooled enough to halt the concrete attack appears to hinge on the dispersal of the core upon exit from the reactor vessel. If it is widely dispersed on the cavity floor, coolability seems assured. If it has fragmented into small particles upon exit from the reactor vessel, then it may be coolable even though it is not widely dispersed. These conclusions assume that some means other than conduction through the containment wall is available for the removal of heat from the containment. If adequate removal of heat from the containment does not occur, the decay heat may eventually boil all the water from the reactor cavity and overpressurization of the containment may occur due to a combination of steam pressure and accumulation of non-condensable gases.

11.4 Relationship Between the Systems Analysis and Accident Process Analysis

The accident begins with a pipe break or other initiator and continues until the containment fails. To determine how the accident will progress, it is necessary to know which of the normal protective and emergency systems of the reactor are available. This information comes from the systems analysis. Each end point on the event tree represents a different combination of systems available to perform the necessary functions.

Figure 11-10 shows the functions required to shut down the reactor safely, as well as, those needed to mitigate the effects of a core melt:

RT	- Reaction Termination
ECC	- Emergency Core Cooling
CI	- Containment Isolation
PAHR	- Post-Accident Heat Removal
PARR	- Post-Accident Radioactivity Removal

Table 11-3 lists examples of some of the systems used to carry out some of these functions.

The relationship between the systems analysis and the accident process analysis goes both ways. The accident process analysis needs to know which systems are operable and which are failed. The event tree analysis depends upon the accident process analysis to determine the plant damage states in physical terms and to indicate the timing of the events. That is, the event tree describes, for each end point, the plant state in terms of systems that are operable and systems that are inoperable. The accident process analysis is required to go beyond this, to be able to state conclusions such as: the core is uncovered from M minutes to N minutes and appreciable damage to the clad is expected before reflooding; or, the core is uncovered at R minutes, melting begins at S minutes, and reactor vessel is expected to fail at T minutes. This information is needed, in turn, to support analysis of the likelihood of the recovery of failed systems in time to prevent and/or mitigate the postulated accidents.

Simple accident analyses are often performed implicitly during the event tree analysis. For example, an analyst examining an event tree notes that all injection to the core ceases after a certain time. He concludes at once that core melt is inevitable for this sequence. Likewise, if all heat rejection capacity from the containment is lost, then eventual containment failure may be assumed. However, these simple conclusions can be reached only in a small portion of the sequences of interest. Take the case where heat transfer capability from the containment has failed but in which the core is being kept covered by the recirculation of water from the sump. Whether or not this recirculation is likely to continue successfully after containment breach depends on factors like the temperature of the sump water, the water level, and the net suction requirements of the pump, and cannot be determined without a detailed analysis. Such an analysis is needed to discover how much time is available to restore the ability to transfer heat from the containment, and this time is required to calculate the probability of recovery.

Even in cases such as failure to scram or loss of all injection following a LOCA where the core melt begins relatively early, the timing results are important in determining how likely the operator is to take the actions required to mitigate the accident. Thus, neither the outcome, in physical terms, nor the final probability of the sequence can be computed until the accident process analysis is complete. At this point, it may seem that a Level 1 PRA could never be quantified since the timing information would not be available. The solution to this is that timing from other PRAs for similar reactors is used for sequences that are as close as possible to those in question.

The relationship of the accident process analysis to the event tree analysis and to the fission product release and transport analysis and to the offsite consequence analysis is illustrated in Figure 11-11. For the simplified example shown, there is only the initiator, Event A, and three systems, B, C, and D. System C is dependent on System B, so the failure of System B implies the failure of System C. (This dependency is common where the same hardware is used for injection and recirculation: failure of the pumps or valves

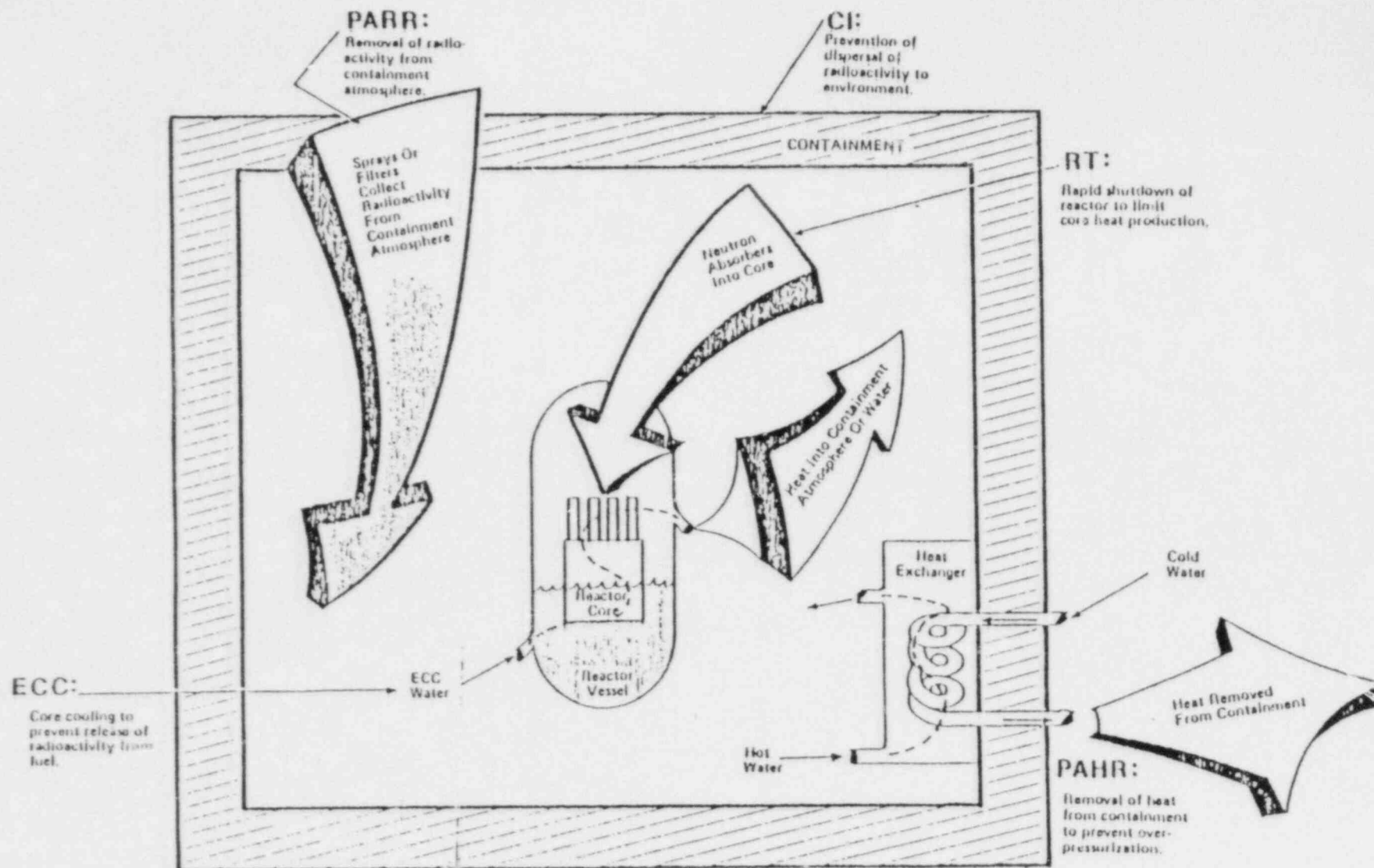


FIGURE 11-10
 LIGHT WATER REACTOR LOSS OF COOLANT ACCIDENT (LOCA)
 ENGINEERED SAFETY SYSTEM (ESF) FUNCTIONS

TABLE 11-3
EXAMPLES OF ENGINEERED SAFETY FEATURES

- Emergency Core Cooling (ECC)
 - High Pressure Injection
 - Low Pressure Injection
 - Accumulators

- Post-Accident Radioactivity Removal (PARR)
 - PWR - Containment Spray
 - BWR - Suppression Pool and Filter System

- Post-Accident Heat Removal (PAHR)
 - PWR - Recirculation Through Heat Exchanger from the Sump
 - BWR - Recirculation Through Heat Exchanger from the Suppression Pool

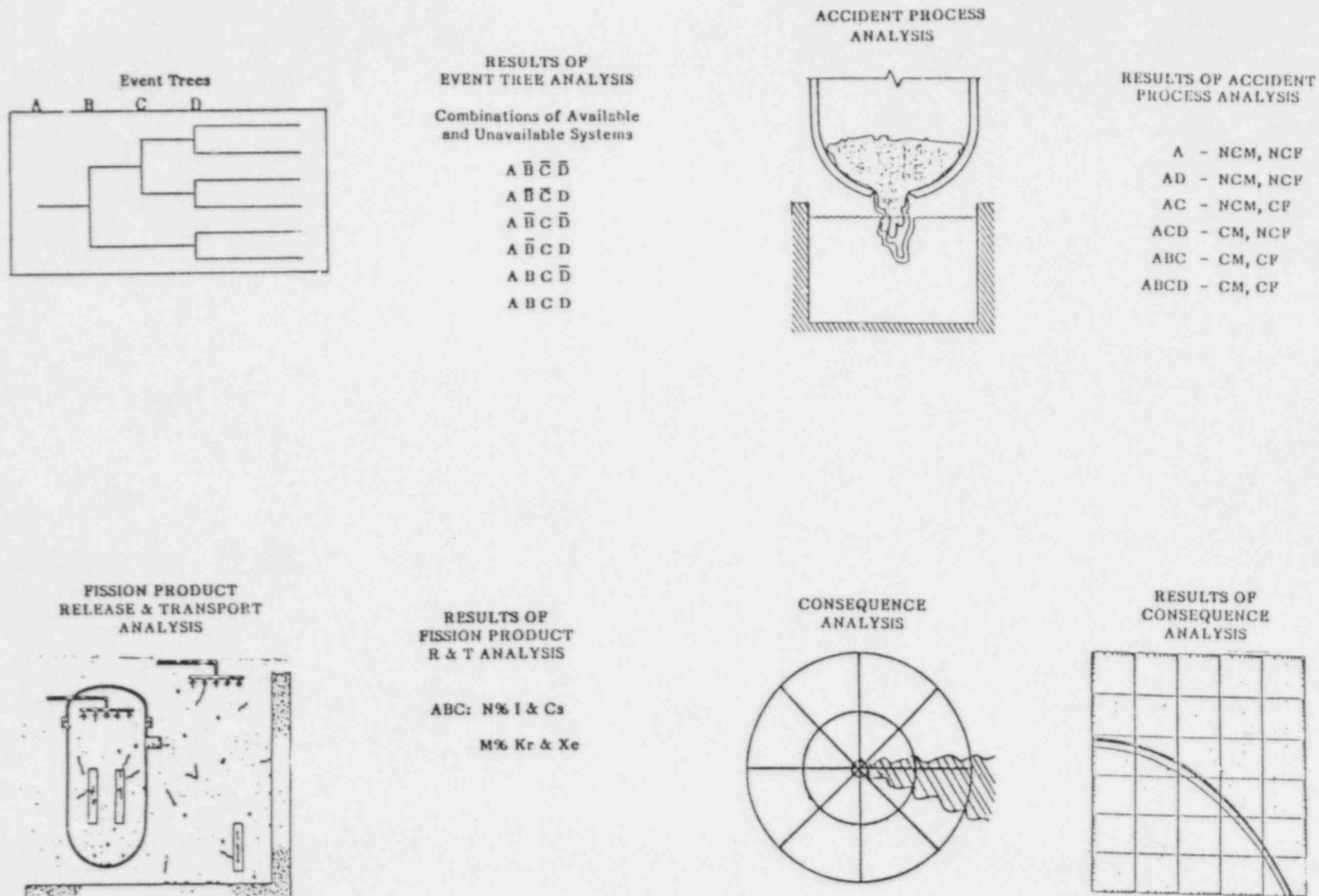


FIGURE 11-11
RELATIONSHIP OF DIFFERENT PORTIONS OF A PRA

in the injection mode means that recirculation is very unlikely to succeed.) Thus, in this example, there are only six possible end states, sequences, or combinations of operable and failed systems. The accident process analysis determines which sequences lead to core damage, which to containment failure, and which to both. The analysis also provides the times for important events and other information. The results of the accident process analysis form part of the input for the fission product release and transport analysis which determines the amounts released to the environment. This information is used in turn by the consequence analysis to determine such offsite results as estimates of early fatalities or latent cancer incidence.

Figure 11-12 provides more detail on how the various portions of the model interrelate. To begin the accident process analysis, information is needed about the initial conditions in the core and the reactor coolant system as well as the boundary conditions for the reactor coolant system and the containment. The information should include any previous history of thermal shock and fatigue cycles which may affect the strength and response of the systems. The blowdown and injection phases of the accident process analysis receive little attention in descriptions of the PRA process since they are similar to the analyses performed for design basis accidents. Since the design basis approach does not consider degraded core conditions, the following portions of the analysis are encountered only in the probabilistic approach. Core degradation and melting, reactor vessel failure, and core-containment interactions have been discussed in the preceding sections. The next section discusses the response of the containment, including failure modes. Fission Product Release and Transport is the next topic in this course.

11.5 Containment Considerations

As mentioned earlier, the RSS showed that the risk to the offsite population was dominated by those low probability but high consequence events in which the core melts and the containment fails. An essential part of the accident analysis is consideration of the containment. Not only are the increases in internal pressure and temperature of interest, but the amount of hydrogen and other non-condensibles must be tracked and the inventory of water, in liquid and vapor phases, must be accounted for. Finally, the behavior of the fission products in the containment determines how much radioactive material will be available for release to the environment if the containment fails.

Various potential containment failure modes are shown in Table 11-4. Steam explosions have already been discussed. Even if they are considered to be possible, the relative probability of this failure mode is admitted to be small. If there is no heat removal from the containment, some sort of overpressure failure is the most likely mode for most containment designs. The ultimate pressure capability of the containment may be exceeded by an excess of steam (often due to failure of the steam suppression function), non-condensable gases, the ignition of hydrogen, or some combination of these sources. Not all combinations of these sources are possible. For example, a very high steam partial pressure will suppress hydrogen combustion.

Exceeding the temperature limits of the containment was not considered a potential containment failure mode in the RSS. Recent work indicates that it may be important for the smaller pressure suppression containments. In these cases, the drywell boundary is relatively close to the reactor vessel so that radioactive transfer is particularly effective in heating the steel pressure vessel. Failure is expected to be due to seal degradation at penetrations.

Isolation failures did not receive much attention in the RSS and were assigned a relatively low probability. Some recent reconsiderations of earlier work that showed

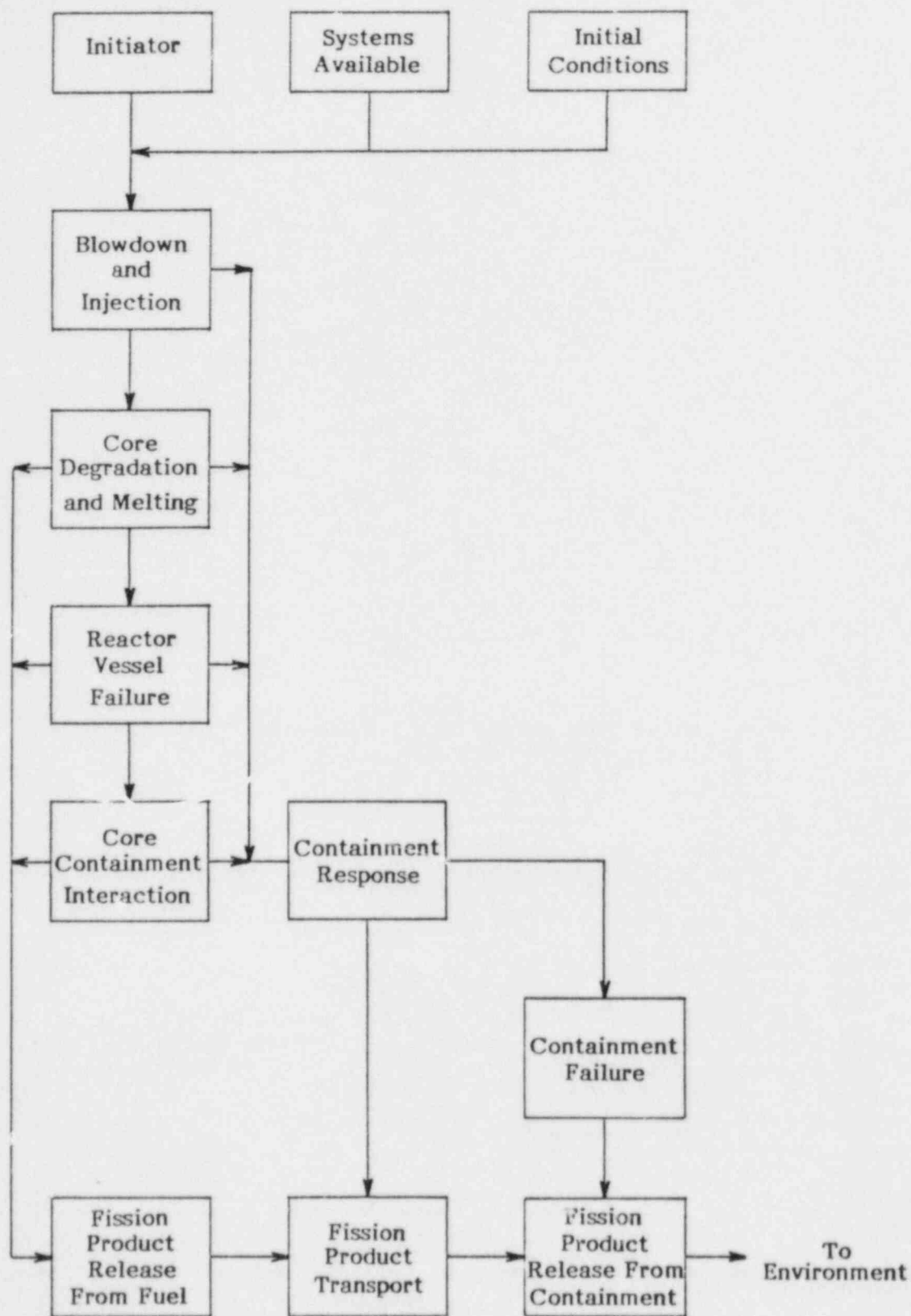


FIGURE 11-12
STEPS IN THE ACCIDENT PROCESS ANALYSIS

TABLE 11-4
CONTAINMENT FAILURE MODES

- Steam Explosion
- Overpressurization Due To Steam Generation
- Overpressure Due To Noncondensable Gases
- Hydrogen Explosion
- Overtemperature Failure
- Containment Isolation Failure
- Basemat Meltthrough

overpressurization or hydrogen combustion failures are now indicating that the containment may not fail for these sequences as first thought. In some cases, this is due to new calculations which predict less generation of non-condensable gases and in others it is due to the installation of igniters which will prevent the global ignition of hydrogen. If these failure modes, which previously dominated risk, are eliminated or greatly reduced in relative probability, then the isolation failure mode becomes of greater importance.

In the RSS it was assumed that the debris bed was never coolable, so that if the containment did not fail by steam explosion, overpressurization, or hydrogen combustion, it was assumed that the containment would be breached by continued concrete attack, i.e., the corium would melt through the thick basemat and allow the molten core to escape into the rock or soil underneath. Compared to the other failure modes in which the hole in the containment is above ground, the basemat meltthrough releases very few fission products to the atmosphere so the immediate offsite consequences are relatively slight. It is now considered more likely that the debris bed will be coolable so that the concrete attack will be halted before the basemat is penetrated.

For basemat meltthrough, the hole location is known and the size is not very important. For the above ground failures, neither the location nor the size of the breach can be predicted with any accuracy. In the past, hole areas between 0.1 and 10 square feet have typically been assumed for calculations. The size of the hole has a large effect on the rate of depressurization and can have a significant effect on the amount of fission products released to the environment. It has been suggested that containment failure will take the form of numerous small fissures. If this is the case, the escape of all but the very smallest particles might be severely retarded.

Reactor containments are divided into two types: dry and pressure suppression. A dry containment is one that does not contain a reservoir of water to suppress steam; it relies on the size of the structure, sprays, and fan coolers to accommodate any steam release that may occur. Most PWR containments are dry, often denoted large, dry containments because of their size (typically 1 to 2 million cubic feet). Pressure suppression containments come in two major forms. All BWR containments include a large pool of liquid water. The containment is designed so that any steam from the safety/relief valves or from a broken reactor coolant pipe inside containment is directed into this suppression pool where it is condensed. The term pressure suppression containment is often taken to apply only to these BWR designs. A few PWRs have pressure suppression containments: in these, the water inventory is in the solid form and they are referred to as ice condenser containments. Because of the steam condensing features, the volume of a pressure suppression containment is smaller than that for a dry containment.

Major offsite consequences occur only if a substantial amount of radioactivity is released from the containment. The design of the containment is such that it is seriously challenged only by accidents in which the core melts and the primary pressure boundary fails. The containment can be bypassed by isolation failures or by interfacing system failures (Event V). Except for Event V, every sequence with major offsite consequences found in PRAs so far has involved containment failure.

To estimate when the failure of this last barrier to the radionuclide release will occur and how much material will be available for dispersion in the environment, it is necessary to keep track of all the mass and energy additions to and removals from the containment starting at the beginning of the accident. The thermal storage capacity of all the large masses of steel and concrete must be considered, as well as the effects of engineered safety features such as containment sprays. Table 11-5 lists some of the phenomena

TABLE 11-5
SOME OF THE PHENOMENA THAT MUST BE INCLUDED IN A
CORE-MELT CONTAINMENT ANALYSIS

- Gas Composition (steam, oxygen, combustible gases, and inert gases)
- Condensing Heat-Transfer Coefficients to Structures
- Temperature Profiles in Structures
- Sprays, Coolers, and Suppression Systems
- Hydrogen Combustion
- Heat-Source Redistribution
- Conditions Relevant to Steam Explosion

included in a complete analysis. The results of the containment analysis are the variation with time of such factors as containment atmosphere temperature and pressure, sump or pool level and temperature, and hydrogen concentration. The containment analysis continues until the pressure or temperature limits of the containment are exceeded or until it is clear that they will not be exceeded. The general features of a compartment in a containment model are shown in Figure 11-13. Each volume has a vapor and a liquid region, with mass and energy transfer between them as well as with the regions of neighboring compartments. Heat transfer to conductors and leakage are included.

11.6 Accident Process Analysis Models

The accident is usually analyzed in parts because different computational tools are required for each portion. Until the core begins to deform, a detailed thermal-hydraulic model can be used. Sometimes variations of the models or unrealistic assumptions are required to treat reflood periods since the blowdown codes are often unable to model the injection of cold water into the hot core. The degradation and melting of the core is often handled by a separate code. Specific computer models may be used to describe the behavior of the fuel rods and the containment. Table 11-6 summarizes the types of computer models utilized and Table 11-7 lists the types of information required for a complete analysis.

While there are many codes which treat various portions of the accident, the MARCH/CORRAL package is the only one which treats most of the phenomena involved and which has received widespread use in the U.S. Table 11-8 lists the features of these codes and Figure 11-14 shows the interrelationship of the submodels in the two programs. The tasks of the various submodels are explained in Figure 11-15, which shows the required information flows. CORRAL is primarily concerned with the release, transport, and removal of fission products and will be discussed further in the following topic.

MARCH was first developed for the RSS in the early 1970's by Battelle and has been improved steadily since that time. It can model the entire accident progression although it is also capable of accepting blowdown information from another calculation if a more detailed thermal-hydraulic code is being used to model that portion of the accident. MARCH runs relatively fast and has been used to evaluate proposed mitigation and prevention systems as well as for accident evaluation. Currently perceived inadequacies in MARCH are listed in Table 11-9. Some of these shortcomings are now being addressed. In other areas there is such a lack of basic experimental and theoretical evidence that an improved model cannot be agreed upon. In some areas this is not as great a drawback as it sounds due to the fairly narrow limits placed on the process in question by gross thermal constraints. The NRC is developing a new integrated code package denoted MELCOR, which will replace not only MARCH2 (the current version of MARCH), but CORRAL/MATADOR (for fission product transport) and CRAC2 (for offsite consequence analysis).

Figures 11-16 through 11-21 present MARCH results from a typical accident where a small LOCA is the initiator and the core melts because the emergency core coolant system fails to function. The water level in the reactor vessel reaches the top of the core by 80 minutes, and core melt follows about half an hour later (see Figures 11-16 and 11-17). The containment temperature and pressure increases that occur when the lower head fails and the core falls into the flooded reactor cavity are swiftly brought under control by the containment sprays which are operating in this sequence (see Figures 11-19 and 11-20). Figure 11-21 shows that the hydrogen concentration reaches the lower flammability limit shortly after the core-concrete interaction begins.

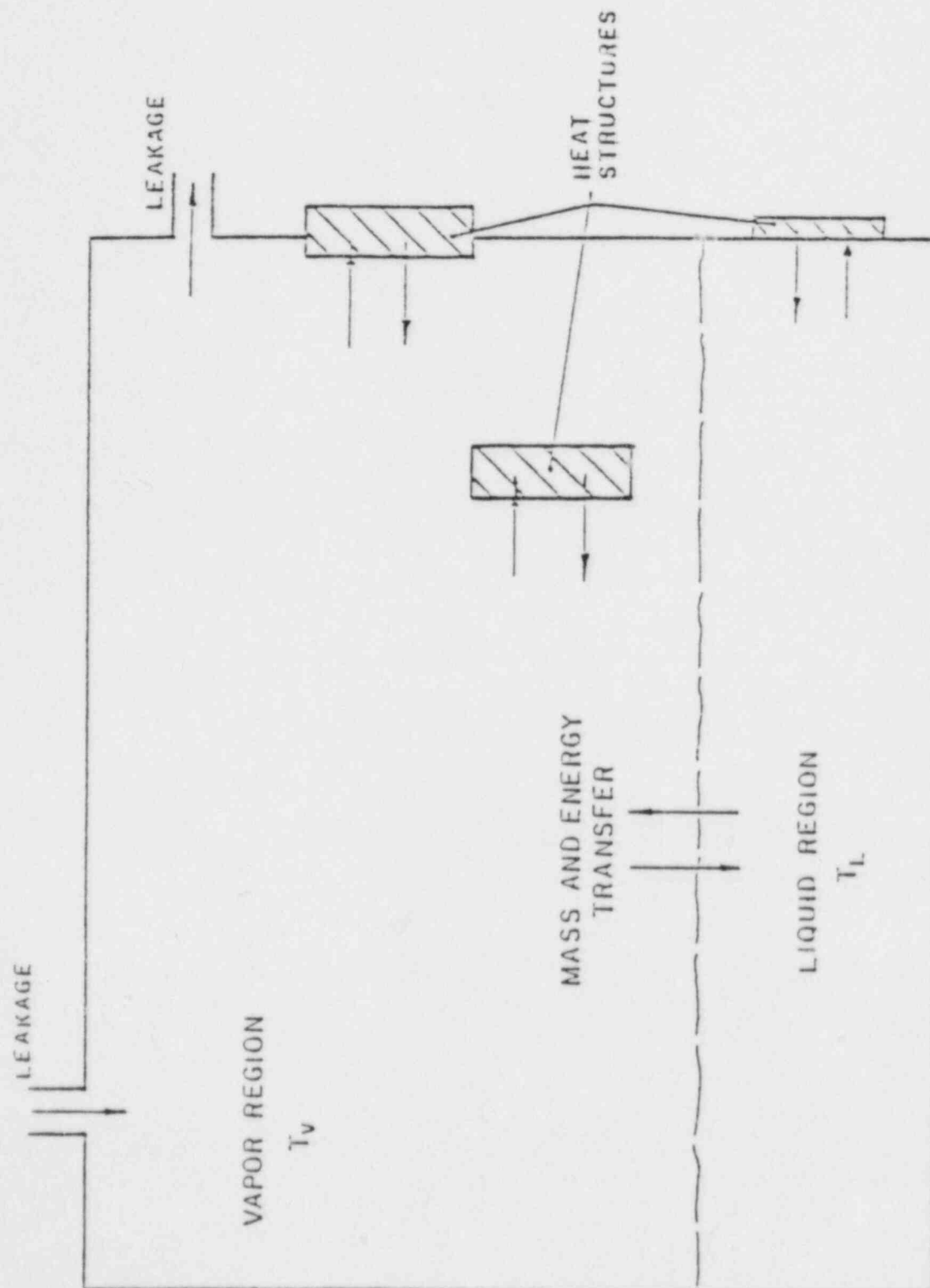


FIGURE 11-13
GENERAL COMPARTMENT FEATURES

TABLE 11-6
SUMMARY OF TYPES OF COMPUTER MODELS
UTILIZED IN ACCIDENT PROCESS ANALYSIS

- System Transient
- Subchannel Thermal-Hydraulics
- Blowdown, Refill, Reflood, Heatup
- Core Wide Hydraulics (optional)
- Neutronics
- Fuel Pin Thermal
- Containment
- Core Degradation and Melting
- Reactor Vessel Failure
- Core Entry into Containment
- Core-Concrete Interaction
- Steam Explosion
- Hydrogen Combustion

TABLE 11-7
TYPICAL DATA REQUIRED TO MODEL CORE MELT AND CONTAINMENT RESPONSE

<u>System or Component</u>	<u>Parameters Included</u>
General Containment Data	Total volume; number of compartments; volume and dimensions of compartments; initial pressure, temperature and humidity.
Heat Sink	Number and compartment location of heat sinks, materials in each sink including density, heat capacity, and thermal conductivity; heat transfer area, thickness, and heat transfer coefficient.
Ice Condenser (if applicable)	Mass of ice; temperature of ice; temperatures of water drained from ice bed; temperature of gas leaving ice bed.
Suppression Pool (if applicable)	Mass of water; temperature of water; water volume; air volume.
Containment Floor (used for concrete attack)	Thickness, density, thermal conductivity, temperature, and composition of concrete basemat.
ECC Tanks	Pressure, temperature, and water mass of accumulators and/or upper head injection tanks.
ECC Pumps	Start time, nominal flow rate, nominal and shutoff pressure of all pumps, including high pressure injection, safety injection, low head pumps, and any additional pumps; NPSH, maximum temperature to avoid pump cavitation.
Heat Exchangers	Heat exchanger capacity; primary and secondary flow rates and temperatures for ECC and containment spray heat exchangers.
ESF Containment Coolers (if applicable)	Number and location of coolers; air-flow rate and inlet temperature; secondary flow rate and inlet temperature.
ESF Containment Spray	Flow rate, temperature, and spray-drop diameter of containment spray system.

TABLE 11-7 (continued)

<u>System or Component</u>	<u>Parameters Included</u>
Auxiliary Feedwater (if applicable)	Flow, temperature, and start time of auxiliary feedwater pumps.
Water Supply Parameters	Amount of water in condensate storage tank; amount of water in RWST; fractional value of RWST to start recirculation of ECC and containment sprays; minimum sump volume to avoid cavitation.
Core	Initial thermal power; total number of lattice positions in core; total number of fuel rods in core; active fuel height, liquid level; mass of UO_2 , Zircaloy, and miscellaneous metal; fuel rod diameter; cladding thickness; density, conductivity, and heat capacity of core material; peaking factors, burnup.
Vessel	Core diameter; flow area; cross-sectional area; mass, heat capacity, temperature, and heat transfer area of internal structures; mass, diameter, and thickness of bottom head.
Primary System	Volume of primary system; initial primary steam volume; pressure; safety relief valve pressure setpoint; and rated capacity.
Steam Generator (if applicable)	Initial mass of water in steam generator; volume of steam generator; setpoint of secondary steam generator relief valve.

TABLE 11-8
MARCH/CORRAL CODE PACKAGE

- MARCH - Thermal-hydraulic behavior of meltdown accident
Response to initiating event
Fuel melting within core region
Pressure vessel attack by molten fuel
Boil-off of water in reactor cavity
Concrete penetration by molten fuel
Containment pressure-temperature history
- CORRAL - Radionuclide transport and deposition in containment
- Time-dependent release of radionuclides to the environment

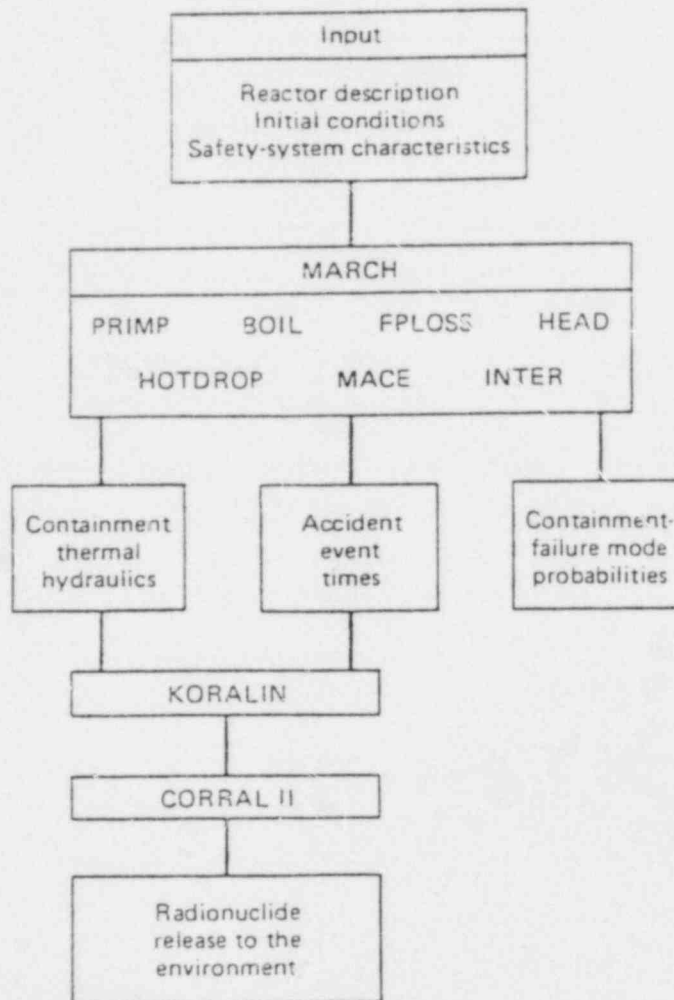


FIGURE 11-14
OVERALL RELATIONSHIP BETWEEN MARCH AND CORRAL

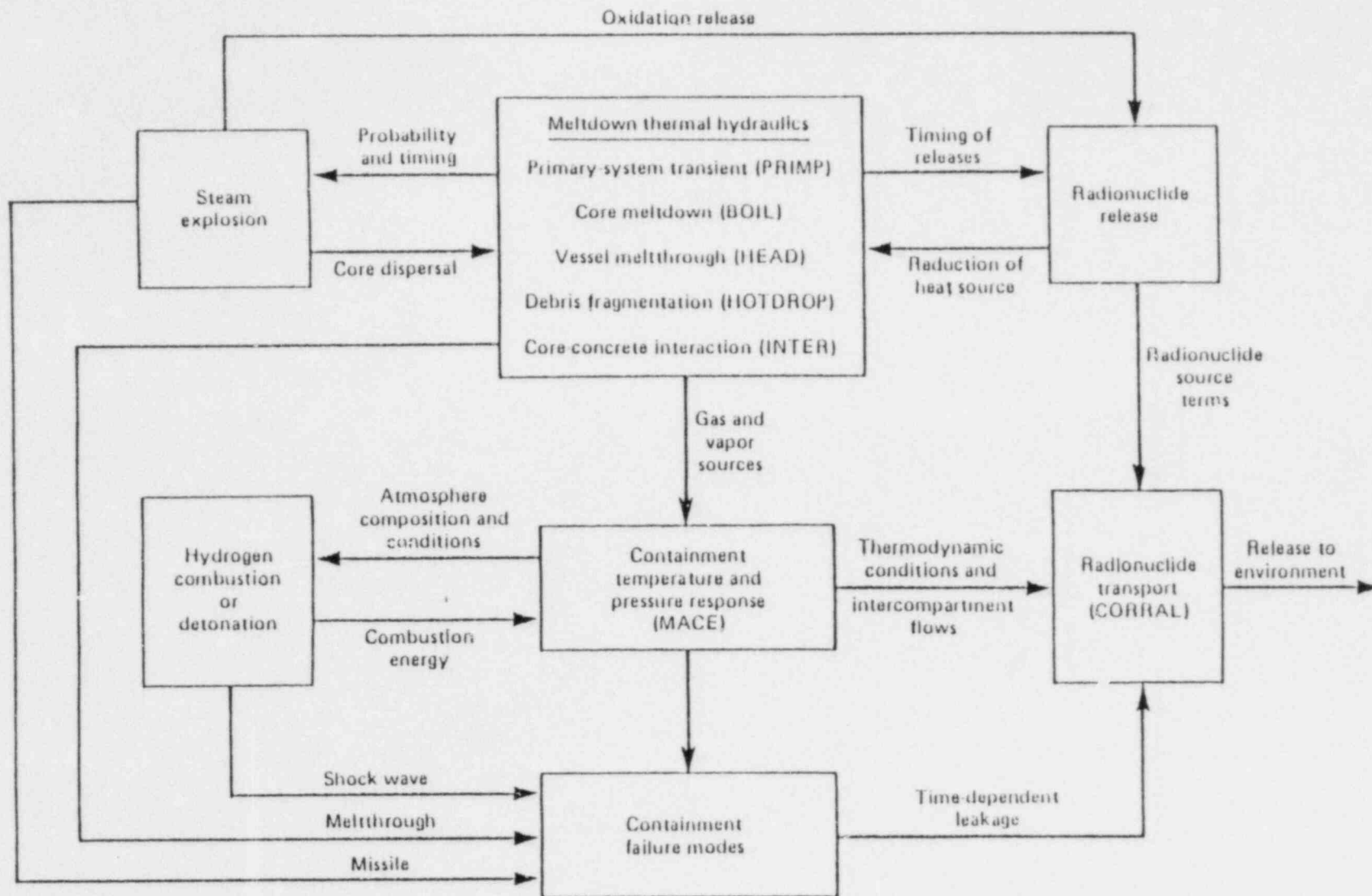


FIGURE 11-15
SUBROUTINE FLOW IN MARCH AND CORRAL

TABLE 11-9
MARCH CODE INADEQUACIES

- Simplistic Modeling of Phenomena
- Not Modeling Various Phenomena
- Not Modeling RCS Components
- Cladding Deformation No Rupture Modeled
- Core Debris Modeled as a Composite of Spheres
- Occurrence of Steam Explosion Inevitably Yields Containment Failure

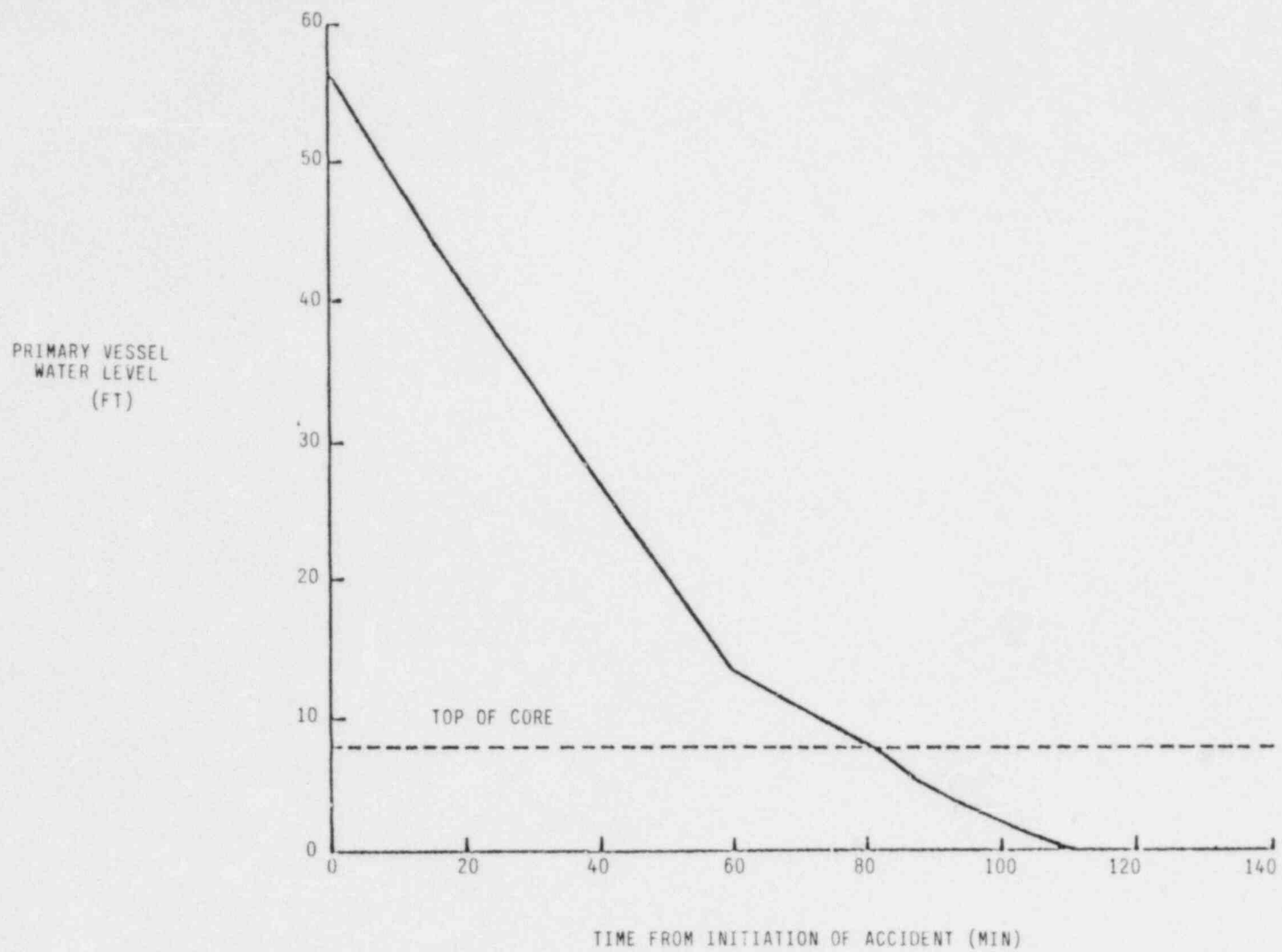


FIGURE 11-16
PRIMARY VESSEL WATER LEVEL-SMALL LOCA (0.75 IN) WITH LOSS OF ECC

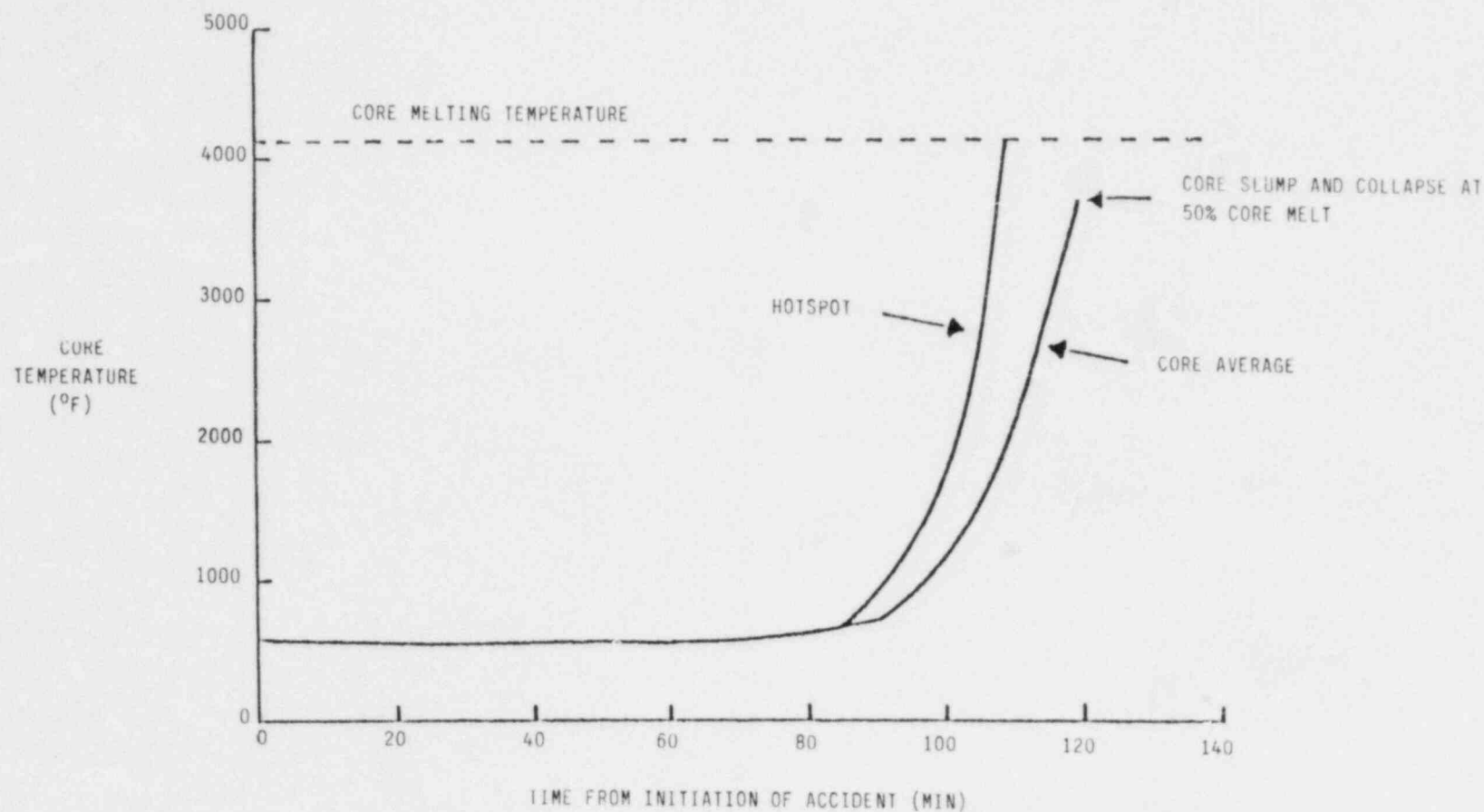


FIGURE 11-17
CORE AVERAGE AND CORE HOTSPOT TEMPERATURES-
SMALL LOCA (0.75IN) WITH LOSS OF ECC

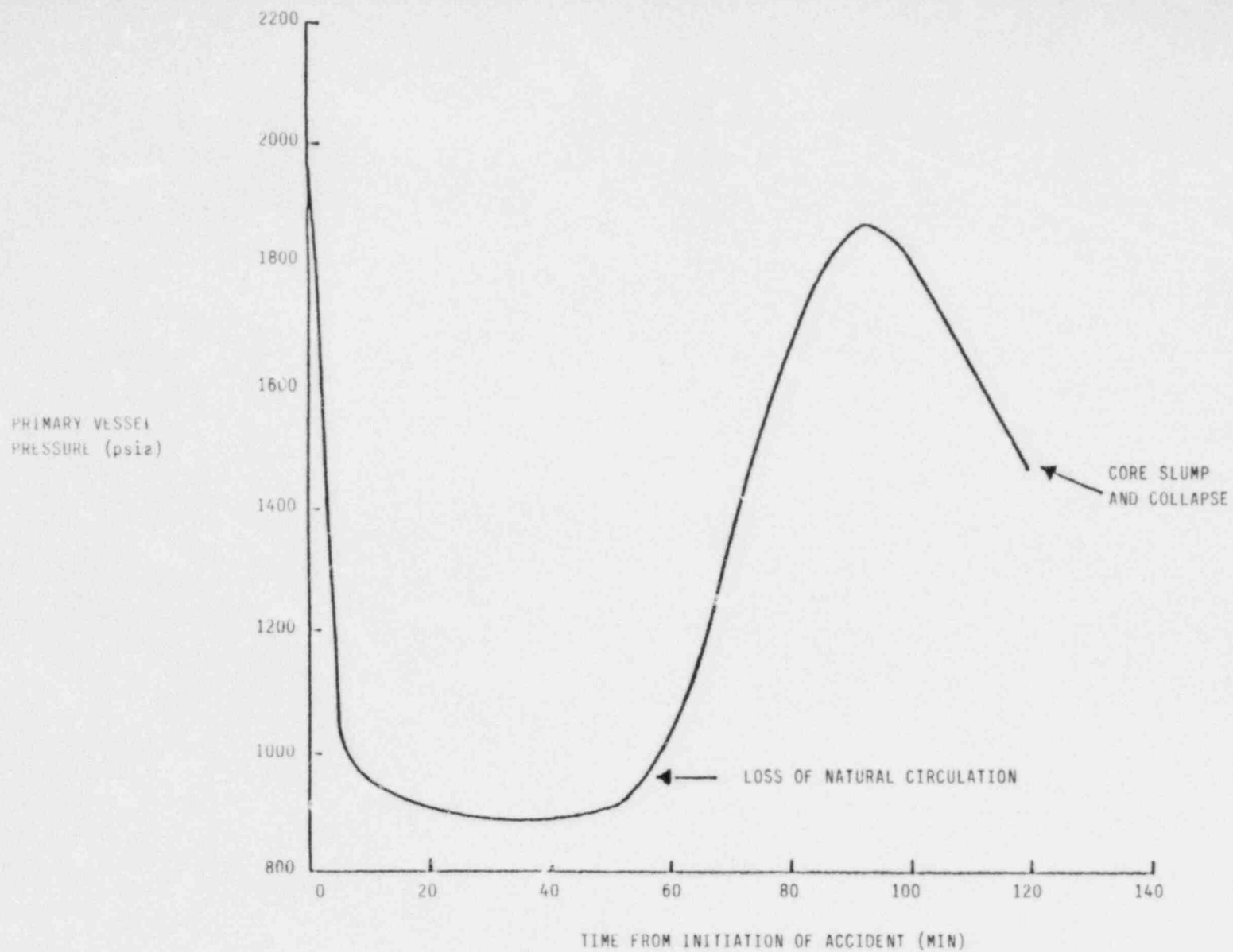


FIGURE 11-18
PRIMARY VESSEL PRESSURE-SMALL LOCA (0.75 IN) WITH LOSS OF ECC

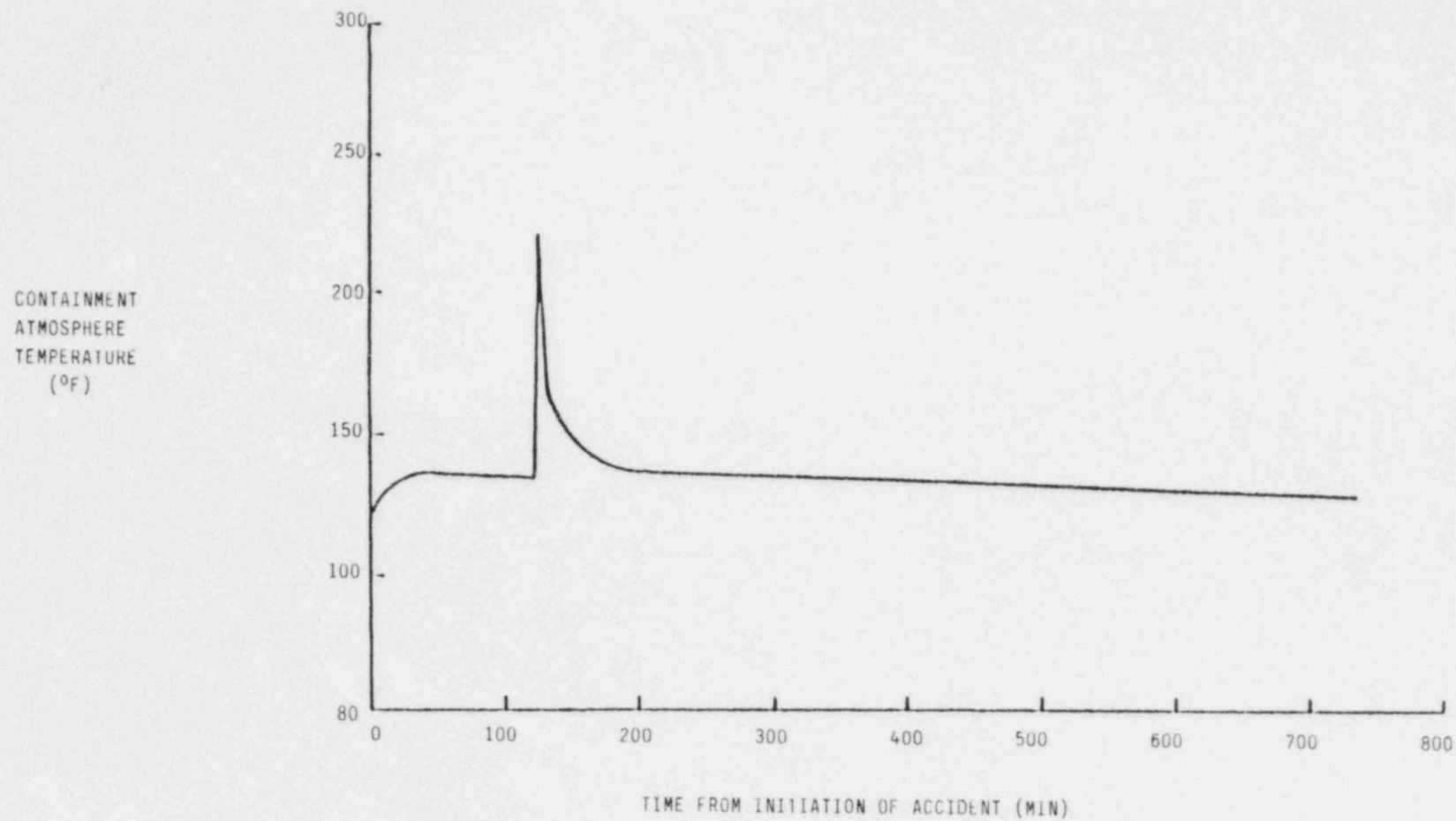


FIGURE 11-19
CONTAINMENT ATMOSPHERE TEMPERATURE-SMALL LOCA (0.75 IN) WITH LOSS OF ECC

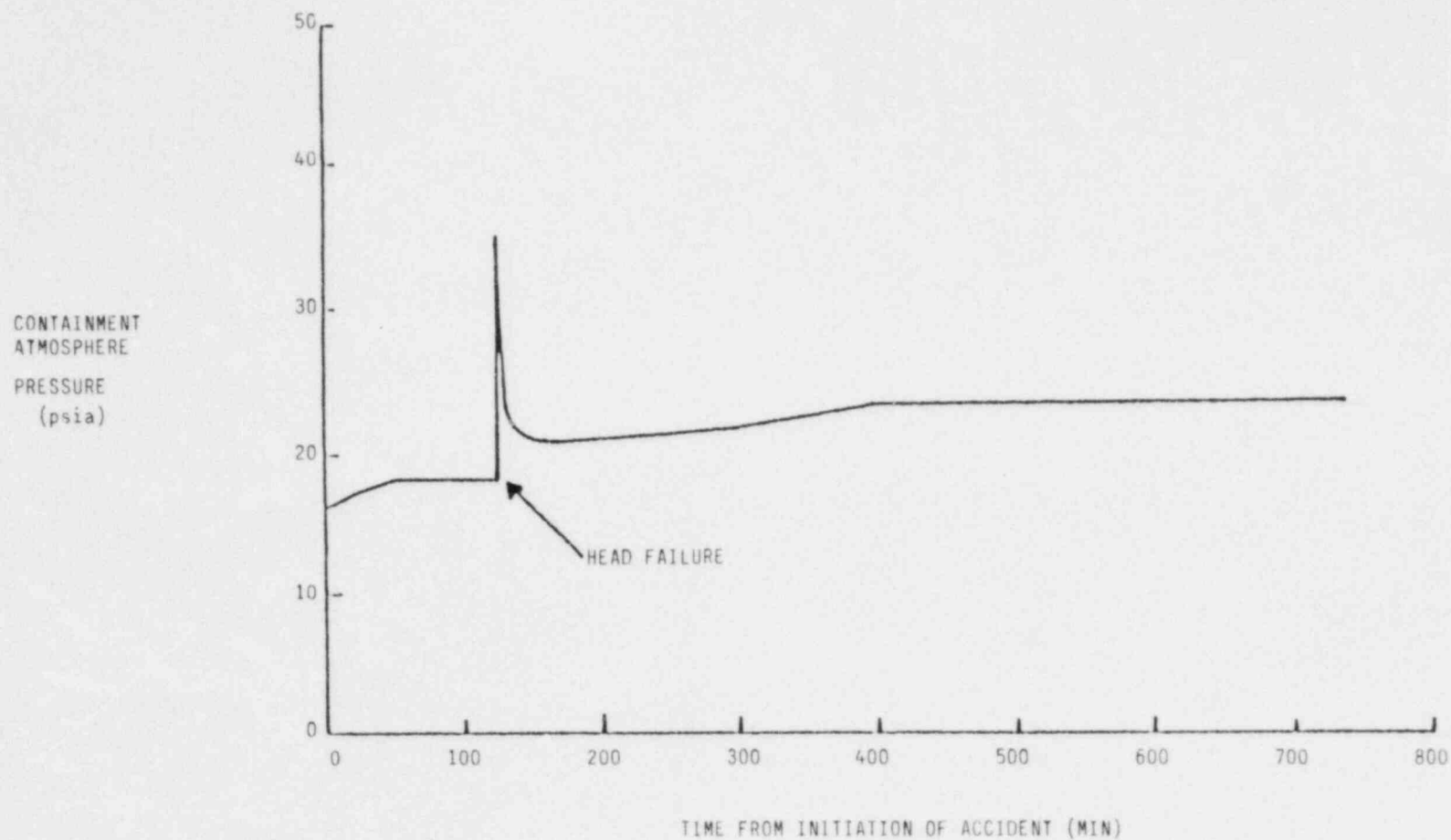


FIGURE 11-20
CONTAINMENT ATMOSPHERE PRESSURE-SMALL LOCA (0.75 IN) WITH LOSS OF ECC

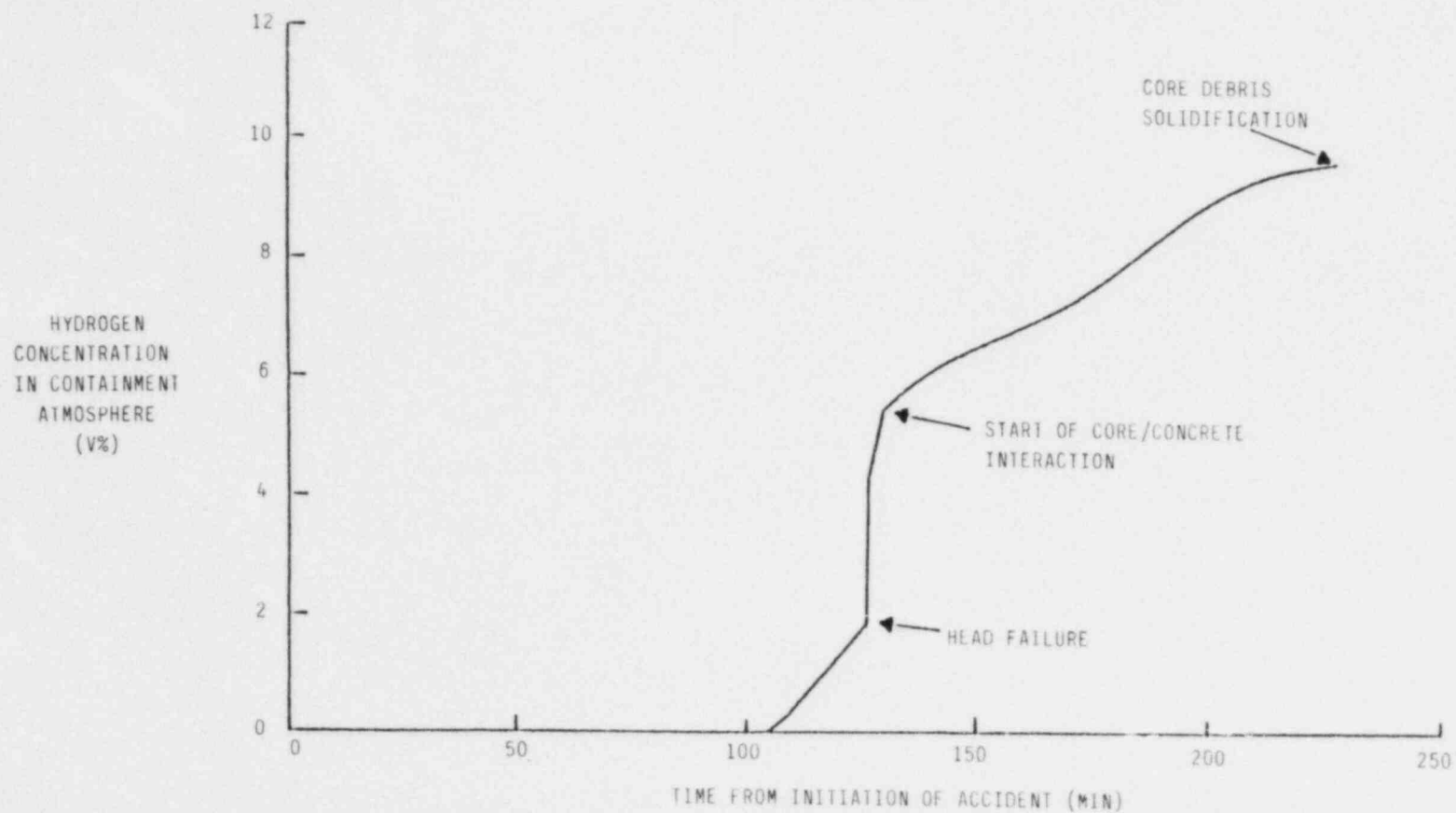


FIGURE 11-21
HYDROGEN CONCENTRATION IN CONTAINMENT ATMOSPHERE-
SMALL LOCA (0.75 IN) WITH LOSS OF ECC

11.7 Summary

The accident process analysis translates the combination of system failures known as an accident sequence into an estimate of the time and extent of physical damage to the plant. The event tree analysis delineates the various sequences of system failures and plant challenges. Knowledge of the accident processes is required to determine whether core melt, containment failure, or both are inevitable, and to estimate the timing of the important events for these sequences. By taking the thermal and material properties of the core, reactor vessel, and internals into account, by calculating the magnitude of heat flows and steam production, and by related considerations, the accident process analysis is able to provide reasonable and consistent estimates of plant damage. Whether or not the core melts is of primary interest, other results from the accident process analysis are often used. For example, the time to the onset of cladding failure or to the beginning of core melt is useful in computing the probability of operator actions to mitigate the accident. The time to containment failure indicates how much time might be available to evacuate the area surrounding the reactor site.

Although portions of the accident process cannot be predicted in detail, overall heat balances provide definite bounds on the times for certain significant events such as the beginning of clad deformation or the failure of the reactor vessel. Since the heat sources and sinks for the vessel and core are well-known, there is little question that these bounds are reasonable. In other areas such as the rate at which non-condensable gases are generated during the core attack of the concrete basemat, the results of the accident process analysis are more open to question.

Despite questions regarding their absolute accuracy, the results of accident process analysis are required to complete the accident sequence delineation and to supply input data for the fission product transport and offsite consequence analyses.

TOPIC 12

FISSION PRODUCT TRANSPORT AND RELEASE

12. FISSION PRODUCT TRANSPORT AND RELEASE

12.1 Introduction and Overview

The consideration of the degradation of the reactor core and its effects consists of two parts. The portion denoted Accident Processes, which has just been discussed, treats the changes in the physical and chemical state of the core as well as the flows, pressures, and temperatures that occur in the reactor vessel, coolant system, and containment. The second part is concerned with the spread of the radioactive material which was initially safely contained within the fuel rods. The fission products comprise almost all of this material and form only a very small fraction of the total mass in the system. While the fission products produce the heat which drives the core degradation and melting processes, the fission products that escape the core exert a negligible influence on the temperatures and flows in the system which control the form and distribution of the radionuclides. To make the calculations as easy as possible therefore, the accident process analysis is done first. These results are used in a second analysis to determine the form and location of the radionuclides during the course of the accident.

The radionuclides which escape from the fuel rods are of interest because it is their release from the containment constitutes a risk to the general public. There are numerous measures of the risk due to a nuclear power plant. The core melt frequency is the only risk measure which does not require the computation of the amount of radioactivity released. The Three Mile Island accident demonstrated that a core degradation accident in which a minimal amount of radiation is released is still of great concern to the public. Nonetheless, only the release of substantial amounts of radioactive material will cause adverse health consequences offsite. Therefore the computation of the amount of radioactivity expected to be released from the important hypothetical accidents is required for a complete risk analysis.

The paths that the radionuclides take from their original locations in the fuel rods to the outside atmosphere are diverse and complex. Changes in physical and chemical form may occur along the way. Radioactive decay may change the element involved during transport. Some of the fission products are elements not often encountered and little is known about their chemistry, especially at elevated temperatures with steam present.

The first step the fission products take toward their possible release from the containment is escape from the fuel matrix and the fuel rods. To reach the outside atmosphere, the radionuclides must traverse the primary coolant system until they reach the containment and remain airborne there long enough to be released when the containment fails. There is also the possibility that some particulate material deposited within the containment may be resuspended and swept out of the containment following the breach. Natural removal processes operate continuously along the path the radioactive material must traverse as well as during the time they spend in any one location. If the engineered safety functions are operating, there will be additional removal processes available.

These removal processes depend upon the temperatures and flow regimes encountered, so each sequence will be different. However, there are too many dominant sequences to be able to perform the fission product transport and consequence analyses for all of them, and in any event, many sequences produce results which are similar to the results of other sequences. Therefore, some grouping of sequences occurs after the accident process analysis and a further grouping takes place after the fission product transport analysis. From the point of view of fission product transport, similar sequences are those

with similar times for core melt and containment failure, and similar flows and temperatures in the paths taken by the radionuclides. The actual initiating event is irrelevant if it does not affect these factors. For the consequence analyses, similarities are sought in release fractions, release time and duration, and the energy associated with the release. These quantities determine the concentrations of radionuclides to be expected downwind of the reactor. From the radionuclide concentrations, risk measures such as early fatalities or latent cancer fatalities are computed.

Figure 12-1 shows the major elements of a complete PRA. Both the accident process analysis and the fission product transport analysis are required to progress from the event tree stage to the release description stage. At the completion of the event tree analysis the status of all the major systems is known, including their failure modes. This supplies the information needed for the accident process analysis, which in turn produces the flows, times, and temperatures required for the fission product transport analysis. The output of this analysis is a description of the release. The amount of radioactivity released is usually expressed in fractions of the amount of that nuclide or nuclide group originally present in the core. This information will be available for selected sequences only. The sequences are then grouped together, and the release fractions, times, and energy chosen for that group or category. The frequency of the category is the sum of the frequencies of the sequences included in it.

Figure 12-2 shows the elements of the fission product transport analysis. The complete analysis draws on many submodels and relationships which must be known before the analysis can be started. Separate models may be used to model the escape of fission products from the molten corium or the condensation of steam on particles, for example. A separate model is usually used to model the transport of particles by steam flow through the reactor coolant system, and the relationships governing the changes in the physical states of the fission products must be known. The possibilities of revaporization and resuspension of material deposited on walls must also be considered. Thus, the fission product transport model is a large and complex model due to the number of factors that must be considered.

12.2 Types of Release

The different stages in the release of the fission products have been denoted different "types" of release as shown in Table 12-1. The gap release is also called the cladding rupture release or the burst release. It will occur when the core reaches a temperature in the 800-1100° C range. The exact temperature will depend upon the burnup, amount of helium prepressurization, and other factors. The internal pressure of the fuel rod is considerably above that in the reactor vessel when the cladding fails, so most of the accumulated gases in the spaces between pellets and between the pellets and the cladding are swept out of the rod at the time of clad failure. This may include as much as one quarter of the noble gases and a few percent of the volatile elements. The fraction is so small because most of the gaseous fission products are still contained within the fuel pellets when the clad fails. Typically, the burst release would consist of 1 to 5 percent of the Xe and Kr and a fraction of a percent of the I and Cs. Relative to other types of release which follow if the core subsequently melts, the gap release is relatively small. If the degradation process stops short of core melt, as in Three Mile Island, the gap release may be the largest contributor. Experiments at Oak Ridge indicate that the values used for the gap release in the Reactor Safety Study (RSS) may have been very high.

The diffusion and leach releases have largely been ignored to date. Like the gap release, their contribution to the total release is small if the fuel subsequently melts. "Diffusion"

FIGURE 12-1
PRA ELEMENTS

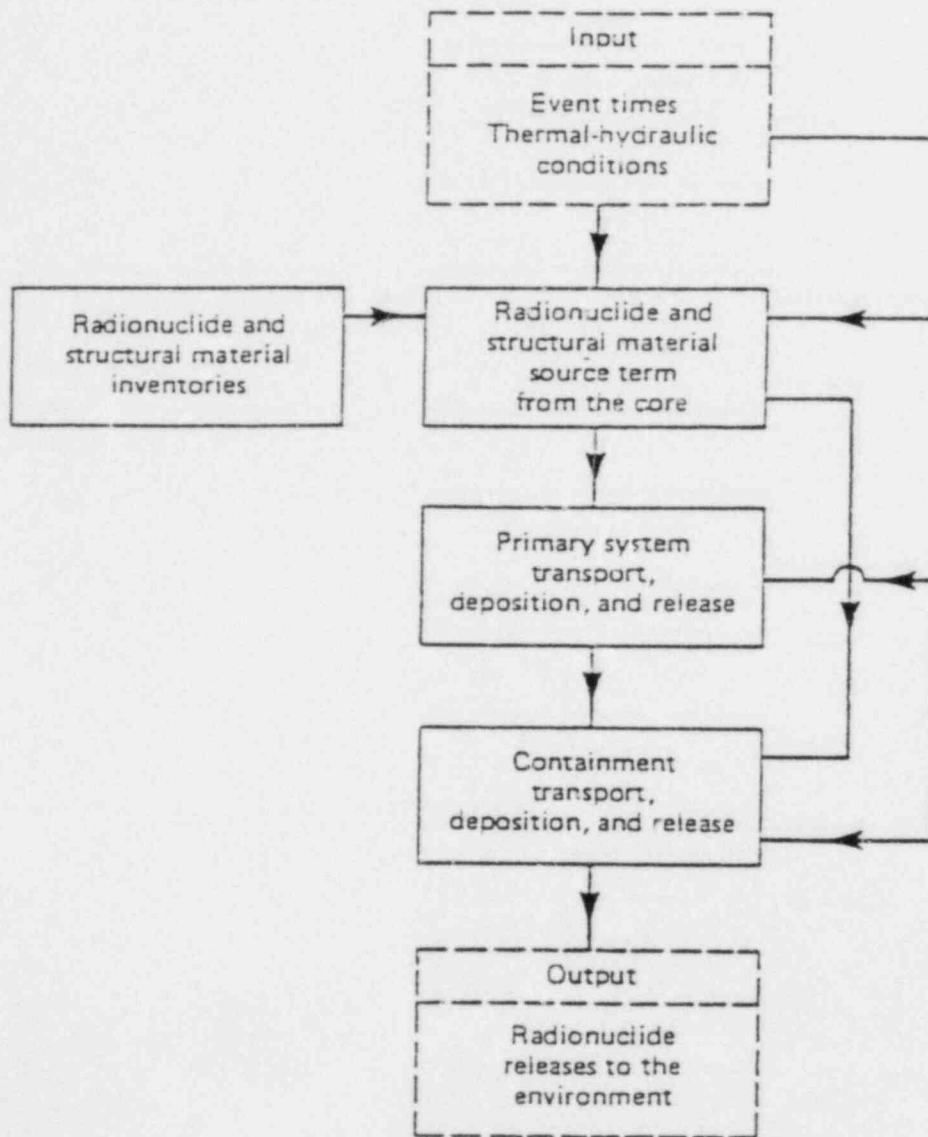


FIGURE 12-2
ELEMENTS IN THE ANALYSIS OF RADIONUCLIDE
BEHAVIOR IN THE REACTOR

SOURCE: PRA Procedures Guide (NUREG/CR-2300). 1981. Pg. 8-3.

TABLE 12-1

TYPES OF RELEASE TO CONTAINMENT ATMOSPHERE

- Cladding Rupture (GAP) - Noble Gases and Volatiles
- Diffusion - Through Failed Cladding from Unmelted Fuel
- Leach - Into Water Through Failed Cladding
- Oxidation - Depends on Fragment Size and Dispersal
- Melt - Evaporation or Boiling from Surface of Melt
- Vaporization - From Molten Core in Contact with Concrete

refers to the diffusion of fission product atoms from the interior of the fuel pellet to the surface where it is available for release. The diffusion process has two stages: first the inert gas or volatile molecule, driven by the increased pressure differential between the inside and the outside of the fuel pellet, diffuses to the nearest grain boundary. Then it moves along the grain boundary to the surface. Of course the atoms already at the grain boundaries at the time of cladding rupture will proceed directly to the surface. This release mechanism is important if the fuel remains at elevated temperatures (e.g. above 1400 C) for extended periods of time after the cladding is breached. The diffusion release rates are strongly dependent upon temperature: it doubles for each 100C rise in temperature so the diffusion releases are very rapid at 2000C and above.

The "leach" release refers to the leaching of fission products from the fuel matrix into liquid water surrounding the pellet. For this to happen, the core degradation must be terminated by reflooding after the clad has deteriorated and before the fuel has melted. Such releases occurred at Three Mile Island. Leach releases are generally omitted in PRAs because PRAs consider severe accidents that proceed to core melt. Considering the amount of radioactive material released, disregarding the leach release is largely justified since the offsite risk is minimal for accidents terminated short of core melt.

An "oxidation" release occurs when the core material oxidizes. For some fission products, the oxides are more volatile than the elemental form, but for most the oxides are less volatile. The case where fission products become oxidized sometime after they leave the vicinity of the core when they are in an area of the containment with a more oxidizing atmosphere is considered to be a chemical transformation in transit rather than an oxidation release.

Oxidation may occur in an air atmosphere with free oxygen or in a steam atmosphere. In a steam environment, the oxygen needed to form the oxide is taken from water molecules producing hydrogen as part of the process. The RSS used the term "oxidation release" to refer to the oxidation of fuel in an air atmosphere that may follow the fragmentation of the core in a steam explosion. The Procedures Guide (Sections 8.2.2 and 8.3.2) refers to this as a "Fragmentation release". Little work has been done on this release mechanism since steam atmospheres are more likely to occur. Oxidation is also possible in a steam environment. The rate of sintering of UO_2 and the rate of release of volatile fission products from heated fuel pellets are both more rapid in the presence of steam than in inert or reducing atmospheres. This release mechanism is now termed the fuel oxidation release, to distinguish it from the fragmentation release. There has not been much work in this area because if the fuel subsequently melts, all the volatiles will certainly be released, and the exact release rate in the period between cladding rupture and fuel melting may not be of great importance.

If the accident proceeds to a complete core melt, the so-called "Melt" release will be the largest single source. The term applies to the release of fission products from the molten core. Alloys of iron and nickel and the control rod materials will melt first. The cladding and fuel have higher melting points and will melt last. Eutectics are compounds or alloys which have lower melting points than their constituents. They form preferentially as solid materials are heated during the melting process. These chemical transformations will form compounds which did not exist in the core before melting, altering the melting points of the substances containing the radionuclides of interest. As the molten core progresses downward to the bottom of the reactor vessel it will acquire more structural materials and, for BWRs, material from the control rod drive mechanisms. The term "corium" is often used for this molten mass composed of all these different materials.

The melt will contain fission products only in trace amounts. Due to the high temperatures of the molten core, and remaining noble gases, iodine, and cesium will be released very quickly. Remaining fission products with high vapor pressures at the corium temperature will be released in vapor form from the surface of the melt. The presence of all the cladding, control rod, and structural material in the corium makes the chemistry exceedingly complex. It is clear that the temperature of the molten core is of primary importance. Still to be determined is the applicability of laboratory experiments to the full-scale situation. While considerable work has taken place since the Reactor Safety Study, a new model for the melt release has not yet been adopted.

Figure 12-3 shows the sort of data that is required for a melt release model. This particular plot shows recent ORNL results. It should be noted that these results have not met with universal acceptance although the evidence was sufficient to convince the ORNL authors that these values were correct. For example, noble gases are generally considered more volatile than iodine yet these results show the same curves for both. Some researchers have pointed out that this work fails to adequately account for the fact that most laboratory measurements are made in inert atmospheres while a steam environment is likely for a real accident. Others have disputed the values used for certain of the constants involved, or pointed out that the data do not properly reflect the flow regime, surface area, pressure, and other factors.

The term "vaporization" release is misleading; "melt-concrete" release or "sparging" release would be a better term. As was pointed out in the preceding section, the molten corium attacks the concrete upon which it falls after the reactor vessel fails. This decomposition of the concrete generates non-condensable gases which pass upward through the corium to escape. In doing so they sparge or carry with them small particles of liquid or solid material from the melt. Vapors are also released that condense to form particles shortly after leaving the melt. The bulk of the released materials will be non-radioactive: UO_2 , structural material, or concrete. A very small portion of them will be radioactive. Most of the experimental work in this area has been done at Sandia. The current evidence seems to be that the particle size distribution peaks around 2 microns. Several new computer codes to model this core-concrete interaction are under development: CORCON and WECHS to name two.

12.3 Physical and Chemical States and Removal Processes

It is evident from this discussion that the fission products that escape from the core can exist in a number of different states. Figure 12-4 shows these states and Table 12-2 shows the melting and boiling points of some of the substances of interest. The vapor state may be the most obvious state for the released materials, but only the noble gases and perhaps a very small fraction of the iodine which is in organic form will remain in the vapor state indefinitely. The term "particle" refers to either a liquid or solid aerosol. As the fission products move away from the core they encounter progressively cooler temperatures. Many radionuclides which leave the core in the vapor phase will condense before traveling very far as the boiling points in Table 12-2 indicate. In most cases water will be condensing also. Water condensation preferentially takes place on a particle, so essentially all particles will find themselves incorporated in a water drop if massive steam condensation is taking place. The other states shown in Figure 12-4 also occur: vapors will dissolve into water on the walls or in droplets in the air, particles will be deposited on surfaces, and so on.

Numerous removal processes will operate on the fission products during their transit from the core to the outside atmosphere. Natural processes such as particle

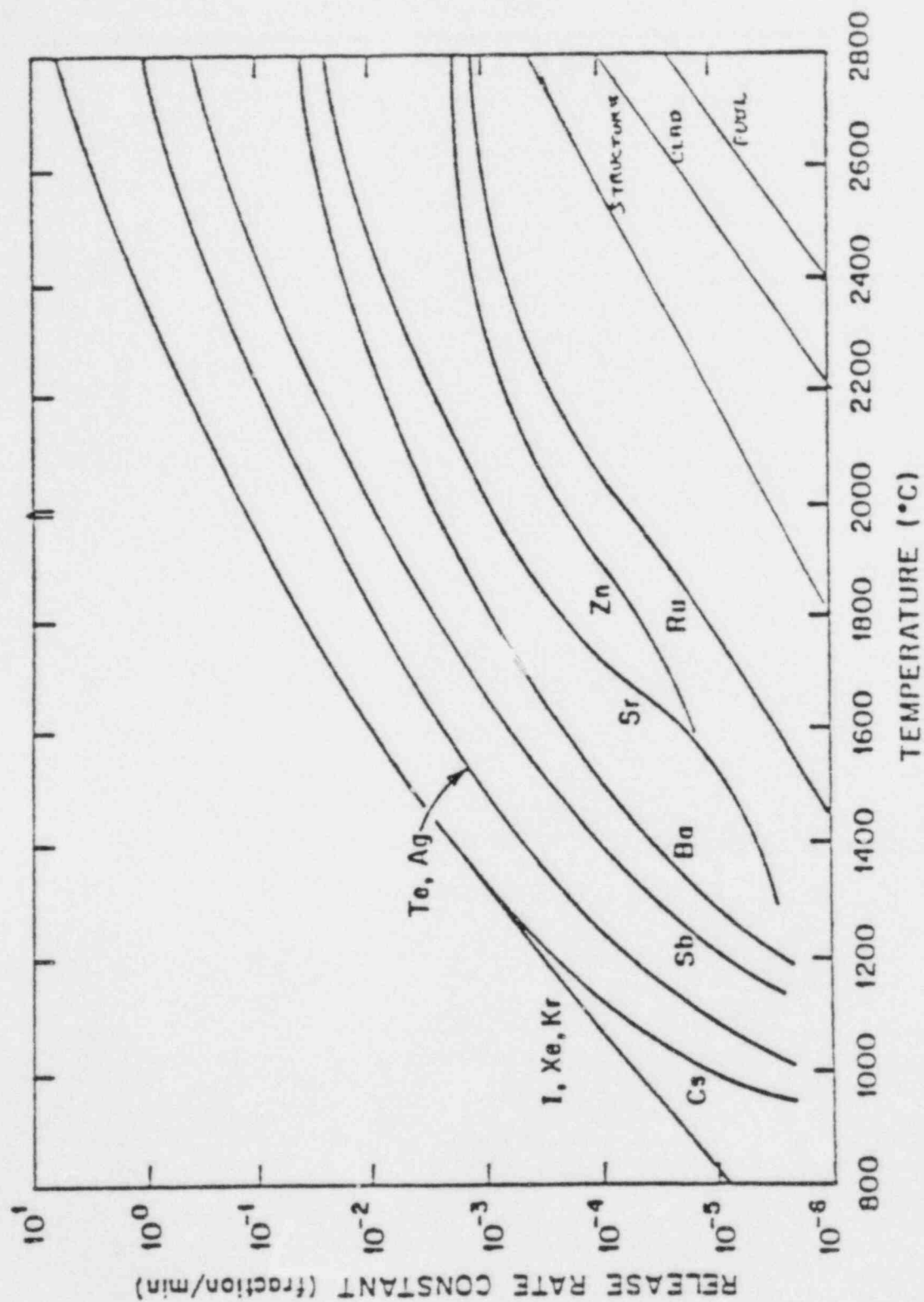
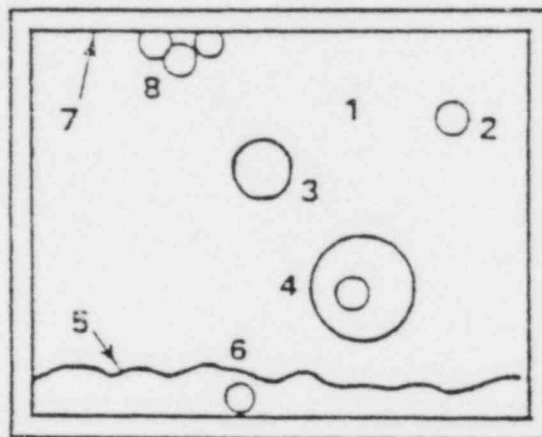


FIGURE 12-3
FISSION PRODUCT RELEASE RATE CONSTANTS FROM FUEL - SMOOTHED CURVES



- | | |
|-------------------------------------|----------------------------------|
| 1. Vapor | 5. Vapor dissolved in bulk water |
| 2. Particle | 6. Particle in bulk water |
| 3. Vapor dissolved in water droplet | 7. Vapor sorbed on surface |
| 4. Particle in water droplet | 8. Particle deposited on surface |

FIGURE 12-4
FISSION PRODUCT STATES

TABLE 12-2

MELTING AND BOILING POINTS OF REACTOR CORE CONSTITUENTS

<u>Material</u>	<u>Melting Point (C)</u>	<u>Boiling Point at 1 Atm. (C)</u>
U	1132	3818
UO ₂	2800	3200
Zr	1852	4377
Stainless Steel	1400-1500	
I ₂	114	184
Cs	28	678
CsI	620	1280
CsOH	272	
Sr	769	1384
Ru	2310	3900
Cd	321	765
In	157	2080
Ag	962	2212
Sn	232	2270

agglomeration and settling as well as engineered removal processes such as spray and filter removal, are included in these removal processes. Some other natural deposition processes are sorption, diffusion, diffusiophoresis, thermophoresis, and impaction. In addition to the physical changes such as those due to state change and agglomeration, chemical changes are likely and radioactive decay may alter the element involved.

The TMI accident showed that the iodine and cesium chemistry had not been considered adequately. Only a very small amount of the iodine released from the core was subsequently located in the containment. It now seems that the formation of cesium iodide (CsI) is much more likely than was realized heretofore. There is much more cesium than iodine in the fission products generated by U-235 nuclear fission, so there is plenty of cesium available to react with all the iodine. (The atomic fraction of cesium in irradiated fuel is typically on the order of 0.004, which is an order of magnitude greater than the atomic fraction of iodine.) Table 12-2 shows that the vaporization temperature of CsI is considerably higher than that of either of its constituents in elemental form.

Results from TMI-2 late in 1982 indicated the presence of another removal mechanism which has not been considered before. The first remote examinations of the upper plenum showed the radiation levels to be much higher than expected. Measurements showed that this was largely due to cesium isotopes. A water wash reduced the radiation levels only slightly, but a nitric acid leach was much more successful. Thus it appears that the cesium had penetrated the stainless steel and had been immobilized there. A reaction between cesium hydroxide (CsOH) and stainless steel is suspected. Laboratory tests have shown that cesium can indeed penetrate and become bound in stainless steel under proper conditions. All light water reactors contain structures with a great deal of surface area in the upper plenum: steam separators and driers in BWRs and control rod drive mechanisms in PWRs. The surface area in the upper plenum may be as great as 10,000 square feet, thus providing a large surface area for this removal mechanism.

The exact impact of these recent developments in estimating the amount of fission products that are likely to escape to the outside world in case of a hypothetical core melt accident (including containment failure) remains to be seen. The importance of these findings cannot be denied, however. The iodine and cesium isotopes are the dominant ones for most types of radiation dose. Tellurium isotopes are also very important in determining doses and very little is known about the chemical reactions of tellurium. Indium, cadmium, and tin from the control rods will also be in vapor phase in the hottest region near the melting core and their presence may complicate the chemical reactions considerably.

12.4 Release Categorization and Computer Codes

Table 12-3 illustrates the radionuclide grouping or classification scheme adopted by the Reactor Safety Study. The order is generally one of increasing boiling points. Although they may be given off from the melt in vapor form, the boiling points of the elements in the last five groups are low enough that most models have treated them as particles. In the RSS and all the other PRAs up to this time (1984), all the radionuclides were treated as being present in elemental form except for a small fraction of the iodine which was assumed to be in organic form and which was modeled as being methyl iodide. It was suspected that much of the material in the last few groups would be present as oxides, but the boiling points for either form were so high that the distinction was not considered important. Now it appears that very little of the iodine and cesium may be present in the elemental form. CsI seems to be the most probable form for iodine except in very unusual sequences where there is very little water present, and CsOH appears the most likely form for cesium. If these chemical compounds do indeed form as suspected, their

TABLE 12-3

RSS RADIONUCLIDE CLASSIFICATION SCHEME

• Noble Gases	Xe, Kr
• Halogens	I, Br
• Alkali Metals	Cs, Rb
• Tellurium Group	Te, Se, Sb
• Alkaline Earths	Sr, Ba
• Transition Metals	Ru, Mo, Pd, Rh, Tc
• Lanthanides & Actinides	La, Nd, Eu, Y, Ce, Pr, Pm, Sm, Np, Pu, Zr, Nb

behavior under many conditions will be significantly different than that of the elemental forms which were assumed before.

To take all these complications into account, and keep track of the various radionuclides as they move through different compartments with different temperatures, some sort of computer program is usually employed. Table 12-4 lists some of these codes. Some of these codes treat only restricted parts of the entire problem. The most widely used code has been CORRAL, which was the original program developed in the early 1970s for the RSS. It was largely based on a series of results from the Containment Systems Experiment which was conducted at Hanford in the 1960s. CORRAL was upgraded to CORRAL-II in 1977. The latest version, released in the first half of 1983, had enough changes that it is denoted MATADOR rather than CORRAL-III. It does not reflect some of the latest information about the chemical form and removal mechanisms for cesium and iodine, however, since general agreement has not been reached on these issues.

In most PRAs it is feasible to run the fission product transport model for only about a dozen combinations of sequence and containment failure modes. Since there are usually 5 to 15 dominant sequences and several important containment failure modes, release information is therefore available for only a small fraction of the cases of interest. Some form of grouping is thus required in order that conclusions may be drawn about all the important accidents which will lead to a release and in order that sufficient information will be available for the consequence analysis. This usually takes the form of the development of release categories, and the assignment of all the sequence - containment failure mode combinations to a release category. For example, the AH, S₁H, and S₂H sequences with overpressure failures may all be assigned to the same category, and the release information for the one case for which it is available is then assumed to apply to the other two cases.

The most important factors in developing release categories are the amount of radioactivity released and the timing of the release. The energy of the release is also important. Obviously all these things depend to a large extent on the containment failure mode. If no other information is available, categorization by containment failure mode is a good start. For example, basemat melt-through will give much lower releases than an overpressure release no matter what the system failures involved. The timing of the release is also very important. For BWRs it is important to distinguish those accidents in which the containment fails before the core melts from those in which the core melts first. In the latter event, which is almost always the case in PWRs, the time between the core melt and the containment failure is important since it allows time for removal mechanisms to operate before the radioactive material is released to the outside world.

The result of this entire activity is a summary of the accidents involving core melt and containment failure. Table 12-5 shows the familiar summary table from the RSS. On the right side we find the release fractions for each of the nuclide groups for each release category. The probability or frequency on the left side is the frequency for all the sequences which were placed in that category. Actually, in the RSS the situation is somewhat more complicated since a smoothing technique, not currently employed, was used which changed the frequency for each category from the actual sum of the frequencies of the sequences included. In the center are the other parameters needed to characterize the release and which are needed as input for the consequence analysis. A table like this is the result of the entire PRA process up to this point. The fission product transport analysis is just the final step.

TABLE 12-4

AVAILABLE COMPUTER CODES

- Thermal-Hydraulic Conditions
 - MARCH2

- Release From Fuel
 - CORSOR
 - START

- Transport and Retention in the Primary System
 - TRAP-MELT

- Molten Core - Concrete Interactions
 - WECHS
 - CORCON

- Transport and Retention in Containment
 - CORRAL and CORRAL-II
 - MATADOR
 - NAUA
 - TRAP-CON

TABLE 12-5
SUMMARY OF ACCIDENTS INVOLVING CORE

SUMMARY OF ACCIDENTS INVOLVING CORE

RELEASE CATEGORY	PROBABILITY per Reactor-Yr	TIME OF RELEASE (Hr)	DURATION OF RELEASE (Hr)	WARNING TIME FOR EVACUATION (Hr)	ELEVATION OF RELEASE (Meters)	CONTAINMENT ENERGY RELEASE (10^6 Btu/Hr)	FRACTION OF CORE INVENTORY RELEASED (a)								
							Xe-Kr	Org. I	I	Cs-Rb	Te-Sb	Ba-Sr	Ru (b)	La (c)	
PWR 1	9×10^{-7}	2.5	0.5	1.0	25	520 (d)	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}	
PWR 2	8×10^{-6}	2.5	0.5	1.0	0	170	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}	
PWR 3	4×10^{-6}	5.0	1.5	2.0	0	6	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}	
PWR 4	5×10^{-7}	2.0	3.0	2.0	0	1	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}	
PWR 5	7×10^{-7}	2.0	4.0	1.0	0	0.3	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}	
PWR 6	6×10^{-6}	12.0	10.0	1.0	0	N/A	0.3	2×10^{-3}	8×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}	
PWR 7	4×10^{-5}	10.0	10.0	1.0	0	N/A	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}	
PWR 8	4×10^{-5}	0.5	0.5	N/A	0	N/A	2×10^{-3}	5×10^{-6}	1×10^{-4}	5×10^{-4}	1×10^{-6}	1×10^{-8}	0	0	
PWR 9	4×10^{-4}	0.5	0.5	N/A	0	N/A	3×10^{-6}	7×10^{-9}	1×10^{-7}	6×10^{-7}	1×10^{-9}	1×10^{-11}	0	0	
BWR 1	1×10^{-6}	2.0	2.0	1.5	25	130	1.0	7×10^{-3}	0.40	0.40	0.70	0.05	0.5	5×10^{-3}	
BWR 2	6×10^{-6}	30.0	3.0	2.0	0	30	1.0	7×10^{-3}	0.90	0.50	0.30	0.10	0.03	4×10^{-3}	
BWR 3	2×10^{-5}	30.0	3.0	2.0	25	20	1.0	7×10^{-3}	0.10	0.10	0.30	0.01		3×10^{-3}	
BWR 4	2×10^{-6}	5.0	2.0	2.0	25	N/A	0.6	7×10^{-4}	8×10^{-4}	5×10^{-3}	4×10^{-3}	6×10^{-4}	6×10^{-4}	1×10^{-4}	
BWR 5	1×10^{-4}	3.5	5.0	N/A	150	N/A	5×10^{-4}	2×10^{-9}	6×10^{-11}	4×10^{-9}	8×10^{-4}	8×10^{-14}	0	0	

(a) A discussion of the isotopes used in the study is found in Appendix VI. Background on the isotope groups and release mechanisms is found in Appendix VII.

(b) Includes Mo, Rh, Tc, Co.

(c) Includes Nd, Y, Ce, Pr, La, Nb, Am, Cm, Pu, Np, Zr.

(d) A lower energy release rate than this value applies to part of the period over which the radioactivity is being released. The effect of lower energy release rates on consequences is found in Appendix VI.

Table 12-6, also from the RSS, is an accompanying table which indicates which sequences were placed in which categories and indicates the frequency of each individual sequence. Of course only the most probable sequences for each type of initiating event can be shown in a summary table such as this.

12.5 Summary

The field of fission product transport is very active at this time. Many assumptions which were made in the early 1970s during the Reactor Safety Study have recently been questioned. Experimental research has shed some light on certain areas, but much remains to be done. Even with experimental data in hand, the problem of the applicability of laboratory tests, often small scale or conducted in an inert atmosphere, to actual accident conditions with all their complicating factors may never be completely resolved.

The problems associated with the chemical form of cesium and iodine have been discussed above. The question of organic iodides is also open, and possibility of the formation of HI and HOI has been raised. In any system where the compounds of interest are present only in trace amounts, the applicability of bulk chemical results is always a problem as are complications brought about by an element or compound which may be present only in small amounts but which is many times more concentrated than the fission products.

The ignition of hydrogen under actual containment conditions following a severe accident remains a problem. Ignition models must include the presence of steam. The extent of mixing in the containment is difficult to estimate. While igniters may have eliminated the possibility of a global burn when power is available, the effect of these intermittent burns on the chemical form of the fission products has not been thoroughly considered.

Loss by radioactive decay during the time between the start of the accident and containment failure has generally not been considered because the time was originally thought to be quite short (on the order of several hours) so the effects would be negligible. Now it appears that for some sequences, the time to containment failure may be quite long. Igniters and mitigative measures such as alternate water sources may prolong the time to containment failure to days. The next generation of fission product transport codes may include radioactive decay.

Since the fission product transport model depends heavily on the results of the accident process computation, there has been some interest in coupling the two computer programs. This will probably be accomplished in the near future by the use of compatible disk or tape files rather than merging the two programs, since the resulting code would be quite large and the problems treated are rather different.

None of the computer codes available have been verified and validated to the extent desirable for great confidence in their results. Verification means an independent check of the coding to assure that the computer instructions faithfully reflect the equations and logic on which it is supposed to be based. Validation means the comparison of the computer program's results with actual experiments. One of the problems here is the lack of appropriate experiments. Most of the large-scale containment experiments were done more than a decade ago and the quality and extent of the data are not really adequate for current needs. The SACSHA series of tests in Germany may partially rectify this problem.

TABLE 12-6
DOMINANT ACCIDENT SEQUENCES VERSUS RELEASE CATEGORIES

		Release Categories					Core Melt		No Core Melt	
		1	2	3	4	5	6	7	8	9
LOCA PWR A	AB- α 1×10^{-11}	AB- γ 1×10^{-10}	AD- α 2×10^{-8}	AD- β 1×10^{-11}	AD- β 4×10^{-9}	AB- ϵ 1×10^{-9}	AD- ϵ 2×10^{-6}	A- β 2×10^{-7}	A 1×10^{-4}	
Probability	2×10^{-9}	1×10^{-8}	1×10^{-7}	1×10^{-8}	4×10^{-8}	3×10^{-7}	3×10^{-6}	1×10^{-5}	1×10^{-4}	
LOCA BWR A	AE- α 2×10^{-9}	AE- γ 3×10^{-8}	AE- α 1×10^{-7}	AGJ- δ 6×10^{-11}	A 1×10^{-4}					
Probability	8×10^{-9}	6×10^{-8}	2×10^{-7}	2×10^{-8}	1×10^{-4}					

PWR Small LOCA S ₂	S ₂ B- α 1×10^{-10}	S ₂ B- γ 1×10^{-9}	S ₂ D- α 9×10^{-8}	S ₂ DG- β 1×10^{-12}	S ₂ D- β 2×10^{-8}	S ₂ B- ϵ 8×10^{-9}	S ₂ D- ϵ 9×10^{-6}			
Probability	1×10^{-7}	3×10^{-7}	3×10^{-7}	3×10^{-7}	3×10^{-7}	2×10^{-6}	2×10^{-5}			
BWR Small LOCA S ₂	S ₂ J- α 1×10^{-9}	S ₂ E- γ 1×10^{-8}	S ₂ E- γ 4×10^{-8}	S ₂ CG- β 6×10^{-11}						
Probability	2×10^{-8}	1×10^{-7}	4×10^{-7}	4×10^{-8}						

PWR Transient T	TMLB'- α 3×10^{-8}	TMLB'- γ 7×10^{-7}	TML- α 6×10^{-8}		TML- β 3×10^{-10}	TMLB'- ϵ 6×10^{-7}	TML- ϵ 6×10^{-6}			
Probability	3×10^{-7}	3×10^{-6}	4×10^{-7}	7×10^{-8}	2×10^{-7}	2×10^{-6}	1×10^{-5}			
BWR Transient T	TW- α 2×10^{-7}	TW- γ 3×10^{-6}	TW- γ 1×10^{-5}							
Probability	1×10^{-6}	6×10^{-6}	2×10^{-5}	2×10^{-6}						

SOURCE: Reactor Safety Study (WASH-1400). 1975. Main Report, Pg. 79.

TOPIC 13
CONSEQUENCE ANALYSIS

13. FUNDAMENTALS OF CONSEQUENCE EVALUATION

13.1 Introduction

The consequence evaluation assesses the offsite effects of postulated accident sequences identified in other phases of the PRA. The PRA results from the steps that precede the consequence analysis are limited to an identification of plant damage states and potential release categories. These do not, in themselves, provide any indication of the impact on humans or the environment. To evaluate the effects of a serious reactor accident offsite, consequences such as number of mortalities or evacuation cost must be estimated. The consequence evaluation performs this task. Because of the large amounts of data to be manipulated, a computer program is usually employed.

Consequence analysis may also be used to make siting recommendations for new plants or to evaluate the efficacy of alternative designs, emergency planning, and mitigation measures. The locations of the existing reactors have been evaluated in the Siting Study (NUREG/CR-2239) by the use of a consequence computer code. The consequence model could also be used to evaluate such things as different evacuation routes and the effectiveness of evacuation versus sheltering.

Figure 13-1 illustrates the steps in a consequence assessment. First the distribution of radioactive material in the environment must be known. This is computed based upon the radiological release information and meteorological data. Since the accident is hypothetical, it would be inappropriate to use the atmospheric conditions for any one specific time in the past. Instead, the meteorological data for some past year is sampled to determine statistically how the radioactivity released from the containment may be expected to be distributed in the surrounding environment. Thus, even though we may treat the release information as exact known quantities, the nature of atmospheric transport is such that the airborne and deposited concentrations can only be stated as expected distributions. This follows directly from the fact that a hypothetical accident may, or may not, happen sometime in the future is being considered.

Once the radionuclide concentrations are known, the population distribution and land use data are utilized to compute the human economic effects. The calculation of the human effects is complicated by the fact that the people living nearest the reactor may be in the process of evacuating the area when the cloud of radioactive material passes over them. The assessment of the health effects requires a great deal of dosimetry and health effects data. The end results of the consequence evaluation are values for such quantities as early fatalities, latent cancer fatalities, and relocation cost.

There are four basic models which constitute a complete consequence model:

- Atmospheric Dispersion Model
- Pathways Model
- Dosimetry Model
- Health Effects Model

Each of these models is discussed in the following sections.

13.2 Atmospheric Transport and Diffusion

Material released from the containment may be transported away from the site by air or water. Transport by air is so much more effective that its effects dominate and

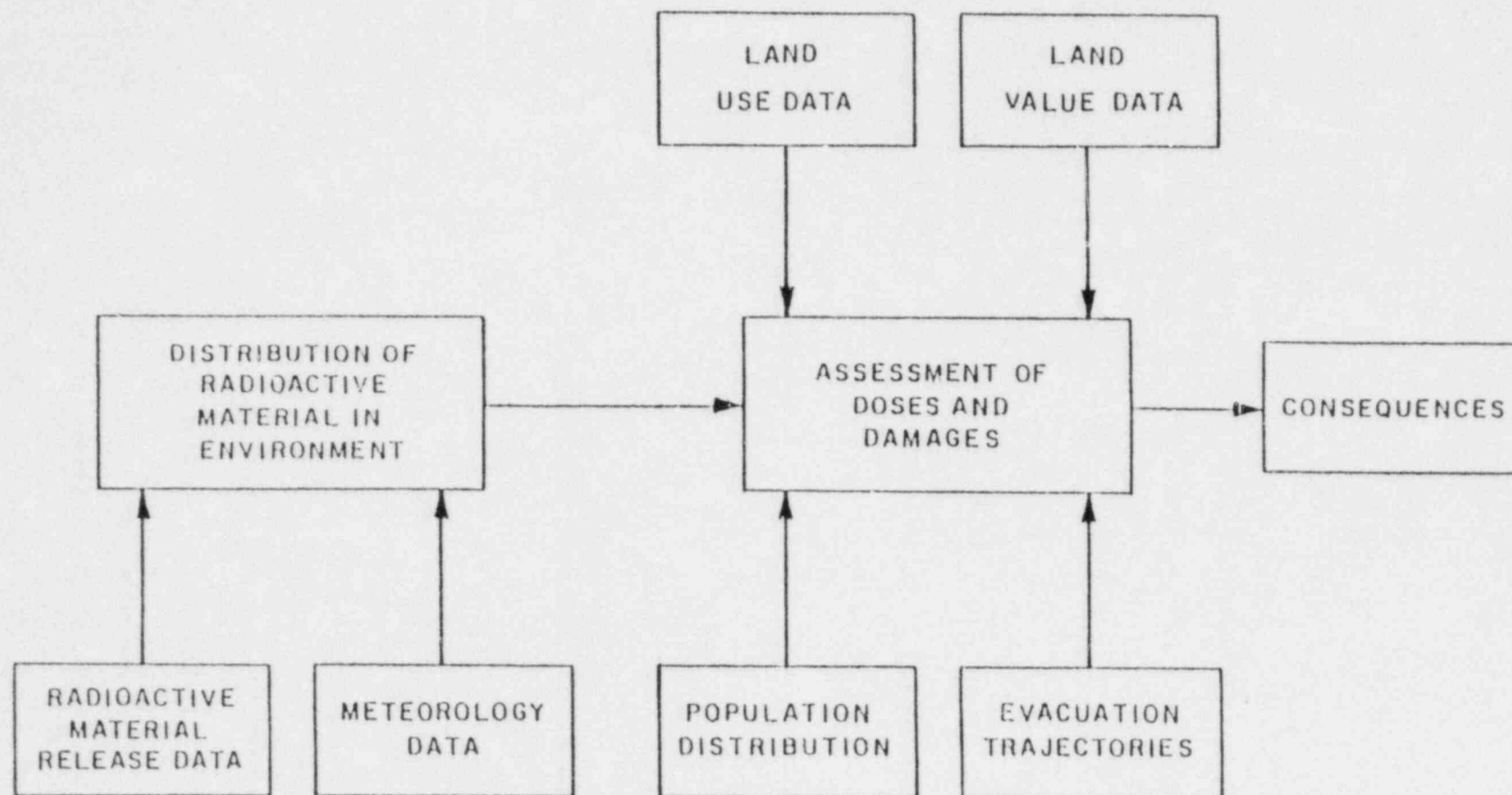


FIGURE 13-1
CONSEQUENCE ASSESSMENT

dispersion through water is usually ignored. Any material released above ground is transported away from the containment by the wind and dispersed by laminar and turbulent diffusion in the vertical as well as the horizontal direction.

The gaseous fission products, such as xenon and krypton, may be expected to remain airborne until they decay. Although some of the other radionuclides will decay while airborne, most of the material with half-lives on the order of several hours or more will be deposited on the surface of the earth: on the ground or the sea, perhaps on grass or tree leaves. Radiation is received from all the radioactive particles in a person's vicinity. The airborne radioactivity will be carried away with the wind but that which is deposited will remain, so both the concentration in the air and that on the ground are of interest.

To compute the spread of the released radioactivity for any specific time and place, the wind direction, wind speed, and atmospheric stability must be known. The atmospheric stability is a quantity which gives an indication of how vigorous the mixing is. All three of these quantities are functions of time, location, and height. Since meteorological data are collected for relatively few locations, simplifying assumptions must be made about the representativeness of the data available. Radioactive particles may be deposited by both wet and dry deposition processes, so precipitation information is needed as well. Numerous other factors complicate the calculation of the air and ground concentrations downwind from the source. Some of these include duration of release, particle size distribution, surface roughness, land-sea effects, clouds, albedo, effects of buildings and cities, and mixing depth. Some of these will be discussed briefly later on. The term "albedo" refers to the amount of energy reflected from the ground. This is important because the air near the ground is heated by the ground, and the ground temperature is determined by how much of the sun's energy it absorbs.

Since wind direction determines the path of the plume, which way the wind is blowing at the time of the release will be the single most important factor in determining how many (and which) people may receive a radiation dose as a result of an accident at a specific location at a given time. The importance of wind direction in determining the number of people that may be affected is illustrated by Figure 13-2, which shows the distances and directions from a proposed nuclear plant on the Potomac River south of Washington, DC, which was never built. The sector population out to 50 miles, for the NNE sector is almost 2,000,000. That for the SSE sector is about 12,000. When a large number of meteorological records are processed to determine statistically the number of people likely to be exposed, the importance of the wind direction decreases because of its variability. The RSS ignored wind direction since the RSS was calculating consequences for numerous sites.

The direction that the plume of released material will travel is determined by the wind direction, how fast it travels is determined by the wind speed, and how much it spreads out as it travels is controlled by the stability. Figure 13-3 illustrates the effects of stability on a typical plume from a smokestack. The reference point in discussing atmospheric stability is the adiabatic lapse rate. This is the rate at which the temperature of a parcel of air will change due to pressure as it rises or falls in the atmosphere if it exchanges no energy with the surrounding air. If the atmosphere is stable, the temperature profile is such that any parcel displaced slightly from its location will tend to return to that location. There will be very little mixing in such conditions. If the atmosphere is unstable, the temperature change with height is such that the parcel will tend to move even further away from its original location. Mixing will be very vigorous under these conditions. Neutral means that there is no force on the displaced parcel either way. Mixing is moderate under neutral conditions. Figure 13-3 also shows

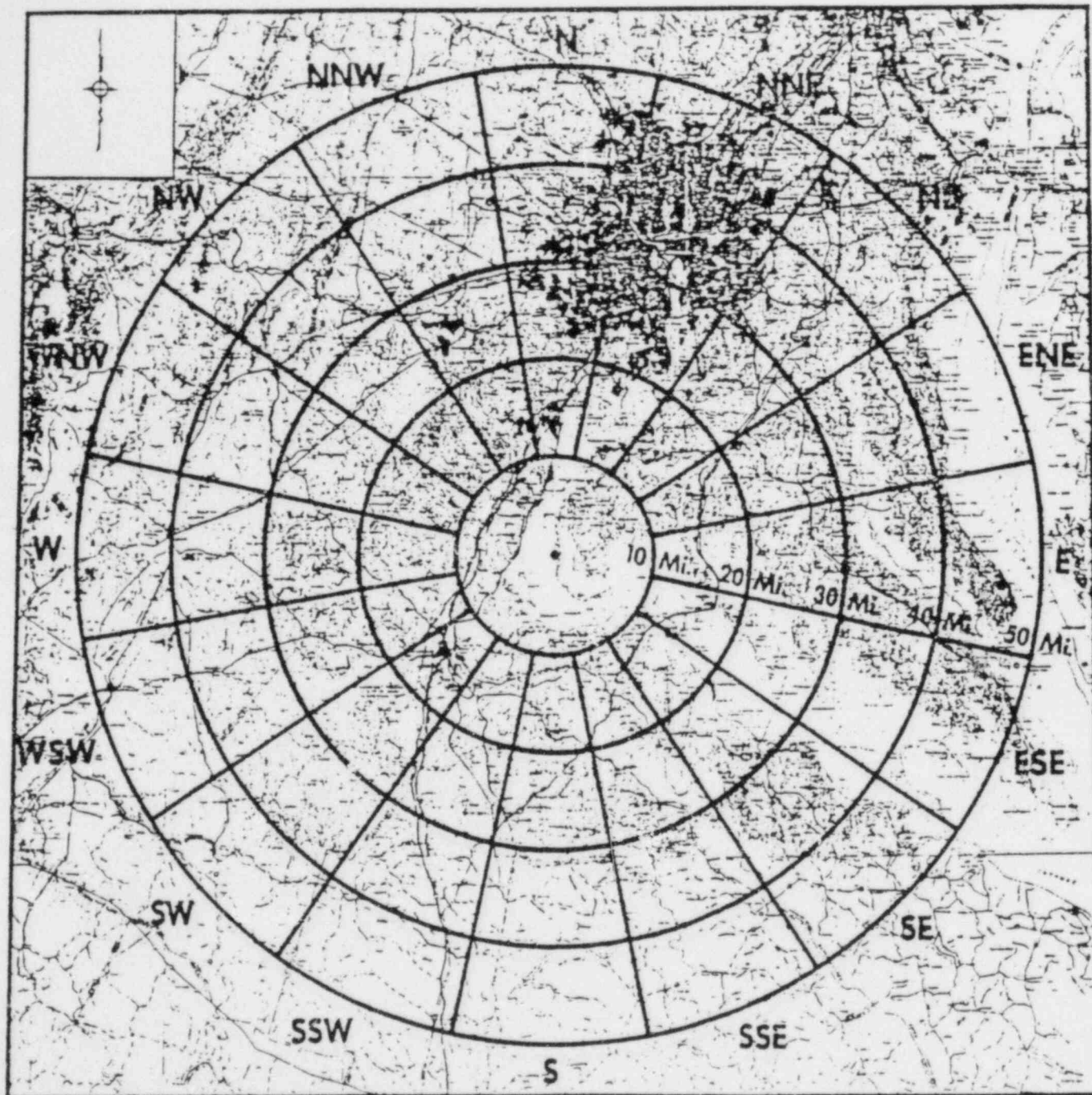


FIGURE 13-2

AREA SURROUNDING THE DOUGLAS POINT NUCLEAR GENERATING STATION

SOURCE: Douglas Point Nuclear Generating Station Final Safety Analysis Report.
Potomac Electric Power Co.

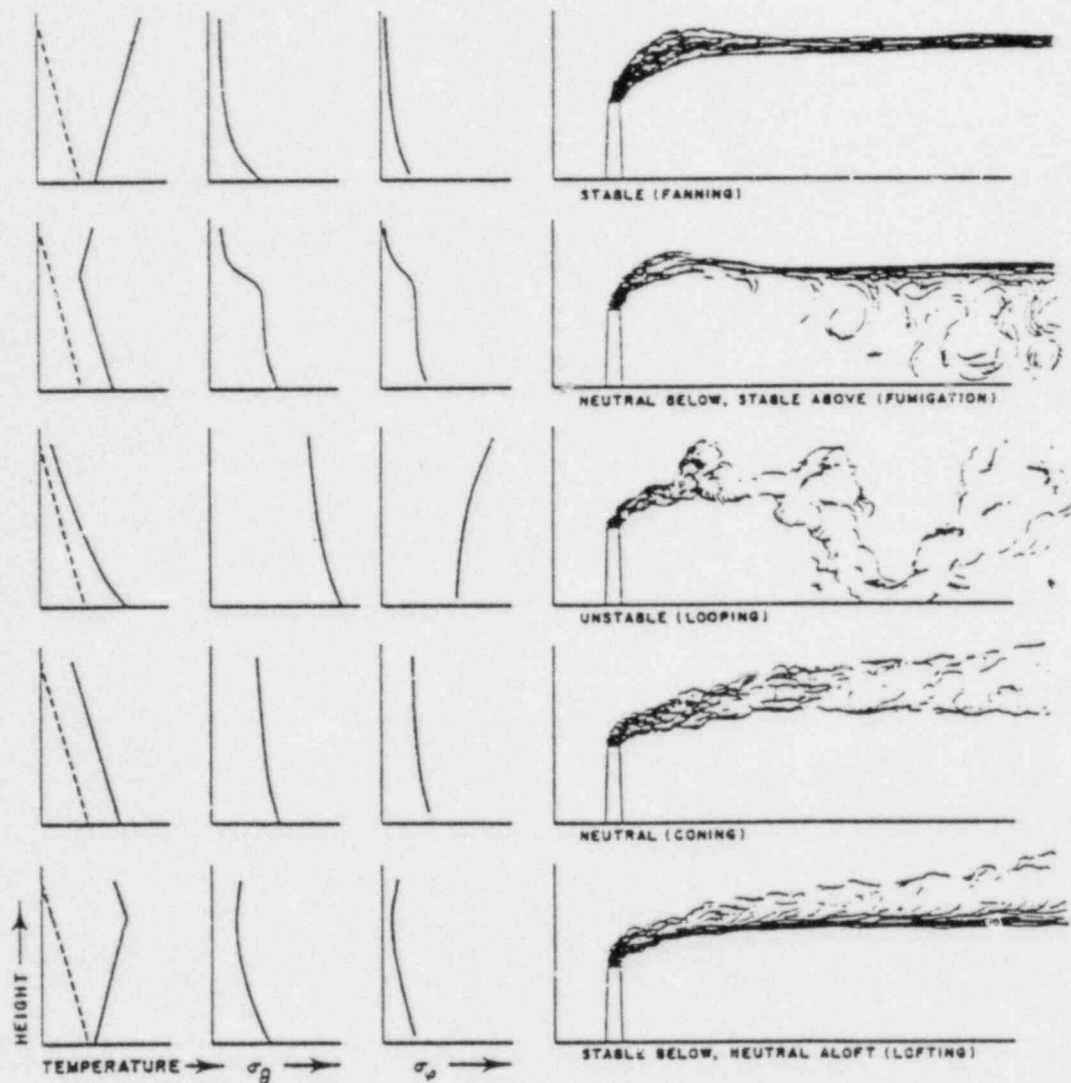


FIGURE 13-3
VARIOUS TYPES OF SMOKE-PLUME PATTERNS
OBSERVED IN THE ATMOSPHERE

SOURCE: Slade, D.H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg. 59.

how the standard deviations of the horizontal and vertical wind directions change with height. The amount of mixing in the atmosphere can be estimated from these values as well as the vertical temperature profile. More detail and the numerical definitions of the stability classes can be found in the Procedures Guide (NUREG/CR-2300), page 9-20ff. A method of determining the stability class which uses both the vertical temperature change and the wind speed is presented there also.

The vertical temperature structure of the atmosphere, and hence the amount of mixing, changes with the time of day. This is shown in Figure 13-4. Unstable conditions with vigorous mixing prevail in the afternoon and stable conditions with very little mixing occur from midnight to dawn. The wind speed also affects the amount of mixing. As might be expected, high wind speeds promote mixing.

This diurnal effect is due to the fact that the ground is a much better emitter and absorber of radiation than air. Thus, during the day the ground warms up faster than the air in the lower atmosphere and at night it cools off faster. The ground temperature affects the temperature of the air close to it, which in turn affects the vertical temperature profile in the lower part of the atmosphere. Figure 13-4 shows what happens on a sunny day; the air next to the ground warms up until it becomes unstable, at which point it mixes with the air just above it. By 1600 a well-mixed warm layer over 1000 feet thick has been established. After sunset the ground radiates rapidly and a cool stable layer of about 500 feet has formed above the ground.

Because weather reports describe the wind in general terms, for example, from the south at 10 mph, we often get the impression that wind speed and direction are relatively stable on a scale of tens of minutes, and perhaps on a scale of several hours. That this is not the case is illustrated in Figure 13-5 which shows some typical wind records. Note that time increases to the left in these records. The top three records show both speed and direction; the last record shows direction only. Note the conditions known as light and variable winds at the right-hand side of the second record and in the last record. As may be imagined, predicting plume travel and concentrations is extremely difficult for such conditions.

The wind speed and especially the wind direction vary with location as well as with time. This is especially true when the area in question displays much topographic relief. Figure 13-6 illustrates some of the problems that hilly terrain may cause. The figures on the plot are wind roses. The length of the line in each direction is proportional to the fraction of the time that the wind blows from that direction. It is obvious that the location of the recording station in this area has great effect on the observed wind direction.

The wind direction may also vary with height as shown in Figure 13-7. The direction change with height is much greater at night than during the day because the stable conditions at night greatly reduce the amount of vertical mixing. The more vertical mixing there is the more invariant the wind direction will be with height. If the air is divided into vertical layers with very little mixing between layers, it is not uncommon to have completely different wind directions in the layers.

The wind roses encountered above can be used to show the wind speed distribution as well. The top illustration in Figure 13-8 compactly displays both the frequency of the wind direction and the speed distribution as a function of direction. For the location shown, for example, winds over 15 mph almost always come from the SW or WSW. The wind rose shows the direction FROM which the wind is blowing because meteorologists always talk in terms of the direction FROM which the wind is blowing, and

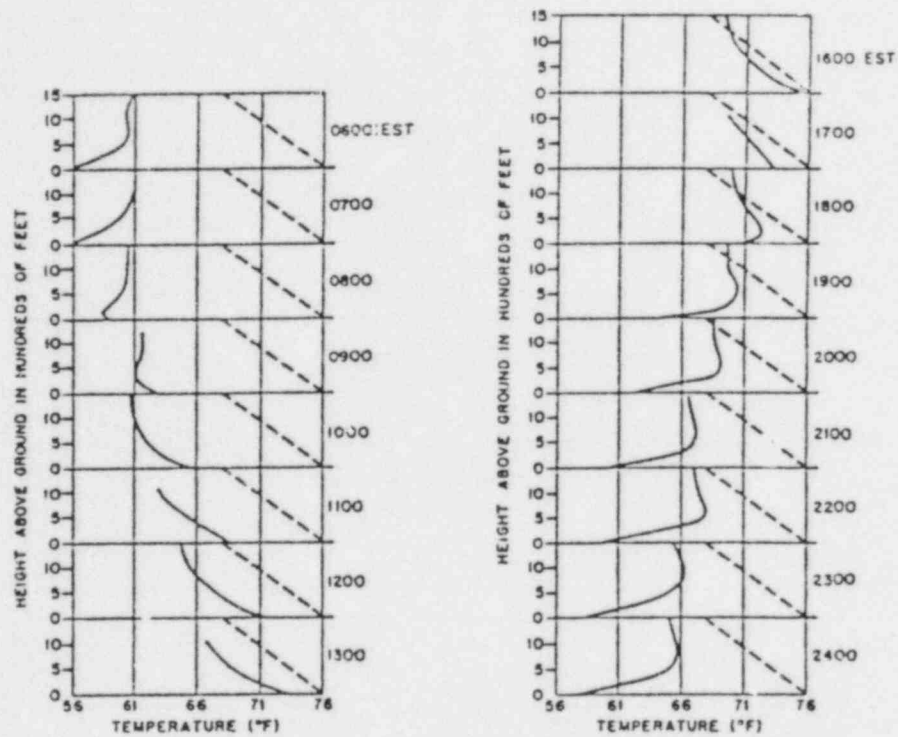


FIGURE 13-4
THE AVERAGE DIURNAL VARIATION OF THE VERTICAL
TEMPERATURE STRUCTURE AT THE
OAK RIDGE NATIONAL LABORATORY DURING
SEPTEMBER - OCTOBER, 1950

SOURCE: Slade, D.H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg. 35.

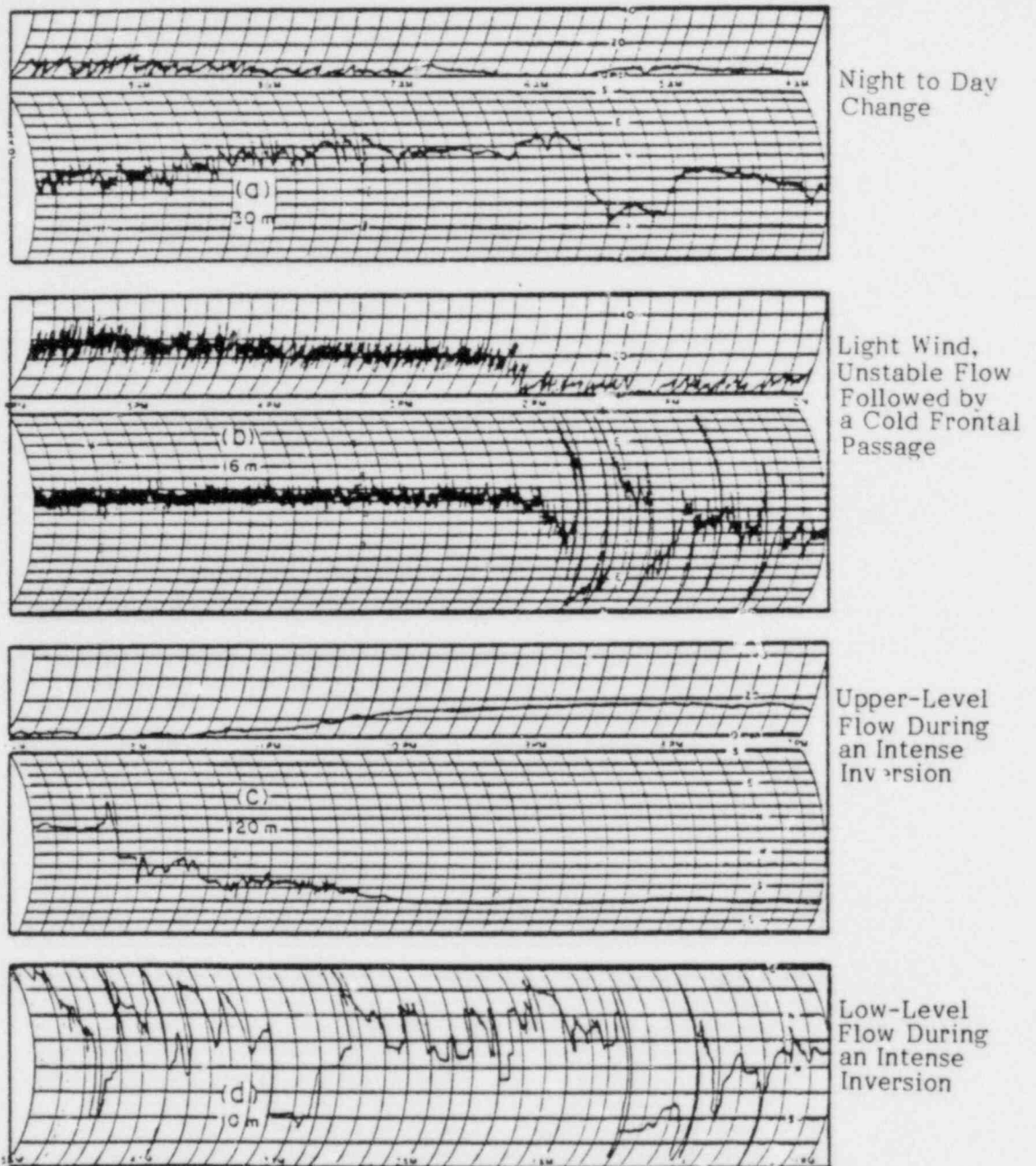


FIGURE 13-5
TYPICAL HORIZONTAL WIND-SPEED
AND DIRECTION TRACES AT VARIOUS HEIGHTS

SOURCE: Slade, D. H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg.49.

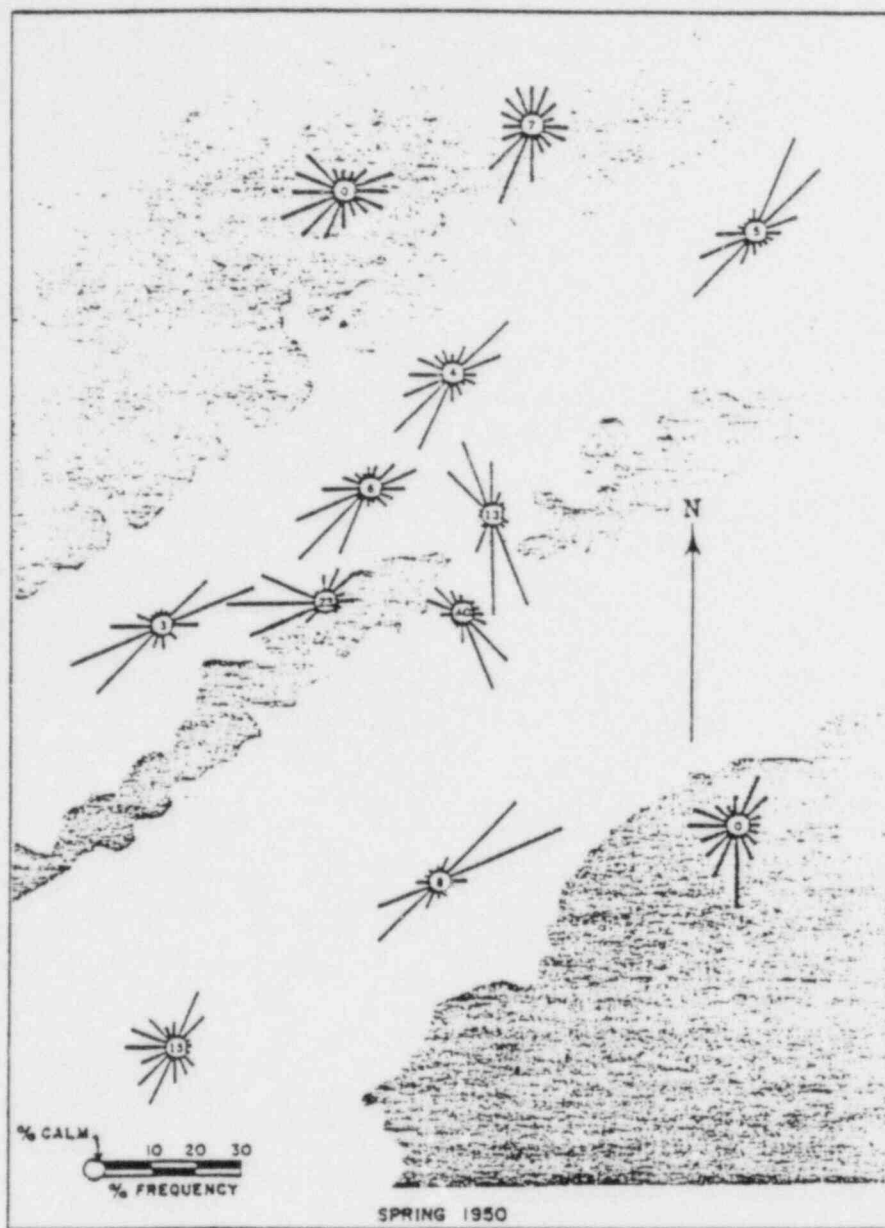


FIGURE 13-6
 MAP OF THE HILLY AREA SHOWING WIND FLOW
 BY MEANS OF MASSED WIND ROSES
 (SHADED AREAS REPRESENT ELEVATED TERRAIN)

SOURCE: Slade, D.H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg. 30.

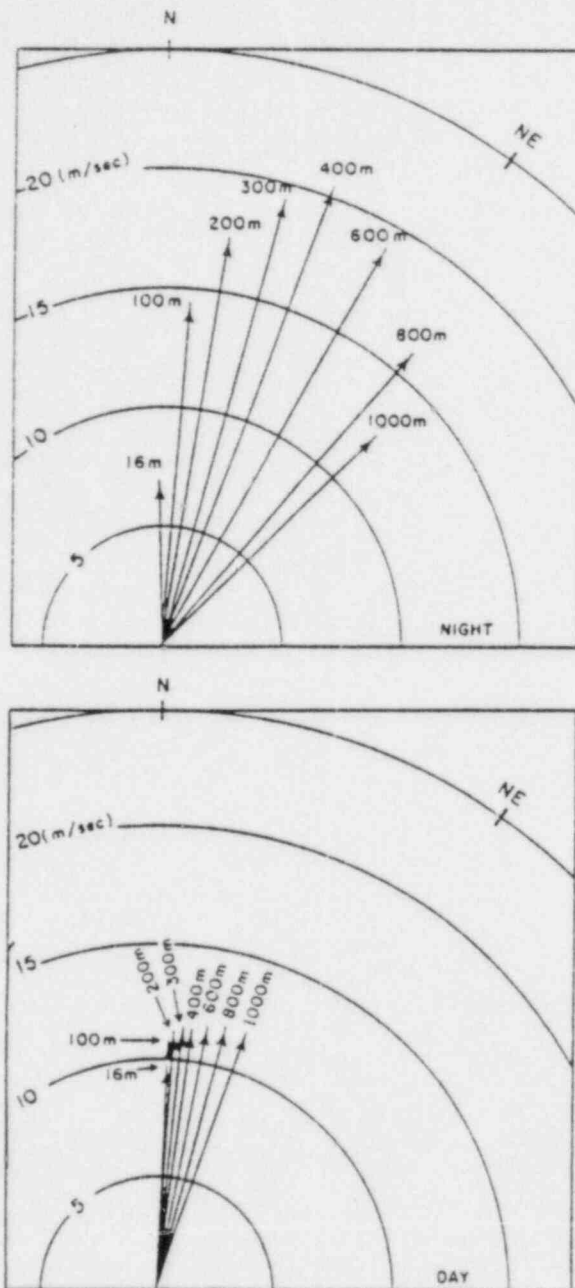
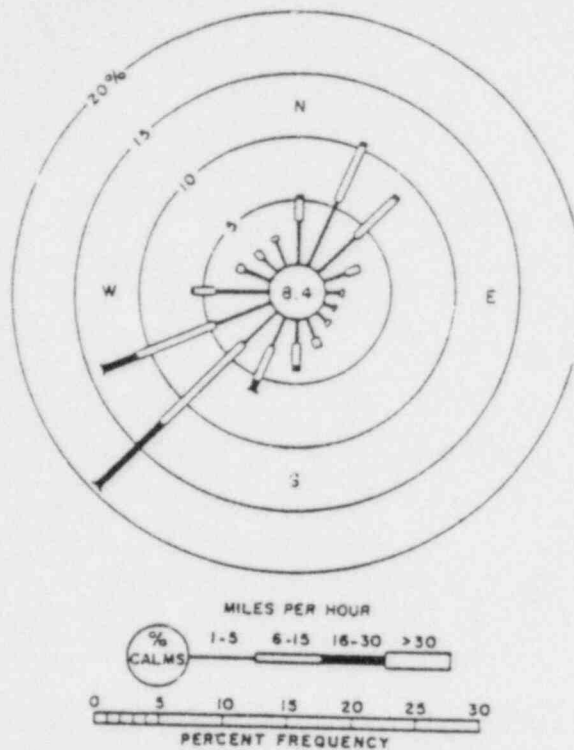


FIGURE 13-7
AVERAGE VECTORS CONSTRUCTED
FROM NIGHT AND DAY WIND OBSERVATIONS

SOURCE: Slade, D. H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg. 43.



A TYPICAL WIND ROSE WITH WIND-SPEED INFORMATION.

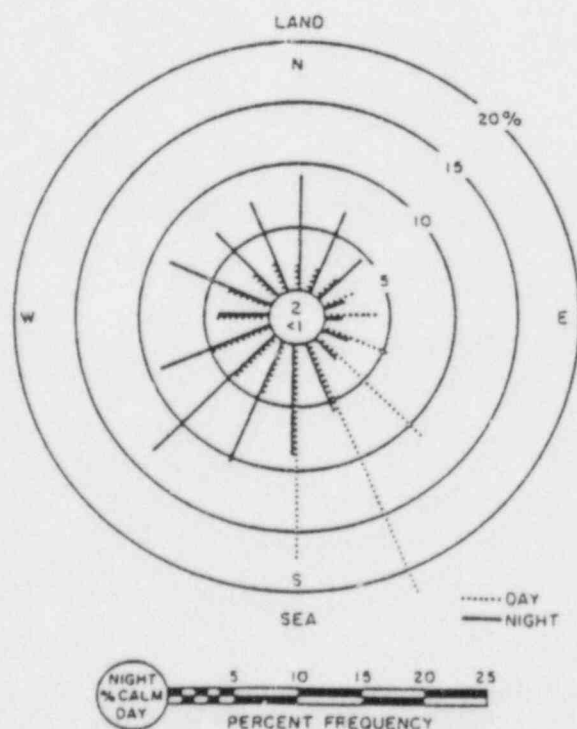


FIGURE 13-8
A DAY-NIGHT WIND ROSE SHOWING
THE DIURNAL EFFECT OF THE SEA BREEZE

SOURCE: Slade, D.H. Meteorology and Atomic Energy,
U.S. Atomic Energy Commission, 1968. Pg. 29

meteorological data is usually recorded in this form. For plume dispersion, however, it is the direction TO which the wind is blowing that is used. It is necessary to carefully record whether each data collection gives direction FROM or direction TO.

As discussed above, the diurnal variation has a profound effect upon the lower layers of the atmosphere. The largest diurnal effects upon the wind occur at the boundary between land and water. During the day, the land heats up faster than the water, so the warmer air over the land rises and is replaced by cooler air from over the water. This is termed the sea breeze (or lake breeze) and is the reason so many people flock to the seashore in the hot summer months. In the evening the flow is reversed but the land breeze is not usually as vigorous as the sea breeze. The lower illustration on Figure 13-8 utilizes the wind rose format to illustrate the diurnal effect.

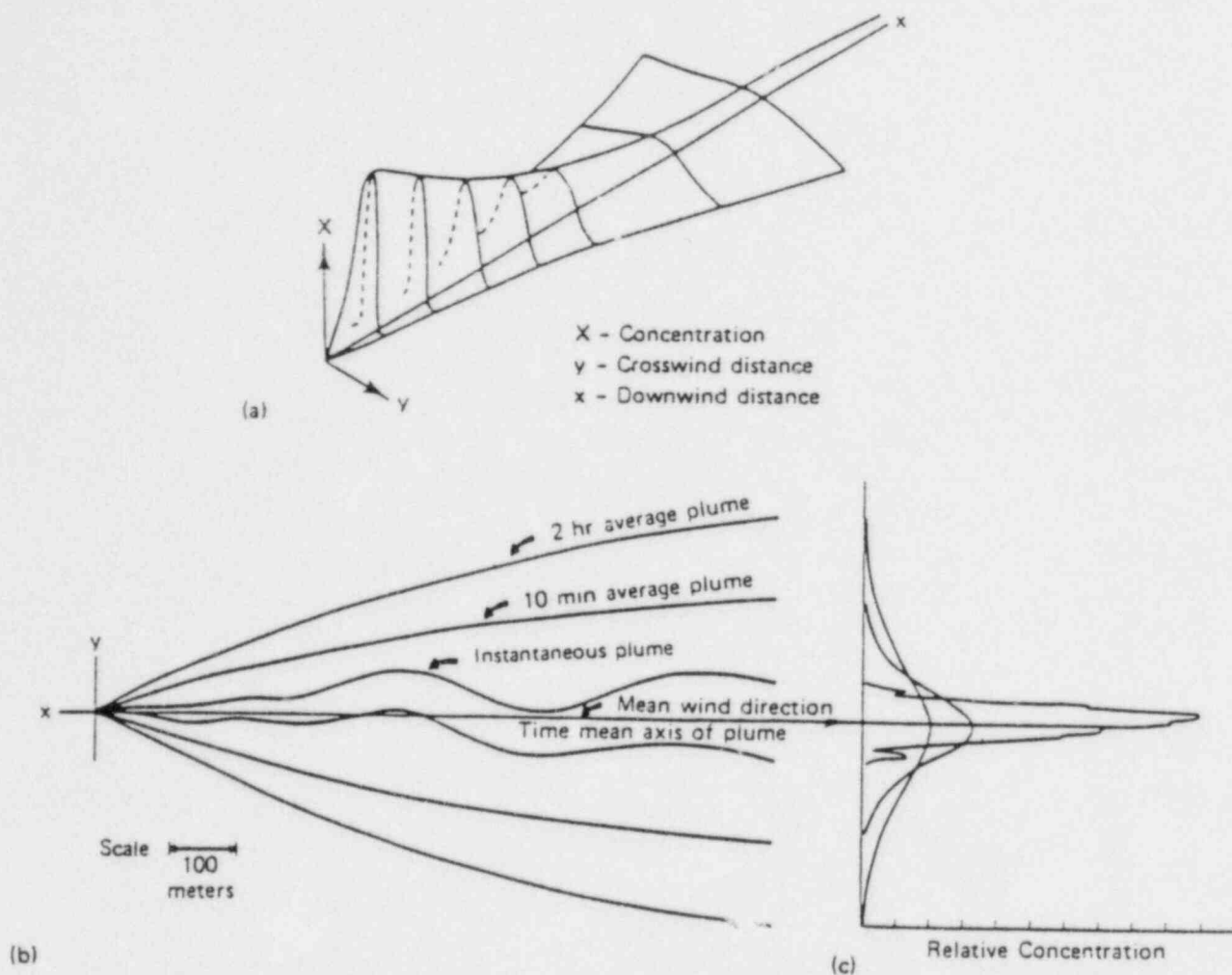
Almost all simple models (and some more complex models as well) of a plume of material dispersing from a localized source utilize the Gaussian distribution in the horizontal and vertical crosswind directions. Figure 13-9 shows that the plume concentration is a function of the length of time over which the measurements are averaged.

If the plume is photographed at any instant, it will have some sort of meandering path as shown in the lower drawing. Time-averaging produces the smooth contours usually shown in plots. The equation for the Gaussian plume for an observer on the ground ($z=0$) is given in Table 13-1. Note that this equation contains the wind speed in the denominator, and so is undefined for $u = 0$. Therefore, special treatment is required when the wind speed is very low.

Table 13-1 also contains two different sets of equations for computing the dispersion coefficients, σ_y , and σ_z , for stability classes A through F. There were originally seven stability classes, but the seventh class, G - Very Stable, occurred so infrequently that it has been dropped. Plots of Briggs' dispersion coefficients are shown in Figure 13-10. Note that these dispersion coefficients are claimed to be representative only for open country and a limited range of distances from the source. Due to the lack of reliable results for other terrains and distances, these values are often used in circumstances where their appropriateness is open to some question.

The radioactive material in the air does not remain there indefinitely. An inert gas molecule will remain there until it decays, but almost all the other radioactive material will be in liquid or solid material particulate form and hence subject to aerosol removal processes before it decays. Dry deposition refers primarily to gravitational settling, aided by agglomeration which creates larger particles which settle faster. There is also some removal by diffusion and by impaction as the wind blows through trees and grass. Dry deposition rates usually fall between 0.1 and 10 cm/sec. The choice of the value input to the computer model can have a very large effect upon the radiation doses calculated.

Particles are also removed by precipitation. Water condenses preferentially on dust particles, so if a water droplet condenses on a radioactive particle and later falls to the ground, the particle it contains is removed. This is called rainout. The falling drops also acquire some particles by impaction as they fall. This is known as washout. Wet deposition or precipitation scavenging, when it is occurring, removes particles much faster than dry deposition. Both wet and dry deposition rates measured in the field vary widely; the variation in the wet deposition rates is especially large. The data are so scattered that quite different deposition rates may easily be derived depending on the approach and the data used. Wet deposition rates appear to vary by two or three orders of magnitude with space and time, partially due to the variations in the rainfall rate.



(A) SURFACE CONCENTRATION PATTERN DOWNWIND FROM AN ELEVATED SOURCE; (B) APPROXIMATE OUTLINES OF A SMOKE PLUME OBSERVED INSTANTANEOUSLY AND OF PLUMES AVERAGED OVER 10 MIN. AND 2 HR; (C) CORRESPONDING CROSS-PLUME DISTRIBUTION PATTERN.

FIGURE 13-9
REPRESENTATIONS OF A PLUME FROM A POINT SOURCE

SOURCE: Slade, D.H. Meteorology and Atomic Energy. U.S. Atomic Energy Commission, 1968. Pg. 57.

TABLE 13-1
GAUSSIAN DISPERSION EQUATION AND EQUATIONS
FOR THE DISPERSION COEFFICIENTS

A. Gaussian Dispersion Equation

$$\chi(x, y, z = 0) = \frac{Q}{\pi u \sigma_y \sigma_z} \exp \left[- \frac{y^2}{2(\sigma_y)^2} - \frac{h^2}{2(\sigma_z)^2} \right]$$

where

χ = concentration
 u = wind speed
 h = release height
 Q = release rate

B. Formulas for $\sigma_y(x)$ and $\sigma_z(x)$ for Open-Country Conditions ($10^2 < x < 10^4$ Meters)

Pasquill Stability Category	Martin and Tikkvart (1968)		Briggs (1973)	
	σ_y	σ_z	σ_y	σ_z
A	$0.3658x^{0.9031}$	$0.00024x^{2.094} - 9.6$	$0.22x(1 + 0.0001x)^{-1/2}$	$0.20x$
B	$0.2751x^{0.9031}$	$0.055x^{1.098} + 2.0$	$0.16x(1 + 0.0001x)^{-1/2}$	$0.12x$
C	$0.2089x^{0.9031}$	$0.113x^{0.911}$	$0.11x(1 + 0.0001x)^{-1/2}$	$0.08x(1 + 0.0002x)^{-1/2}$
D	$0.1471x^{0.9031}$	$1.26x^{0.516} - 13.0$	$0.08x(1 + 0.0001x)^{-1/2}$	$0.06x(1 + 0.0015x)^{-1/2}$
E	$0.1046x^{0.9031}$	$6.73x^{0.305} - 34.0$	$0.06x(1 + 0.0001x)^{-1/2}$	$0.03x(1 + 0.0003x)^{-1}$
F	$0.0722x^{0.9031}$	$18.05x^{0.18} - 48.6$	$0.04x(1 + 0.0001x)^{-1/2}$	$0.016x(1 + 0.0003x)^{-1}$

SOURCE: Reactor Safety Study (WASH-1400). 1975.
Appendix VI, Fig. A-5.

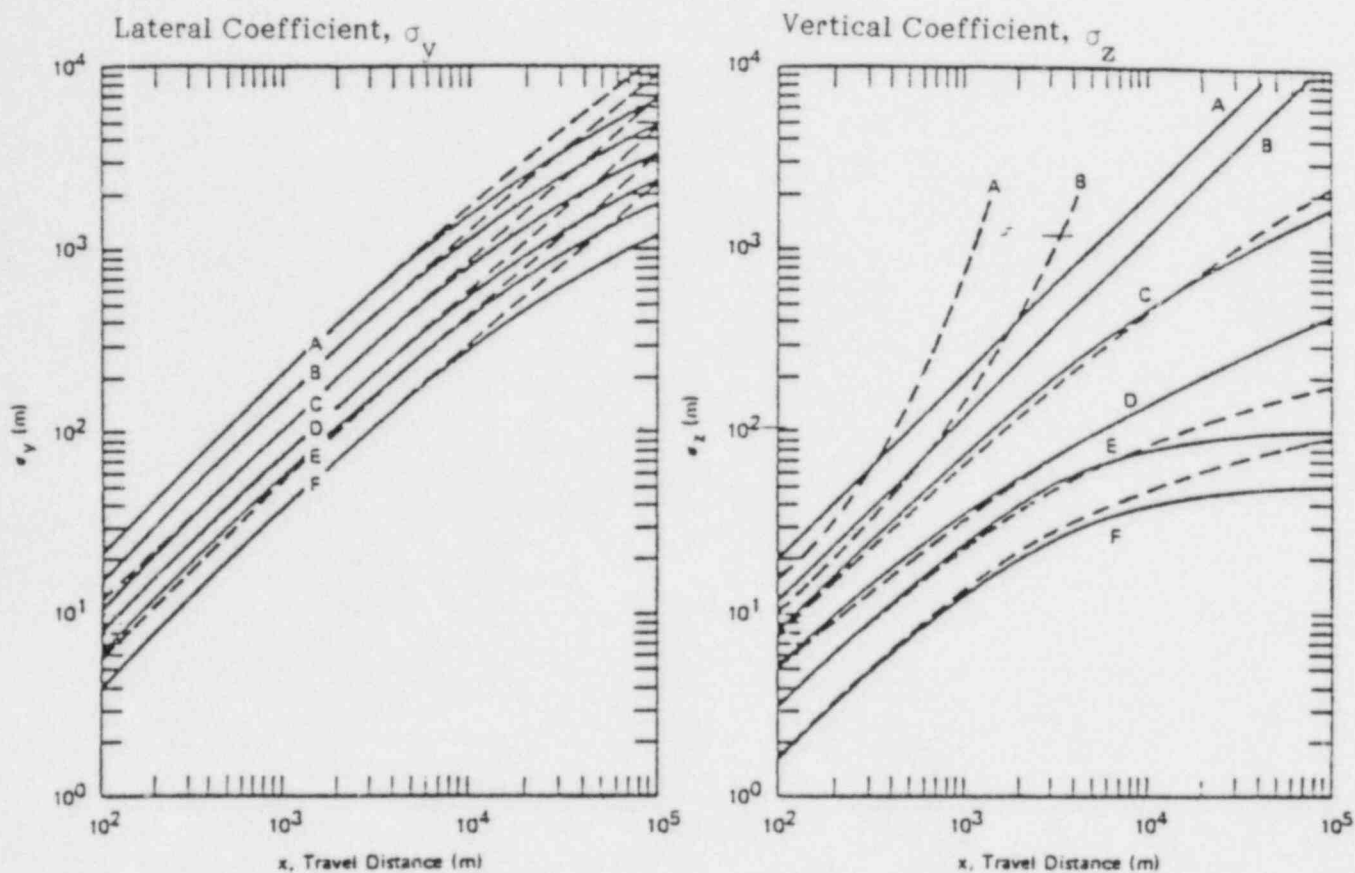


FIGURE 13-10

BRIGGS RURAL-DATA-BASED DISPERSION COEFFICIENTS (SOLID CURVES)
 COMPARED WITH THE PASQUILL-GIFFORD COEFFICIENTS (BROKEN CURVES)

SOURCE: Reactor Safety Study (WASH-1400). 1975.
 Appendix VI, Pg. 6.

Frequently, the rainfall rate is not available, and the rates that are recorded are generally not applicable to a wide area. Since the probability of rainfall is low, the wet deposition rate does not usually determine the dose in the bulk of the cases modeled. When rainfall does occur during or shortly after a release, more severe consequences can result; the maximum number of early casualties are usually computed when rain causes heavy deposition in a densely populated area just outside the evacuation radius.

Some of the problems encountered when trying to accurately model the dispersion of fission products from the site are:

- Tower data exist only up to 80-100 meters
- Radiosondes, which give $T(z)$ and $v(z)$, are sent up only at about 100 locations in the USA only once or twice a day
- Modeling of wind shifts and wind shear is difficult
- Nuclide reactions after release are poorly known
- Deposition data, both wet and dry, are sparse and the results are scattered
- The concentration near ground level often varies significantly from concentration only 10-20 meters up
- Hilly terrain makes modeling difficult
- The meteorological data may not be representative of the entire region
- Deposited material may be resuspended.

The foremost problem is the lack of data. Meteorological towers are found primarily only at reactor sites and at major airports. Considering the area over which the model is utilized, this is very little data. And that data extends up to an elevation of only about 100 meters. Above that height, the data is limited to radiosonde results which are limited in both time and location, so that the variation of wind direction, wind speed, and wind direction with height is poorly known.

13.3 Pathways to Man

Once the radionuclide concentration in the air and on the ground at a certain location has been computed, the next step is to consider how the radiation reaches the people at the location. Figure 13-11 illustrates four major pathways:

- Immersion (external, from air)
- Inhalation (internal, from breathing)
- Ingestion (internal, from eating and drinking)
- Radiation from the ground (external).

The relative importance of these pathways varies with the distance from the reactor, the weather, and the exposure time. The ingestion dose is usually ignored in computing acute

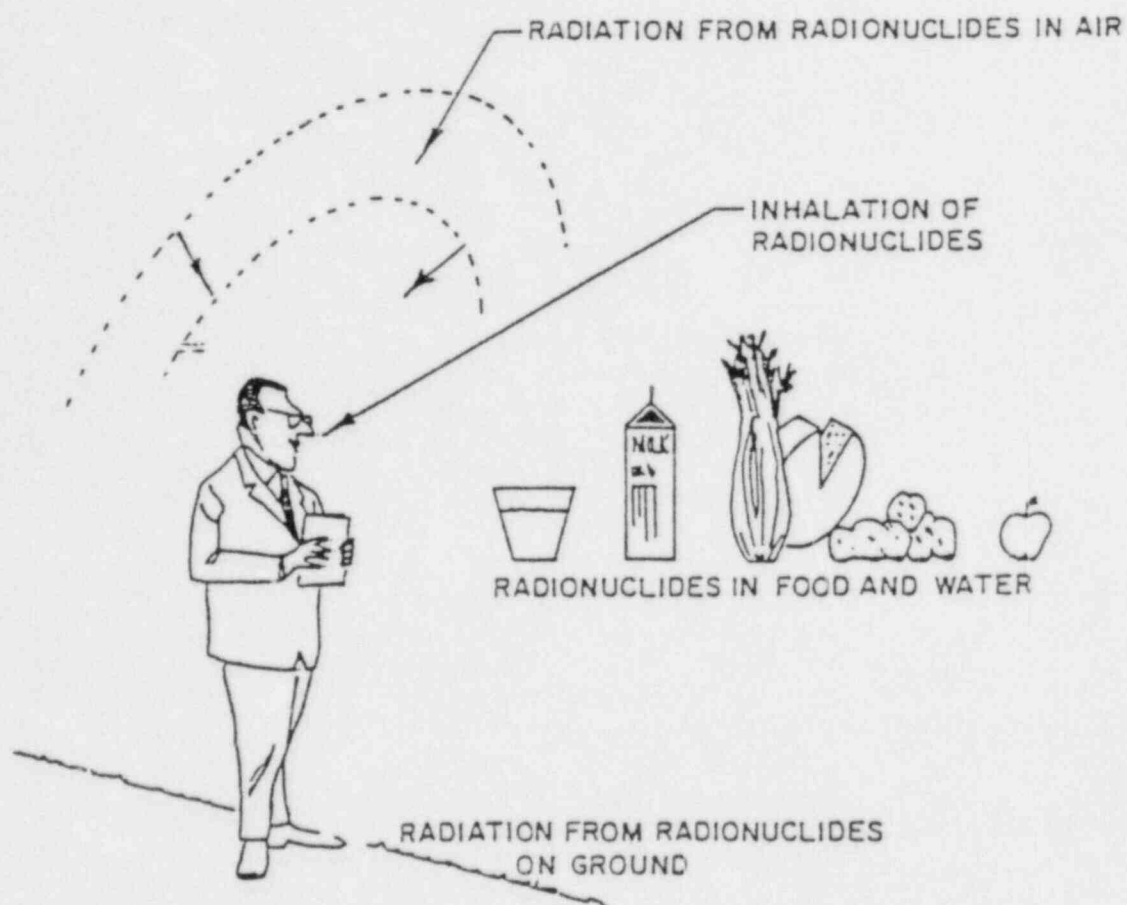


FIGURE 13-11
PATHWAYS TO MAN

effects. It is impossible to generalize about the relative importance of the other three pathways because their importance varies greatly depending on the radionuclide composition of the release and the organ for which the doses are being computed. The dose contribution from each of these three pathways (immersion, inhalation, ground) should be computed for every case. For specific instances, the relative importance of these pathways can be stated. The bone marrow dose is usually the most important factor in determining early fatalities. For the bone marrow and given a BWR-1 release, for typical weather conditions without rain, and less than one mile from the reactor, the immersion, inhalation, and ground contributions are all about the same magnitude for exposure times on the order of several hours or less. The exposure from immersion and inhalation from the cloud ceases once the cloud has blown by, but people in the area continue to receive exposure from the ground until the area is decontaminated or the area is evacuated. Thus, if the exposure times are long, the ground dose can eventually dominate the total dose. Tables 9-6 and 9-7 in the Procedures Guide show other examples of the relative importance of these pathways.

The immersion dose comes just from being in (or near) a "cloud" of airborne radionuclides. It is also called the cloud dose or "cloudshine", and it is easily calculated once the concentration in the air is known. The contribution of the inert gases to the total dose is largely via the external cloud pathway since their contribution via the inhalation pathway is usually not as large as it is for the other radionuclides. This is due to the fact that the inert gases are absorbed into the body from the lungs much less readily than are other elements.

Radiation from the ground, also called "groundshine", is similar except that the radiation comes from radioactive particles deposited on the ground on which the person is situated. If it is not raining, the dry deposition rate is low enough that the radiation dose from the ground is usually on the same order as the inhalation dose. A heavy rain, however, may wash out enough particles from the plume to make radiation from the ground the dominant contributor to the total dose over a limited area, even for short exposure periods.

To receive a cloudshine or groundshine dose, the recipient need not be in direct contact with the radionuclide. If some amount of material is placed between the recipient and the source, the recipient will be partially shielded from the radiation emitted by the fission products. Thus, a person sitting in a car on a contaminated highway would receive less dose than a person standing on the highway due to the attenuation of the radiation by the steel in the floor, seats, etc., of the car. A very small amount of liquid or solid will provide effective shielding for beta radiation. Gamma radiation is more penetrating, and the reduction in dose depends upon the mass of the shield material. Therefore, a person in a stone or brick house would receive less cloud exposure from a passing cloud than a person in a wooden house under similar circumstances.

The inhalation dose results from breathing air containing radioactive material. Except for the noble gases, some of the radionuclides inhaled will be retained in the nose, throat, or lungs and from there may pass on to other parts of the body. The International Commission on Radiation Protection (ICRP) lung model is generally used to model the absorption into the body. Where the radionuclides will end up depends on the element; iodine will be concentrated in the thyroid, calcium in the bones, and so on. The largest part of the inhalation dose comes from particles contained in the plume as it passes over a populated area. However, particles deposited on the ground during the passage of the plume may later become resuspended and then inhaled. The importance of the inhalation of resuspended particles increases with the length of the exposure period. It is very important for chronic doses and in determining whether a given area must be interdicted or decontaminated.

The ingestion pathway is much more complicated than the others since the radionuclides, except those in drinking water, have to be taken up by the plants and then be consumed by humans in either vegetable or animal form. Figure 13-12 illustrates a few of the many pathways available. The milk pathway is particularly important. There are many reasons for this. First, the dairy cow consumes a large amount of vegetation. If this vegetation is contaminated, several significant radionuclides (e.g., Cs-137, I-131, and SR-90) are concentrated in the milk. Second, milk is often consumed in the area of production and the time delay between production and consumption is short. Most other foodstuffs are stored for months, allowing the short-lived radionuclides to decay away. Third, milk is also a major food for children. Finally, milk is the primary pathway for I-131, one of the more common fission products. Its half-life is 8.5 days, so in food pathways, other than fresh milk, the bulk of it decays before ingestion.

The ingestion dose contributes very little, if anything, to the early effects from a severe reactor accident and is usually not computed. The importance of the food pathway is that it may determine how the area surrounding the reactor must be treated in the months and years following the accident. If the ground concentration is high, the land may have to be interdicted, i.e., withdrawn from human use, in order to keep people from accumulating a harmful groundshine dose.

It also may be necessary to restrict the use of crops grown on the land or the human ingestion of animal products, such as meat and milk, from the area in order to keep ingestion doses within required limits. Figure 13-13 shows the types of interdiction in decreasing order of severity from the source. Closest to the reactor, human entry may have to be prohibited for years. Further away, decontamination of land may be sufficient. Still further out it may be sufficient to destroy vegetable crops and milk. Obviously, the less restrictive conditions hold the more heavily contaminated regions; i.e., milk impoundment would be required in all four of the regions shown in Figure 13-13.

Note that this discussion of interdiction and the severity of offsite effects is generally predicated upon the older understanding of the form and amount of fission products that may be released from a serious core melt accident. If the current indications about the transport and retention of radionuclides are proven to be approximately correct, there may be a lot less material available for dispersion outside the containment and the offsite consequences will be considerably diminished from those implied in the foregoing discussion. For example, land interdiction or decontamination might not be required except on the plant site.

13.4 Dosimetry

Dosimetry is the process of calculating the radiation dose given the concentration of the various radionuclides in air, water, and food. As mentioned above, computing the whole-body immersion dose is fairly straightforward. The case is similar for the dose from the radionuclides deposited on the ground. The inhalation dose and ingestion dose are more difficult to compute because only a certain fraction of the material taken into the body will be absorbed, and there are many different paths a given radionuclide may take within the body. Figure 13-14 shows a model for the retention of material inhaled. Further, the material absorbed may be eliminated by the body before decay.

Most of the units in common use in dosimetry are defined in Table 13-2. The term person-rem (man-rem) is used to express population dose. It is simply the number of people involved times the average dose received by an individual in the group. The quality factor is a measure of how damaging a type of radiation is to the body. Alpha

FOOD PATHWAYS

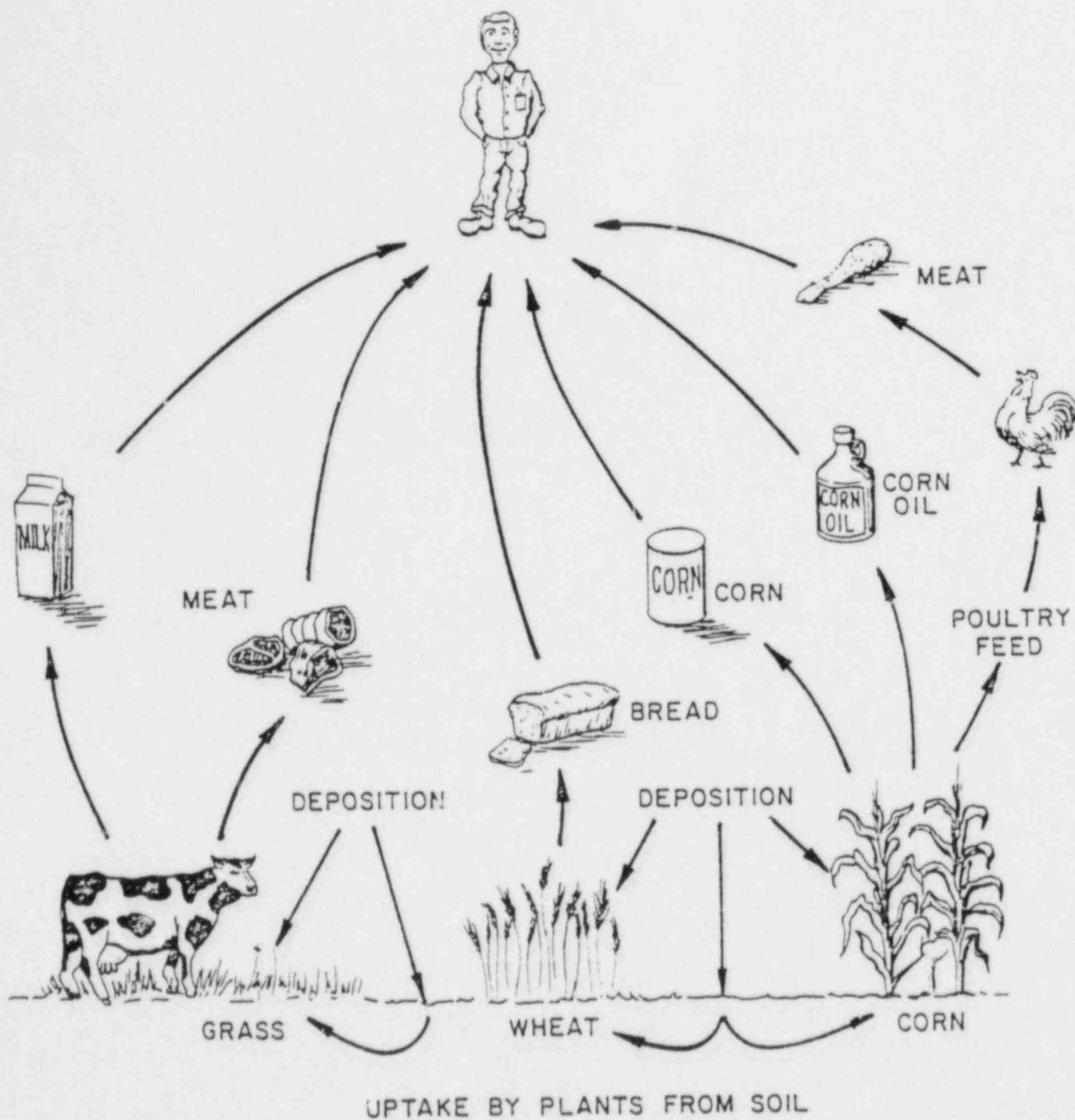


FIGURE 13-12
PRINCIPAL RADIONUCLIDE EXPOSURE PATHWAYS

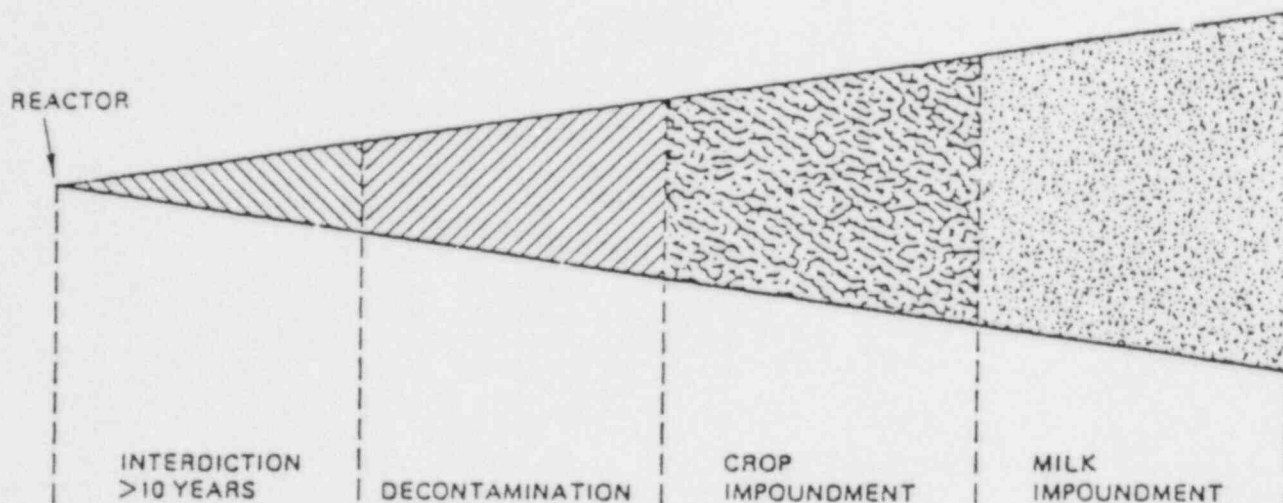


FIGURE 13-13
SIMPLIFIED INTERDICTION MODEL

SOURCE: Reactor Safety Study (WASH-1400). 1975.
Appendix VI, Pg. 11-2.

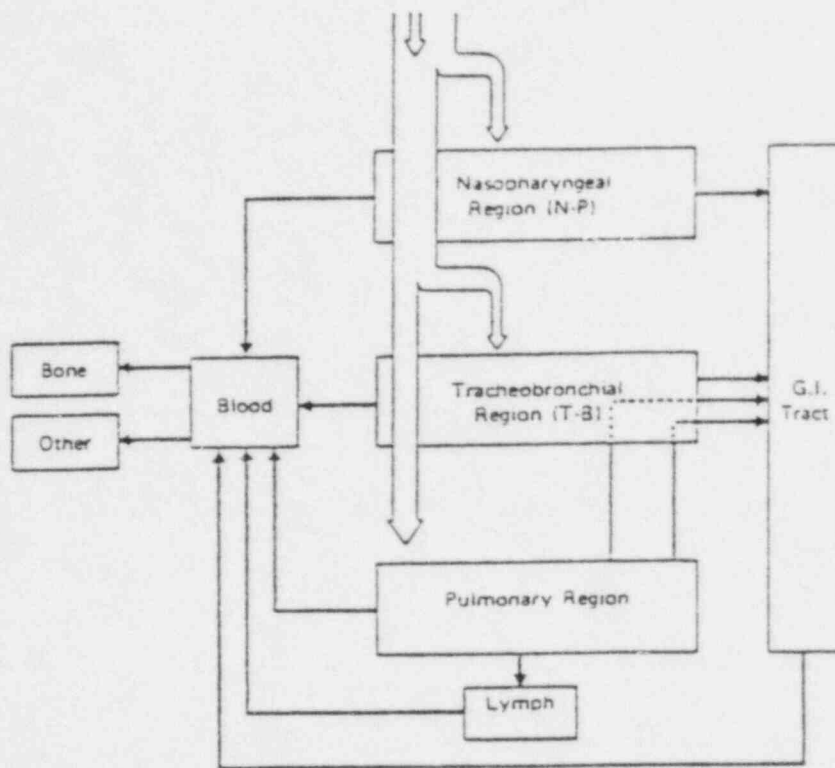


FIGURE 13-14
RETENTION MODEL

SOURCE: Reactor Safety Study (WASH 1400). 1975.
Appendix VI, Pg. 8-19.

TABLE 13-2

RADIATION AND DOSAGE UNITS

Roentgen (R) - is a unit of exposure of x- or gamma radiation based on the ionization that these radiations produce in air. An exposure of one roentgen results in 2.584×10^{-4} coulomb per kilogram of air, or 1 esu per cc of air standard temperature and pressure.

Rad - is a unit of absorbed dose for any ionizing radiation. One rad is 100 ergs absorbed per gram of any substance.

Gray (Gy) - is the MKS unit of absorbed radiation dose, $1 \text{ Gy} = 1 \text{ J/kg} = 100 \text{ rad}$.

Rem - is a unit of dose equivalent which is numerically equal to the dose in rads multiplied by appropriate modifying factors such as RBE (or QF) or DF. One rem is equivalent in biological damage to 1 rad of 250 kV x-rays.

Sievert (Sv) - is the MKS unit of dose equivalent, $1 \text{ Sv} = 100 \text{ rem}$. The Sv is related to the Gy as the rem is to the rad by an RBE a quality factor.

Relative Biological Effectiveness (RBE) - is a factor expressing the relative effectiveness of radiations with differing linear-energy-transfer (LET) values, in producing a given biological effect. This unit is now limited to use in radiobiology.

Quality Factor (QF) - is another name for a linear-energy-transfer dependent factor by which absorbed doses are to be multiplied to account for the varying effectiveness of radiations. This unit is used for purposes of radiation protection and is similar to the RBE unit used in radiobiology.

Dose Distribution Factor (DF) - is a factor expressing the modification of biological effect due to nonuniform distribution of internally deposited radionuclides.

Curie (Ci) - is a unit of activity, equal to 3.7×10^{10} radioactive disintegrations per second.

QUALITY FACTORS

<u>Radiation</u>	<u>QF</u>
X-rays, gamma rays, beta rays, and electrons of all energies	1.0
Fast neutrons and protons up to 10 MEV	10
Alpha particles	10

particles are more damaging than electrons (beta particles) because their mass is much greater and their energy is transferred to tissue in a very short distance.

Table 13-3 lists the types of radiation typical of the radioactive material in reactors. Gamma and beta radiation are the chief kinds of radiation emitted by fission products. Gamma radiation is a pulse of very high frequency electromagnetic radiation similar to X-rays. Beta radiation is an electron. An alpha particle is a helium nucleus or two protons and two neutrons. Fission products generally do not decay by emitting alpha particles, so the only alpha emitters in the radioactive material that escapes from containment after a severe accident are the heavy atoms like uranium and plutonium. The radionuclides which may escape from a light water reactor in an accident, do not emit significant numbers of neutrons. LET is an abbreviation for Linear Energy Transfer, that is the amount of energy transferred from the particle to the surrounding medium per distance traveled in the medium.

Alpha and beta radiation originating outside the body are not of as much concern as gamma radiation because they are absorbed at or near the surface of the skin. Gamma radiation is sufficiently penetrating that it does not matter too much whether the source is inside the body or outside it. The danger for alpha and beta radiation comes primarily from inhaled or ingested material which is located within the body where it will cause damage when the atom decays.

The ease with which radioactivity can be measured and the interest in small doses during the days of atmospheric bomb testing has led to substantial knowledge in this area. Widely accepted data is available in tabular form for all the organs of interest, different age groups, and all the radionuclides likely to be encountered. Regulatory Guide 1.109 and NUREG-0172 have been the common sources of this information. Some of the factors have changed significantly since the RSS was completed in the mid-1970's, but these changes do not affect the nuclides which largely determine the doses from severe reactor accidents and so the changes do not have a significant effect upon the consequences computed by PRAs.

13.5 Health Effects

The health effects model determines the risk to an average individual, in probability values for death or injury, of a given dose to a specific organ of the body. Everyone receives small radiation doses every day, and the effects of these small doses are not clear. Figure 13-15 illustrates some of the doses and sources of background radiation as well as showing other doses of interest. Note that the scale is exponential, and that background and cosmic ray doses vary over an order of magnitude just with location and elevation. Most people receive some medical and dental doses each year as well.

Health effects are divided into early, late, and genetic. Early effects are those that manifest themselves in the first year. These effects often appear in the first days after the exposure and include early or acute injuries and fatalities. The dose to the bone marrow usually determines the number of early fatalities, although the dose to the lung and gastro-intestinal tract may also be important. Early injuries (morbidity) are most commonly due to large doses to the thyroid, lungs, or gastro-intestinal tract. Late effects are those that appear in the exposed individual after the first year, primarily cancer. Genetic effects are more difficult to estimate and are often excluded from consideration.

The energy transfer in human tissue damages the body because it ionizes molecules in the cells, particularly water molecules. The ionization results in the formation of free

TABLE 13-3

TYPES OF RADIATION IN REACTOR PRODUCTS

<u>Type</u>	<u>Description</u>	<u>Characteristic</u>
a - alpha particle	helium nucleus	high LET, large mass
b - beta particle	electron	high LET, low mass
g - gamma radiation	electromagnetic	low LET, penetrating

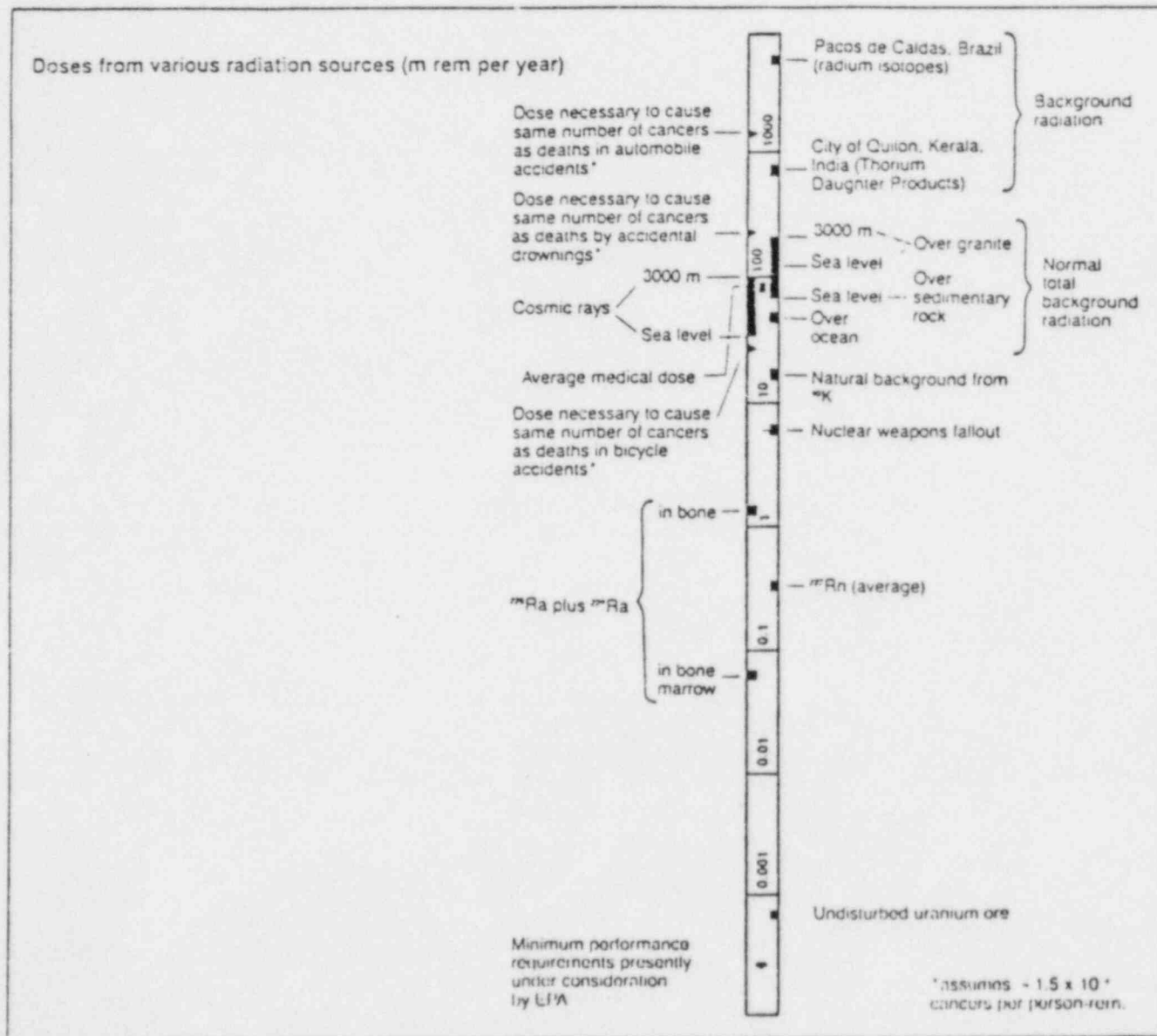


FIGURE 13-15
COMMON DOSES FROM VARIOUS SOURCES

Source: Hinga, K.R. Disposal of High-Level Radioactive Waste by Burial in the Sea Floor, Environmental Science and Technology. Vol. 16, No. 1, 1982.

radicals which are highly reactive and break chemical bonds, thereby altering other molecules in the cells. If the radiation dose is sufficiently large, enough molecules are ionized and enough free radicals are formed that the cell dies fairly quick after the dose is received. If the dose is smaller, the cell may not die but damage may be done nonetheless. Some of the molecules altered by the free radicals will be DNA, and a change in the DNA molecule may cause any new cells created from the damaged cell to be different from the original cell. Some of these new altered cells will lack the normal growth restraints, which is cancer. The body possesses some limited repair mechanisms which can compensate for a certain amount of radiation, but little is known about how they work.

The early effects are treated as threshold phenomena in most cases; that is, a threshold is established and individuals exceeding that threshold are included as injuries or fatalities. In the real world, of course, there are no precise thresholds, and an exposure that causes death to one may not cause death to another, so the threshold is a range of doses. In consequence modeling, when large numbers of people are being considered, the use of a specific dose level has been found satisfactory.

The relationship of radiation dose to the occurrence of cancer sometime later is not as straightforward as the relationship of dose to early effects. Whereas, early effects are usually shortly evident in all those who receive exposures near or exceeding the threshold, cancer may appear later in only a small portion of an exposed group. Thus, the effect of an exposure to a group becomes evident in the excess rate of cancer of a particular type, excess with respect to a normal or controlled group of similar individuals. For the specific individual who has been exposed, the chances of cancer appearing later can only be stated probabilistically. The problem is complicated by the fact that all of us are exposed to many low-level cancer-causing factors each day. It is often difficult to distinguish cancer caused by an occupational or accidental radiation dose from that due to the myriad other carcinogens to which an individual is exposed.

There are many models linking the radiation dose with the excess risk of cancer incident. Three of them are shown in Figure 13-16. The linear model has been used for many years. A few years ago some other models were proposed that reduced the risk of cancer due to the lower doses. Neither of the two nonlinear models shown has enough support to be widely adopted. Reanalysis of the amount of radiation emitted by the Hiroshima and Nagasaki bombs has led to a reevaluation of the evidence on the survivors. It appears now that the linear model may not be as bad as suspected. Note that Figure 13-16 shows a zero threshold, that is, no matter how small the dose there is some excess risk of cancer. While this is widely held to be the case, the evidence is very difficult to interpret once the dose levels reach background levels since so many other facts, such as smoking, complicate the analysis.

All radiation-induced cancers, except leukemia, have latency periods on the order of decades. The reason for this delay between the radiation exposure and the time when the effects manifest themselves is not known. Some cancers may remain latent as long as 40 years. The absolute risk used to express the incidence of latent cancers in the RSS is shown in Figure 13-17. There is also a relative risk model in which the current death rate is increased by a percentage based on the exposure.

The use of high doses of radiation in treating cancer may seem paradoxical in light of the foregoing. At high doses most of the irradiated cells are killed as explained above. A high radiation dose to a large portion of the body would therefore result in death. In cancer treatment, the radiation is confined to a very small portion of the body - the part expected to be cancerous. Most of the irradiated cells will be killed, leaving very few to

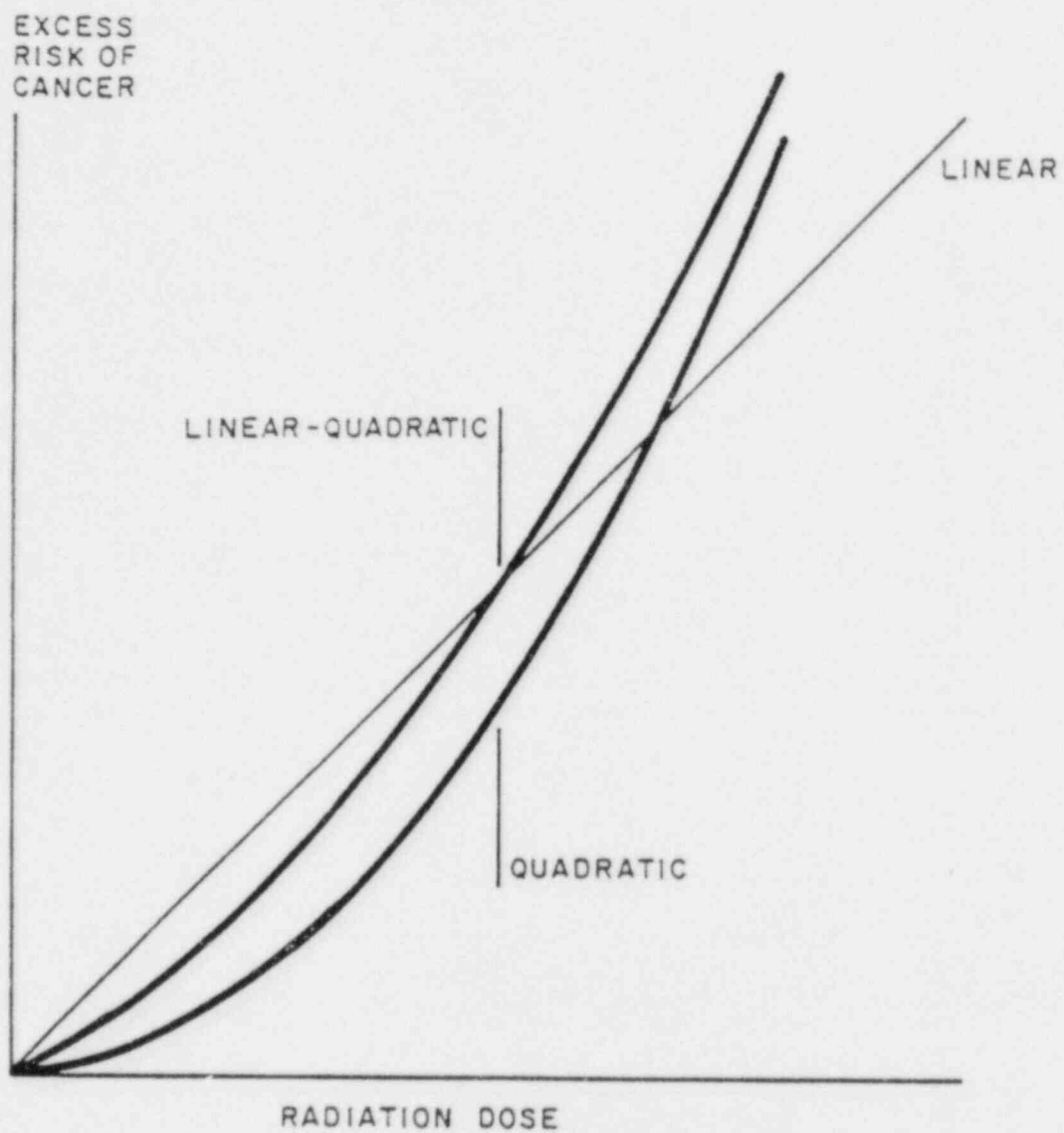


FIGURE 13-16
POSSIBLE RELATIONSHIPS BETWEEN
DOSE AND EXCESS RISK OF CANCER

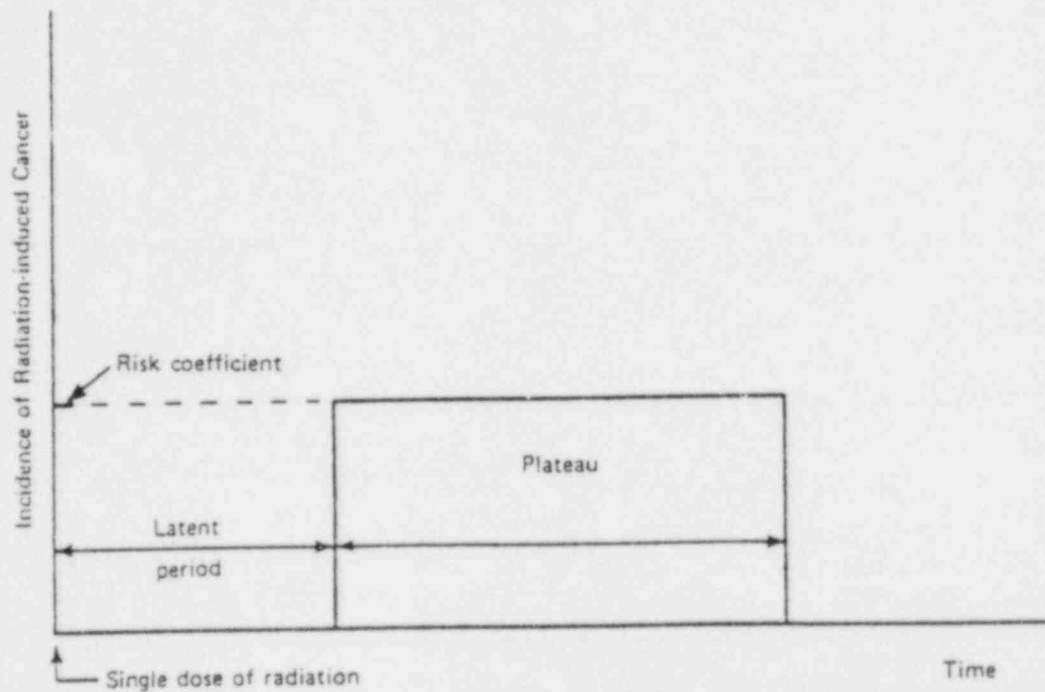


FIGURE 13-17
BASIC MODEL FOR LATENT CANCER FATALITIES

SOURCE: Reactor Safety Study (WASH-1400). 1975.
Appendix VI, Pg. 9-21.

produce mutant offspring. For those few that survive the radiation and may cause cancer, the latency period is so long that cancer resulting from the radiation treatment is not of great concern.

13.6 Mitigation Measures

Mitigation measures are any actions taken to reduce the effects of the release of radioactive material. Some of the measures are taken immediately; evacuation, sheltering, relocation, or the distribution of iodine blockers. Others are long term, such as land interdiction or decontamination or the impoundment of the vegetable or animal products from the affected area.

If there are no people near the plant where the air and ground concentrations will be the greatest, then the early health impact on the offsite population will be greatly reduced, indeed, deaths might be avoided altogether even for quite large releases. Thus, evacuation of the area surrounding the plant in case of an accident, was proposed many years ago. This measure has been considered more carefully since the Three Mile Island accident and there has been a great deal more emphasis on emergency planning and evacuation. The delay until the evacuation is ordered, and between the order and the time people begin to leave, and the evacuation speed are all important. Sometimes specific evacuation routes are considered, but usually a simple radial evacuation is modeled. In some cases, the entire area within a certain distance of the plant is evacuated, in others the distance to be evacuated is greater in the downwind direction, resulting in an evacuated area shaped like a keyhole as shown in Figure 13-18. The number of fatalities calculated are often very sensitive to the values chosen for the evacuation speed. More details about the evacuation models is contained in Appendix E of the Procedures Guide.

Sheltering is the term applied to having the nearby population take shelter at their present location rather than evacuate. This might mean remaining in the basement and breathing through several layers of wet cloth until the cloud has passed. Depending on the magnitude of the release, the evacuation rates and the number of people involved, sheltering is dependent upon such items as the fraction of houses with basements and the prevalent types of exterior construction, for example, wood versus stone or brick. Figure 13-19 shows the general nature of how the indoor and outdoor concentrations may be expected to vary. The time to leave is clearly at time T, but this time will vary from building to building (it is dependent upon the building's ventilation ratio, among other things) as well as the wind speed, so it is difficult to develop general guidelines to cover all the likely conditions.

During the Three Mile Island event, potassium iodide pills were actually procured, but they were not distributed. Discussions held after the panic subsided did not produce a consensus whether they should be issued in case of future events. Thyroid blockers such as potassium iodide, work by providing so much iodine to the body (especially the thyroid gland) that any radioiodine that is encountered later is likely to be excreted immediately because of the great surplus already available.

Long term mitigation measures can be carefully planned since there is time to survey the contaminated areas and determine exactly what levels of radiation are present. Interdiction and the impoundment of vegetable and animal products from the contaminated area have been discussed above. In some marginal areas it may be possible to decontaminate the area sufficiently to make interdiction unnecessary. For open land, decontamination usually takes the form of deep plowing. In settled areas, decontamination might take the form of washing the roofs and walls of houses and paved

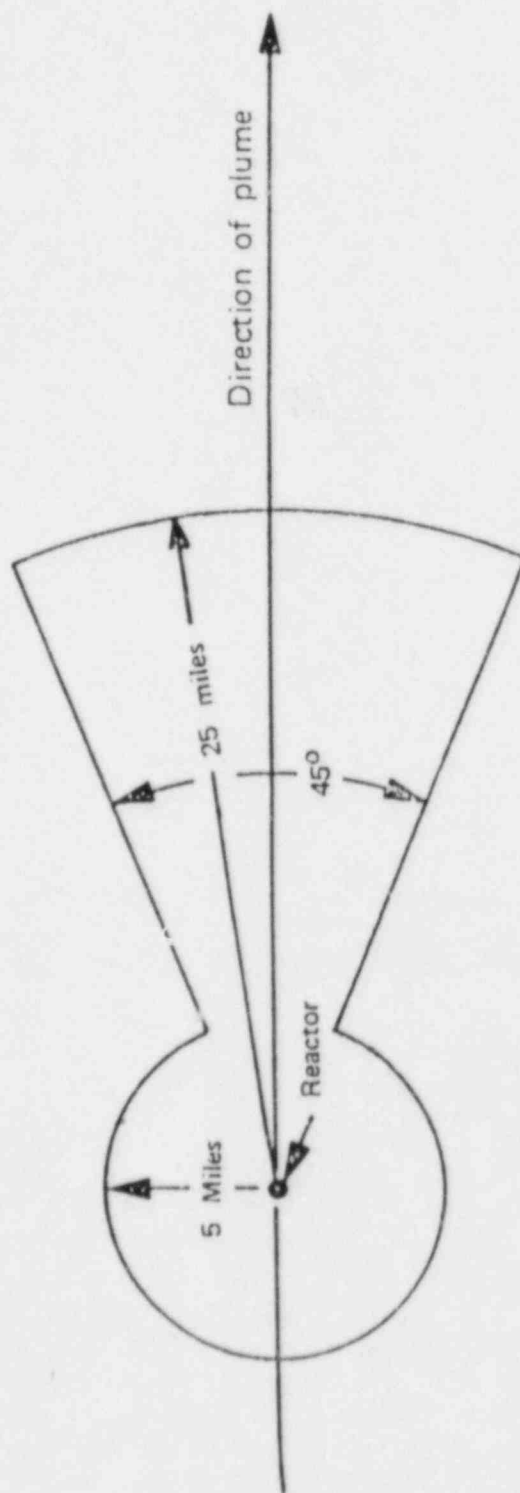


FIGURE 13-18
EVACUATION AREA USED FOR CCST CALCULATIONS

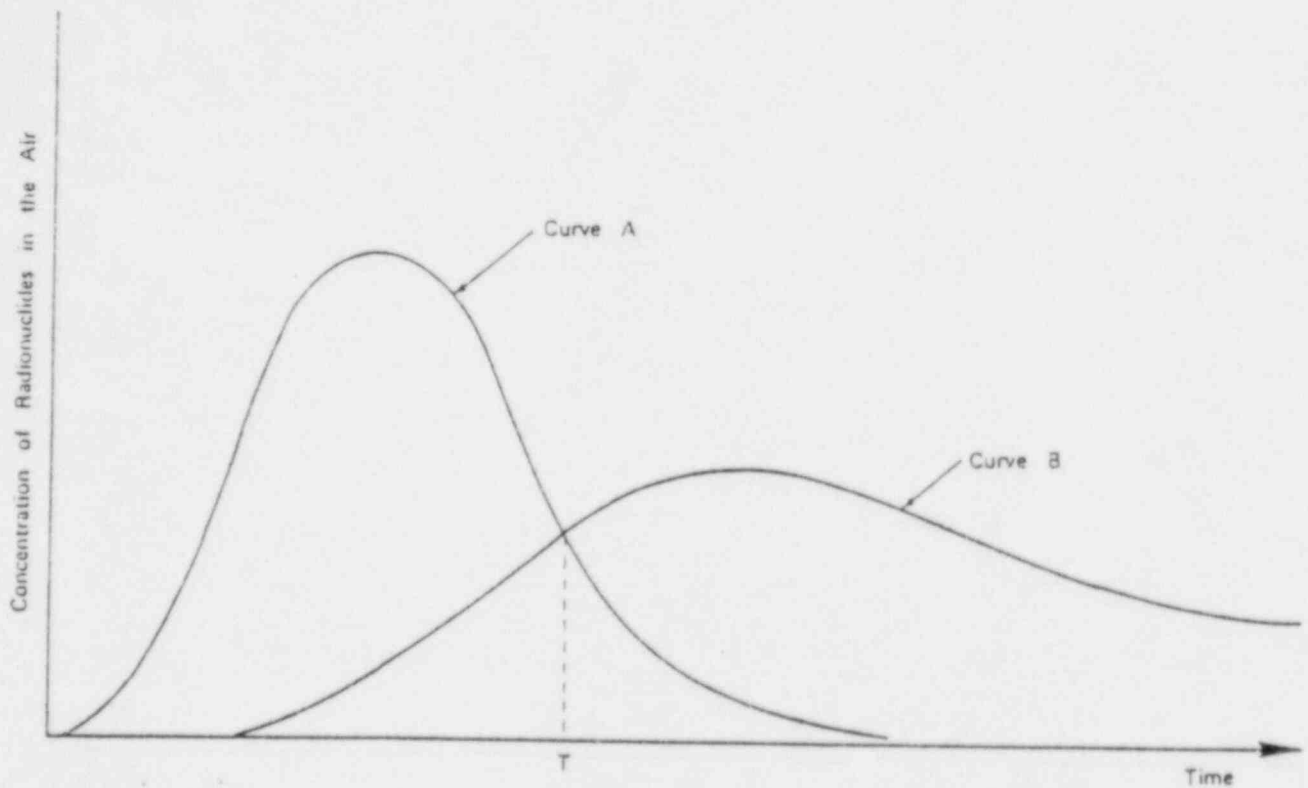


FIGURE 13-19
CONCENTRATION OF RADIOACTIVE MATERIAL OUTDOORS (CURVE A)
AND INDOORS (CURVE B) AS A FUNCTION OF TIME DURING THE CLOUD PASSAGE

SOURCE: Reactor Safety Study (WASH-1400). 1975.
Appendix VI, Pg. 11-10.

areas. Lawns might have to be plowed and reseeded. In other cases, it might be necessary to replace all the topsoil and paved surfaces to achieve suitably low levels of contamination. The pathways model, shown in Figure 13-20, shows why sometimes this would be required. The direct pathway from "soil" to "man" could consist of activities such as gardening or children playing in dirt. The resuspension of fission products already deposited is also possible as the lines from "vegetation" and "soil" to "man" indicate.

13.7 Computer Codes

There is so much data involved in a complete consequence model that only with the aid of a computer is it feasible to carry out the evaluation in any detail at all. As has been pointed out above, a great deal of meteorological, demographic, dosimetry, and health effects data must be manipulated in the course of the evaluation. Table 13-4 lists some of the consequence codes which have been developed so far. CRAC was the original consequence code for reactor accidents, developed in the early-1970's for the Reactor Safety Study. Some of the features of CRAC and almost all the other codes used in the U.S. are shown in Table 13-5.

CRAC was rather straightforward in many areas; for example, the dispersion model used was the straight-line Gaussian plume. Evacuation was assumed radially outward from the reactor. The evacuation began immediately upon notification and very slow average speeds were used to make the evacuation progress realistic. When the people of a sector were overtaken by the cloud while evacuating, they were assumed to remain at the location where they were overtaken until the cloud completely passed over them.

The consequence analysis performed with CRAC for the RSS had some unusual features since it was designed to determine the risk due to the first 100 reactors in the country. It used meteorological data for six reactor sites. Each site was taken to be representative of an entire region, and the 68 sites of the first 100 projected reactors were all assigned to one of these six regions. Wind speed and stability from each of the six sites was assumed to be representative of the entire region out to a distance of 500 miles. Wind direction was ignored. The rationale for this was that with so many sites being considered, and with only meteorological information for six, the assumption that wind direction would be purely random was fairly good. The population distribution for all 68 sites was considered in the computation.

CRAC2 is an updated version of CRAC developed in the late-70's for such purposes as site evaluations, emergency planning, and general risk assessment. Improved versions of the plume rise, washout, and dispersion models were introduced. Sheltering was introduced, and the evacuation model was improved by the addition of the delay between notification and the start of evacuation so that more realistic speeds could be used for the actual movement. The exposure of the evacuees to the entire cloud when overtaken was replaced by a simple calculation of exposure time. Site meteorological data was still assumed to be representative of the entire region, but a new sampling technique was introduced. In CRAC a stratified sampling method was used which ensured that each time of day was fairly represented in the sample. In CRAC2, prior sorting by category was used to make certain that each type of weather condition was included at the proper frequency.

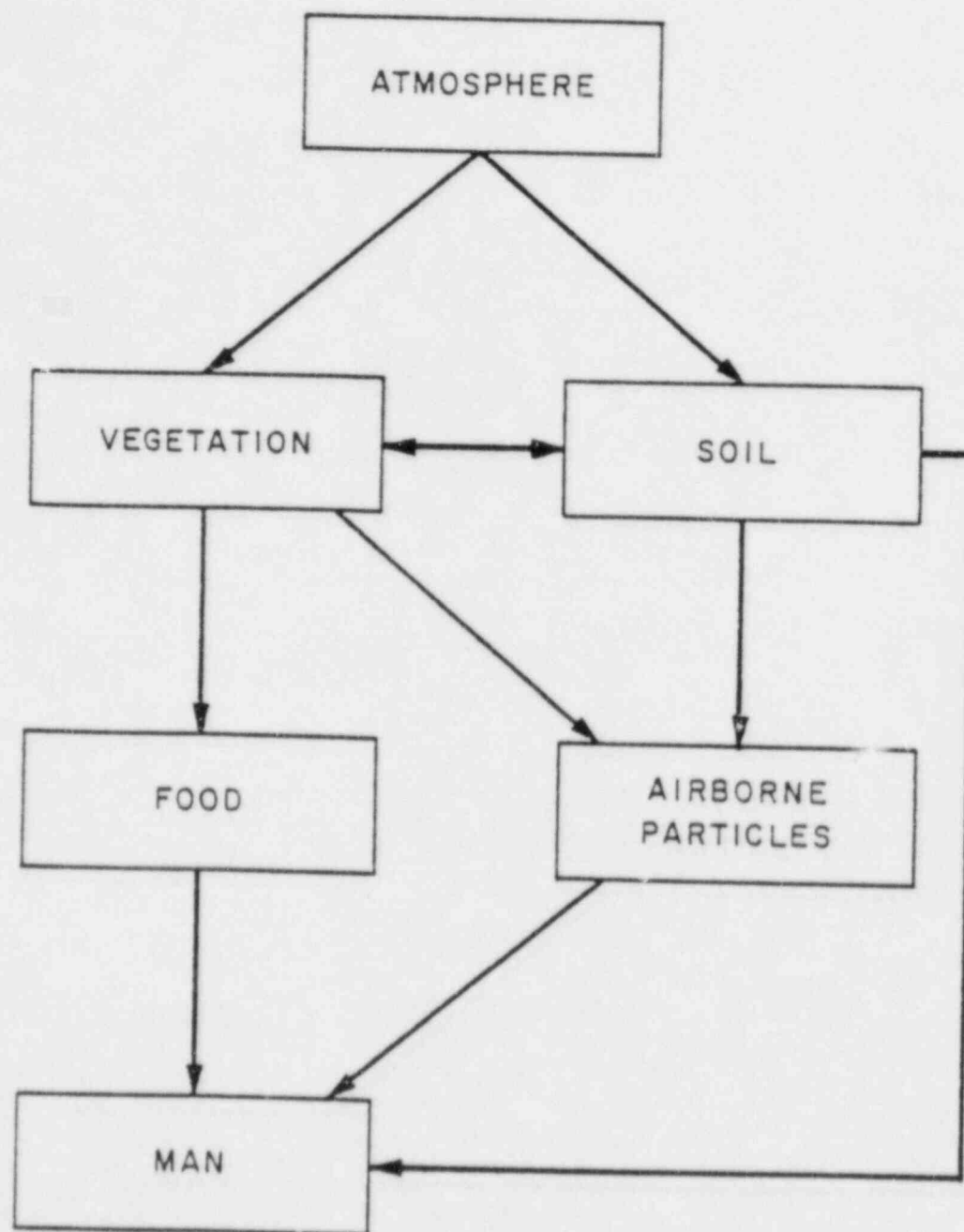


FIGURE 13-20
RADIONUCLIDE PATHWAY INTERACTIONS

TABLE 13-4

CODES AVAILABLE TO COMPUTE ACCIDENT CONSEQUENCES

CRAC	- Original RSS Code
CRAC2	- Derivative of CRAC
CRACIT	- Proprietary Modified Version of CRAC
NUCRAC	- Proprietary Modified Version of CRAC
UFOMOD	- German Consequence Code
TIRION	- United Kingdom Consequence Code
ALICE	- French Consequence Code
ARANO	- Finnish Consequence Code

TABLE 13-5

U.S. CONSEQUENCE CODES COMMON FEATURES

Meteorological Data (including sampling techniques)

Demographic Data

Numerous Radionuclides

6-10 Classes of Radionuclides

Wet and Dry Deposition (no washout in NUCRAC)

Evacuation

Inhalation, Ground, and Immersion Doses

Whole-Body and Several Organs

Mortalities and Morbidities

Crop Impoundment, Decontamination, Interdiction

CRACIT and NUCRAC are proprietary versions of CRAC2 which were developed for specific PRAs. The location of Zion on the shore of Lake Michigan was the justification for the extensive modifications made to CRAC2 to produce CRACIT. The major changes are:

- The straight-line plume model is not used - rather the model computes the trajectory of each segment of the plume as the wind changes with time.
- The actual terrain was modeled for the region within about 9 miles of the plant.
- Specific evacuation routes were identified for each sector within the evacuation radius.
- About ten sources of meteorological data were used, each assumed to be representative of a region in the vicinity of the plant.

NUCRAC was a less ambitious undertaking. The dry deposition model was much improved by the inclusion of a particle size distribution and a detailed settling model, and a detailed chronic exposure model via the food pathway was developed. However, it does not include a rainout model. The advantages and disadvantages of these four consequence codes are summarized in Table 13-6.

Even though a thoroughly debugged version of a consequence code may be properly installed on the computer system to be used, the prospective user is not ready to begin running the program. Large amounts of data must be gathered and put into the proper form as input data. Some of this material is invariant with the site being considered, the dosimetry and health effects data, for example, and may be supplied with the program. Other types of data are specific to the reactor site and will have to be gathered if this is the first use of a consequence code for that site.

The required input data may be divided into five groups:

- Description of site environs (including weather)
- Description of release
- Mitigation measures (including evacuation)
- Dosimetry and health effects
- Type of output desired.

The type of input data required for each area is specified in Tables 13-7 through 13-11. Much of this data, such as the meteorological, demographic and land use, and dosimetry data, is extensive and is usually supplied on tape.

The inexperienced user should exercise caution in specifying the types and extent of output required. There are numerous options available, and many of them produce copious amounts of output. The printout may be especially voluminous if detailed results of the intermediate stages in the computations are requested. More than 80 different consequence measures are available in the current version of CRAC2; many of these are not widely used. Plotting of the results is not generally available, so only tabular information is output.

The results of a consequence evaluation are usually given in plots known as CCDFs. This stands for Complementary Cumulative Distribution Function. The CCDF is a plot showing the frequency of exceeding a given consequence measure of damage.

TABLE 13-6

COMPARISON OF U.S. CODES

CRAC	<ul style="list-style-type: none"> • Original RSS Code - Superseded by CRAC2
CRAC2	<ul style="list-style-type: none"> • Advantages <ul style="list-style-type: none"> - Runs relatively fast - Only site meteorological data required • Disadvantages <ul style="list-style-type: none"> - Straight-line plume inaccurate when wind shifts markedly (e.g., shore locations) or in hilly terrain - Single site weather data may cause inaccuracies if the site is not representative of region
CRACIT	<ul style="list-style-type: none"> • Advantages <ul style="list-style-type: none"> - Plume travel more realistic - especially for shore or valley location • Disadvantages <ul style="list-style-type: none"> - Considerably more meteorological data required - Terrain data required - Code is considerably more complex - Takes longer to run
NUCRAC	<ul style="list-style-type: none"> • Advantages <ul style="list-style-type: none"> - Better dry deposition model - More detailed chronic exposure pathway • Disadvantages <ul style="list-style-type: none"> - Size distribution of released particles largely known - More input required - Increased running time - Washout ignored

TABLE 13-7

SITE AND ENVIRONS INPUT DATA

- A. Specification of Grid System
 - Number of Sectors (usually 16)
 - RADII

- B. For Each Grid Point:
 - Population
 - Fraction of Land Farmed
 - Type of Crops (e.g., dairy, non-dairy)
 - Month of Planting
 - Month of Harvest
 - Land Value

- C. Economic Data
 - Cost of Relocation, Interdiction, Decontamination, Evacuation, Substitute Milk Source, etc.

- D. Meteorological Data
 - Weather Records for One Year
 - Type and Extent of Sampling
 - Model Parameters

- E. Topography
 - Elevation and Surface Roughness if included in model

TABLE 13-8

RELEASE DESCRIPTION INPUT DATA

A. For Each Radionuclide Considered

- Name
- Amount
- Half-Life
- Type (e.g., inert gas, halogen, etc.)
- Daughter/Parent

B. Nature of Release

- Start Time
- Duration
- Warning Time for Evacuation
- Energy Associated With Release
- Height of Release
- Building Parameters for Wake Calculation

C. Parameters for Each Type of Nuclide

- Deposition Velocity
- Washout Coefficient

TABLE 13-9

MITIGATION INPUT DATA

A. Evacuation Parameters

- Delay Between Warning and Start of Evacuation
- Effective Evacuation Speed
- Shielding Factor While in Transit
- Radius of Circular Evacuation Area
- Width of Downwind Evacuation Area
- Radius of Downwind Evacuation Area

B. Sheltering Parameters

- Shielding Factors for Each Type of Shelter
- Types of Shelter Available
(e.g., fraction of houses that are brick, fraction with basements)
- Maximum Distance and Sectors for Sheltering
- Fraction of Non-Evacuating Population Expected to Seek Shelter

C. Contamination Levels Requiring

- Milk Impoundment
- Crop Impoundment
- Decontamination
- Interdiction

TABLE 13-10

HEALTH EFFECTS INPUT DATA

A. Dosimetry

Conversion factors to obtain dosage for the organs of interest from immersion, inhalation, and radiation from the ground

B. Acute Effects

Number of effects as a function of dose for the organs of interest

C. Latent Effects

Number of effects and time to appearance as functions of dose for various organs for early and chronic exposure

D. Chronic Exposure Pathways Data

Amount depends on complexity of pathways model

TABLE 13-11

TYPE OF OUTPUTS AVAILABLE

- A. Outputs Requested
e.g., early fatalities, latent thyroid cancer, area requiring decontamination
- B. Scales for Each Output Requested
- C. Detailed Print Options

Figure 13-21 is the summary CCDF from the RSS, which may be familiar. It shows the frequency of exceeding any number of fatalities per year for several causes of accidental death. The frequency of median number of deaths per year could also be used if a single number was needed to express the results of the consequence evaluation, but a considerable amount of information is lost in reducing the CCDF to a single number.

It is important to be aware of and keep track of the uncertainties in the consequence evaluation. Many of the events and occurrences modeled in the consequence evaluation are random or highly variable processes which can only be described statistically.

The very process of treating these processes statistically introduces uncertainties. Secondly, the models may contain inaccuracies due to the limitations on our knowledge. Finally, to make the evaluation manageable, it is necessary to group certain things in classes or categories. For example, the population in a sector is treated as all being at the center point of the grid, the accident sequences are placed in release categories, and atmospheric mixing is treated by the use of stability classes. This need for grouping also introduces uncertainties. The reliability of the results depends upon having a measure of all these uncertainties. Standard methods of statistical analysis can be used to track them through the evaluation so that confidence limits may be placed upon the results.

13.8 Items for Further Research

Areas where further research would be very useful are listed in Table 13-12. The first four items are generally more important than the last four. The substantial dispersion model improvements needed to model hilly terrain or local effects such as sea breezes were discussed briefly above in conjunction with CRACIT. The complexity added to the model was considerable, as were the data requirements introduced by using many sources of weather information. There is no generally accepted conclusion as to whether or not this added complexity and increased running time is warranted.

The expense and difficulty of doing large-scale, realistic deposition experiments and the very large variability in the results when such experiments are conducted, indicates that progress in this area will be slow. Even if better wet deposition data were available, the lack of temporal and spatial resolution of the rainfall rates still would preclude accurate modeling of deposition due to rainout and washout.

The problem posed by long-duration releases has been realized for some time. A more detailed dispersion model, such as the one in CRACIT, resolves (at substantial cost) most of the problems associated with the weather conditions changing during the course of the release. The complications posed by radionuclide composition, particle size, and chemical form changing during the release have not been examined in detail since so little is known in this area.

Interesting research is currently underway on the chemical forms of the more important fission products and the newly discovered retention mechanisms that operate passively in the reactor coolant system and the containment. If these investigations in fission product transport show that much less material will escape from the containment than had been previously thought, then the amount of radioactive material released, even from the most severe class of accidents, may be so low that some of the areas in consequence evaluation in which there is now a great deal of uncertainty may become less pressing.

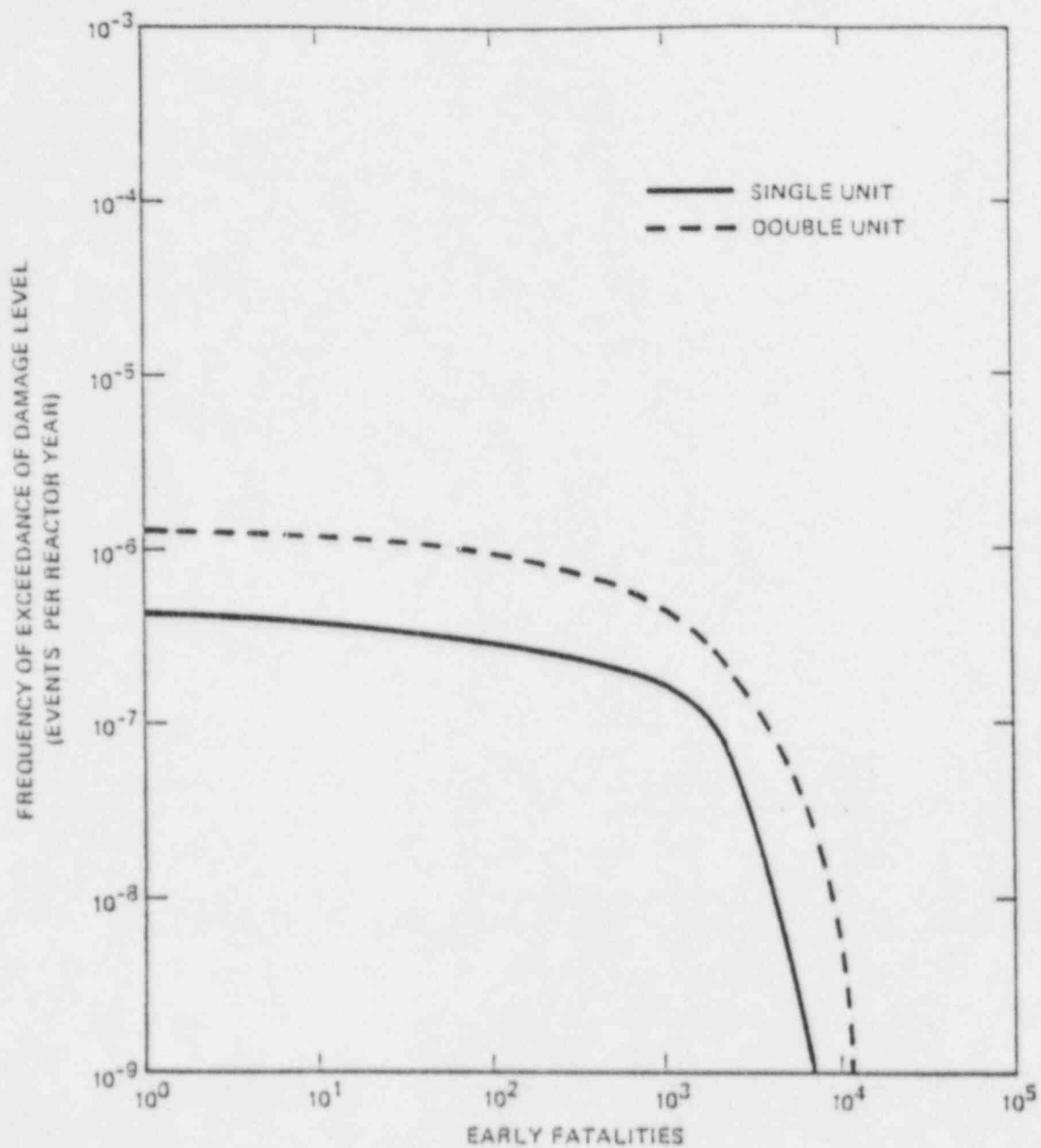


FIGURE 13-21
COMPARISON OF SINGLE AND DOUBLE UNIT
RISK OF EARLY FATALITY
(MEAN VALUES)

TABLE 13-12

ITEMS DESERVING FURTHER STUDY

- Differences in Modeling Required to Treat Complex Terrain or Dominant Meteorological Occurrences (e.g., sea breezes)
- Wet and Dry Deposition Processes
- Time-Dependent Nature of Long Duration Releases
- Dependencies on Particle Size and Chemical Form
- Chronic Exposure Pathway Modeling
- Costs and Effectiveness of Decontamination Procedures
- Economic Losses, Including Costs Associated With Health Effects
- Sensitivity to Source Term Assumptions

TOPIC 14
PRA INTEGRATION

14. PRA INTEGRATION

14.1 Introduction

Probabilistic risk assessments (PRAs) are extensive and complex projects that require large amounts of time and resources to complete satisfactorily. The scope of a PRA may range from an analysis of a few engineered safety systems to a full assessment that includes the effects of all the external hazards and computes all the risks to the offsite population. The objectives of the PRA naturally determine the scope of the project, so the first step in organizing a PRA is to clearly define the objectives and to determine the scope of the project.

It may be desirable to extend the scope of the project slightly beyond the minimum required by the objectives in order to utilize the material generated in the PRA for other purposes. By properly structuring the analysis and organizing the data, it may be possible to produce a study and a body of information that has wider uses with only a small amount of effort above that strictly required by the PRA. Three discrete levels of scope are commonly defined:

- Level 1 - Systems Analysis
- Level 2 - Systems, Accident Process, and Containment Failure Analysis
- Level 3 - Systems, Accident Process, Containment Failure, and Offsite Consequences Analyses

A Level 1 PRA consists of an analysis of the design and operation of the reactor and its supporting systems. The end result is a description of the sequences of events that are most likely to lead to a core melt and their expected frequencies. The emphasis is primarily on event trees for the accident sequences and the fault trees of the front line and important support systems. A Level 1 PRA does not concern itself with the frequency or mode of containment failure nor with the amount of radionuclides released or the consequences of that release. External events may or may not be included. The Level 1 PRA provides an assessment of plant safety only in terms of core damage frequency. It provides no information as to the nature of the offsite risk and does not distinguish between sequences with potentially high consequences and those with much smaller offsite consequences. The Level 1 PRA does allow insight into which systems in the plant are most likely to contribute to a core melt and how adequate the design, operation, and procedures are to safeguard the integrity of the reactor core.

A Level 2 PRA consists of all of the above plus analyses of the accident processes which will take place following the onset of core degradation, consideration of the possible failure modes of the containment, and the transport of fission products from the fuel to the containment and the release of some of the fission products upon the failure of the containment. In addition, to the results produced by a Level 1 PRA, a Level 2 PRA provides information about the time and mode of containment failure and predicts the amount of radioactivity released by each sequence or groups of sequences. Therefore, the accident sequences can be grouped according to severity of release. This provides some insight into the magnitude of offsite risk posed by the plant, but only in the most qualitative form.

A Level 3 PRA continues on to determine the offsite risk quantitatively by completing the consequence analysis, thus permitting a complete public health and economic estimate of the risk posed by the plant. Like the Level 1 PRA, the Levels 2 and 3 PRAs may or may not include the effects of external events. If external events are included, the specific events considered and the depth of the investigation will depend in part on the plant's location.

14.2 Information Requirements

Because of the depth and breadth of a complete PRA, large amounts of information are required. Of course, the amount of information needed is much larger for a Level 2 or 3 PRA than for a Level 1 PRA. Likewise, the amount of information required increases considerably when external events are included. The required information for any level PRA may be separated into four broad categories:

- Information about the plant design and operation
- Failure rate data (both generic and plant-specific)
- Information about PRA methods, statistics, the computer codes to be used, etc.
- Information about the site.

The information in the fourth category will consist of the material required if an external events analysis is to be performed or if the consequences analysis is included.

A Level 1 analysis requires the final safety analysis report (SAR); 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 a description of the plant design and operation that is as complete as possible. Other studies performed on the plant may also prove useful. Discussions with design engineers and plant personnel should be held throughout the PRA to ensure that the information used in the analysis is complete, current, and 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. The time at which the PRA study is done (for example, before or after initial operation) will influence both the amount and the detail of the available information.

For a Level 2 analysis, additional detail is needed on the reactor coolant system to allow thermal-hydraulic modeling. Dimensions, masses, and materials of the containment are required to compute the containment response. If a complete structural analysis is to be performed to determine the containment failure location and pressure, then detailed information on the design and construction of the containment structure is needed. For the fission product transport model, the surface areas of various materials in the reactor coolant system and containment must be available.

In addition to the above, site-specific meteorological, demographic, land use and value, and mitigation (e.g., evacuation) data are required. General pathways, dosimetry, and health effects information is usually sufficient and is often supplied with the computer model.

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 and the location of equipment is necessary to analyze susceptibility to fires and floods.

14.3 PRA Tasks

To meld the PRA together into a coherent whole, numerous tasks and subtasks must be integrated together. This will be much easier if the tasks have been carried out as part of a well-planned and directed effort, and if a team approach has pervaded the entire project. The task of combining the results of the many portions into a complete whole will be difficult, if not impossible to carry out thoroughly, if each group in the project has worked in isolation from the persons employed on the other tasks. The major tasks in a complete Level 3 PRA including external events are:

- Systems Analysis
- Accident Process and Containment Analysis
- Consequence Analysis
- External Events Analysis
- Uncertainty Analysis

Since the final uncertainty results will depend upon the uncertainties in every stage of the PRA, it is extremely important that the people responsible for the uncertainty analysis are completely involved in the four major tasks from the beginning. These major tasks and the subtasks that comprise the first three are summarized below.

Figure 14-1 illustrates the major steps in the development of a PRA and the connections and feedback between the various steps. Figure 14-2 is a different illustration of the PRA process, showing in more detail the various subtasks involved.

System Analysis - This task consists of the five subtasks briefly described below. It constitutes a major portion of the risk assessment. 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.

Event Tree Development - The event tree development subtask delineates the various accident sequences. This activity includes an identification of initiating events and the systems that respond to each initiating event. 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. Separate event trees are generally constructed for each initiating event or class of initiating events having a unique event tree structure.

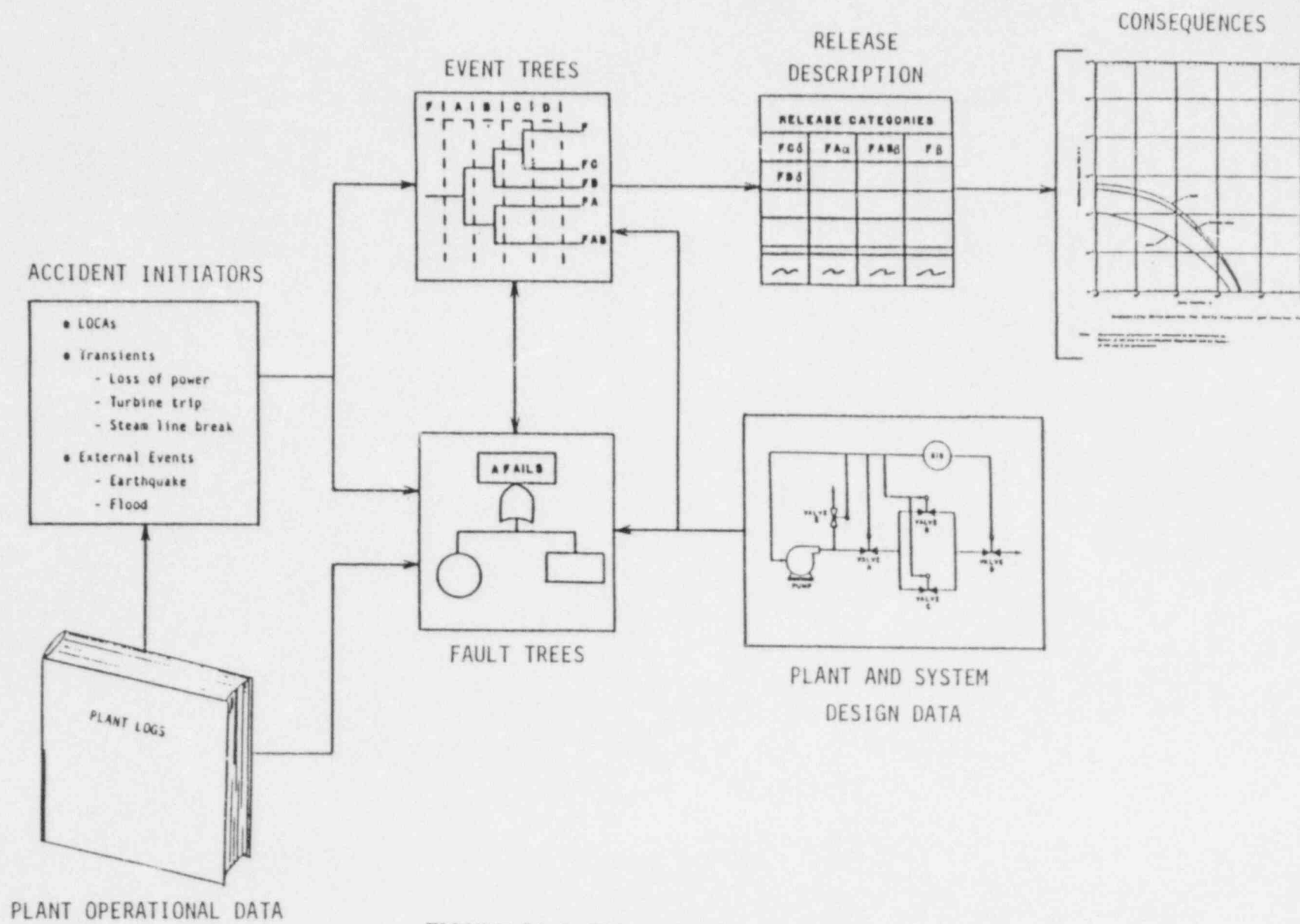


FIGURE 14-1 PRA ELEMENTS

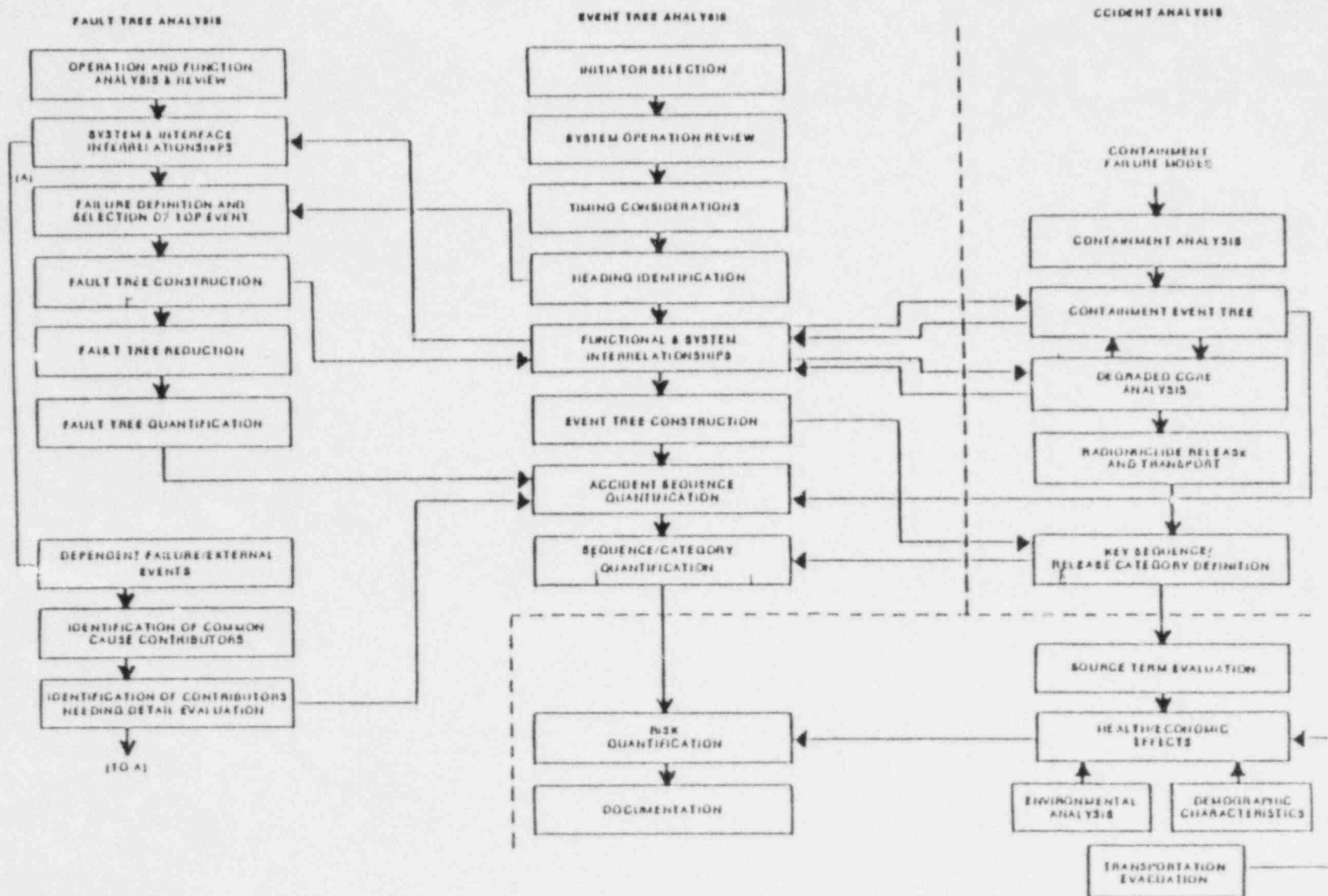


FIGURE 14-2 GENERAL PRA ACTIVITY FLOW DIAGRAM

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. Common cause contributors and potential systems interactions should also be included to ensure proper integration into the analysis.

Analysis of Human Reliability and Procedures - Past PRAs have shown the importance of human errors. This analysis involves a review of testing, maintenance, and operating procedures to identify and quantify 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.

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.

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 is used to identify and quantify the combinations of events that constitute the accident sequence.

Accident Process and Containment Analysis - PRAs performed at Levels 2 and 3 include analysis of the progress of the core degradation, the transport of fission products from the fuel, and of the response of the containment. This analysis is important for determining the consequences of various core melt accident sequences and consists of three subtasks. The results of this analysis constitute the products of a Level 2 PRA and consist of an identification of containment failure modes and a prediction of the fraction of the initial radionuclide inventory released to the environment for each accident sequence.

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 modeling of these processes. The results are insights into the phenomena and timing of the degradation and melting of the core and a prediction of the stresses placed upon the containment.

Analysis of Containment Failure - 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. For example, containment failure may cause core melt if the recirculation pumps keeping the core covered lose net positive suction head (NPSH) when the containment fails.

Analysis of Radionuclide Release and Transport - For each core melt accident that is postulated to breach the containment, it is necessary to estimate the fraction of the inventory of radionuclides that would be available for release to the environment. A computer model is used to track the radionuclides released from the reactor fuel during the accident and to assess their transport and deposition inside the containment before containment failure. The result of this analysis is a prediction of the rate of fission product released into the environment.

Consequences Analysis - To assess the plant risk to the surrounding population, it is necessary to calculate the consequences of the release in addition to the frequency of the accident and the quantity of released radionuclides. Consequences are generally expressed as early fatalities, latent cancer fatalities, and similar measures. To perform this task, the analyst uses a computer model that begins with the radionuclide releases from the containment and analyzes their transport through the environment to determine the time-dependent concentrations in the air and on the ground downwind of the plant. This is all done for a statistically representative sample of weather conditions. Information on pathways, dosimetry, mitigation measures and 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. 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.

Analysis of External Events - External events, frequently excluded from risk assessments, include such occurrences as fires, earthquakes, and floods. This task uses the models developed in the plant system analysis which are either analyzed independently from the perspective of external events or else are modified to treat external events explicitly. Additional event trees are developed to delineate the external event sequences to be analyzed. The results of the external events analysis may be incorporated into the analysis at several different places as discussed in Section 10.

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 are 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 may provide insight into the possible range of results.

14.4 Integration of the Tasks

Integration of the numerous tasks in a PRA involves much more than just taking the output from one group and passing it to another group as input. Even if no iteration is required, the scheduling must be such that the information is available when needed. More importantly, the output of the first task must contain the information required by the second task, in a form that is readily usable. Thus, it is the job of the technical director to ensure that each task leader understands what output is required and what form it must be in. Detailed schedules and clear and complete task definitions are prerequisites for a smooth integration.

When iteration between tasks is required, then the involved task groups obviously must coordinate closely. This will be facilitated by written task objectives and interfaces so that the limits of each task are known before the first iteration. Leaving the details of the iterative interaction to be worked out by the task groups during the first one or two iterations is likely to result in certain parts of the work being duplicated and other portions not considered at all.

On a project scale, the interrelationships to be considered are those shown by the arrows and lines in Figure 14-1. In some cases, one or more tasks provide the integrations link. For example, the accident process and containment failure analyses provide the integrating link between the box labeled "Accident Sequence Delineation" in Figure 14-1 and the box labeled "Accident Damage Categories."

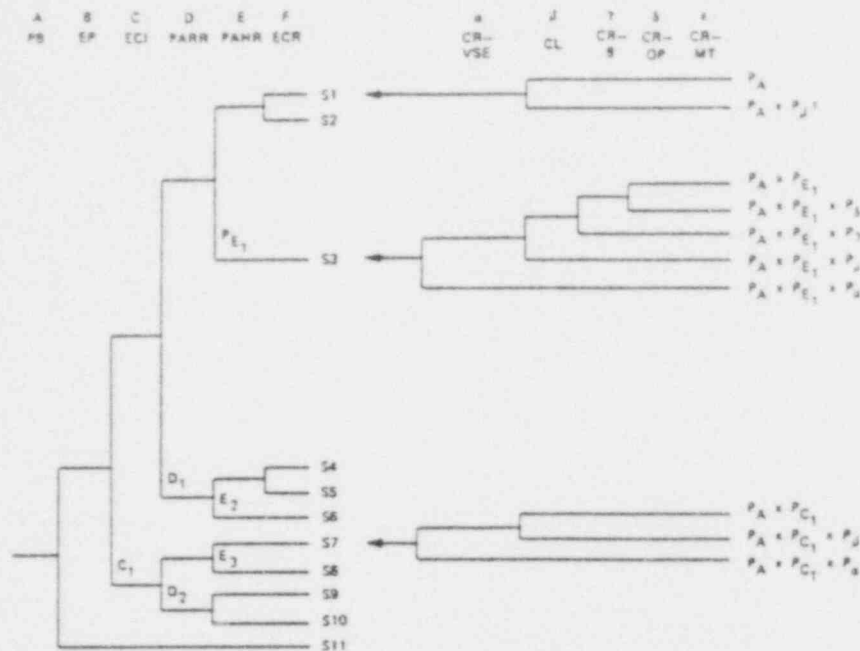
In other cases, a particular method provides the links needed to integrate the relationships between the various tasks or subtasks. For example, the accident sequence event trees provide the formal link between the initiating events and the system failures. Similarly, the fault trees provide the means of linking the system failures with component faults and operator errors. The relationship between system failures and containment failure modes, on the other hand, is not so formal of a process: the initiating event and the system failures define the sequence and physical models are used to estimate the stresses placed upon the containment. The link between the containment failure modes and the release categories is provided by the fission product transport analysis.

The integration process is often considered part of the quantification task since it is at this point that all other tasks are brought together in the process of starting from the basic failure rate data and deriving the final numerical values for the project. Some steps such as the utilization of the failure rate data in quantifying the fault trees is straightforward and requires little discussions. Some of the steps which are not so obvious are those between the event trees and the release categories:

- Link event tree sequences to containment tree
- Eliminate unnecessary combinations
- Group remaining sequences by release category
- Calculate sequence probabilities
- Calculate release category frequencies.

These steps have been discussed at different points in the preceding sections, but this listing shows how they are used together in the integration procedure.

One of the major steps is the linking of the event trees for the system failures with those for the containment response. As illustrated in Figure 14-3, different end points in the systemic event tree may require different containment trees. It is also clear that the number of discrete sequences, when the containment failure modes are considered, can become quite large. This problem is treated in several ways. First, the end points in which the containment does not fail or only fails by basement melt-through are not considered further since the offsite consequences are negligible compared to those containment failures in which a hole above ground allows the radioactive material direct passage to the atmosphere. Also, end points of low relative probability and low consequences may conservatively be lumped in with other end points. Finally, the remaining sequences are grouped into release categories or consequence bins.



† Represents a spectrum of leakage rates that should not be interpreted in terms of the failure definition for CL on the Containment Event Tree.

FIGURE 14-3
LINKING OF ACCIDENT AND CONTAINMENT EVENT TREES

SOURCE: Reactor Safety Study (WASH - 1400). 1975. Appendix I, Pg. I-31.

14.5 PRA Objectives

If they are to be useful, the results of the PRA must be substantiated and fully documented. This is a large and time consuming task. It is the responsibility of the PRA project management to ensure that the documentation is complete and easily readable and that the data and other bases for assumptions are set forth in sufficient detail. All major assumptions made in the analysis should be discussed and, where possible, supporting analyses in the literature should be cited. The report should describe all tasks of the analysis in enough detail to permit the reader to understand how the plant systems work, to independently calculate the frequencies of the dominant accident sequences, and to at least understand the derivation of quantities that are important in the assessment of public risk.

Table 14-1 illustrates a possible analysis team composition for a Level 3 PRA. In addition, due to the quantity and nature of the reports generated, in the later stages of the project several typists, draftsmen, and graphic artists will be required.

Computer codes will be needed for the analysis. The number of codes and particular ones to be used depend on the scope of the analysis and the preference of the analysts. Computers compatible with the programs must be available.

Members of the analysis team occasionally will 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.

It is desirable for all the analysis team to have offices located in the same area for the duration of the project. This improves communication among the members of the team and facilitates consistency in approach and assumptions. Adequate office space and computer access should be secured before the beginning of the study.

14.6 Schedule and Manpower

A PRA consists of many tasks and subtasks, as discussed above. Several of the tasks can be performed in parallel; others depend on the products of a previous task and hence must be performed sequentially. The experience of the personnel, the availability of data and the computer programs, and the total manpower assigned will all affect the scheduling of a PRA. Among other factors that may affect the effort needed are the age of the plant, its operational status, the available documentation, peculiarities of containment design, and the availability of similar analyses on similar plants.

Table 14-2 contains estimates of the effort required (presented in the Procedures Guide). A discussion of this table, task by task, may be found in Subsection 2.4.1 of the Procedures Guide.

The minimum amount of time needed to complete a Level 1 PRA is about one year. Allowing only 12 months from start of funding to publication of the final report is a very ambitious goal and requires high manpower availability at the beginning of the effort in addition to a large writing and editorial effort at the end. Compressing the entire PRA into this short of a period does not make the best use of either personnel or funds. The technical quality may suffer in such an accelerated project unless there is team leadership, completeness, and consistency from the beginning. If a recent PRA for a similar plant is available and the objectives allow many of the system models and most of

TABLE 14-1
TYPICAL PRA TEAM MAKEUP

1	Team Leader/Integrator
7	Systems Analysts
1	Human-Reliability Specialist
2	Data Analysts
2	Sequence-Quantification Specialists
3	Physical Process Analysts
1	Structural Analyst
2	Radionuclide-Transport Analysts
2	Environmental Transport Specialists
8	External Event Analysts (if included)

TABLE 14-2
ESTIMATED MANPOWER PER TASK

<u>Task</u>	<u>Manpower Estimate (man-months)</u>	
Initial Information Collection	1-2	
Event Tree Development		
Systems Modeling	29-38	
Human-Reliability and Procedure Analysis	2-3	
Data Development	5-6	
Accident Sequence Quantification	9-12	Level 1 = 51-86
External Events*	14-18	
Uncertainty Analysis	3-4	
Development and Interpretation of Results	2-3	
Analysis of Physical Processes	15-137	
Analysis of Radionuclide Release and Transport	5-20	
External Events*	3-4	Level 2 = 78-285
Uncertainty Analysis (additional)	2-8	
Development and Interpretation of Results (additional)	2-30	
Analysis of Environmental Transport and Consequences	3-4	
External Events*	1-2	
Uncertainty Analysis (additional)	1-2	Level 3 = 80-295
Development and Interpretation of Results (additional)	1-2	

*May or may not be included in the analysis.

the failure data from this PRA to be used instead of developing new models and data for the plant being analyzed, then a schedule extending over less than a year is certainly feasible. In this case, however, the resulting PRA is not a detailed PRA of the actual plant. The RSSMAP studies are examples of this type of analysis.

It is more usual for a complete PRA to take 16 to 24 months to complete. This includes several months for preparation, review, and revision of the final report. The final report for a Level 3 PRA including analysis of external events occupies several large volumes. Completeness and consistency in such a large document requires several months of effort by the team leadership and a few chosen personnel from the analysis staff. Thus, it may be possible to complete the technical analyses for a Level 1 PRA in a year or less, but the final report will take several more months to prepare. It is not unusual for a PRA to require two years to complete and some have taken much longer. Note that the RSS should not be used for comparison. Being the first major study of its kind, a great deal of effort was expended in data collection and development as well as in model, methods, and computer code development that has not been repeated in any subsequent PRAs.

14.7 Assurance of Technical Quality

The assurance of technical quality refers only to the assurance of quality for the PRA itself. Theoretically, a PRA is of high technical quality if it accurately and completely portrays and reflects reality. This is a very difficult attribute to measure. Therefore, a PRA is considered to be of high technical quality if it satisfies all of the following:

- PRA methods are used correctly and appropriately
- Information about the plant is complete and current
- Methods, assumptions, and judgments are clearly set forth
- Data bases are appropriate and utilize all available sources
- Development of the risk indices is scrutable from the data base through the sequence results
- Documentation is clear and complete.

There is no simple or certain formula for the quality of 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 care taken in the initial planning of the program will have a great effect on the quality of the study. 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 leadership.

To achieve quality in general, PRAs should be reviewed at four levels: study team, plant operating personnel, peers, and management. The first review of the work done should be carried out by the technical director and an internal peer group. Although this review should cover all aspects of the study, it is at this level that inappropriate methods and insufficient data bases are identified with the greatest confidence. It is desirable to have the PRA reviewed by persons familiar with the plant design and operation, as well as with the utility operating practices. Technical errors concerning representation of the

plant and misinterpretation of operating procedures should be identified in this review. The peer review should be carried out by 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. The level of review should concentrate on perspective, scope, and product suitability in meeting program objectives. The reports from the peer review should be part of the management review.

14.3 Summary

In summary, the performance of a PRA requires the successful blending of a number of different skills and disciplines. The degree to which this can be successfully done largely determines the success of the overall study.

Integration of PRA tasks goes far beyond tracking technical progress on the various tasks. Successful integration includes the selection of the appropriate analytical techniques in such a way that those techniques are fully compatible with one another. In addition, PRA integration must include the assurance of technical quality.

Without successful integration of PRA tasks, the study will remain, at best, a collection of disjointed parts. Through the integration of tasks, the study becomes more cohesive and complete.

TOPIC 15
STRENGTHS AND LIMITATIONS

15. STRENGTHS AND LIMITATIONS

15.1 Introduction

As in any complex, multidisciplinary study, the results in certain areas are considered to be stronger than those in other areas. That is, in some areas there is greater confidence that the results are accurate, the uncertainty is low, and that no important factors have been overlooked. A weak area is one where many severe limitations must accompany the results; perhaps the underlying data base was sparse or not entirely appropriate, or perhaps it is an area where human knowledge and experience are very limited, or maybe certain assumptions had to be made for reasons outside the control of the analysis team. This entire question has been discussed in some detail in NUREG-1050 from which much of the following discussion is drawn.

The strength or weakness of a given area only partially reflects the time and effort that have gone into the analysis; it may reflect the complexity inherent in the phenomena involved or it may indicate the level of human knowledge about the area. Finally, there are certain events that are both random and infrequent, so that our observation time is so limited that a good deal of uncertainty would remain if our understanding of the event was much better than it currently is.

It cannot be expected that all the disciplines utilized in a PRA will have reached the same level of development or maturity. For example, the methods of reliability analysis have been used in various forms and in many different areas since World War II, whereas, the analysis of core melt progression was first done in the 1970's (in any detail) and is unique to nuclear reactor technology.

The strength of an area of PRA may be characterized by its level of development or its maturity. The level of maturity depends on the stability of the method, the degree of realism, the degree of uncertainty, whether major progress is desired to improve the method, and whether it is feasible to achieve that progress, especially in the short-term. Using these indicators of maturity, the overall level of maturity of each PRA element can be gauged. Decisions based on mature methodologies, in general, are expected to elicit more confidence than decisions based on less mature approaches.

A "stable" method is one that has not changed for a considerable period of time. An "unstable" method is one subject to fast-moving developments. Applying, or using the results of an unstable method requires greater caution. This does not, by any means, imply that a stable method is always highly accurate and free of error.

The level of maturity in the various elements of a PRA study also depends on the nature and degree of uncertainties in the results and the degree of realism in the models, because both must be reasonably appropriate for the desired application. Uncertainties arise because the available data are insufficient to allow some parameter to be characterized with the desired precision, there is no consensus in the technical community on the issue, or the facts are simply unknown. The realism of a model may be decreased by the introduction of conservative estimates as a substitute for unknown information or merely for the purpose of simplifying the model. The realism of a method refers to the extent that approximations or conservatisms have been knowingly or unknowingly introduced because of unknowns, merely to simplify the models, or perhaps because by error.

It is important to recognize that uncertainties are not unique to PRA. Uncertainties due to a lack of data or knowledge about system response, human behavior, or accident phenomena are present in estimates made by means of PRA techniques as well as in deterministic modeling or so-called engineering judgment. They reflect current experience and information as well as the state of the overall technology. PRA analyses display uncertainties more explicitly than do some other analytical approaches, even though the extent of the uncertainty may be the same or less. A proper uncertainty analysis provides an estimate of how much this lack of experience and knowledge affects engineering insights drawn from PRA. This is done by propagating uncertainties through the analysis or by performing sensitivity analyses. Thus, the treatment of uncertainties should logically be considered a strength of PRA rather than a limitation.

15.2 Plant Modeling and Model Evaluation

The methods currently in use (event and fault trees) are basically the same as those used in the RSS, although refinements have been made to improve the scope and depth of modeling. This aspect of PRA is generally considered to be mature, except for the treatment of dependent or common cause failures. The major limitations are in the areas of completeness, representativeness, and validity.

Completeness - Some types of events (e.g., sabotage) are explicitly excluded from present day PRAs, principally because of difficulty in quantifying the initiating event. Also, certain events that were not identified in the model might occur. However, considering the variety of existing PRAs, the fact that a substantial base of operating experience is available for analysis, and the fact that the understanding of applicable physical processes and system characteristics is fairly well developed, completeness does not appear to be the principal limitation in this area.

The existence of important omissions remains a concern. There is always the possibility that the PRA models are incomplete. The analyst may not have identified or adequately defined certain events. Some events are specifically excluded from the models because they are known or thought to be highly improbable. Although completeness cannot be demonstrated, except within the very rough bounds of operating experience, the consensus of the PRA community is that most of the major insights obtained from PRA are valid. Analyses of operating history are being performed to determine the interactions and dependent failures that have occurred. This knowledge is fed back to the analyst so that modeling techniques can be improved. Thus, with time, the impact of possible incompleteness on the overall numerical values should decrease.

Representativeness - The degree to which plant models represent plant behavior is a problem that cannot be definitively determined at this time. However, it is believed that current models contain a conservative bias that is intentionally inserted by the analysts when phenomena are poorly understood. For example, success/failure criteria are often taken from information in the Final Safety Analysis Report, which has a strong conservative bias. A similar case is the situation where no credit is taken for operation of a system at less than design output.

The accuracy with which a model represents true plant or system behavior is difficult to assess. Modeling, by its nature, implies an abstraction and an approximation of physical reality. The extent of the problem cannot be quantified at this time because there are few references against which accuracy can be gauged. Over the years there will be some improvement in this aspect as more operational data are acquired.

In addition to the conservative choices of success criteria, conservative bias has been intentionally inserted into the modeling process by the often conservative approximations used for modeling thermal-hydraulics and related phenomena. Conservatism (and possibly some non-conservatism) arising from these approximations have not been quantified. However, the resulting limitations do not negate the usefulness of model results if the limitations are properly recognized when interpreting the results.

Validity - Many elements of a PRA can be validated through the use of operating or experimental data or through reliable analysis. However, the validation of the frequency of rare events depicted in system modeling is not subject to experimental validation.

Because PRA modeling involves very rare core melt events, complete validation in an experimental or experiential sense is not achievable. For many sub-elements of the analysis, validation either through operating and experimental data or through reliable analysis is feasible and has been partly accomplished. For entire sequences and for dependent failures, historical data analysis, including the analysis of accident precursors, can be used for validation to some extent. Some important aspects of PRA system modeling cannot be experimentally validated. Fortunately, this does not seem to represent a major limitation to the usefulness of most PRA insights.

Another issue is the extent to which dependent failures are properly modeled or quantified. While this issue is complex, the consensus is that there has been significant progress in this area in the years since the RSS. If a decision-maker in any particular application is aware of the possible uncertainties arising from this aspect, it is unlikely that the insights from these analyses would be invalidated.

15.3 Data

Since the RSS, data on initiating events has improved, but in general the generic data base has not changed much and only limited causal data is available. Some PRAs use extensive studies of plant-specific data to augment the generic data base. However, there is no standard guidance for the use of generic data base. However, there is no standard guidance for the use of generic versus plant-specific data. In general, the data base and treatment of data can be considered to be reasonably mature. To improve the data base significantly would require substantial industry support. The uncertainty in the data base is random and varies with the type of data.

In general, the PRAs have relied heavily on generic data supplemented with plant-specific data. The amount of analyzed data on transient initiating events has significantly increased since the publication of the RSS. The amount of data for LOCA initiating events is sparse and the accuracy and precision of the estimates of frequencies for these events have not improved. Generic component failure data, applicable to general PRA evaluations, have not significantly improved in accuracy or precision. They have benefited from studies of LERs in some cases; however, few causal data are available, and the overall understanding of root failure causes has not improved significantly. The availability of dependent failure data has improved marginally, and quantitative estimates in this area remain largely subjective. The improvements that have occurred have not had a major effect on either the numerical results of PRAs or on the insights.

Two conceptually different sources of uncertainty appear in the data base for component and system failures. The first is a natural variability of failure rates in the existing population for each piece of hardware. The second arises from imperfect knowledge of the actual behavior. The latter source can be reduced over time as more data are

accumulated; the former will remain a source of uncertainty, though not a source of errors.

15.4 Human Errors

Past experience has shown that human actions can be important in the initiation of accident sequences, can cause failures of systems or functions given a random initiating event, or conversely can rectify or mitigate an accident sequence once initiated (recovery). The current methodology is reasonably mature, except for the treatment of cognitive errors. The basic techniques for analyzing the effect of most human interactions on plant safety was developed in the RSS and they have since been refined and formalized. The identified limitations in the techniques have stimulated rapid improvement in the analyses of human interactions.

The analysis of human actions is complicated by a number of factors. Such analysis does not lend itself to simple models as do mechanical, hydraulic, or electrical components. Classifying human action into the success or failure states used in the logic models for the plant equipment does not account for the wide range of possible human actions. A generally applicable model of the parameters that affect human performance is not yet available, and the analysis of dependent failures involving operators has often focused on dependencies between the operators rather than interdependencies between the operator and the plant.

The uncertainties in human error rates are within the stated uncertainty bounds. These limitations are more likely to affect the estimates of accident frequency than the estimates of consequences. The uncertainties associated with the data base affect the confidence that can be placed in calculated human error probabilities (HEPs). However, PRA allows a relative interpretation of the results so that an order of magnitude level of accuracy may be sufficient to identify potentially significant human errors and to determine their importance in accident sequences.

Future improvements should substantially increase the understanding of human behavior under accident conditions. Limitations to the detailed description of human interactions will still exist, and they should be recognized. Both the qualitative description of the human interaction logic and the quantitative assessment of those actions rely on the virtually untested judgment of experts. Additional work is needed to develop simple mathematical models of human performance and to identify the parameters that affect human performance in accident situations.

15.5 Summary of System Modeling

System modeling in PRA studies is usually considered to be very mature, significantly more mature than the study of accident progression phenomena, and comparable in maturity to the analysis of offsite consequences. The techniques of fault trees and event trees have advanced considerably since their initial application in the RSS. The uncertainties in system unavailabilities or sequence frequencies are usually dominated by uncertainties in the human error and dependent failure estimates rather than by the uncertainties in the data base. The conclusions and insights that PRA system modeling affords are usually reasonably sound, if appropriate consideration is given to the uncertainties and if great numerical accuracy is not required for the particular application. Most important, system modeling has provided insights about the relationships among systems, failures, and phenomena that could not have been obtained in any other way.

15.6 Accident Process Analysis

Since the TMI accident, severe accident research has expanded broadly, the primary purpose being to acquire information about severe accident behavior for possible use in regulation. Large experimental and mechanistic code development efforts have been initiated or redirected to explore important severe accident phenomena.

All the past PRAs contain considerable uncertainty associated with the processes that accompany the degradation of the core, the behavior of the molten core in the reactor vessel and upon the containment floor, and the response of the containment to the stresses placed upon it. The current models of thermal-hydraulic processes in a reactor vessel containing degraded or partially molten core are extremely crude. Because the geometry cannot be specified after degradation has commenced, it is not clear how much models in this area can be improved. In accidents that provide full core melt, the timing differences between very detailed and the current general models may not prove to be significant. Detailed models will be of greatest use in investigating core damage accidents like TMI, in which cooling is recovered before melt.

While full-scale melt-water and melt-concrete experiments are not feasible, considerable progress has been made since the RSS and theoretical work, model development, and small-scale experiments using non-radioactive molten metal are continuing. There is increasing evidence that steam explosions in the reactor vessel and in the containment are not capable of failing the containment. There is still much to be done in characterizing the dispersal of the debris bed that may follow reactor vessel failure, the size of the corium particles formed, and the coolability of the resulting debris bed. These and other questions may be answered in the next several years as a result of ongoing research, although the question of how well the laboratory-scale experiments represent a full-scale accident may never be completely answered.

15.7 Containment Analysis

The stresses placed upon the containment are computed during the accident process analysis. The response of the containment in purely structural terms is not too difficult to calculate with considerable accuracy and confidence. The difficult part is determining the time of containment failure, the hole size, and the failure location. These three factors are very important in determining the amount of fission products released to the environment.

The hole size determines the depressurization rate as well as the type of flow out of the containment. Sensitivity studies with computer models have shown that hole size can have a considerable effect on the fraction of fission products released from the containment. The failure location can determine whether the radioactive material is released into a building where considerable condensation and particulate removal is likely or that the material is released directly to the atmosphere. The source term increases dramatically if the containment fails before or very shortly after reactor vessel failure. If containment integrity is maintained for several hours after core melt, then natural and engineered mechanisms (e.g., deposition, condensation, filtration) can significantly reduce the quantity and radioactivity of the aerosols released to the atmosphere.

An additional complication is that some recent analyses have taken radiative transfer into account and predicted that, for some accident sequences in BWR Mark I containments, the containment will fail due to overtemperature rather than overpressure. This mode of failure has received very little attention. It is believed that the failure mechanism will be degradation of the penetration seal material, but little is known about what effective hole size may be expected.

The failure of penetration seals due to high temperature can be investigated in the laboratory, but the nature of overpressure failures may require experiments with actual containments. Over the next decade, containments from old, decommissioned reactors or from reactors that were started but never completed should become available. Hopefully, some of this equipment can be used for experiments to determine the parameters that control the fraction of fission products released. Until then, the uncertainty associated with these parameters must remain high.

15.8 Fission Product Transport Analysis

The characteristics of radionuclide releases to the environment are described in terms of various timing and location parameters, the thermal energy release rate, and, most importantly, the quantities of radionuclides released. The quantities of radionuclides available for release from the plant depend on the processes by which radionuclides are released from the fuel and transported through the reactor coolant system, the containment, and possibly, the buildings external to the containment before reaching the environment. Analyses have shown that both natural and engineered retention mechanisms can significantly reduce the amount of fission products eventually reaching the environment. These mechanisms operate all along the path from the fuel to the outside atmosphere. Some processes like the chemical reaction of cesium with stainless steel may not require long periods of time. Others, like the gravitational settling of small aerosols in the containment are strongly dependent on the amount of time available.

The fission product transport analysis involves a wide range of phenomena, some of which are not well understood. The uncertainties surrounding the estimation of source terms is not random in nature but arise basically from a lack of knowledge. The best indications are that the methods used in the RSS for estimating source terms are conservative and that the uncertainties are larger than those associated with modeling, data, and human error.

Shortly after the TMI accident, questions were raised about the realism of the methods used to analyze source terms in the RSS and subsequent PRAs. In 1981, the NRC published an evaluation of the "The Technical Bases for Estimating Fission Product Behavior During LWR Accidents" (NUREG-0772). As a result of deficiencies identified in that and other reviews, a number of research programs have been undertaken to improve the ability to model radionuclide release and transport in severe accidents. The NRC's Source Term Reassessment Study, IDCOR, and other studies are evaluating the effect of improved analysis capabilities on predicted source terms. It appears that some of the source term assumptions made in the RSS and used unchanged through the early 1980's, especially with regard to cesium and iodine, may change considerably by 1990.

15.9 Summary of Accident Process, Containment, and Fission Product Transport Analysis

Many uncertainties are associated with the predictions of severe accident progression, containment response, and source terms. Considerable effort is being made to better define and reduce those uncertainties. Presently, few sensitivity studies exist, the validation of models and codes for the broad range of severe accident phenomena is extremely limited, and quantitative uncertainty estimates are not available. Current research can be expected to provide a better characterization of source term uncertainties and, in some important areas, reduce the conservatism in PRA analyses.

A key issue is the depth of analysis required to accurately predict radionuclide behavior. It is currently not clear how much the uncertainties can be reduced through the use of complex models and how much bias is associated with the simpler models. Major advances are currently being made in the understanding of processes controlling radionuclide release and transport. However, processes that are closely coupled to the progress of extensive fuel damage, such as the release of the less volatile radionuclides from fuel or the generation of hydrogen during core slumping, will likely always have large uncertainties because of the difficulties associated with experimental validation.

15.10 Consequence Analysis

The consequence analysis estimates the frequency distribution and magnitude of offsite human health, economic, and land use effects for those accident sequences that result in releases of significant amounts of radioactivity from the containment.

Models have been developed which describe the atmospheric transport, dispersion, and deposition of radioactive materials and then predict their resulting interactions with and influence on the environment and man. Consequences can include early fatalities and injuries, latent cancer fatalities, genetic effects, land contamination, and economic costs.

The first comprehensive assessment of consequences was performed in the RSS. Since that study, modeling capabilities have been improved, model evaluation studies have been performed, and existing models have been applied to provide guidance for planning and decision-making in areas such as emergency planning and reactor siting. Some studies have been performed to examine the importance of transport via liquid pathways.

Uncertainties in offsite consequence prediction have not yet been assessed comprehensively. What currently exists is a large body of parametric (or sensitivity) analyses in which consequences are calculated for a range of plausible values of a key parameter or model. The PRA Procedures Guide (NUREG/CR-2300) tentatively identified the important contributors to uncertainty in the offsite consequence analysis. There is, of course, the magnitude of the source term, but its uncertainty is due to difficulties in the analyses which precede the consequence analysis as were just discussed. The form and effectiveness of emergency response, principally evacuation, makes a large difference in the predicted early fatalities if the amount of radioactive material released is large enough to exceed the lethal threshold near the plant. The rate of dry deposition from the plume directly affects the magnitude of early health effects and the distances to which land use restrictions or crop impoundments may be required. The modeling of wet deposition affects the low probability, high consequence end (tails) of the distributions of all consequences. The data for both wet and dry deposition is sparse and widely scattered. Finally, there is no general agreement upon the dose response relationships for somatic and genetic effect for low doses, although this may be remedied in the next several years. It also appears that the condensation of moisture in the release plume could have a significant impact on resulting consequences.

Even though the uncertainties in offsite consequence analysis have not been thoroughly examined, their general magnitude can be inferred from the results of many existing sensitivity studies. For estimates of the consequences resulting from very large source terms at a highly populated site, and given that the source term is known, it has been crudely estimated that the mean early fatalities could range from approximately a factor of 10 above present "best" estimates to nearly zero. This broad range is in a large part due to uncertainty in the effectiveness of the evacuation. The uncertainty in the mean predicted population dose (man-rem) is estimated to be a factor of 3 or 4, while the

uncertainty in the predicted mean number of latent cancer deaths (which depends on the population dose) is approximately a factor of 10. Major contributors to uncertainty, as well as the magnitude of uncertainties, depend strongly on assumptions about source terms and site characteristics. In general, the uncertainties are larger in the magnitude of the extremely low probability, high consequence portion ("tails") of predicted consequence frequency curves.

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

15.11 External Events

External initiators include seismic events, fires and floods inside the plant, external floods, high winds, aircraft, barge and ship collisions, noxious or explosive gases offsite, etc. These are in contrast to "internal accident initiators" which are caused by active or passive plant equipment failures, operator errors, and/or loss of offsite power. External events are considered separately because the methods for treating them are different from the method for treating so-called internal events. Both "internal initiating events" and "external initiating events" are misnomers, since the former category is usually taken to include accidents starting with the loss of offsite electric power, while the latter usually includes internally initiated fires and floods.

The analysis of external events has seen major advances since the RSS. The basic approach taken in the probabilistic analysis of initiating events consists of quantifying the expected frequency of the initiating event, determining its effects on various pieces of equipment, and determining the resulting effect of any degradation or failures on plant performance.

Much active developmental work is in progress, and abilities in this area should continue to improve. However, the uncertainties associated with such analyses are still significantly larger than those associated with internal initiating events, principally because of uncertainties associated with the development of the hazard curves. At the present time, even with the increased maturity, the methodologies have not progressed to the point where the uncertainties are even of the same order of magnitude as those for internal events. The principal benefit of external event analyses lies in the qualitative assessment of their effect on components, systems, and structures and the relative importance to safety of such functions. For each of the major external initiating events, the sections that follow discuss the level of maturity of the analysis.

The methodology for assessment of seismic events, internal fires and floods, and high winds has reasonably matured for qualitative assessments but not for quantitative application. Therefore, little confidence should be placed in any estimates of the risk from external initiators compared to those from internal initiators.

The risks from other external initiators are generally considered to be low, because of either the very long recurrence time associated with the event or the NRC's deterministic treatment of these areas. However, additional research is needed to develop screening criteria for selecting from these potential accident initiators those that might need to be considered in risk assessment.

15.12 Summary

PRA, like other disciplines, has a number of identifiable strengths and limitations. The strengths tend to be related to the fact that PRA provides a rigorous, detailed means of addressing the complex issues of risk and reliability. The limitations are primarily related to the uncertainties which are inherent in PRA.

By fully recognizing the strengths and limitations, PRA analysts can attempt to capitalize on the strengths and address the limitations. In this respect it may be true that the nature of the limitations, in an absolute sense, is not as important as the recognition of those limitations.

TOPIC 16
NATURE OF PRA RESULTS

16. NATURE OF PRA 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 development of complementary cumulative distribution functions (CCDFs) 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 is required to provide the proper interpretation and perspective to the numerical results.

16.1 Quantitative and Qualitative Results

Some of the types of information generated by a PRA are listed in Table 16-1. Qualitative as well as quantitative results are important. The following discussion is from Section 13.3 of the Procedures Guide (NUREG/CR-2300).

The qualitative insights derived from analyzing and interpreting the quantitative results are an important product of the analysis. Qualitative insights are developed by analyzing the results of the analysis to identify the plant features that contribute significantly to risk. These insights can be guided in several ways.

One common practice involves an analysis of the most probable cut sets of the dominant accident sequences; that is, the sequences that contribute the most to risk. The most probable cut sets of these sequences represent the most probable ways the sequence can occur. An examination of the cut sets of the dominant accident sequences provides one indication of the plant features that contribute significantly to risk.

If an expression for the combination of failures leading to the accident sequences has been developed, the identification of significant contributors to risk is a straightforward exercise. If the matrix formalism has been used, the same information can be obtained by tracing back through the event trees to identify the sequences that contribute most to a particular plant damage state, then examining the fault trees for the systems involved in the particular sequence to identify potential cut sets, and finally examining the cause tables to ascertain the most important failure modes.

The results are often analyzed to determine the contribution to risk from classes of events, such as types of initiating events, testing and maintenance, or human errors. The matrix formalism is, perhaps, advantageous for finding the contribution due to particular initiating events. This is done by simply adding the entries in a particular row of the matrix. For classes of primary events, the approach of first generating an equation for the sequence in terms of failure combinations may be advantageous because the contribution of each particular event is shown explicitly.

Further insight can be gained by performing an importance analysis on the results. A variety of importance measures have been developed to obtain different insights into the relative importance of various events (plant features) to the result. These importance measures take into account not only the probability of the event but also the number and

TABLE 16-1
TYPES OF INFORMATION GENERATED BY PRA

- Quantitative Measure of the likelihood of specific accident sequences
- Probabilities of system failures
- Estimates of accident consequences in terms of radiological doses to public and associated health effects
- Identification of dominant contributors to accident sequences
- Insights into how nuclear power plant systems interact with one another
- The risk significance of external events such as fires, floods, earthquakes, etc.
- The relationship between system operability states and accident phenomena

probabilities of the cut sets to which the event contributes. The importance calculations may show that a given event, while not being the most probable event in a given sequence, may be the most significant because it contributes to many different cut sets. "Significant" in this sense generally means those events that have the most potential for changing risk if the probability of the event changes.

Frequently, the study leads to insights into plant design and operational peculiarities. Although these insights may not show up in the dominant accident sequences or as significant contributors to risk, they might still be of value and should be documented in the discussion of results.

Examples of qualitative insights that could be derived from the RSS include the relative importance to risk of sequences initiated by small break LOCAs and transient events as well as the importance of human errors, testing, and maintenance to system unavailabilities. Such insights, of course, apply only to the particular plant under study. Caution must be exercised in drawing generic conclusions on the basis of one particular study.

Another important dimension to the interpretation of results is a qualitative discussion of the uncertainties in the answers and the principal sources of these uncertainties. The insights derived from the uncertainty and sensitivity analyses add valuable perspective to the results. This is particularly true if the most significant contributors to risk are accompanied by large uncertainties in assumptions or data.

The uncertainties in the data should be carried through the analysis where possible, and studies of model sensitivities should be performed where needed. However, it is important to recognize that useful results can be obtained even though the estimates may have large uncertainties. Many of the insights gained in the analysis are not strongly affected by the uncertainties associated with the analysis. The most important product of the analysis is the framework of engineering logic generated in constructing the models; the numerical estimates of frequencies need only be accurate enough to distinguish risk-significant plant features from those of lesser importance.

The patterns, ranges, and relative behavior that are obtained can be used to develop insights into the design and operation of a plant, insights that can be gained only from an integrated consistent approach like PRA. These insights are applicable to regulatory decision-making, although they should not be the sole basis for such decisions. Comparative evaluations can identify the features of the plant that are significant contributors to predicted risk. Similarly, the level of regulatory efforts addressed as items with little influence on the predicted risk can be evaluated in a better context. The ordering of dominant accident sequences provides a framework for value impact analyses of plant modifications. The plant models can be used as a tool for optimizing surveillance intervals and preventive maintenance programs, improving procedures, and providing perspective to operations personnel on potential multiple fault events. Employed early, PRA techniques can be used to guide the design process and to establish priorities for quality assurance activities. If properly developed, they also present a rational method for interpreting operational data.

Thus, PRA techniques can serve as a valuable adjunct to the methods currently used in decision making in both industry and government. Although they are not yet developed to the point where they can be used without caution, they do provide a framework of integrated engineering logic that can be used to identify and evaluate critical areas that influence the availability or the safety of the plant.

16.2 Specific Examples of PRA Results

Figure 16-1 illustrates an event tree for a LOCA induced by a transient, usually a stuck-open relief valve. Strictly speaking, only the part of the tree shown by dashed lines is the transient-induced LOCA tree. The part of the tree above the dashed portion indicates the possible trains of events if the stuck-open relief valve recloses. Each of the core melt sequences identified in an event tree such as Figure 16-1 may be described in detail as shown in Tables 16-2 and 16-3, which list the important cut sets and explain the terms used in the cut sets.

Once all the dominant sequences have been quantified and described, and the accident process, containment, and fission product transport analyses have been done for the most important sequences, it is possible to group the sequences into release categories as shown in Table 16-4. To a certain extent this grouping is by the mode of containment failure. The descriptions of each release category are required if the results are to be interpreted at this point.

If the PRA is concluded with the consequence analysis, then the results may be given in terms of CCDFs. Figure 16-2 reproduces the well-known summary of CCDF from the RSS. It showed BWRs to be somewhat safer than PWRs, but in any event the risk of death from a reactor accident was much lower than that from many other man-caused risks in our society. This finding is illustrated in Figure 16-3, which compares the Limerick risk and the RSS BWR risk with that from air crashes, total man-caused risk, and total natural risk.

Tables 16-5 through 16-16 are summaries of some of the PRAs completed to date. These tables indicate the differences in scope, level, and nature of results available to date.

16.3 Insights From PRAs

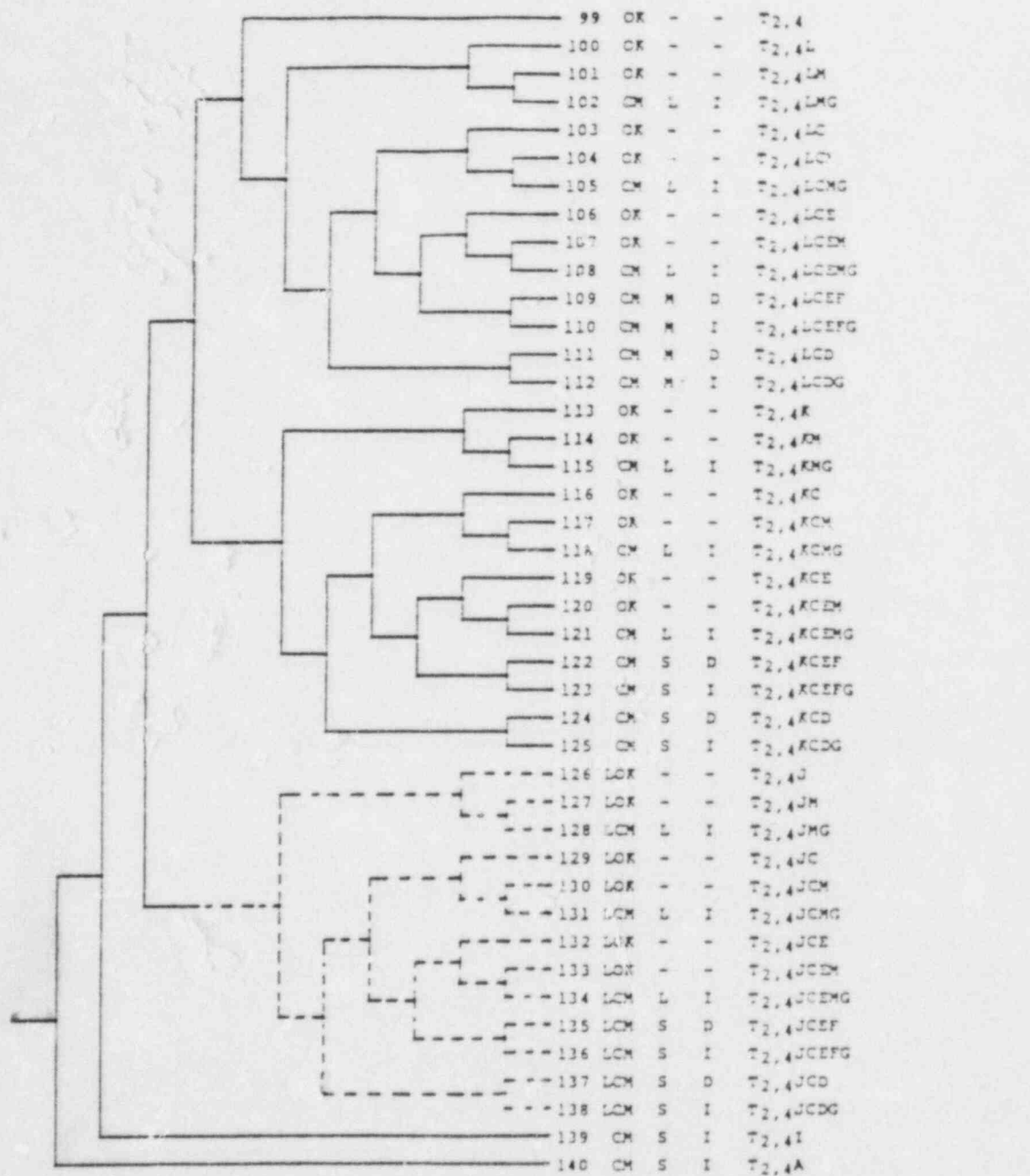
Almost a decade has passed since the publication of the RSS and over a dozen PRAs of nuclear power plants have been completed. It is now possible to draw some general insights from all this material. The following material is based on NUREG-1050, "Probabilistic Risk Assessment: Status Report and Guidance for Regulatory Application," which summarized the insights gained to date.

16.3.1 Broad Insights Regarding Core Damage and Offsite Risk

The following insights regarding the nature of core damage accidents and offsite risk have been derived from PRAs completed to date.

1. The estimated probability of accidents leading to core damage is generally higher than had been thought prior to the publication of the RSS.
2. The range of current core damage frequency estimates covers about two orders of magnitude: from about 10^{-5} per year to 10^{-3} per year. The variability of the results appears largely attributable to plant design and operation, site characteristics, the scope of the studies and the PRA methods employed, and analytical assumptions. However, design and operational differences make it difficult to predict with confidence the estimated core damage frequency of a plant without performing a plant-specific PRA.

TRANSIENT	R/S	S/R	S/R	I/C	I/C	F/M	F/M	L/P	C/S	S/D	C/S	S/Q	R/S	C/M	R/L	SEQUENCE
T _{2,4}	A	I	J	K	L	C	D	E	F	M	G	N	O	P	Q	



LEGEND: RESULT CM TIME REL TIME

OK = NON CORE MELT L = LONG (> 20 HOURS) I = IMMEDIATE

CM = CORE MELT M = MODERATE (> 3 HOURS) D = DELAYED

LOK = TRANSIENT INDUCED LOCA NON CORE MELT S = SHORT (< 3 HOURS)

LCM = TRANSIENT INDUCED LOCA CORE MELT

FIGURE 16-1
TRANSIENT SYSTEMIC EVENT TREE

TABLE 16-2
TYPICAL ACCIDENT SEQUENCE DESCRIPTION

T_4 LCD - Sequence #111

This sequence is initiated by a loss of normal AC power (T_4), followed by a failure of supply water to the shell side of the isolation condenser (IC) to allow it to remain in service (L), the failure of the feedwater coolant injection system (FWCI) to provide coolant at high pressure (C), and the failure of the operator to manually depressurize the reactor coolant system to allow the low pressure coolant systems to operate (D). The phenomenology of this sequence is essentially identical to that of sequence T_4 KCD. The only difference is that for this sequence the initial success of the IC followed by the failure of ICMUP extends the start of core melt from one-half hour to two hours.

The frequency of this sequence is estimated to be $3E-5$ /reactor year, and it contributes 9% to the total core melt frequency.

Dominant Cut Sets

<u>Cut Set</u>	<u>Cut Set Frequency (% Contribution)</u>	
$T_4 * FTR-OS-PWR * MDP * FW-PMP-BKR-FAIL * ICM-10-MOV-FTO$	3.9E-6	(15)
$T_4 * FTR-OS-PWR * MDP * SWS-MECH-FAIL * ICM-10-MOV-FTO$	3.4E-6	(13)
$T_4 * FTR-OS-PWR * MDP * CTS-FAIL-MU-FWCI * ICM-10-MOV-FTO$	2.9E-6	(11)
$T_4 * FTR-OS-PWR * MDP * FW-PMP-PPS-TOM * ICM-10-MOV-FTO$	2.3E-6	(9)
$T_4 * FTR-OS-PWR * MDP * AC-GTG-LOF * FTR-ICM-10$	2.1E-6	(8)
$T_4 * FTR-OS-PWR * MDP * G/T-BKR-FAIL * FTR-ICM-10$	1.7E-6	(6)

TABLE 16-3
TYPICAL EVENT DESCRIPTIONS

<u>Event</u>	<u>Event Description</u>
T4	loss of normal AC power transient; $f(T4) = 0.20/R \text{ yr.}$
FTR-OS-PWR	failure to recover offsite power to 2 hours; $p(FTR-OS-PWR) = 0.24.$
MDP	operator fails to manually depressurize the reactor coolant system; $p(MDP) = 7E-2.$
FW-PMP-BKR-FAIL	failure of FWCI pump breaker; $p(FW-PMP-BKR-FAIL) = 6.8E-2.$
ICM-10-MOV-FTO	failure of isolation condenser makeup valve ICM-10; $p(ICM-10-MOV-FTO) = 1.7E-2.$
SWS-MECH-FAIL	mechanical failure of service water system to provide cooling to FWCI train pumps; $p(SWS-MECH-FAIL) = 5.8E-2.$
CTS-FAIL-MU-FWCI	failure of condensate transfer system to provide makeup flow to FWCI; $p(CTS-FAIL-MU-FWCI) = 5.1E-2.$
FW-PMP-PPS-TOM	FWCI pump pressure permissive sensor out for test or maintenance; $p(FW-PMP-PPS-TOM) = 4E-2.$
AC-GTG-LOF	gas turbine generator fails; $p(AC-GTG-LOF) = 6E-2.$
G/T-BKR-FAIL	breaker failure prevents the loading of emergency AC buses onto the gas turbine; $p(G/T-BKR-FAIL) = 5.1E-2.$
FTR-ICM-10	operator fails to locally recover ICM by manually opening valve ICM-10; $p(FTR-ICM-10) = 1E-2.$

TABLE 16-4

PWR LARGE LOCA ACCIDENT SEQUENCES vs. RELEASE CATEGORIES

Core melt No core melt								
Release Categories								
1	2	3	4	5	6	7	8	9
Dominant Large LOCA Accident Sequences With Point Estimates								
AB- α 1×10^{-11}	AB-Y-10 1×10^{-10}	AD- α -8 2×10^{-8}	ACD- β -11 1×10^{-11}	AD- β -9 4×10^{-9}	AB- ϵ -9 1×10^{-9}	AD- ϵ -6 2×10^{-6}	A- β -7 2×10^{-7}	A 1×10^{-4}
AF- α 1×10^{-10}	AHV-Y-11 2×10^{-10}	AH- α -8 1×10^{-8}		AH- β -9 3×10^{-9}	ADP- ϵ -10 2×10^{-10}	AH- ϵ -6 1×10^{-6}		
ACD- α 5×10^{-11}	AB- δ -11 4×10^{-11}	AF- δ -8 1×10^{-8}			AHV- ϵ -10 1×10^{-10}			
AG- α 9×10^{-11}		AG- δ -9 9×10^{-9}						

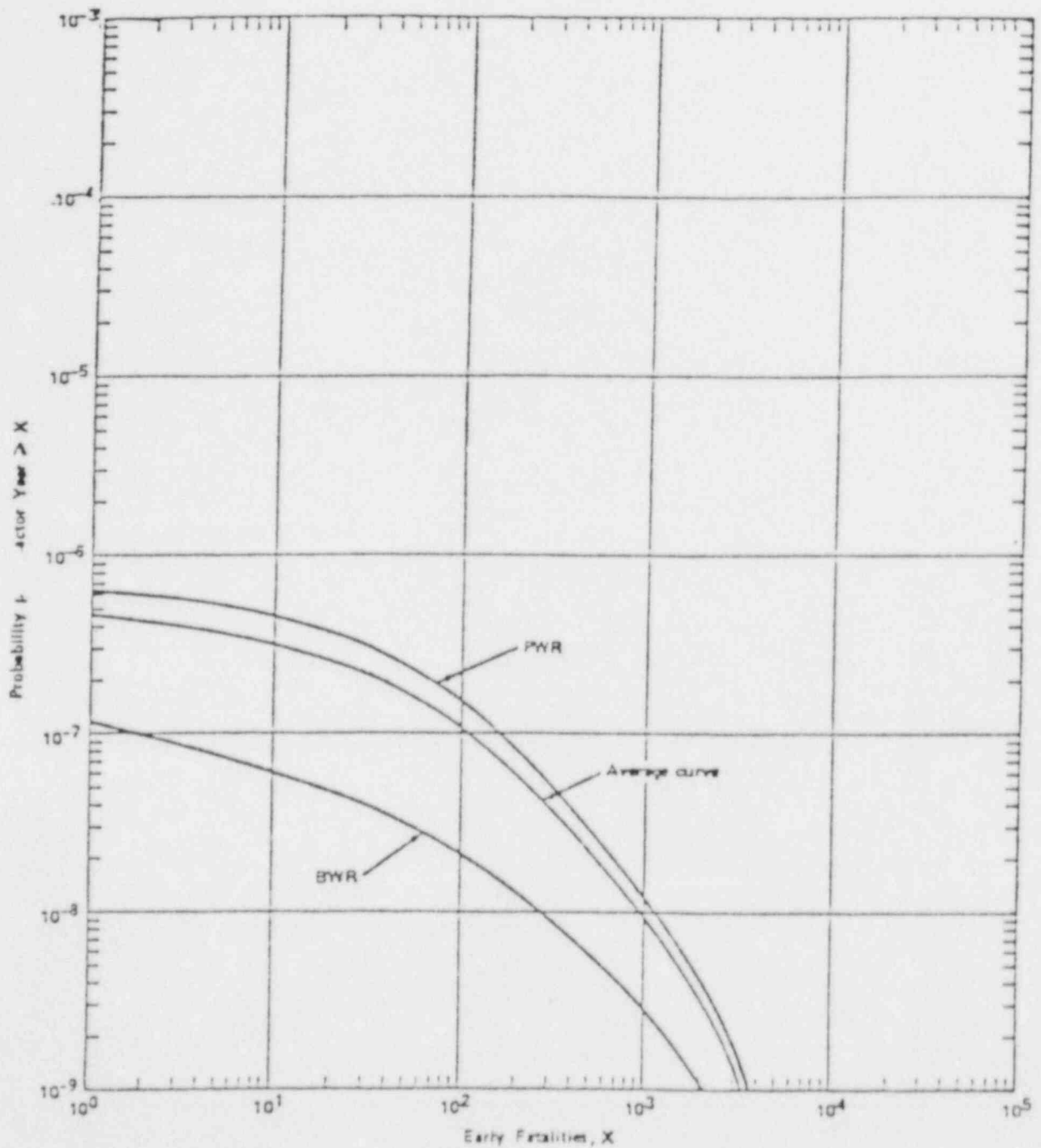


FIGURE 16-2
PROBABILITY DISTRIBUTION FOR EARLY FATALITIES
PER REACTOR YEAR

Note: Approximate uncertainties are estimated to be represented by factors of 1/4 and 4 on consequence magnitudes and by factors of 1/5 and 5 on probabilities.

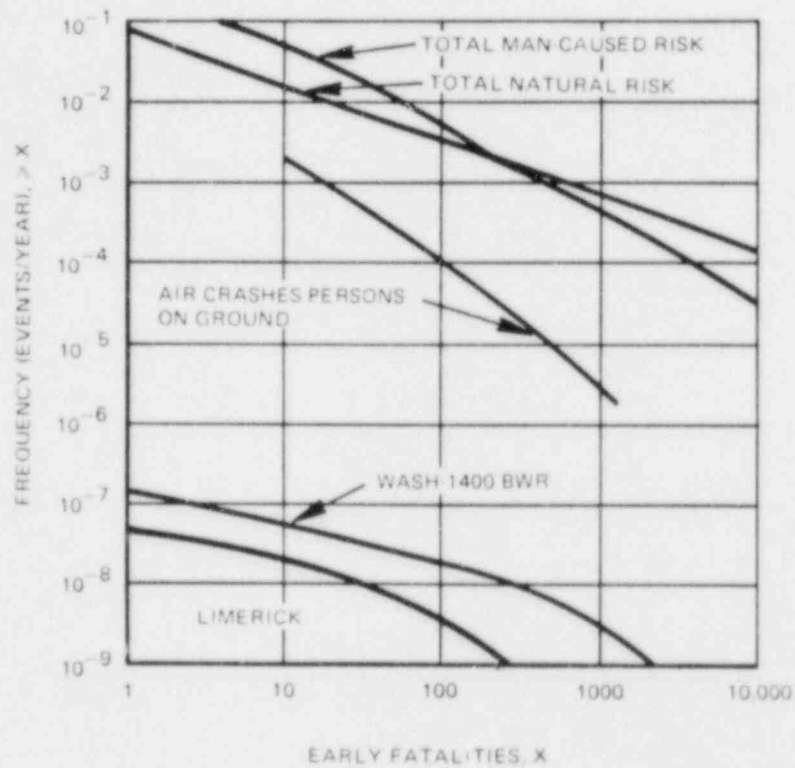


Figure 16-3. Limerick/WASH-1400 Risk Comparison

TABLE 16-5
SURRY (RSS) PRA RESULTS

Purpose: Assessment of Societal Risk Due to Nuclear Power

Scope: Full PRA

Accident Delineation:

- Fault tree and event tree system modeling
- Conservative success criteria assumed
- Range of external events considered

Consequences:

- Extensive offsite consequence analysis employed CRAC code
- Simplified evacuation model used
- Not site-specific

Quantitative Results:

Core Damage Frequency:	4×10^{-5}
Expected Early Fatalities:	4.1×10^{-5} per reactor year

TABLE 16-6
PEACH BOTTOM (RSS) PRA RESULTS

Purpose: Assessment of Societal Risk Due to Nuclear Power

Scope: Full PRA

Accident Delineation:

- Fault tree and event tree system modeling
- Conservative success criteria assumed
- Range of external events considered
- Initial detailed analysis of accident processes

Consequences:

- Extensive offsite consequence analysis employed CRAC code
- Simplified evacuation model used
- Not site-specific

Quantitative Results:

Core Damage Frequency:	3×10^{-5}
Expected Early Fatalities:	4.6×10^{-6} per reactor year

TABLE 16-7
OCONEE (RSSMAP) PRA RESULTS

Purpose: Apply Abbreviated WASH-1400 Methods to Additional Plants

Scope: Abbreviated System Modeling

Accident Delineation:

- Success criteria somewhat less stringent than WASH-1400
- Survey and analysis search for dominant contributors.
Based on WASH-1400
- External event analysis outside of study scope
- Detailed accident process analysis

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	8×10^{-5}
Expected Early Fatalities:	Not Applicable

TABLE 16-8
SEQUOYAH (RSSMAP) PRA RESULTS

Purpose: Apply Abbreviated WASH-1400 Methods to Additional Plants

Scope: Abbreviated System Modeling

Accident Delineation:

- Success criteria similar to WASH-1400
- Survey and analysis search for dominant contributors. Based on WASH-1400
- External event analysis not within study scope
- Detailed accident process analysis

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	6×10^{-5}
Expected Early Fatalities:	Not applicable

TABLE 16-9
GRAND GULF (RSSMAP) PRA RESULTS

Purpose: Apply Abbreviated WASH-1400 Methods to Additional Plants

Scope: Abbreviated System Modeling

Accident Delineation:

- Examination of external events not within study scope
- System modeling approaches same as other RSSMAP studies
- Some attempt to quantify operator recovery
- Detailed accident process analysis

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	3×10^{-5}
Expected Early Fatalities:	Not Applicable

TABLE 16-10
CALVERT CLIFFS (RSSMAP) PRA RESULTS

Purpose: Apply Abbreviated WASH-1400 Methods to Additional Plants

Scope: Abbreviated System Analysis

Accident Delineation:

- Examination of external events not within scope
- System modeling approaches same as other RSSMAP studies
- Detailed accident process analysis

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	2×10^{-3}
Expected Early Fatalities:	Not Applicable

TABLE 16-11
CRYSTAL RIVER (IREP) PRA RESULTS

Purpose: Improve System Modeling and Develop PRA Expertise

Scope: Detailed System Modeling

Accident Delineation:

- Fault tree and event tree system modeling
- Success criteria less stringent than WASH-1400
- External events not considered within study scope
- Accident processes based on engineering judgment

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	3.3×10^{-4}
Expected Early Fatalities:	Not Applicable

TABLE 16-12
ANO-1 (IREP) PRA RESULTS

Purpose: Improve System Modeling and Develop PRA Expertise

Scope: Detailed System Modeling

Accident Delineation:

- Fault tree and event tree system modeling
- Realistic success criteria
- External events not considered within study scope
- Accident processes based on engineering judgment

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	5×10^{-5}
Expected Early Fatalities:	Not Applicable

TABLE 16-13
BROWNS FERRY (IREP) PRA RESULTS

Purpose: Improve System Modeling and Develop PRA Expertise

Scope: Detailed System Modeling

Accident Delineation:

- Fault tree and event tree system modeling
- Success criteria less stringent than WASH-1400
- External events not considered within study scope
- Accident processes based on engineering judgment

Consequences:

- No consequence analysis performed

Quantitative Results:

Core Damage Frequency:	2×10^{-4}
Expected Early Fatalities:	Not Applicable

TABLE 16-14
BIG ROCK POINT PRA RESULTS

Purpose: Design

Scope: Full PRA

Accident Delineation:

- Used success criteria based on best-estimate of system capabilities
- System analysis techniques similar to WASH-1400 (fault tree/event tree)
- Plant-specific seismic analysis performed. Other external events believed unlikely
- Privately developed codes for accident process analysis

Consequences:

- Offsite consequence analysis employed CRAC code
- Site-specific population distribution and meteorological data used

Quantitative Results:

Core Damage Frequency:	1×10^{-3}
Expected Early Fatalities:	Not Applicable

TABLE 16-15
LIMERICK (PRA, REV. 4) PRA RESULTS

Purpose: Siting and Design

Scope: Full PRA

Accident Delineation:

- System modeling techniques similar to WASH-1400 (fault tree/event tree)
- Success criteria based on best-estimate of system capabilities
- Analysis of external events outside study scope
- Privately developed codes for accident process analysis

Consequences:

- Modified CRAC code used to model site-specific consequences
- Used WASH-1400 evacuation model

Quantitative Results:

Core Damage Frequency:	2×10^{-5}
Expected Early Fatalities:	2.4×10^{-6} per reactor year

TABLE 16-16
ZION (ZIP) PRA RESULTS

Purpose: Siting

Scope: Full PRA

Accident Delineation:

- Non-standard probabilistic, matrix format approach to system modeling
- Made use of vendor information to establish "realistic" success criteria
- Extensive seismic analysis performed. Other external events considered but believed unlikely
- Updated detailed accident process analysis

Consequences:

- CRACIT code used for consequence analysis. Uses variable direction plume trajectory and variable direction evacuation model
- Site-specific analysis

Quantitative Results:

Core Damage Frequency:	5×10^{-5}
Expected Early Fatalities:	Not Available

3. Most core melt accidents do not lead to very large offsite consequences. A very wide range of potential consequences for core melt accidents exists, depending on many factors. The core melt accidents that do lead to large offsite consequences generally involve the early failure of containment (relative to the time of core melt) or containment bypass.
4. Plants meeting all applicable NRC regulatory requirements have been found to vary significantly in terms of quantitative measures of risk and in terms of the key accident sequences that dominate risk.
5. The results of the PRAs indicate that accidents beyond those considered in the design basis are the principal contributors to offsite risk. This conclusion indicates that the designers, operators, and regulators have been generally effective in reducing the risks from anticipated operational occurrences and design basis accidents.
6. For low probability accidents which involve a major offsite radiological release, PRA has provided important insights about the nature of offsite consequences:
 - Latent cancer risk is an important element of the public health risk. Earlier thinking had been that prompt fatalities and contamination were the principal concerns.
 - Given a core melt, the estimated onsite economic loss is generally much larger than estimated offsite property damage.
 - Differences from site to site for estimated prompt fatality risk are very large, but are much less for latent cancer risk.
7. Among the important qualitative findings are:
 - Operational considerations are important to overall risk and may be comparable to the importance of design considerations. Human errors play an important role in overall reactor safety.
 - Containment performance is a key element in determining overall risk to the public.
 - Small LOCAs and transients are dominant accidents and risk contributors in most PRAs; large LOCAs are usually not important contributors to overall risk.
 - Earthquakes and internal fires seem to play an important role in risk, although this conclusion is very tentative and varies from plant to plant.
 - At this time, the uncertainties in estimating the risk from external initiators are sufficiently large that comparisons with the risk from internal accident initiators are tenuous at best.
 - Airborne radionuclide pathways are far more important contributors to offsite risk than liquid pathways.

8. Insights from a study of all licensee event reports (LERs) from 1969-1981 (the precursor study) are not much different from those gleaned from existing PRAs, if the failures contributing to the TMI accident, the Browns Ferry fire, and the Crystal River transient are assumed to have been reasonably remedied and auxiliary feedwater improvements are assumed to have been made as required after the TMI accident.
9. While much attention is normally placed on dominant accident sequences and ways to reduce risk further, one of the most important insights gained from PRAs is the need to maintain the reliability of important safety systems and components at or near the levels assumed in the PRA. Degradation of such systems or components can sharply increase risk.

16.3.2 Insights Regarding Accident Sequences

The PRAs completed to date have yielded a number of insights regarding accident sequences. These insights include:

1. Systems that are important for assuring reliable operation and preventing core damage accidents are not necessarily the same as those which are important in reducing offsite risk.
2. A few types of accident sequences tend to dominate the risks in all the plants studied. However, the dominant accident sequences can be expected to be different for different plants; the reasons for the dominance are plant-specific and relate to design and operational differences. Different assumptions made during the PRA analysis also can explain some of the differences observed in the results.
3. Some of the key accident sequences are generic, while others constitute safety issues that are quite plant-specific. Many times the PRAs have been useful in suggesting cost-effective remedies.
4. Despite the plant-specific differences and resultant uncertainties in estimating accident sequence frequency, generic studies to support regulatory decision-making generally can be accomplished effectively by grouping the plants into classes which have similar accident sequences that dominate core melt frequency or risk.
5. The failure of long-term heat removal is a large functional contributor to core melt frequency for both PWRs and BWRs. It is mainly associated with LOCAs in PWRs and with transients in BWRs.
6. The accident sequences that are dominant contributors to offsite risk are either those that enable radioactivity to bypass the containment or those that result in containment failure before or shortly after core melt.
7. PRAs have indicated situations where system success criteria based on licensing considerations may be overly conservative for realistic severe accident estimations. Resolution of these questions may result in an overall estimation of lower risk from some accidents.
8. The dependency of multiple systems on a common support system (e.g., pump cooling or room cooling) is a major contributor to accident sequences. However, these sequences generally include a long delay before radioactive material is released, providing the plant operator with the opportunity to recover from the initial failure.

16.3.3 Additional Insights on External Initiators

The completed PRAs have also yielded new information regarding external event accident initiators. These insights include:

1. The results of the analysis of external initiators seem highly plant-specific. For seismic and flooding events, the specifics of one plant's PRA results do not seem to be transferable to another plant even though it may be a similar type. Important fires are similar in that there is major involvement with cables or control areas affecting multiple redundant safety systems.
2. For seismic events:
 - The significant seismic contributors to core damage or risk identified to date are generally larger than the safe shutdown earthquake.
 - Most of the major contributors result from plant structures failing under seismic loads and disrupting the operation of safety systems.
 - Local ground-subsoil geological conditions are important in all seismic analyses accomplished in PRAs to date.
3. Most of the fires that have been found to be important to risk are those whose likelihood and/or severity are substantially reduced by the new NRC regulatory approach now being implemented.
4. For high winds, metal-sided structures are more fragile than concrete structures or equipment and are more likely to fail and compromise overall plant safety.
5. Those external initiators involving the plant site, such as earthquakes, external flooding, and high winds, are generally accompanied by loss of offsite power, which contributes to associated system unavailabilities.

16.4 Summary

The plant PRAs which have been performed to date have yielded a variety of insights into the nature of reactor risk. This topic has attempted to show that PRA results can be used in a number of different ways, depending on the specific needs of the analyst who is interpreting the results.

In some cases, PRA results can be used directly. In other cases, however, the results, themselves, may require analysis before conclusions can be drawn. The analyst must use as much care in interpreting results as in developing those results. Without this care, the final step of a PRA, its interpretation, may be flawed.

TOPIC 17
LWR PRA APPLICATIONS

17. LWR PRA APPLICATIONS

17.1 Introduction

PRA is an analysis technique that identifies and delineates the combinations or sequences of events that, if they occur, will lead to a severe accident (e.g., a core melt). It also estimates the frequency of occurrence for each sequence of events and then predicts the consequences. As practiced in the field of nuclear power, PRAs focus on core damage accidents since they pose the greatest potential risk to the public and the largest economic risk to the utility.

By using a uniform methodology, PRA integrates, in a realistic manner, information about plant design, operating practices, operating history, component reliability, human reliability, the physical progression of core melt accidents, and potential environmental and health effects. It uses both logic models and physical models. The logic models depict the combinations of events that could result in a core damage accident and can be used to determine the frequencies of each combination. The physical models estimate the progression of the accidents in time and then predict resulting damage. For example, the sequences of events that can lead to LOCA and the probabilities that these sequences will occur, are identified by a logic model, while the analysis of containment response to the accident is based on a physical model. The risk associated with any type of accident is the product of the frequency of occurrence and the consequent damage. The information extracted from a PRA in the form of predicted frequency of occurrence, resulting damage, and risk provides quantitative and qualitative insights into those aspects of plant design and operation which are the most significant contributors to risk.

The public health effects and economic losses resulting from a core damage accident which involves the release of radioactive fission products into the environment can be assessed by means of a consequence code. This computer program utilizes several constituent models. The environmental transport model uses site-specific meteorological data to predict the spread and fallout of the released radionuclides in the vicinity of the plant. The pathways, dose, and health effects models use local demographic, dosimetry and health effects data to predict the mortalities and morbidities expected to occur in the surrounding population. Throughout the analysis, realistic assumptions and criteria are used. When information is lacking or controversy exists, the analysis may introduce conservatism, increase uncertainties, or evaluate bounds, but the goal of the PRA is to be as realistic as possible. An integral part of the risk assessment process should be an uncertainty analysis, which includes not only uncertainties in the data but also uncertainties arising from modeling assumptions.

A number of PRAs of varying scope have been completed in the last decade. Almost a dozen studies have assessed core damage sequences, and some of these have evaluated the containment response as well. Several other studies have gone further and assessed the public risk. Some of these studies are listed in Table 17-1. The reasons for some of the recent Level 3 PRAs are given in Table 17-2. A number of other PRA studies of much narrower scope have also been performed. For example, several years ago, the NRC studied the reliability characteristics of all auxiliary feedwater systems, using a simplified, prescriptive analytical approach. Also, PRA techniques have been used to study specific accident sequences, such as anticipated transients without scram (ATWS). Some of the studies related to PRA are given in Table 17-3.

TABLE 17-1
PUBLISHED U.S. LWR PRA STUDIES

<u>Plant</u>	<u>Type</u>	<u>MWE</u>	<u>Utility</u>	<u>Op. Lic.</u>	<u>Program</u>
Surry 1, 2	PWR W3	775	VEPCO	72-73	RSS
Peach Bottom 2, 3	BWR4 MKI	1100	PECO	73-74	RSS
Sequoyah 1	PWR W4	1148	TVA	80	RSSMAP
Oconee 3	PWR B&W	860	DUKE	74	RSSMAP
Calvert Cliffs 2	PWR CE	850	BGECO	74	RSSMAP
Grand Gulf 1	BWR6 MKIII	1250	MPL	82	RSSMAP
Crystal River 3	PWR B&W	825	FPCO	76	IREP
Arkansas One 1	PWR B&W	836	APLCO	74	IREP
Browns Ferry 1	BWR4 MKI	1067	TVA	73	IREP
Zion 1, 2	PWR W4	1100	CONED	73	ZIP
Indian Point 2	PWR W4	873	CONED	71	ZIP
Indian Point 3	PWR W4	965	PASNY	75	ZIP
Limerick 1, 2	BWR4 MKII	1055	PECO	85-87	ZIP
Big Rock Point 1	BWR	75	CPCO	62	CPCO
Millstone 1	BWR 3 MKI	652	NEU	70	IREP
Calvert Cliffs 1	PWR CE	845	BGECO	74	IREP

TABLE 17-2
PLANT-SPECIFIC RISK ASSESSMENTS

- Various Utilities for Various Reasons
 - Limerick: New plant - site considerations
 - Zion/Indian Point: Older plants - siting, design
 - Big Rock Point: Old plant - design, modification
 - Yankee Rowe: Old plant - design

- NRC IREP Program

TABLE 17-3
PRA RELATED STUDIES

- Industry
 - Industry Degraded Core Program (IDCOR)

- U.S. Department of Energy (DOE)
 - Five Year R&D Program

- U.S. Nuclear Regulatory Commission (NRC)
 - Interim Reliability Evaluation Program (IREP)
 - Risk Methodology Integration and Evaluation Program (RMIEP)
 - Integrated Safety Assessment Program (ISAP)
 - Accident Sequence Evaluation Program (ASEP)
 - Severe Accident Sequence Analysis (SASA)
 - Severe Accident Risk Reduction Program (SARRP)
 - Methods Development
 - Generic Issues

Although the purposes of these assessments varied considerably, each study had one or more of the following objectives:

1. Identification and assessment of dominant contributors to core damage or offsite risk
2. Assessment of the plant-specific importance of TMI-related requirements and issues
3. Assessment of offsite risks at sites located in areas with high population densities
4. Assessment of specific generic safety issues
5. Operational training of plant personnel
6. Development and integration of PRA methodology
7. Training in the performance of PRAs
8. Assignment of priorities in the use of resources
9. Assessment of operating experience and events
10. Improvement of operating, testing, and maintenance procedures
11. Development of technical information to support recommendations on siting criteria
12. Evaluation of emergency response procedures

17.2 General Applications

As mentioned above, PRA is an engineering and analysis tool that, like other tools, can be used in a variety of ways. These uses can be divided into two types:

- Assessment of an existing plant
- Comparison of alternative designs.

In either case, the entire plant or only a portion of it can be considered. In the first case, the PRA would be conducted after the plant is in operation or construction is nearing completion. In the second case, PRA would be used when the plant was still in the formative design stages. As in any division, there are some cases which do not fit neatly into either. Consider the case where a PRA of an operating plant is conducted to determine whether any major safety improvements are warranted, and if so, which of the proposed modifications would be the most cost-effective. This use of a PRA contains elements of both the types given above.

More specifically, PRA can be used to determine one or more of the following:

- Component Failure Rates
- System Reliability
- System or Plant Design-Cost Optimization
- Plant Availability
- Frequency of Plant Damage States
- Public Risk

Generally, an objective on this list includes all of the preceding items. For example, if a PRA were conducted to discover the frequency of plant damage states, then all the information and most of the analyses needed to determine component failure rates, system reliabilities, and plant availability would be developed in the course of reaching the main objective of the study.

Some areas when PRA techniques have been used to generate information used in making decisions are:

- Improved Safety Research Program
- Auxiliary Feedwater System Study
- Analysis of Generic Issues to Determine Unresolved Safety Issues
- Alternative Containment Design Study
- Diesel Generator Testing Criteria.

The study of auxiliary feedwater systems is an example of the application of PRA techniques to only one system at a large number of plants. Specific applications of PRA in the regulatory process are:

- Resolution of Ranking of Generic Safety Issues
- Evaluation of Proposed Regulatory Requirements
- Assessment of Design or Operational Adequacy
- Safety Review Methods and Priorities
- Evaluation of Improved Safety Features
- Assessment of Proposed Backfit Requirements
- Inspection Priorities.

Many of these uses place little or no reliance on the absolute values obtained for the core damage frequency or offsite risk. Often, it is relative changes in risk or a comparison in risk reduction that is utilized. In other cases, it is the relative importance of various

systems or the type of accident sequences which dominate. By using PRA techniques, NRC has been able to screen proposed generic safety issues on a technical basis and allocate resources to those which are the most important. For the licensing of future plants, PRA techniques will be required in the design stage. PRA measures provide the benefit (i.e., risk reduction) values for use in cost-benefit analyses of proposed modifications. So far, the alterations identified by PRA as particularly effective have had very low cost to benefit ratios. The results of the Big Rock Point PRA were part of the justification used by the utility to avoid making certain expensive backfits at this old, low-power reactor.

17.3 Applications of PRA in Regulation

PRA techniques generate useful information and insights regarding the design and operation of a nuclear power plant. These should be useful to the regulatory agency by providing an improved understanding of the full range of accident sequences and their relative importance. This topic has been addressed by NUREG-1050, Probabilistic Risk Assessment (PRA) Reference Document, Section 2, from which the following material is drawn.

Both probabilistic and deterministic analyses are available to the NRC for use in making regulatory decisions. Because the limitations and uncertainties in the analysis are explicitly presented in the PRA approach, it may seem that the probabilistic analysis is much less trustworthy. This is not often the case. No technical analysis is 100 percent complete or possesses zero uncertainty; simplifying assumptions and judgments are part of both types of study. In most instances, the uncertainties identified by PRAs are also inherent, but not identified, in the more deterministic analyses. Therefore, it is important that the decision-maker understand all significant strengths and limitations so as to make more effective use of all available analyses, including the information contained in PRAs. There are many types of regulatory decisions, and the weight given to the quantitative PRA results should vary depending on the degree of precision necessary. Each analysis, whether deterministic or probabilistic, must be evaluated as to whether the assumptions and boundary conditions employed are sufficiently valid and the results sufficiently robust to justify its use in making regulatory decisions.

17.3.1 Allocation of Resources

Because of its integrated nature and greater reliance on realistic information, a PRA presents the best available information concerning the specific ways in which the critical safety functions at nuclear power plants can fail to be performed. This is true even though the models may be incomplete and uncertainties are associated with quantification of the models. PRA information should be used as appropriate to guide and evaluate the activities designed to improve the state-of-knowledge regarding the safety of nuclear power plants. The resources of the NRC, as well as those of the industry, are limited. The application of PRA techniques and insights from previous PRA studies are useful tools in allocating resources to the areas most likely to reduce risk and increase safety.

The nature of the decisions necessary to allocate regulatory resources does not require great precision in PRA results. It is sufficient to place the research efforts and safety issues into broad categories of risk impact (e.g., high, medium, and low). A potential safety issue would not be dismissed unless it were clearly of low risk. Thus, the body of completed PRA studies can be used for this categorization even though they do not fully represent all the different nuclear power plants, provided the nature of these differences is reasonably understood and can be qualitatively evaluated. PRA provides

documentation of a comprehensive and methodical safety analysis, which enhances debate on the merits of specific aspects of the issue and reduces the reliance on more subjective judgments.

PRAs should also be used appropriately to guide the overall direction of inspection and enforcement efforts. Information derived from PRAs indicates that certain surveillance tests and maintenance activities are significant contributors to plant risk and frequency of plant damage. If a generic risk profile is available, it can be used to identify critical surveillance testing and maintenance activities that have the potential, if not done properly, of significantly altering the predicted plant risk or severe core damage frequency. Generation of such information for each class of operating plants should assist a reactor inspector in focusing inspection effort on the critical activities at each facility. In a similar manner, these generic insights (available by reactor class) provide valuable information to both the licensee and the regulator in understanding, and allocating resources to correct, potentially significant operational occurrences at a plant, even if a plant-specific PRA is not available.

17.3.2 Generic Regulatory Applications

PRAs provide additional information and insights which can aid in rulemaking and the development of regulatory guides and branch technical positions. Such activities could be aimed at either reducing risk or relaxing regulatory requirements that do not have a significant impact on risk. The systems, components, and operational practices that the completed PRAs have found to have a significant impact on risk or core melt frequency can be used to develop conclusions based on generic types of plants. The number of plant types derived in such a study may be large since many of the features that are important for risk occur in the balance-of-plant where there is less standardization of design. It is best not to rely on small differences in numerical results. Thus, sorting the reactor population into a large number of generic classes will not often be necessary.

Many times the qualitative insights drawn from PRAs could be more important than the quantitative insights. Much information can be gained from limited studies of specific issues using simplified systems reliability analyses. While these limited studies are insufficient to accurately predict the absolute level of risk, they can identify problems relatively, as was done in the plant-specific studies of auxiliary feedwater systems.

17.3.3 Plant-Specific Regulatory Applications

Verification that a given level of safety (or risk) is likely to be achieved is a reasonable use of PRA results. The final numerical results of a PRA may be used, provided that the scope and data base are known, and that the underlying assumptions, methods, uncertainties are clearly understood. Numerical PRA results should be used in conjunction with other conventional regulatory tools. The information presented in a PRA can be a useful tool for the direction of regulatory attention and resources; however, the quantitative results of a PRA cannot be used in a compliance versus noncompliance sense. The stated uncertainties in a plant-specific PRA, compounded by the inability to quantify modeling uncertainties in any but a subjective manner, make it very difficult to determine formally with any degree of confidence that a specific safety limit in terms of public risk or frequency of core melt is met.

A plant-specific PRA, performed in the design process, can yield a tremendous amount of information about expected plant performance that would be useful in development of the detailed design. Such information would also be of use to the regulator. Because of the lack of specific design details in some areas and "as-built" drawings, the results of

such analyses cannot be considered a true prediction of plant risk or of the frequency of core damage. Rather, such analyses generate useful information on potential weaknesses in the design and allow evaluations of the efficacy of corrective design modifications. A plant-specific risk study can be used to evaluate the importance of operating events and to assess the safety of the plant when certain equipment is not operable. Consideration of the consequences and relative probabilities of the dominant accident sequences in training emergency response personnel could improve the criteria for declaring emergencies and the guides for the diagnosis and prognosis of accidents. The PRA models can be used in evaluating the advisability of plant shutdown when equipment is out of service beyond the times allowed in current technical specifications.

After a plant-specific PRA has been performed, steps should be taken to monitor the performance of the plant to ensure that the level of safety estimated in the study is maintained. The PRA should be an ongoing project that is continually used and updated, rather than a completed document which sits on the shelf. The PRA should be used in the context of a safety or reliability assurance program to evaluate operational occurrences and to check the significance of operational data as they are acquired.

17.3.4 PRA and Regulatory Decision-Making

The previous section discussed the uses of PRA in regulation. However, at this time, the role to be played by PRA in regulatory decisions is not clear. There is no magic formula to use in making decisions. The weight to be given to any type of information, including PRAs, will vary from case to case depending on the issue, the results of the PRA and the nature of the other information available.

It is difficult to present the results of a PRA, especially the uncertainty and sensitivity analyses, in an effective manner. A selection of those uncertainties most important to the decision should be presented in a concise and complete manner. Some important factors that should be considered in determining the weight to be given to PRA results are:

1. Do the scope and depth of the PRA study reasonably match the needs of the decision?
2. Do results of peer reviews conducted on the study add or subtract from the strength of the results?
3. What are the qualitative insights from the study? For example, do the qualitative insights as to the nature of the dominant accident sequences appear reasonable from an operational or engineering sense? This includes an assessment of the degree of realism associated with the study.
4. What is the impact of alternative regulatory actions on the estimated risk, together with the ease and costs of implementation?

5. What are the magnitudes of the quantitative estimates, as well as the results of sensitivity analyses and the bounds and likely biases of the major uncertainties surrounding the point-estimates? Where the reasonable upper bound of the PRA estimate indicates that the issue does not warrant regulatory attention, then substantial weight may be given to the quantitative PRA results. Similarly, the quantitative results may be given substantial weight in a decision to take regulatory action, if the lower bound estimate indicates a safety concern. Between these extremes the quantitative results cannot be the principal basis for making a decision, but the qualitative and quantitative results can provide unique perspectives and information to the decision-maker on the performance of the plant.

A major concern with regard to the use of PRA results is the tendency either to go too quickly to the bottom line (which is the weakest part of a PRA), or to dismiss the PRA entirely as being too uncertain. Neither reaction is appropriate. Safety goals, or other types of numerical criteria, tend to drive the user to the bottom line in spite of all the cautions to the contrary. The most valuable results of a PRA are usually the design and operational insights derived from the analyses. The patterns, ranges, and relative behaviors obtained from the logic models are used to develop insights into plant design and operation. These insights can only be gained from an integrated, consistent approach such as PRA. The results of a PRA must present these insights clearly and concisely. The uncertainties and the underlying assumptions must be summarized in a straightforward manner. Only when this is done can PRA be fully utilized in the regulatory process.

17.4 Examples of PRA Programs

Tables 17-4 through 17-11 present brief synopses of some important PRA projects. Tables 17-12 through 17-18 list some of the alternative concepts that have been evaluated utilizing PRA techniques.

TABLE 17-4
INDUSTRY DEGRADED CORE PROGRAM

- Industry Response to NRC Rulemaking
- PRA as Basis for Program
- Identification of Dominant Sequences
- Identification of Significant Systems/Features
- Establishment of Risk Profile
- Determination of Importance of Prevention or Mitigation Features
- Establishment of Industry Position

TABLE 17-5
NATIONAL RELIABILITY EVALUATION PROGRAM (NREP)

- Systematic Risk Evaluation Of All Operating Commercial Nuclear Plants
- Phased Program Beginning In 1982
- NREP Procedures Guide As First Phase
- NREP Has Been Replaced By ISAP

TABLE 17-6
DOE FIVE YEAR R&D PROGRAM

- PRA Development Summary
 - increased utilization
 - design/cost optimization
 - PRA implemented as part of design process

- Risk Based Design Approach

- Acceptance of Integrated PRA Approach
 - regulatory agencies
 - utilities

- Integration of PRA
 - methods, data
 - benefits, acceptance

TABLE 17-7
IREP OBJECTIVES

- Identify Dominant Accident Sequences for Plants Under Study
- Develop Foundation for Future Analysis
- Expand Cadre of Experienced PRA Practitioners
- Evolve Procedures for Future IREP Analyses On All Plants

TABLE 17-8
ACCIDENT SEQUENCE EVALUATION PROGRAM

- Review of Existing PRA Results
- "Generic" Risk Profile of LWRs
- Common Terminology
- Basis for Assessing Proposed Design Changes

TABLE 17-9
SEVERE ACCIDENT SEQUENCE ANALYSIS (SASA)

- Study Of Accident Processes
 - Browns Ferry
 - Zion
- Factors That Lead To Release
- Measures To Take After Core Melt
- Study Of Containment Strategies
 - Types
 - Failures

TABLE 17-10
METHODS DEVELOPMENT

- Common Cause Analysis
 - floods (NOAH)
 - location dependent (COMCAN)
 - Seismic Safety Margin Research Program (SSMRP)
 - systems interaction

- System Modeling
 - modularized fault tree analysis
 - sequence level evaluation
 - GO code modularization

TABLE 17-11
GENERIC ISSUES

- Station Blackout
- Auxiliary Feedwater Reliability
- DC Power Reliability

TABLE 17-12
PROPOSED PREVENTIVE/MITIGATIVE CONCEPTS

- Concept Objectives
 - reduction of risk
 - existing risk
 - reevaluation of potentially new dominant sequences

- Alternative Decay Heat Removal Concepts

- Advanced Mitigation Concepts

- Hydrogen Mitigation

- Alternate Containment Concepts

- Reduction of Probability for Human Error

TABLE 17-13
CONCEPT OBJECTIVES

- Improvement of Risk as the Goal
- Evaluation of Existing Risk
 - plant specific
 - type of PWR
 - type of BWR
 - Decision on Dominant Risk Scenarios
- Identification of Dominant Risk Scenarios
- Reevaluation of Potentially New Dominant Sequences

TABLE 17-14
ALTERNATIVE DECAY HEAT REMOVAL CONCEPTS

- Efficacy Very Plant Dependent
- PWR - Feedwater Transients, Small LOCAs
 - improve auxiliary feedwater reliability
 - improve high pressure injection reliability
- BWR - For Loss of Suppression Pool Cooling - Loss of Feedwater Transient
 - improve residual heat removal reliability
 - improve high pressure service water system reliability
- Independent Add-On System (when decay heat removal is significant to meltdown probability). Target failure rates $< 10^{-1}$ failures per demand.
- Special Emergencies
 - sabotage
 - earthquake
 - airplane crash
- Concepts - PWR
 - add-on auxiliary feedwater train
 - add-on high pressure injection train
 - alternate RHR train
 - closed loop auxiliary feedwater train
 - passive feedwater train
 - passive makeup or circulation pump (steam ejector)
- Concepts - BWR
 - add-on core cooling circuit with heat exchanger and pump
 - high pressure
 - complete depressurization with low pressure
 - simultaneous depressurization and cooling
 - analogous to HPCI or LPCI and heat exchanger

TABLE 17-15
MITIGATION CONCEPTS

- Containment-Atmosphere Mass Removal - "Venting" (post scrubbing by suppression pool or ice condenser)
- Energy Dilution - Increased Containment Volume Venting to Large Volume
- Suppression of Burning Combustibles
 - inerting
 - halons
 - water mist
- Controlled Burning of Combustibles
- Core Retention Devices
 - core catchers
 - cavity flooding (active, passive cooling)
- Missile Shields for Steam Explosions
- Containment Heat Removal - Passive or Active

TABLE 17-16
HYDROGEN MITIGATION

- Determination of Necessity
 - evaluation of plant-specific risk
 - potential for risk reduction
- General Emphasis - Small Containments
 - BWR - but relatively low risk
 - PWR - ice condenser containment
- Interim Rulemaking
 - requirement for H₂ mitigation for small and intermediate containments
 - no requirements for large containments
- Inerting - Nitrogen, Carbon Dioxide, Halon
 - pre-accident
 - post-accident
- Deliberate Ignition
- Filtered Vent
- Water - Fogging
- Gas Turbine
- Catalytic Hydrogen Absorption
- High Expansion Aqueous Foams

TABLE 17-17
ALTERNATE CONTAINMENT CONCEPTS

- Stronger Containment
- Shallow Underground Siting
- Deep Underground Siting
- Increased Containment Volume
- Filtered Atmospheric Venting
- Compartment Venting
- Thinned Base Mat
- Evacuated Containment
- Double Containment
- Evacuated Nearby Receiver Volume
- Large, Carbonate-Free, Meltable Mass Within Containment Below Vessel
- Most Favorable Based on Value-Impact Comparisons

TABLE 17-18
QUALITATIVE VALUE-IMPACT MATRIX

REDUCTION IN RISK ↓	CURRENT SURFACE PLANTS	EVACUATED CONTAINMENT THINNED BASE MAT	DOUBLE CONTAINMENT	SHALLOW UNDERGROUND SITING	
			STRONGER CONTAINMENT INCREASED CONTAINMENT VOLUME		
		FILTERED ATMOSPHERIC VENTING	COMPARTMENT VENTING		DEEP UNDERGROUND SITING
	→ INCREASE IN COST →				

APPENDIX A
REFERENCES

PRA FUNDAMENTALS COURSE REFERENCES

- (1) American Nuclear Society (ANS) and Institute of Electrical and Electronic Engineers (IEEE), 1983. PRA Procedures Guide, NUREG/CR-2300, Washington, DC.
- (2) U.S. Nuclear Regulatory Commission, 1981. Fault Tree Handbook, NUREG-0492, Washington, DC.
- (3) U.S. Nuclear Regulatory Commission, 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Nuclear Power Plants, WASH-1400, NUREG-75/014, Washington, DC.
- (4) Gilluly, J., et al, 1951. Principles of Geology, W.H. Freeman and Company, San Francisco, California.
- (5) Hansen, R.J., 1970. Seismic Design for Nuclear Power Plants, Massachusetts Institute of Technology Press, Cambridge, Massachusetts.
- (6) Press, F. and R. Siever, 1978. Earth, W.H. Freeman and Company, San Francisco, California.
- (7) Electric Power Research Institute, 1978. ATWS: A Reappraisal, Palo Alto, California.
- (8) Swain, A.D. and H.E. Guttman, 1981. Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandia National Laboratories, Albuquerque, New Mexico.
- (9) U.S. Nuclear Regulatory Commission, 1984. Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application (Draft), NUREG-1050, Washington, DC.
- (10) Pickard, Lowe, and Garrick, Inc., 1983. Seabrook Station Probabilistic Safety Assessment.

DISTRIBUTION

U.S. Government Printing Office
Receiving Branch (Attn: NRC Stock)
8610 Cherry Lane
Laurel, MD 20707
250 copies for RG

U.S. Nuclear Regulatory Commission (25)
Office of Nuclear Regulatory Research
Washington, DC 20555
Attn: C. Belote/DRAO

JRB Associates
8400 Westpark Drive
McLean, VA 22102
Attn: Lala Curry

NUS Corporation
16885 West Bernardo Drive
San Diego, CA 92127
Attn: G. William Hannaman

Energy Incorporated (2)
1851 S. Central Place, Suite 201
Kent, WA 98031
Attn: Jon Young
Tim Leahy

Battelle Columbus Laboratories
505 King Avenue
Columbus, OH 43201
Attn: Fred L. Leverenz

Science Applications International Corp.
1710 Goodridge Drive
P. O. Box 1303
McLean, VA 22102
Attn: Ernest Lofgren

3141 C. M. Ostrander (5)
3151 W. L. Garner
6400 A. W. Snyder
6410 J. W. Hickman
6411 A. S. Benjamin
6412 A. L. Camp
6414 D. M. Ericson, Jr.
6414 W. R. Cramond (33)
6415 F. E. Haskin
6415 R. L. Iman
6417 D. D. Carlson
7200 J. M. Wiesen
7220 R. R. Prairie
8024 M. A. Pound

NRC FORM 335 12-84 NRCM 1102 3201 3202 SEE INSTRUCTIONS ON THE REVERSE		U.S. NUCLEAR REGULATORY COMMISSION		REPORT NUMBER Assigned by TDC and NRC NUREG/CR-4350/1 of 7 SAND85-1495/1 of 7	
2 TITLE AND SUBTITLE Probabilistic Risk Assessment Course Documenta- tion Volume 1 - PRA Fundamentals				3 LEAVE BLANK	
5 AUTHOR(S) Roger J. Breeding Timothy J. Leahy Jonathan Young Energy Incorporated				4 DATE REPORT COMPLETED MONTH YEAR July 1985	
7 PERFORMING ORGANIZATION NAME(S) AND MAILING ADDRESS (Include Zip Code) Reactor Systems Studies, Div. 6414 Sandia National Laboratories Albuquerque, NM 87185				6 DATE REPORT ISSUED MONTH YEAR August 1985	
10 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Division of Risk Analysis and Operations Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, DC 20555				8 PROJECT TASK WORK ORDER NUMBER A1321	
12 SUPPLEMENTARY NOTES				9 PERIOD COVERED (Include dates)	
13 ABSTRACT (200 words or less) <p>The full range of PRA topics are presented, with special emphasis on systems analysis and PRA applications. Systems analysis topics include system modeling such as fault tree and event tree construction, failure rate data, and human reliability. The discussion of PRA applications is centered on past and present PRA-based programs such as WASH-1400 and the Interim Reliability Evaluation Program, as well as on some of the potential future applications of PRA. The relationship of PRA to generic safety issues such as station blackout and Anticipated Transient Without Scram (ATWS) is also discussed.</p> <p>In addition to system modeling the major PRA tasks of accident process analysis, and consequence analysis are presented. An explanation of the results of these activities and the techniques by which these results are derived forms the basis for a discussion of these topics. An additional topic presented in this course is the topic of PRA management, organization, and evaluation. This discussion explains the relationship of sound management, proper organization, and thorough evaluation to the performance of a credible risk assessment.</p>					
14 DOCUMENT ANALYSIS & KEYWORDS DESCRIBE TOPIC Probabilistic Risk Assessment, Systems Analysis, Applications, Fundamentals				15 AVAILABLE STATEMENT Unlimited	
16 IDENTIFIERS OPEN ENDED TERMS				16 SECURITY CLASSIFICATION This page Unclassified 17 NUMBER OF PAGES 18 PRICE	

120555078877 1 1AN1RG
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555