
Probabilistic Safety Analysis Procedures Guide

Sections 1 - 7 and Appendices

Prepared by R. A. Bari, A. J. Buslik, N. Z. Cho, A. El-Bassioni, J. Fragola,
R. E. Hall, D. Ilberg, E. Lofgren, J. O'Brien, I. A. Papazoglou,
P. K. Samanta, T. Teichmann, W. Vesely, A. Unione, R. Youngblood

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

8509110037 850831
PDR NUREG
CR-2815 R PDR

NOTICE

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

NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 1717 H Street, N.W.
Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

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

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

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

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

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

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

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

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

Probabilistic Safety Analysis Procedures Guide

Sections 1 - 7 and Appendices

Manuscript Completed: July 1985
Date Published: August 1985

Prepared by
R. A. Bari, A. J. Buslik*, N. Z. Cho, A. El-Bassioni*, J. Fragola**,
R. E. Hall, D. Ilberg, E. Lofgren**, J. O'Brien, I. A. Papazoglou,
P. K. Samanta, T. Teichmann, W. Vesely***, A. Unione****, R. Youngblood

Brookhaven National Laboratory
Upton, NY 11973

* Staff, U. S. Nuclear Regulatory Commission
** Science Applications, Inc.
*** Battelle's Columbus Laboratories
**** Lotus Reliability Associates

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A3758

ABSTRACT

A procedures guide for the performance of probabilistic safety assessment has been prepared for interim use in the Nuclear Regulatory Commission programs. It will be revised as comments are received, and as experience is gained from its use. The probabilistic safety assessment studies performed are intended to produce probabilistic predictive models that can be used and extended by the utilities and by NRC to sharpen the focus of inquiries into a range of issues affecting reactor safety. This first volume of the guide describes the determination of the probability (per year) of core damage resulting from accident initiators internal to the plant (i.e., intrinsic to plant operation) and from loss of off-site electric power. The scope includes human reliability analysis, a determination of the importance of various core damage accident sequences, and an explicit treatment and display of uncertainties for key accident sequences. The second volume deals with the treatment of the so-called external events including seismic disturbances, fires, floods, etc. Ultimately, the guide will be augmented to include the plant-specific analysis of in-plant processes (i.e., containment performance). This guide provides the structure of a probabilistic safety study to be performed, and indicates what products of the study are valuable for regulatory decision making. For internal events, methodology is treated in the guide only to the extent necessary to indicate the range of methods which is acceptable; ample reference is given to alternative methodologies which may be utilized in the performance of the study. For external events, more explicit guidance is given.

TABLE OF CONTENTS

	Page
ABSTRACT.....	iii
LIST OF FIGURES.....	ix
LIST OF TABLES.....	x
PREFACE.....	xi
ACKNOWLEDGMENTS.....	xiii
1. INTRODUCTION.....	1-1
1.1 Objectives.....	1-1
1.2 Scope of the PSA Procedures Guide.....	1-1
1.3 Approach of the PSA Procedures Guide and Selected Methodology.....	1-3
1.3.1 Factors Conditioning Choices of Methodology and Scope in PSA Studies.....	1-5
1.3.1.1 The Sensitivity Studies.....	1-5
1.3.1.2 Special Reporting Requirements.....	1-5
1.4 Documentation of a PSA Study.....	1-5
1.5 Organization of the PSA Procedures Guide.....	1-6
1.5.1 Plant/PSA Familiarization and Scoping.....	1-6
1.5.2 Accident Sequence Definition.....	1-6
1.5.3 Reliability Data Assessment and Parameter Estimation...	1-7
1.5.4 Accident Sequence Quantification.....	1-7
1.5.5 Display and Interpretation of Results.....	1-7
2. PSA ORGANIZATION AND MANAGEMENT.....	2-1
2.1 Introductory Remarks.....	2-1
2.2 General Aspects.....	2-1
2.2.1 Management and Organization.....	2-1
2.2.2 Personnel.....	2-2
2.2.3 Technical Organization.....	2-3
2.3 Technical Quality Assurance.....	2-4
2.3.1 General Definitions and Objectives.....	2-4
2.3.2 Formal TQA Requirements.....	2-5
2.4 Interactive Review.....	2-5
2.5 Approximate Anticipated Level of Effort.....	2-6
3. PLANT/PSA FAMILIARIZATION AND SCOPING.....	3-1
3.1 Purpose.....	3-1
3.2 Scope.....	3-1
3.3 Input.....	3-1
3.4 Assumptions and Methods.....	3-2
3.4.1 Determination of Function/System Relations.....	3-3
3.4.2 Determination of Initiating Events.....	3-3
3.4.3 Determination of Mitigating Systems Requirements and Other Special Conditions.....	3-5
3.4.4 Determination of Initiating Event Groups.....	3-6
3.4.5 Review of Operational Data for Multiple Failures.....	3-6
3.4.6 Survey of Regulatory Concerns.....	3-7
3.5 Products.....	3-7

	<u>Page</u>
4. ACCIDENT SEQUENCE DEFINITION.....	4-1
4.1 Event Tree Development.....	4-1
4.1.1 Purpose.....	4-1
4.1.2 Scope.....	4-1
4.1.3 Input.....	4-1
4.1.4 Assumptions and Methods.....	4-1
4.1.5 Products.....	4-2
4.2 Fault Tree Development.....	4-3
4.2.1 Purpose.....	4-3
4.2.2 Scope.....	4-3
4.2.3 Inputs.....	4-4
4.2.4 Assumptions and Methodology.....	4-5
4.2.5 Products.....	4-8
4.3 Human Reliability Analysis (HRA).....	4-10
4.3.1 Purpose.....	4-10
4.3.2 Scope.....	4-10
4.3.3 Process Considerations.....	4-10
4.3.4 Quantification of Human Error Probabilities (HEPs).....	4-12
4.3.4.1 General Requirements for Documentation of HRA Results.....	4-12
4.3.4.2 Expert Judgment.....	4-13
4.3.4.3 Performance Process Simulation.....	4-13
4.3.4.4 Performance Data Analysis.....	4-14
4.3.4.5 Dependency Calculations.....	4-14
4.3.5 Method Specific Documentation.....	4-15
4.3.5.1 Confusion Matrix.....	4-15
4.3.5.2 Direct Numerical Estimation.....	4-15
4.3.5.3 Influence Diagrams.....	4-16
4.3.5.4 LER-HEP Methodology.....	4-16
4.3.5.5 Maintenance Personnel Performance Simulation (MAPPS) Model.....	4-17
4.3.5.6 Multiple Sequential Failure (MSF) Model.....	4-17
4.3.5.7 Operator Action Tree (OAT) - Time Reliability Correlation.....	4-18
4.3.5.8 Paired Comparisons.....	4-18
4.3.5.9 Success Likelihood Index Method/Multi-Attribute Utility Decomposition (SLIM/MAUD).....	4-19
4.3.5.10 Technique for Human Error Rate Prediction (THERP).....	4-19
4.4 Special Tasks.....	4-20
4.4.1 Impact of Physical Processes on Logic Tree Development.....	4-20
4.4.1.1 Impact of Physical Phenomena on Accident Sequences.....	4-20
4.4.1.2 Linkage of Accident Sequence Event Trees With Containment Event Trees.....	4-21

	<u>Page</u>
4.4.2 Qualitative Dependence Analysis.....	4-21
4.4.2.1 Purpose.....	4-21
4.4.2.2 Scope.....	4-22
4.4.2.3 Assumptions, Methods, and Procedural Steps....	4-24
4.4.2.3.1 Identification of Dependences.....	4-24
4.4.2.3.2 Further Search for Dependences.....	4-28
4.4.2.3.3 Incorporation of Dependences Into the Logical Models.....	4-29
4.4.2.3.4 Incorporation of Dependences in the Event Trees.....	4-30
4.4.2.3.5 Incorporation of Dependences in the Fault Trees.....	4-31
4.4.2.4 Regulatory Issues Related to the Qualitative Dependence Analysis Task.....	4-31
References.....	4-35
5. RELIABILITY DATA ASSESSMENT AND PARAMETER ESTIMATION.....	5-1
5.1 Purpose.....	5-1
5.2 Scope.....	5-1
5.3 Inputs and Outputs.....	5-1
5.4 Assumptions, Methods, and Procedural Steps.....	5-3
5.5 Initiating Events.....	5-5
5.5.1 Initiating Event Definition.....	5-5
5.5.2 Data Sources, Parameter Selection, and Parameter Estimation.....	5-5
5.6 Component Data.....	5-6
5.6.1 Component Basic Event Definition.....	5-6
5.6.2 Plant-Specific Data Sources and Data Gathering.....	5-6
5.6.3 Model and Parameter Selection.....	5-8
5.6.4 Estimation of Component Failure, Repair, Test, and Maintenance Parameters.....	5-12
5.7 Human Error Data.....	5-15
5.8 Documentation of the Data Analysis Performed.....	5-16
5.8.1 Initiating Events.....	5-16
5.8.2 Component Basic Events.....	5-16
5.8.3 Human Error Events (Procedural Errors).....	5-17
6. ACCIDENT SEQUENCE QUANTIFICATION.....	6-1
6.1 Accident Sequence Boolean Equations.....	6-1
6.1.1 Purpose.....	6-1
6.1.2 Scope.....	6-3
6.1.3 Inputs.....	6-3
6.1.4 Methods and Assumptions.....	6-3
6.1.5 Products.....	6-6
6.2 Accident Sequence Binning.....	6-6
6.2.1 Purpose.....	6-6
6.2.2 Scope.....	6-7

	<u>Page</u>
6.2.3 Inputs.....	6-7
6.2.4 Methods and Assumptions.....	6-7
6.2.5 Products.....	6-8
6.3 Sequence Quantification.....	6-9
6.3.1 Purpose.....	6-9
6.3.2 Scope.....	6-9
6.3.3 Inputs.....	6-9
6.3.4 Methods and Assumptions.....	6-9
6.3.4.1 Human Error Screening Calculation.....	6-9
6.3.4.2 Final Results Including Recovery.....	6-10
6.3.4.3 Uncertainty Evaluation.....	6-11
6.3.5 Products.....	6-11
6.4 Importance and Sensitivity Analyses.....	6-13
6.4.1 Purpose.....	6-13
6.4.2 Scope.....	6-13
6.4.3 Methodology for the Importance Evaluations.....	6-14
6.4.4 Methodology for the Sensitivity Analysis.....	6-15
6.4.5 Products.....	6-17
7. DISPLAY AND INTERPRETATION OF RESULTS.....	7-1
7.1 Documentation of a PSA.....	7-1
7.1.1 Summary of a PSA	7-2
7.1.1.1 Report Organization.....	7-2
7.1.1.2 Scope.....	7-2
7.1.1.3 Methods.....	7-3
7.1.1.4 Display and Interpretation of Results.....	7-3
7.1.2 Main Report of a PSA.....	7-5
7.1.2.1 Integration Section.....	7-5
7.1.2.2 Task Description.....	7-6
7.1.3 Appendices of a PSA.....	7-8
References.....	7-9
APPENDIX A: Treatment of Regulatory Issues.....	A-1
APPENDIX B1: TQA Plan Discussion and Exemplification.....	B-1
APPENDIX C: Component Failure Rates.....	C-1
APPENDIX D: Generic Repair Times.....	D-1
APPENDIX E: Generic Surveillance Test Intervals and Test Duration Times.....	E-1
APPENDIX F: Generic Maintenance Intervals and Maintenance Duration Times.....	F-1
APPENDIX G: Initiating Event Frequencies.....	G-1
APPENDIX H: Plant-Specific Frequencies for the Initiating Events.....	H-1
APPENDIX I: Computer Codes for Accident Sequence Evaluation.....	I-1
APPENDIX J: Standardized Accident Sequence Nomenclature.....	J-1

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1.1	Major PSA tasks.....	1-8
2.1	PSA technical structure.....	2-3
4.1	List of failure models for a given system (train, subsystem, component).....	4-26
4.2	List of generic causative factors and corresponding systems (trains, subsystems, components).....	4-26
5.1	Example of data table for initiating event quantification.....	5-18
5.2	Example of data table for component hardware failure.....	5-19
5.3	Example of data table for procedural human errors.....	5-20
6.1	Information flow block diagram.....	6-2

LIST OF TABLES

<u>Table</u>	<u>Title</u>	<u>Page</u>
2.1	Approximate Percentage Effort in Major PSA Areas.....	2-8
3.1	Plant Functions Required For Initiating Events.....	3-3
3.2	Initiators (Not an All-Inclusive List).....	3-4
4.1a	HRA Methods.....	4-11
4.1b	Extreme "Environmental Conditions" (Generic Causes of Dependent Failures) Excerpted from the ANS/IEEE PRA Procedures Guide (NUREG-2300).....	4-27
4.2	Regulatory Issues Related to Qualitative Dependence Analysis...	4-32
4.3	Input and Output of Dependence Analysis Task for Regulatory Issues.....	4-33
5.1	Reliability Data Assessment Task Relationships: Inputs.....	5-2
5.2	Reliability Data Assessment Task Relationships: Outputs.....	5-4
5.3	Plant-Specific Data Sources.....	5-7
5.4	Basic Data to be Extracted from Plant Records.....	5-8
5.5	Component Unavailability Expressions for Standby Systems.....	5-10
5.6	Component Unavailability Expressions for Online Systems.....	5-13
6.1	Accident Sequence Boolean Equations Inputs and Outputs.....	6-6
6.2	Accident Sequence Binning Inputs and Outputs.....	6-8
6.3	Sequence Quantification Inputs and Outputs.....	6-12
6.4	Importance Analysis Inputs and Outputs.....	6-19
6.5	Sensitivity Analysis Inputs and Outputs.....	6-20
7.1	Special Reporting Requirements for Selected Regulatory Issues.....	7-10
7.2	Task Outputs to be Provided with Reports.....	7-12
A.1	Issues of the NRC Ongoing Programs Which Can Provide Information Significant to the Conduct of the PSA Studies.....	A-3
A.2	Issues for Which PSA Perspective is Gained Without Being Specially Addressed by PSA.....	A-6
A.3	Issues of NRC Ongoing Programs for Which Treatment by PSA Will Provide Risk Significance Insight or Input to Their Resolution Programs.....	A-8
C.1	Generic Component Failure Rates (All Values per Hour).....	C-3
G.1	BWR Transient Categories.....	G-2
G.2	Generic Frequencies for BWR Transient Initiators.....	G-3
G.3	PWR Transient Categories.....	G-5
G.4	Generic Frequencies for PWR Transient Initiators.....	G-6
I.1	Computer Codes for Qualitative Analysis.....	I-3
I.2	Computer Codes for Quantitative Analysis.....	I-5
I.3	Computer Codes for Dependent-Failure Analysis.....	I-7

PREFACE

This guide is intended to assist utilities in producing models that can be used and extended by the utilities and by NRC to sharpen the focus of inquiries into a range of issues affecting reactor safety. It has been prepared for use in the Integrated Safety Assessment Program. The Integrated Safety Assessment Program is a comprehensive review for operating reactors to address all of the pertinent safety issues and provide an integrated, cost-effective implementation plan. This program includes a probabilistic safety assessment (PSA) of the selected plants to provide safety perspectives of the issues and a basis for benefit-cost estimates. The actual scope of the PSA will depend on the schedule defined for a particular plant. Plants involved in near term evaluation will probably rely on existing studies, while plants scheduled further out in time may implement a broader work scope. The actual workscope for PSA will be established at the initiation of work on each selected plant. This workscope may embrace all or part of the procedures set forth in this guide.

It is widely accepted that PSAs can be extremely valuable in the area of reactor safety, but it is also widely felt that PSAs have not, as a group, clarified certain issues as much as had been hoped, in spite of much excellent and sometimes pioneering work. Some of the circumstances which contribute to this shortcoming are the following. First, the techniques of PSA are still evolving in some areas. Second, a wide variety of methodologies and assumptions have been used in different PSAs, making it difficult to compare their results. Finally, attempts to modify the model contained in a given study for the purposes of exploring the effects of changes (or of updating an obsolete model) are generally discouraged by the great difficulties involved; many PRAs are presented with the purpose of convincing the reader that the results are plausible, rather than providing the user with an adaptable model of a plant.

In response to the above considerations, this guide adopts the following strategy. In areas undergoing significant methodological development of the applicable methodologies (e.g., systems modeling), great flexibility is allowed. In other areas, where the potential for development appears to be slight but the potential for confusion is substantial, explicit prescription of the methodology is given (e.g., basic event quantification). Generic data are provided (or suggested) to facilitate analysis in those cases where plant specific data are scanty or lacking and to enable critical evaluation of the specific data where it seems called for. Finally, the documentation is prescribed with due emphasis on the needs of future users, as well as the needs of high-level reviewers. This is essential if the useful life of the PSA is to extend much beyond the date of its completion.

The present edition of this guide is the product of several substantial revisions. In this process, comments from many persons, both in industry and at NRC, have been incorporated. However, there remains substantial room for improvement, and additional comments are welcomed.

ACKNOWLEDGMENTS

As was acknowledged in the previous draft, this report has greatly benefitted from two major efforts in this area. These are the IEEE/ANS PRA Procedures Guide (NUREG/CR-2300) and the Interim Reliability Evaluation Program and its procedures guide (NUREG/CR-2728). With regard to the latter, we wish to thank Sandia National Laboratories, especially D. Carlson, for making a draft of the IREP Procedures Guide available to us in May 1982. We also thank J. Murphy for his many suggestions and his work on this Procedures Guide.

1. INTRODUCTION

The overall objective of this guide is to provide NRC and the nuclear industry with a basis for the construction of a plant model that can be used in a cost-effective manner to assess various risk indices in connection with safety decisions for nuclear plants.

1.1 Objectives

Probabilistic risk assessment (PRA) models developed for nuclear power plants provide valuable information and insight that can make important contributions to the process of evaluating safety issues of regulatory significance. This document is written with the purpose of providing guidance in performing studies intended for use in a program that integrates PRA results with deterministic studies to permit an integrated assessment of safety issues at a plant.

In order to prevent undue focus on the bottom line results of PRA and to emphasize this program's responsiveness to current safety issues, the name "PRA" has been replaced with "Probabilistic Safety Analysis (PSA)".

A key aspect of PSA is its versatility. It can be used for

- a) backfitting decisions;
- b) identification of design and operational weaknesses;
- c) providing PSA information usable in the independent process of resolving regulatory issues, including the identification and documentation of cases of overregulation in such areas as "backfit," technical specifications and technical quality assurance;
- d) evaluation of significant occurrences.

Other potential uses of PSA include

- e) reliability assurance,
- f) future safety goal integration and possible implementation,
- g) establishment of priorities for NRC activities,
- h) operator training.

1.2 Scope of the PSA Procedures Guide

In the NREP Options Study (NUREG/CR-2453), Buslik and Bari concluded that PRAs which have the greatest scope have the greatest safety benefit. Those studies which include the calculation of offsite consequences and their probabilities and include external initiating events such as earthquakes can be used for the maximum range of decision making.

Because of the large uncertainties inherent in the analysis of the risk posed by external initiating events and because of the cost associated with performing these studies, the NRC staff initially preferred not to treat the risk from external initiating events at this time. As a result of the safety significance of external events that were highlighted in the PRAs for the Zion and Indian Point plants, however, the staff decided to include external events in this guide. This is done in Volume 2, which begins with Chapter 8.

This guide does not include an analysis of in-plant physical processes (i.e., containment performance) and ex-plant consequences. However, in order to facilitate the subsequent analysis to be carried out by NRC with core melt-down computer codes such as MARCH or MELCOR, guidance is provided on the linkage of PSA results to an NRC containment/consequence analysis package. As consensus is gained on the analysis of containment performance, this guide will be augmented to reflect such consensus. At that time the utilities would include containment performance and ex-plant consequences as an integral part of their analyses.

PSAs to be performed will assume that the accidents are initiated while the reactor is in full power operation. Thus, it is outside the scope of the current studies to include accidents initiated from other modes of operation.

Performers of PSA studies are not expected to do detailed mechanistic analyses associated with their risk studies beyond those already performed for other purposes. For example, they are not required to do the fracture mechanics analysis that would be associated with a vessel thermal shock scenario. Similarly, thermal-hydraulic plant transient analysis (which would yield core or component thermal conditions) to establish plant success criteria is at the discretion of the performers.

In summary, the present version of the procedures guide pertains to studies with the following scope:

- . Includes internal initiating events.
- . Includes accidents initiated only from full power operation.
- . Does not presume detailed mechanistic analysis of plant behavior.
- . Considers initiating events due to natural and energetic phenomena such as earthquakes, tornadoes, fires, floods, explosions, etc.
- . Does not cover analysis of in-plant and ex-plant physical phenomena resulting from a core damage event.
- . Includes probabilistic analysis of containment safeguards.

Furthermore, guidance is given in the following areas:

- . Selection of initiating events: In addition to the events selected for evaluation in WASH-1400, this program recognizes that some additional events should be evaluated; these are discussed in the text in connection with safety issues identified in NRC programs (e.g., Safety Evaluation Program).

- . Use of generic and plant-specific data: For initiating events and system and component failure data, information is provided on the use of data in the evaluation of the probability of accident sequences.
- . Recognition of physical processes which may affect accident delineation: The assumptions to be used for incorporating physical phenomena which may contribute to core damage are provided.
- . Analysis of system interactions: Approaches to incorporating systems interaction in the studies are given.
- . Treatment of uncertainties: Uncertainty, sensitivity, and importance analyses are identified as required ingredients of the PSA studies.
- . Display of results and documentation: The performers of a PSA should report specific products of their studies, to facilitate their own further utilization of their work, and to allow comparison and evaluation by NRC and other reviewers.

1.3 Approach of the PSA Procedures Guide and Selected Methodology

The approach taken in this guide has been conditioned by the following considerations. The usefulness of past PRAs has been limited in part by their inscrutability, and by the diversity of assumptions and data employed in different studies. Clearly, to be useful for the purposes described in Section 1.1, the results of PSA studies should be easily assimilable by the community of reactor safety specialists. In particular, they should lend themselves to comparison with each other. It should be evident why two PSAs obtain dissimilar results; it should be clear whether differences between results computed for different plants arise because of design, methodology, modeling assumptions, or differences in plant-specific failure data. This cannot be achieved without a methodological consistency between the studies.

At the same time, it is inappropriate to prescribe all phases of studies conducted under this program in great detail. PRA is still evolving as a discipline; while there may be some areas in which some consensus exists, there are many others in which significant developments are occurring, and still others where there is some controversy. If a highly prescriptive guide were promulgated, the resulting studies would be deprived of the benefits of ongoing methodological developments, and would be burdened with whatever shortcomings are characteristic of the prescribed methods. Some study flexibility is therefore essential.

In this guide, the goals of flexibility and intercomparability are approached in the following way.

- . In many areas, there is little or no prescription of methodology. The structure of the study is prescribed, and outputs of major tasks are called for as part of the report, but the method of execution is left to the analysts. For example, this is true of the qualitative systems modeling in the Accident Sequence Definition task.
- . In the area of basic event quantification, fairly explicit guidance is given. Differences in pump failure probabilities for different plants

will reflect actual differences in the number of failures experienced.

Previous editions of this document have called for a "baseline evaluation" of the plant model, that is, a quantification of the core damage frequency based on generic failure data, as well as a plant-specific evaluation. This was described as a sensitivity study, intended to highlight design differences between plants by removing the variability in PSA results introduced by data differences. However, the goal of meaningful "baseline" comparisons cannot be reached so easily. In particular, although "realism" is a stated goal of many analyses, the limits of available resources nearly always dictate that approximations be made in the modeling. It is frequently considered obligatory to ensure that the approximations are conservative. In practice, then, analytical resources tend to be allocated in a way that maximizes effort (e.g., in justifying credit for operator action) wherever a conservative approximation gives the least tolerable result, and this can easily lead to a plant-specific pattern of conservatism and realism.

Examples of areas of possible nonuniformity are the following:

assumptions regarding the availability of nonsafety systems, e.g., start-up feedwater pumps;

assumptions regarding nonprocedural or otherwise unusual operator acts;

assumptions regarding operability of components in degraded environments, e.g., under loss of room cooling.

A PWR with a "high" AFWS unavailability may be inclined to take credit for its startup pump. This may have the effect of generating numerical values for risk indices which compare favorably with those of a plant having a lower AFWS unavailability as well as a startup pump. Thus, the questions of interplant comparisons and the associated sensitivities are complex and subtle, and depend on a clear recognition of the underlying assumptions and methods. This accounts for the emphasis on reporting and documentation throughout this guide, and the abandonment of the baseline quantification.

The methods to be used in many of the tasks in the PSAs to be performed under this program will be chosen by the performers of the PSAs. The IEEE/ANS PRA Procedures Guide (NUREG/CR-2300) is a good compendium of several alternative procedures that may be selected. For example, the analyst may choose a large event tree/small fault tree approach to accident sequence definition, rather than a small event tree/large fault tree approach. This would be acceptable, inasmuch as the two approaches yield logically equivalent results. If the analyst chooses a sufficiently novel approach to some tasks, then, through an interactive review process, he may be required to demonstrate and document the equivalence of the novel approach to a standard methodology.

The IREP Procedures Guide (NUREG/CR-2728) is a helpful example of a specific approach to performing a PSA study. In particular, it develops an input/output approach to tasks which facilitates the interfacing between tasks. Hence the IREP Guide may be used by the analyst as a specific procedural approach in those areas in which this guide allows the analyst flexibility in selecting procedures or methods.

1.3.1 Factors Conditioning Choices of Methodology and Scope in PSA Studies

Within the framework described in this guide, there is substantial freedom in choice of methodology, in details of applying chosen methodologies, and in deciding how far beyond requirements to pursue the analysis. However, owing to a number of special requirements of this program, and in light of anticipated extensions, some choices are less desirable than others. Following is a discussion of some of the considerations which affect planning of a PSA study.

1.3.1.1. The Sensitivity Studies

As discussed in Section 6, sensitivity studies are to be performed to assess the effect of hypothetical intercomponent dependences on system reliability and on core damage frequency. This requires fairly complete information on component location and on applicable test and maintenance procedures, and the searches which are called for might influence choice of computer codes.

1.3.1.2. Special Reporting Requirements

A list of special reporting requirements is given in Table 7.1. The fault trees and event trees should be so constructed as to lend themselves to these applications. Choice of computer codes could be affected by this requirement.

1.4 Documentation of a PSA Study

A PSA involves assembling a vast amount of information. Past PRAs have met with varying degrees of success in presentation of this information. Most reports contain passable statements of the general conclusions of the study, and may adequately lend themselves to high-level peer review, but in some cases, it is very difficult to verify results in detail. Typically, the large quantity of necessary information is either not given, or is given in a way that discourages its use. It is especially important that this program avoid such pitfalls. This program is intended to produce a risk-predictive model that can be used and extended by the licensee, by others in industry, and by NRC. This places special demands on the documentation; rather than merely establishing the plausibility of the results, the documentation must support efforts by persons other than the report's authors to verify, and even to modify, the results. One function of the report is therefore to serve as a "user's guide" for the plant model which is developed for the study. Of course, not all readers will become involved in manipulating the model; the report must contain a summary which meets the needs of a high-level peer reviewer.

A number of excellent suggestions appear in a forthcoming EPRI report, in a section entitled "PRA Documentation Features In Support of High Level Peer Review and Detailed Technical Review." Some of these suggestions have been incorporated into the guidance for documentation of studies performed under this program. Certain details of that treatment do not apply here, because of the rather more specific guidance provided for these studies. The main features of the suggested documentation will be summarized below, with changes appropriate to this program. A noteworthy and desirable feature of the EPRI

prescription is its emphasis on "road maps" to help the reader/user find what he needs in the report.

The EPRI approach calls for a three-level report:

- 1) a summary, which serves to communicate the essential features of the scope, methods, results, and conclusions, and which contains directions to the rest of the report;
- 2) a main report, which contains an "integration" of the entire study, detailed descriptions of all the tasks, and the detailed conclusions;
- 3) a collection of appendices, which contain detailed computations and blocks of information supporting models and analyses presented in the Main Report.

The summary will meet most of the needs of a high-level peer reviewer, although even a preliminary NRC audit must venture far enough into the main report to verify that the prescribed task outputs are present. The main report and the appendices must suffice for the detailed technical review and for the subsequent users of the study. To allow for recalculation or alteration by the users, input decks for whatever computer calculations are performed in the study should be provided, both in printed form and in machine-readable form (e.g., magnetic tape). It is anticipated that many of the computer codes used in PSAs of this program will be generally available (e.g., those listed in this guide); codes used in PSA studies which are not generally available should be documented and made available to NRC as part of the study.

The three segments of the report are discussed in more detail in Chapter 7 of this guide.

1.5 Organization of the PSA Procedures Guide

A PSA to be performed under this program will consist of five major tasks (Figure 1.1). This section contains a brief summary of each major task and its relation to the other tasks. The section of this guide in which each major task is described is also shown in Figure 1.1.

1.5.1 Plant/PSA Familiarization and Scoping

In this task, the overall scope of the PSA is examined. Assuming that not all team members are PSA practitioners*, the team as a whole becomes acquainted with how PSA confronts certain basic issues. The plant is surveyed, and the portion of it which needs to be analyzed is defined. Initiating events are considered. Frontline and support systems are defined. Events relevant to current licensing and regulatory issues are incorporated.

1.5.2 Accident Sequence Definition

This task encompasses the main activities required to obtain qualitative definitions of the accident sequences which may lead to core damage.

*See, however, the section on Personnel 2.2.2.

Functional event trees are developed which describe how the various safety functions protect core integrity.

The impact of the human, through procedural and problem-solving or "cognitive" errors, is developed in this task. The PSA approach includes problem-solving human errors concerning recovery of equipment during accidents.

The impact of physical phenomena on accident sequence definition is also incorporated in this major task. Because of the current scope of this program, only those phenomena affecting the events leading to core damage (and not those related to a post-core meltdown containment environment) are incorporated in the accident sequence development. The containment heat removal and postaccident radioactivity removal systems are, however, included in the analysis.

Guidance on the development of systemic event trees and their related fault trees is given in this task. Qualitative dependence analysis is discussed here.

1.5.3 Reliability Data Assessment and Parameter Estimation

This major task is concerned with the quantitative information needs (i.e., data and related models) that will be input to the Accident Sequence Quantification task. The data requirements will be defined by the analysis and information needs that were developed in the Accident Sequence Definition task.

This task includes guidance on data handling for accident initiators and for failures that would be incorporated in the logic trees. Guidance is provided on the use of plant-specific and generic data and on the documentation of data.

1.5.4 Accident Sequence Quantification

This task receives input from the Accident Sequence Definition task and the Reliability Data Assessment and Parameter Estimation task in order to obtain the major quantitative results of the NREP study. This task consists of five main subtasks: generation of Boolean Equations for Accident Sequences; accident sequence classification; sequence quantification; importance and sensitivity analyses.

1.5.5 Display and Interpretation of Results

This task provides guidance on the display and interpretation of results of the study. The report will display the frequency of core damage and the operability of the containment safeguards for each accident sequence. Error bounds and measures of importance will be displayed. In addition, reporting requirements of specific products of the study are summarized in the various sections of the guide. Much of this information is detailed in the previous tasks and is summarized in Section 7.

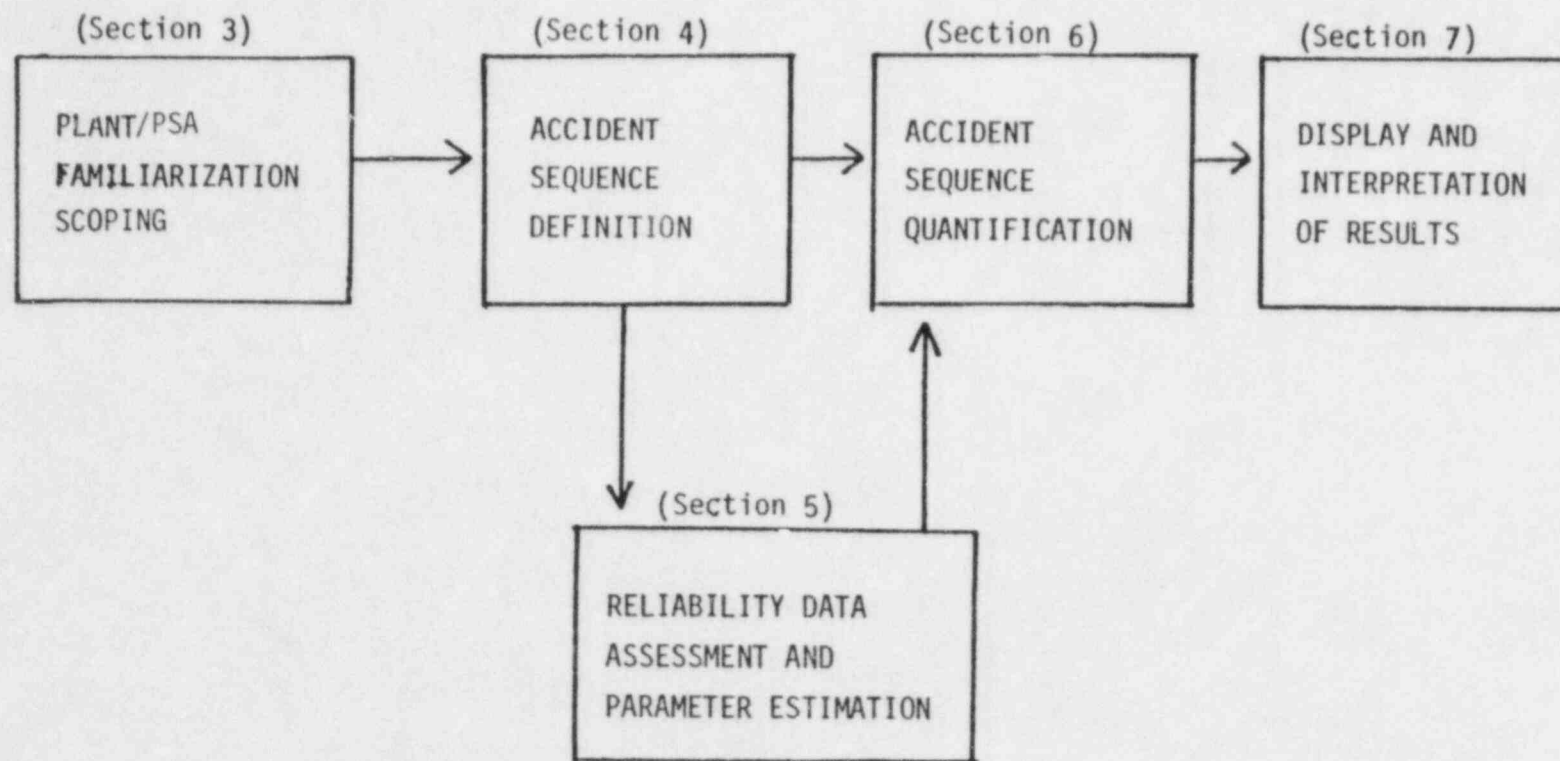


Figure 1.1 Major PSA tasks.

2. PSA ORGANIZATION AND MANAGEMENT

2.1 Introductory Remarks

The aim of PSAs is to provide versatile descriptive and predictive models (of nuclear power plants and their operations) which can be used, varied, and refined by both NRC and its licensees in their safety evaluations* (and the attendant risk considerations).

Discussions of the organization and management of PSAs are given in the IEEE/ANS Procedures Guide (NUREG/CR-2300) and in the IREP Procedures Guide (NUREG/CR-2728). These documents give useful descriptions of, and guidance on, the composition and required background and qualifications of the analysis team, on the schedules and manpower needs of the various tasks, on the reporting and documentation of the results, and on the assurance of quality. These are all areas of primary importance for the successful conduct of a PSA, and the cited documents provide much of their basic framework for both general and specific applications. In addition, a number of other documents dealing with more limited aspects of PSA serve to supplement and illuminate these questions. The more prominent of these are given in the reference list.

Since PSAs must be reviewed by NRC (and will probably be subject to more general external scrutiny), it is essential that they be clearly written, with well defined assumptions, amply documented (and justified) methods, perspicuously presented data, and with supporting tools (such as computer codes) readily accessible or verifiable. It is also desirable that their general content and format be in a sufficiently compatible form to enable them to undergo such reviews in a convenient and efficient way.

The remainder of this chapter deals (broadly) with the way these qualities may be attained. It discusses the general characteristics of a PSA, the assurance of technical quality, and the (related) topic of interactive reviews.

2.2 General Aspects

2.2.1 Management and Organization

In addition to the normal requirements for technical direction and administrative efficacy (and diplomacy), the management and organization of a PSA need special emphasis in the areas listed below. This is to ensure that the PSA will properly serve its function (which may vary somewhat depending on the plant and other circumstances) at a tolerable economic and manpower cost. The particular points requiring careful attention are:

- . choice of levels of detail in relation to the desired output;
- . balancing of technical and manpower resources;

*When properly executed in the manner described in this document, they will also serve as an effective tool for (internal) technical and economic power utility purposes.

- . assurance of technical quality and external interaction and review;
- . scheduling of the work, and timing of extraneous feedbacks and reviews.

The first two of these depend on the individual character of the PSA and the considerations which underlie them are implicit in the remainder of this guide. Depending on the circumstances of the particular PSA, the quality and experience of the PSA team, and the availability of relevant information, it should be possible to streamline the PSA to achieve its desired output with the least effort and the most effectiveness.*

The third topic, assurance of technical quality and external interaction and review, is the subject of the next sections, 2.3 and 2.4. An important aspect of technical quality assurance is continual (or at least regular) review and reexamination by a dedicated part of the PSA team. This area is explored in section 2.3. The whole process is further strengthened by interactive review by relevant external organization (e.g., NRC). This is discussed in section 2.4

The fourth point, relating to the scheduling of work and the timing of external intervention, does merit additional comment. As indicated below, the assurance of technical quality involves both internal and extraneous feedbacks and scrutiny. In order that the overall work flow of the PSA be smooth, it is essential that these external interventions be properly planned and executed. It would be natural to consider reviewing each of the major tasks defined in Figure 1.1 as soon as a reasonably complete set of task results became available. Other, more subtle, stopping points may involve interfaces between different "functional" activities (see 2.3.2 below), if these are sequential, as well as the transition from the "internal" to the "external" analysis if this is done in two distinct phases.

2.2.2 Personnel

PSA requires an unusual combination of analytic grasp, computational skill, and sound and relevant engineering judgment, in order to select, transform, and categorize existing data, to fill any gaps, and to manipulate this material in an efficacious and perspicuous manner. There is little substitute for job experience in this regard, though systematic reviews of other PSAs can help substantially. The PSA project team must demonstrate sufficient relevant experience in key management and analysis roles and sufficient documental training in bulk analysis and support roles to ensure an adequate balance between analytic capability and integrational and practical skills. The cited references supply substantial information on the requirements for personnel. Further comments are given in section 2.3 below on the interaction between the PSA team and the technical quality assurance requirements.

*Colloquially expressed, to produce a "Smart" PSA.

2.2.3 Technical Organization

This subsection outlines the technical structure and major elements of a PSA which are required to attain its desired output, and to be subject to review and manipulation for a variety of safety (and other) applications.

This structure is best summarized in Figure 2.1.

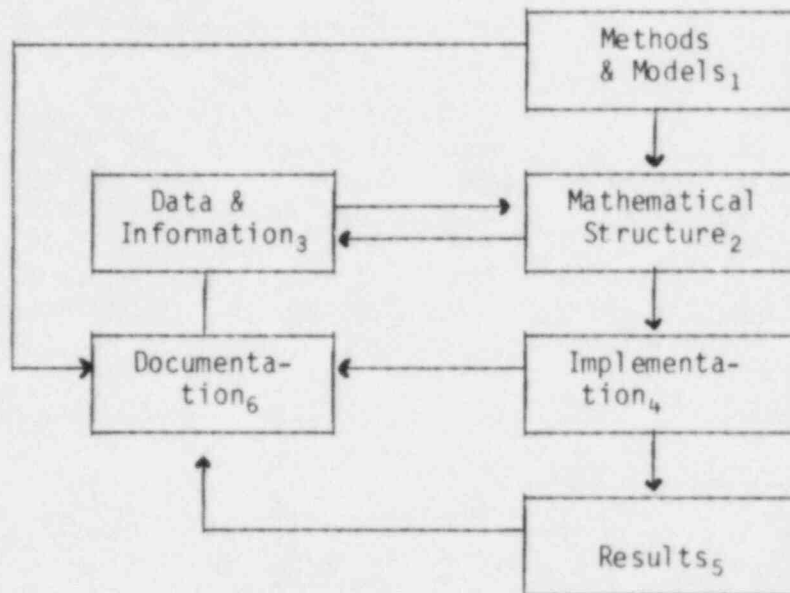


Figure 2.1 PSA technical structure.

The six major facets of the PSA shown in Figure 2.1 are briefly defined below:

1. Methods & Models: This involves the general description of the physical, engineering, and operational bases of normal and anomalous nuclear power plant behavior. The relationship between real plant behavior and the models used must be established and confirmed, and special attention must be given to the verification of performance, systems, and functional success criteria. Careful consideration must also be given to the modeling of operator action (or inaction!). In this regard, reference should be made to NUREG/CR-2254 and EPRI NP 3583. (See reference list for details.)

2. Mathematical Structure: This involves the analytical and mathematical techniques used to describe and quantify the models, and must reflect in a physically valid and mathematically correct and convenient form the model structure used.

3. Data and Information Acquisition: This includes not only the static and operational characteristics of components and systems, but also P&IDs, plant procedures, and operational information, including operator actions. Of particular importance is a thorough list of "initiators" (initiating events), and

a proper correlation of actual plant data, plant specifications, and PSA input data (via "walkdowns").

4. Implementation: This concerns the computational effectuation of the methodology established. It must properly correspond to the methods, must be internally consistent and accurate; must be flexible enough to deal with all reasonable applications; and must be able to handle questions of sensitivity and uncertainty.

5. Results and Presentation: This area (obviously) is crucial in providing a clear, comprehensive, and usable description of the PSA.

6. Documentation: Finally, it is most important to have a complete and accessible description of the detailed elements of (1) through (4) and part of (5) (the overall results) to make possible review, verification, and extended investigation (if desired or necessary).

It may be noted that while items (1) through (4) (and part of (5)) concern the primary substance of a PSA, items (5) and (6) are crucial to its utilization, comprehension, and verification.

2.3 Technical Quality Assurance*

2.3.1 General Definition and Objectives

The technical quality assurance (TQA) of a PSA involves the planned and systematic application of scientific and technical skills and management techniques to achieve a desired level of quality, and depth of understanding, and to provide assurance through objective evidence that it is being done effectively.

The TQA is thus concerned with

- the formal structure;
- the execution;
- the personnel;
- the methods; and
- the documentation

of the PSA. When these have been properly handled, the performers, users and reviewers of the PSA will be able

- to extend and update the PSA;

*This is referred to as TQA (Technical Quality Assurance) in the remainder of this section; it has a broader concept and different orientation to QA as once practiced in the older manufacturing and engineering industries.

- to apply various aspects of it to safety, operational and regulatory concerns;
- to determine, examine, and, if desired, vary the underlying data, assumptions and methods used; and
- to verify the quantitative results and to weigh their objective and subjective (i.e., judgemental) features.

These questions are discussed at greater length in Appendix B.

2.3.2 Formal TQA Requirements

The "formal" TQA program consists of several basic elements:

1. A published procedure
2. A TQA organization
3. A defined set of analytical tools and computational programs
4. A calculational file.

The detail and scope of these elements must depend on the needs of the PSA staff particularly the effort to be exerted, and on desired use(s) of the PSA.

These elements are described more extensively in Appendix B, together with samples of their formal implementation.

The above brief discussion (2.3.1 and 2.3.2), together with the exemplification given in Appendix B, is designed to illustrate the major characteristics of a TQA program. The prescriptive structure described in Appendix B, can help focus the attention of reviewers and other PSA users on the (limited) number of items cited. Other equally acceptable approaches are possible and useful provided they are designed and defined in the light of the PSA objectives.

2.4 Interactive Review

The discussion of TQA given above has indicated both implicitly and explicitly the importance of internal feedback and interaction in the conduct of a PSA. This section discusses the benefits of an interactive review with an appropriate external organization (in the first instance, the NRC). Since the NRC is generally the primary "customer" for the PSA, the objective is to enhance its usefulness for various NRC purposes. The timing and depth of such interaction must therefore be coordinated between the PSA project group and the NRC.

There are two major reasons for employing interactive review in this program. The first reason is fairly traditional: it is generally believed that outside peer review of technical work in progress can make a positive contribution to the validity of the results. The second reason is more specific to this program. The ultimate usefulness of a PSA is not decided solely by

whether the answers have withstood peer review; rather, the success of this program depends on the intercomparability of the studies, and on the adaptability of the studies to future licensing and regulatory concerns or issues. Interactive review can contribute to this by examining the scrutability and adaptability of the work performed on each task, and assessing the documentation of each task.

Certain areas deserve special emphasis. One such area is the list of regulatory concerns (Table 7.1). These should be considered in all phases of the analysis and the review. Specific areas whose treatment should benefit from interactive review are:

- 1) Overall methodological assumptions - there may be a need to demonstrate equivalence if the methods chosen by the utility are sufficiently novel.
- 2) Selection of accident initiators, and choice of appropriate end points for the analysis.
- 3) Event tree construction, including definition and documentation of mission success criteria.
- 4) Plant system analysis and fault tree construction.
- 5) Data base development.
- 6) Accident sequence quantification.
- 7) Uncertainty and sensitivity analysis.

While the stated goals for interactive review are fairly ambitious, it is also necessary to avoid undue disruption of the study. A reasonable balance would be a fairly thorough survey performed at selected milestones. Reviewing each of the five major tasks when they are substantially complete--when preliminary results have become available for use in subsequent tasks--would be a natural partition, which allows for feedback of the review's results into the development of the final outputs of each task. The timing of the review process clearly depends on the timing of the PSA; one possible review schedule was put forth in the NREP Option Study (NUREG/CR-2453).

The team involved in the interactive review should include persons familiar with the procedures and goals of the baseline evaluation, and with the scope and content of the regulatory concerns which this program is intended to address (see Table 7.1 of this guide). The scope of the interactive review goes beyond purely technical issues, however; the review tries to ensure that the study properly addresses the concerns of the intended users, that its content is ultimately accessible to them, and that it provides early and effective feedback to the analysis team.

2.5 Approximate Anticipated Level of Effort

The level of effort involved in the execution of a PSA is strongly influenced by the following factors:

- the context (i.e., the background and experience of the analysts and the availability or accessibility of relevant plant data);
- the application (i.e., is the PSA to be a tool for licensing, regulation, backfitting and/or utility planning, and is it to be in a form allowing continued updating and utilization?);
- the scope (i.e., the levels of plant "risk" considered such as core damage, containment integrity, and ultimate releases (and their potential effects), as well as the comprehensiveness of the perturbing events, such as internal anomalies and external disturbances); and
- the depth (i.e., the degrees of detail in which the various phenomena are considered, which are often dependent on the ultimate applications cited above).

Thus the aggregate effort required to complete a PSA may be expected to vary from plant to plant. Nevertheless, some useful qualitative conclusions can be drawn from (1) a study of the technical and working requirements of a PSA (as given in "PRA Procedures Guide, Vol. 1" NUREG/CR-2300), (2) a review of the experience in the execution of PSA's, e.g., "Experience and Lessons from the Oconee PRA," NSAC/82, and "The Benefit of Preoperational Risk Assessment Based on Experience with Darlington PSE" by F. K. King and V. M. Raina in ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications (San Francisco, Feb.-Mar. 1985), Vol. 2, p. 74-1, and (3) considerations of the recommendations of this guide. It must be recognized, however, that the factors cited above are interrelated, and that they affect the various constituents of a PSA, often in a significant way. The remarks below must be interpreted in this light.

1. Approximately 30% of the effort is devoted to system fault tree development, accident sequence definition, and associated analytic and numerical work in a complete PSA (Level 3) including external events. This depends on the degree of detail (influenced strongly by the applications desired). This ratio may increase if the scope of the initial PSA is limited, but it is executed in a manner to allow expansion.

2. Planning, management and support of the PSA may be expected to take about 15% of the effort.

3. Information and data gathering, including review of previous studies, and training will also involve about 15% of the effort. This fraction will probably be larger for a new PSA team, but may be expected to decline substantially as experience in PSA is developed.

4. Consideration of external events will also involve about 15% of the total effort. This part of the work, and its influence on the other constituents cited above (and below) is, however, very plant and site dependent, and this may affect the other ratios cited.

5. Analysis of containment integrity and ex-plant consequences comprise about 8% and 6% of the effort in a mature PSA, in which the initial Level 1 studies have been done with such extensions in mind. However, these

constituents of the PSA may also display unusual plant, site, and external event sensitivities.

6. The reporting, documentation, and interpretation of the PSA will comprise the remainder of the effort (about 11%). In the present guide, the requirements in this area are quite stringent, and may require a greater relative effort here (with corresponding changes elsewhere). Also, if the PSA is not executed by a predominantly utility team, it may be expected that a very substantial utility contribution will have to be made in this area, again leading to corresponding relative changes in the other categories.

Table 2.1 Approximate Percentage Effort in Major PSA Areas

Planning and Management	-15
Data Collection and Training	-15
System Analytic Development and Quantification	-30
External Event Analysis	-15
Containment Analysis	- 8
Ex-plant Consequence Analysis	- 6
Reports, Documentation and Interpretation	-11

*Footnote: PSAs carried out to date, of varying scope, depth (and format) have involved from 150 to more than 400 man-months of effort.

3. PLANT/PSA FAMILIARIZATION AND SCOPING

This section depends heavily on the IREP Procedures Guide (NUREG/CR-2728) and the IEEE/ANS PRA Procedures Guide (NUREG/CR-2300). More details on this task can be found in these documents.

3.1 Purpose

The purpose of this task is to provide the members of the team with the information necessary for the identification of initiating events, the identification of the success criteria for systems which must directly perform the required safety functions (the "frontline systems"), and the identification of the dependences between the frontline system and the support systems which they require for proper functioning.

The analysis team will include some members who are intimately acquainted with the subject plant, but not necessarily with PSA, and will include other members who, although they are experienced analysts, are unfamiliar with the subject plant. Thus, while some members are becoming acquainted with the plant, others may need to become acquainted with PSA. The object of this exercise is not to turn operations personnel into PSA specialists, any more than the team's PSA practitioners are expected to qualify as operations personnel; but a basic sense of the issues is required of the entire team. (Again, see section 2.2, particularly 2.2.2.)

3.2 Scope

Under the present scope, PSAs will determine the frequency of core damage and the operability of containment systems. However, later extension to the calculation of containment accident phenomenology, radioactive releases from containment, and offsite consequence calculations is planned. This will be done with a computer code MELCOR, which is still in the conceptual stage of development. This means that systems which are required for removal of containment heat and of radioactivity from the containment atmosphere must be considered. Moreover, the studies will include information useful for the study of external events, fires, and floods, as well as for systems interaction studies. The major purpose of this task is to settle the overall scope of the analysis, including what portion of the plant will actually be analyzed, and what events will be considered in the analysis.

The scope of this task also includes familiarization with several issues of concern to nuclear reactor regulation, which will be reflected in the initiating events considered, and the success criteria of the systems required for the mitigation of the various accidents. A discussion of these issues and the areas of a PSA that relate to specific issues is given in Appendix A. This task should include, at a minimum, the issues contained in Table A.1 of Appendix A, as well as those mentioned in Section 7.

3.3 Input

Basic plant information required for plant familiarization and scoping includes the following:

- Final safety analysis report

- Plant technical specifications
- System descriptions
- As-built system drawings
- Electrical one-line drawings
- Control and actuation circuit drawings
- Emergency, test, and maintenance procedures (and possibly some normal operating procedures)
- Analyses pertinent to the determinations of mission success criteria for frontline systems

In addition to the above, the analysts should consult lists of transients such as those in EPRI NP-2230 and other risk studies, and information in NUREG reports discussing regulatory concerns. A number of regulatory concerns are cited in Appendix A of this report, and Table 7.1 of this report gives special reporting requirements.

That portion of the above information not generally available to the intended users of the study should be provided in the Appendices to the study. This is amplified in Section 7.3.3.

Basic information recommended for PSA familiarization includes the following:

- selected PSAs (PRAs) of similar plants
- published in-depth reviews of these or other PSAs
- PRA Review Manual (NUREG/CR-3485).

A survey of selected PSAs would reward those members of the team who are not already familiar with PSA, especially if the analyses have withstood detailed review. Beyond gaining a better sense of what it is that PSAs are after, it is useful to understand why past PSAs have been criticized, and what characteristics of a PSA make it useful (or otherwise). Published reviews of a number of PSAs are by now available. Additionally, the PRA Review Manual (NUREG/CR-3485) lists a number of points which have raised questions in previous reviews. Between the published reviews and the Review Manual, a good deal of material is available to illustrate what to emphasize and what to avoid, both in the conduct of the PSA and in the presentation of it.

3.4 Assumptions and Methods

The following subtasks correspond to those in the IREP Procedures Guide, and this guide should be consulted for more information concerning these tasks. Much of the wording is taken verbatim from this guide.

3.4.1 Determination of Function/System Relations

This subtask identifies the systems directly performing each function important to preventing or mitigating the consequences of a core damage event following a loss-of-coolant accident or transient initiating event. These systems are referred to as frontline systems. The functions referred to above are identified in Table 3.1.

Table 3.1 Plant Functions Required For Initiating Events

-
- | | |
|----|--|
| A) | Render reactor subcritical |
| B) | Remove core decay and sensible heat |
| C) | Protect reactor coolant system from overpressure failure |
| D) | Protect containment from overpressure |
| E) | Scrub radioactivity from containment atmosphere |
-

This subtask also identifies the supporting systems for each of the frontline systems, i.e., it identifies those systems required for their proper functioning. This subtask also produces dependence tables or diagrams showing which systems depend (logically or functionally) on which other systems.

The information required for this task comes from several sources including the Final Safety Analysis report, detailed design diagrams, P&IDs, etc., and from discussions with plant personnel.

The products of this subtask are

1. list of frontline systems,
2. list of support systems,
3. dependence tables or diagrams.

3.4.2 Determination of Initiating Events

Detailed guidance will not be given here concerning development of the plant-specific list of initiating events. Suggestions are made below concerning useful surveys of operational data and programmatic work at NRC, which will help analysts in arriving at an appropriate set of initiators. Some sort of top level deductive process (a master logic diagram) might make the search more systematic. The goal is that the studies be substantially complete within their stated scope; this completeness is the burden of the analysts, not of this guide. If an event under consideration as an initiator is not implicit in the list, and will not otherwise be adequately reflected in the system modeling (the logic trees) and can contribute nonnegligibly to core damage, then it should be added to the list.

Loss-of-coolant accidents are characterized. Special attention is paid to identifying locations of potential loss-of-coolant accidents in systems which interface with the primary coolant system (interfacing systems LOCAs) and in identifying LOCA break locations which could entirely or partially disable responding systems. Lists of LOCA break size ranges are developed which require similar success criteria for the responding systems. This requires interfacing with the subtask on mitigating system requirements (Section 3.4.3).

Transients are identified. The standard list of transients in EPRINP-2230 is used as a starting point, and those applicable to the given plant are identified. A list of typical initiating events (both LOCAs and transients) which should be included in the study are given in Table 3.2 (these are not all inclusive).

Table 3.2 Initiators (Not an All-Inclusive List)

-
1. Turbine Trip
 2. Loss of Offsite AC Power; Degraded Electric Grid
 3. Loss of DC Power
 4. Loss of Instrument and Control Power
 5. Loss of Component Cooling Water
 6. Loss of Main Feedwater
 7. Loss of Service Water
 8. Reactor Coolant Pump Seal Failure
 9. Overcooling Events
 10. Boron Dilution Incidents (PWR)
 11. Instrument Tube LOCAs (Single, Multiple)
 12. Steam Generator Tube Ruptures (PWR)
 13. Scram Discharge Volume LOCA (BWR)
 14. Loss of Instruments and Control Air
 15. Pipe Breaks in Auxiliary Building
 16. Excess Feedwater Events
-

Events of special concern to the NRC should be considered as well. The analysts should review various documents which reflect relevant safety concerns. These include the TMI-2 Action Plan (NUREG-0660), the Systematic

Evaluation Program Report (NUREG-0485), and current lists of Generic and Unresolved Safety Issues. These lists may suggest particular initiating events that should be included (or emphasized) in the NREP study. A summary of the important regulatory issues is provided in Appendix A.

It is possible for accidents to be initiated by internal fires and floods. Such accidents are treated in Volume 2 of this guide.

Plant-specific transient events are identified by a review of operational data for the given plant, and other plants of similar design, and through discussions with plant personnel.

Faults which could cause the reactor to trip and also affect mitigating systems must be identified (for example, support system faults). The IREP Procedures Guide discusses single support system faults which could cause the reactor to trip and which could affect the responding systems. These support system faults are evaluated on a train level. It is recommended that this step be augmented by (1) reviewing licensee event reports (as suggested in the IREP Procedures Guide) as well as other sources of operational data, for the plant under study and other plants (e.g., NUREG/CR-2497), to find additional support (or frontline) system faults which can cause reactor trip (with adverse effects on mitigating systems); and (2) reviewing generic issues and issues of importance in the Systematic Evaluation Program to see if any additional transients initiated by support system faults are identified (see Appendix A).

Subtask Products

1. List of LOCA break sizes
2. List of interfacing system LOCAs
3. List of LOCAs which impact mitigating systems
4. List of transients applicable to the given plant, including both generic and plant-specific transients
5. List of transients initiated by support system faults which impact mitigating systems

3.4.3 Determination of Mitigating Systems Requirements and Other Special Conditions

Each initiator requires certain levels of success of the mitigating systems, and some initiators impose additional conditions which must be reflected in the modeling of the accident sequences.

The success criteria used for the frontline systems are of considerable importance; different success criteria can lead to widely different assessments of risk. For each type of LOCA initiating event, the success criteria, in terms of the number of trains of each system required to perform the plant functions given in Table 3.1, must be identified. Similarly, for each transient, the mitigating system requirements must be identified. Relevant information for this subtask is given in the Final Safety Analysis Report.

However, this may lead to success criteria that are too conservative. If more realistic analyses have been performed, then they should be used and supporting documentation provided. This program does not require new thermohydraulic analyses, but if analyses in support of realistic mission success criteria do not already exist, they may be submitted as part of the study. If FSAR criteria are used, then the effect of relaxing them should be explored in the sensitivity study (Section 6.5.4).

A clear example of an initiator which imposes conditions beyond success criteria is the above-discussed case of support system faults. Similarly, LOCAs may differ not only in size, but also in symptoms displayed to the operator, in effects on automatic actuation systems, in potential for inducing dependent failures, etc. Distinctions of this type must be considered when initiators are grouped into equivalence classes, so that the failures modeled in each accident sequence are properly conditioned on all of the peculiarities of each initiator group.

Subtask Products

1. A table giving, for each initiator, the associated mitigating systems, their success criteria for that initiator, reference to supporting documentation for the success criteria (documentation should be supplied with report, if not already available to the report's audience), and special characteristics of the initiator which affect the modeling assumptions.

3.4.4 Determination of Initiating Event Groups

Using the results of the subtask on mitigating system requirements, group all LOCA and transient initiating events in such a way that all events in the same group have essentially the same mitigating system requirements and impose essentially the same special conditions (challenges to operator, to automatic plant responses, etc.).

Subtask Products

1. List of grouped LOCA initiating events.
2. List of grouped transient initiating events.

3.4.5 Review of Operational Data for Multiple Failures

The credibility of a PSA depends on how it deals with multiple failures. For this reason, analysts performing a PSA are encouraged to review operational experience, in order to ensure that the modeling in the PSA will withstand comparison with reality. Several NRC programs exist for the purpose of directing attention to relevant operational history; NRC will summarize results obtained from these programs in a form suitable for use by persons performing or reviewing PSA studies, and will update this summary as necessary. It is expected that only a subset of this information will apply to any given plant; but events that are judged to reflect on the subject plant should be listed in the study, together with an indication of how they are taken into account in the model. For example, the NRC summary of relevant events may well include multiple strainer blockages, which should be cited in the study, if such an

event is possible at the subject plant, along with an indication of how this is modeled (e.g., "Event MULTSTRUCRUD on the AFWS fault tree is multiple strainer blockage") or how it is reflected in the sensitivity studies.

Many such events will not fit naturally into plant models under present guidelines, which exclude parametric modeling of multiple failures and spatial coupling. This status should be indicated for each event which is considered out-of-scope.

Subtask Products

1. List of multiple failures from NRC survey which are possible at subject plant.
2. Indication, for each such event, of how it is reflected in the plant model, or how it is reflected in sensitivity studies.

3.4.6 Survey of Regulatory Concerns

One purpose of PSA studies is to contribute to regulatory decision making. Appendix A of this guide summarizes areas of current NRC activity which can contribute to a PSA study and which will benefit from PSA studies. It is clear that there are benefits to be gained from performing the studies with these issues in mind, but there are no formal requirements associated with Appendix A.

Note that there are formal requirements associated with issues of special regulatory concern; these are tabulated in Table 7.1.

Subtask Product

1. [OPTIONAL] list of regulatory issues pertinent to subject plant.

3.5 Products

The products of this task as a whole are

1. List of LOCA and transient initiating events grouped according to mitigating system requirements.
2. Table summarizing system success criteria for each LOCA and transient initiating event group.
3. List of frontline systems.
4. List of support systems.
5. Table/diagram relating frontline/support systems and support/ support systems dependences.
6. Results of search of operational data for multiple failures.
7. List of applicable regulatory issues pertinent to the plant under study [OPTIONAL].

4. ACCIDENT SEQUENCE DEFINITION

4.1 Event Tree Development

4.1.1 Purpose

Event trees are developed to delineate the accident sequences to be considered in the analysis.

4.1.2 Scope

The systemic event trees developed in this task will interface with the MELCOR code, to be developed in the future. The success/failure of containment heat removal systems and containment atmosphere radioactivity removal systems will be identified.

4.1.3 Input

This task makes use of information developed in the plant familiarization task--in particular, the lists of initiating events grouped according to mitigating requirements, and the system success criteria. Section 4.4.1, discussing the impact of physical processes on logic tree development, also supplies input to this task. Information from the Final Safety Analysis report and other plant information are also required. The event trees of other risk studies should be reviewed.

4.1.4 Assumptions and Methods

The IREP Procedures Guide proposes the use of event trees which contain headings for frontline systems only. Support systems do not appear on the event trees. We shall call this the small event tree/large fault tree method. Another style of event tree places support systems on the event tree. This style of event tree corresponds to the large event tree/small fault tree approach. The IEEE/ANS Procedures Guide discusses both styles of event trees. The type of event tree where the support systems are placed on the event trees has a variation, discussed on p. 3-82 of the IEEE/ANS PRA Procedures Guide. In this variation, all possible combinations of support system states having the same impact on the front-line systems are grouped together into a "support system state". This approach is also acceptable. Whatever style of event tree is used, adequate documentation must be supplied, and the analysis must be verifiable and traceable.

Whatever style of event tree is used, provision must be made for the possibility that an accident sequence which starts as a transient may later develop into a LOCA sequence. In fact, transitions back to a transient plant state from a LOCA state are possible. Such accident sequences must be accounted for. In particular, failure of pressurizer relief and safety valves to close must be considered, when they have opened, and also reactor coolant pump seal failures under conditions of total loss of all ac power. The failure of pressurizer safety valves to close may be of importance in Anticipated Transients Without Scram sequences.

Issues of regulatory concern are to receive major emphasis in these studies. Section 7 and Table A.1 of Appendix A list such issues. Examples are:

1. reactor vessel failure due to pressurized thermal shock,
2. steam generator tube ruptures,
3. success assumptions used in the analysis Anticipated Transients Without Scram.

As far as steam generator tube rupture sequences are concerned, failure to close of secondary side safety relief valves must be considered. The possibility of water rising into the mainsteam pipe must be considered, as well as the fact that (at least, generally speaking) these pipes are not designed to take water loadings.

The procedural steps in the Accident Sequence Delineation Chapter of the IREP Procedures Guide represent one among several acceptable approaches. Whichever approach is used, both functional and systemic event trees must be given as part of the documentation. The event trees display some of the functional dependences between systems; i.e., cases where failure of one system means that it is impossible for another system to perform its function successfully. Such dependences result in omitting branch points. Omitted branch points also occur if success or failure of a system does not affect the radioactive release associated with a given accident sequence. An effort should be made to arrange the order of the events on the systemic event tree in such a fashion as to minimize the number of sequences that must be considered. Any dependences between functions or systems which are displayed on the event tree must be identified and explained. The system failure definitions and system modeling conditions for each system for each LOCA initiating group and for each transient initiating group must be developed and documented (see, e.g., step 17 of the Accident Sequence Delineation task of the IREP Procedures Guide).

The set of accident sequences must be subdivided into various sets, such that all members of the same set will lead to similar physical responses in the plant. This "binning" of accident sequences is discussed in Section 6.2. At this stage each accident sequence is identified only as a core damage or non-core-damage sequence.

The set of accident sequences developed should be checked against the list of regulatory issues given in Section 7 to identify any changes or additional branches needed for adequate modeling of the specific safety concern. For example, the event trees should contain all the sequences that can lead to a pressurized thermal shock of the pressure vessel and, in particular, those initiated by human errors (see Generic Issue A-49) or control system malfunction (GI, A-47, TMI-II.K.2).

4.1.5 Products

The products of this task are (1) the functional and systemic event trees for LOCAs and transients, (2) the documentation of any dependences between functions or systems which are displayed by omitted branch points in the event trees, and (3) the descriptions accompanying each event tree. Functional and frontline systemic event trees are required as final products regardless of the particular modeling approach.

4.2 Fault Tree Development

The fault tree development task description and the discussion of procedures and methodologies provided in this section draw heavily from Chapter 3 of the IREP Procedures Guide (NUREG/CR-2728). In some cases, e.g., in Section 4.2.4, large fractions of the text that were applicable were excerpted directly from that document and included here. It is noted, however, that there are numerous differences between NUREG/CR-2728 and the material presented herein.

Fault tree development is a major task. It involves modeling of all plant systems with potential risk impact, and thus requires input information from several other analysis tasks.

4.2.1 Purpose

The purpose of the fault tree development task is to construct system models of the frontline and support systems which will subsequently form the basis of the qualitative and quantitative evaluation of the accident sequences delineated in Section 4.1.

4.2.2 Scope

The systems for which fault trees are to be developed are those contained in the frontline and support system lists produced in the plant familiarization task. The tables of success criteria for each initiating event group contain the criteria which, when stated as failure rather than success criteria, become the top events for each frontline system. More than one fault tree may be developed for a given frontline system should success criteria for the system change for differing initiating events or for different accident sequences in an event tree.

It should be noted that special reporting requirements exist for certain systems. These are discussed in Section 7. Fault tree construction should be performed in light of these considerations.

In the large event tree/small fault tree approach, the top events on the fault trees have "boundary conditions" associated with them; the boundary conditions include the assumption that the support system is in the particular state appropriate to the event sequence being evaluated. Separate fault trees must be drawn, for a given system, for each set of boundary conditions.

In the small event tree/large fault tree approach, support system fault trees are developed in the context of the frontline systems they support. The system dependence diagrams developed in the plant familiarization task convey the relationships between frontline and support systems and among support systems. Generally, at least one support system fault tree is necessary for each frontline system it supports.

In the large event tree/small fault tree approach, support systems may appear on the event tree. Each different support system failure state on the event tree must have a separate fault tree associated with it, with the given support system failure state as top event.

The fault trees should reflect all possible failure modes that may contribute to the system's unavailability or the frequency of accident sequences. This should include contributions due to outages for test and maintenance, human errors associated with failure to restore equipment to its operable state following test and maintenance, and human errors associated with accident response where applicable. Potential operator recovery actions for failed or mispositioned components should not be included in the fault trees. Such considerations are often accident sequence specific and component failure mode specific and are best treated in a more limited fashion as described in the accident sequence quantification task.

The following aspects of dependent failures should be reflected in the fault trees:

- initiating event - system response interrelationships;
- common support system faults affecting more than one frontline system or component, through functional dependences;
- correlated human errors associated with test and maintenance activities.
- shared components among frontline systems.

While some sources of common cause failure are treated comprehensively in Volume 2 (fire, flood, etc.), others are not (dust, ice, manufacturing deficiencies). Certain topics of this type are addressed implicitly by the sensitivity analyses called out in Section 6. It is also desirable to consider reflecting possible common cause events in the basic model beyond those which can be explicitly developed, i.e., it may be useful to incorporate parameter treatments of certain multiple failure events. Parametric modelling has continued to develop in the last several years; for a recent review with references, see the paper by Fleming and Mosleh.¹⁰ Note that if such methods are used, the importance of the multiple failure events is to be provided separately when importance calculations are performed.

Regardless of whether parametric methods are employed in developing the basic plant model, the sensitivity studies currently prescribed in Section 6 call for assessment of the systems' potential vulnerability to dependent failures associated with components which are a) similar, b) in the same room, or c) tested in the same way. Therefore, when basic events are being documented, the information supplied should include location, designation of generic type (corresponding to types defined in the generic data base supplied here, which may differ from plant-specific classification schemes), indication of test or maintenance procedures in which the component itself is tested or maintained, and indication of test or maintenance procedures in which the component's state is altered. These procedures (or summaries) should be included as appendices to the report.

4.2.3 Inputs

The basic information requirements necessary to perform the fault tree analyses include products from the plant familiarization task (Section 3), the reliability data task (Section 5), and a significant amount of plant

information. The information requirements are tabulated below and the sources indicated.

1. Frontline systems list.	
2. Support systems list.	Plant
3. System success criteria.	Familiarization
4. System dependence diagrams.	(Section 3)
5. Results of data search for multiple failures.	
6. System event trees.	Section 4.1
7. Event descriptions for systemic event trees.	
8. Generic human error data.	Section 4.3.1
9. Results of cognitive human error evaluation.	
10. Generic and plant-specific data bases.	Reliability Data Assessment (Section 5)
11. Final safety analysis report.	
12. Plant technical specifications.	Basic Plant
13. System descriptions.*	Information (Licensee)
14. As-built system drawings.	Basic Plant
15. Electrical one-line drawings.	Information
16. Control and actuation circuitry drawings.	(Licensee)
17. Emergency, test, and maintenance procedures.**	

4.2.4 Assumptions and Methodology

The process of constructing the system fault tree requires the analyst to choose a fault tree analysis methodology and to make a number of simplifying assumptions.

This procedures guide does not specify or require a particular approach or methodology for use in the systems analysis task, for the following two

*Of the type used in plant/operator training manuals, which are more complete than those contained in the FSAR.

**Some normal operating procedures may also be required.

reasons. The first is that any valid methodology correctly applied will yield identical or equivalent results. The second is that the choice of a fault tree methodology cannot be made independent of the approach taken in the event tree analysis task. The complete methodology required to perform the plant analysis requires compatible approaches to these intimately interrelated tasks. Two basic approaches, with several variants, are well established and widely used. These are referred to as the "fault tree linking" and "event trees with boundary conditions" approaches in the IEEE/ANS Procedures Guide, and as the "small event/large fault tree", and the "large event tree/small fault tree" approaches in this guide. The basic differences in their treatment of the fault tree development task are described in the IEEE/ANS Procedures Guide, on pp. 3-77ff and 6-20ff.

The basic Boolean relationships represented in any fault tree are the operators "AND," "OR," and "NOT." These operators are represented by "gates" in the fault tree. Other less basic operators can be defined in terms of the AND, OR, and NOT operators.

Regardless of the approach used to develop the fault trees, it will be necessary to make a number of assumptions in the process of constructing the trees to simplify and reduce the size of the trees. Most of these assumptions should be generic, as in the examples discussed below, but some system-specific assumptions may also be necessary. In all cases, it is important to clearly specify and document the assumptions made to promote and ensure consistency throughout the analysis, and to preserve traceability in the analysis.

It may not be necessary to construct fault trees for all plant systems. Those systems which do not interface or interact with other plant systems and for which sufficient system wide reliability data exist may not require fault trees. In the case of power conversion system faults, data exist for losses of the power conversion system. This system does, however, interface with other plant systems. It is important to separate out the interfacing faults in the analysis.

To permit proper quantification of accident sequences in which the initiating event may affect the operability of a responding system, system fault events which could also be initiating events (e.g., LOCA events, loss of off-site power) should be explicitly included as appropriate in each system fault tree. In the small event tree/large fault tree approach these initiating events will, generally speaking, occur at the component level. In the large event tree/small fault tree approach, the initiators may appear as boundary conditions on the top event.

To simplify and reduce the size of the fault trees, certain events are often not included owing to their low probability relative to other events. Examples of simplifying assumptions include the following:

- a. Flow diversion paths for fluid systems should be considered only if they could seriously degrade or fail the system (a general rule is that if the pipe diameter of the diversion path is less than one third that of the primary flow path, the diversion path may be ignored).

- b. Spurious control faults for components after initial operation should be considered only in those cases where the component is expected to receive an additional signal during the course of the accident to readjust or change its operating state.
- c. Misposition faults prior to an accident are not included if the component receives an automatic signal to return to its operable state under accident conditions.

These are not endorsed, but are mentioned only as illustrations. Assumptions of this type must be discussed in the report.

The analyst should also examine all available information collected and assembled in the Plant Familiarization Task (Section 3) which contains descriptions of all types of multiple failures that have occurred at the plant being analyzed, and at similar plants, in order to obtain a direct awareness of the potential for multiple independent or dependent failures in the systems, and of the potential for systems interactions.

Examination of Testing Procedures

The testing procedures used in the plant must be closely examined to see if there are potential failure modes which will not be revealed by testing. All such potential failure modes identified must be documented. An example of a failure due to inadequate testing procedures occurred at San Onofre-1 on September 3, 1981, when safety injection valves failed to open upon a valid safety injection system signal. The valves would not open with the design differential pressure across them.

Component Trips Designed to Protect a Component

Trips of pumps and other safeguards intended to protect a component must be carefully identified. They can be a source of common mode failure. For example, spurious trips of auxiliary feedwater pumps on low suction pressure can lead to system failure if recovery does not occur.

Addressing Selected Regulatory Issues

The set of the fault trees developed should include all the necessary aspects of the regulatory issues contained in Table A.1 (App. A) and in Section 7.

Success Trees

In sequences wherein some systems succeed while others fail, it is important to condition the system failures correctly on the other systems' successes. Success trees may be useful for this; an example is given in Section 3 of the IEEE/ANS Procedures Guide. This is not the only method, however, and may be cumbersome. Certain advantages are offered by algorithms which operate on the top event simply by deleting cutsets that violate the system success specified in the sequence (NUREG/CR-2728).

Event Naming

In general, it is extremely useful to encode certain types of information in the event names which appear on the fault trees. For example, system name, component type, component identifier, and failure mode are traditionally included. Different computer codes place different constraints on the event names which are allowable; partly for this reason, it is inappropriate to prescribe here the character-by-character details of a naming scheme. However, certain activities which will be part of this program will benefit greatly if a naming scheme is used which goes beyond that mentioned above, to facilitate searches of fault trees, data bases, and cutset lists for events which relate to:

- generic component types as defined by the generic data base (Table C.1);
- specific entries in the generic data base;
- particular types of human errors.

In addition, it would be desirable if some consistency could be achieved with the coding used in the LER Sequence Coding and Search Procedure (NUREG/CR-1928), although it is on the whole more detailed than may be appropriate.

A generally complete description of the steps involved in the fault tree development process is presented in Section 3.2 of NUREG/CR-2728. This description is, however, limited to the small event tree/large fault tree approach.

4.2.5 Products

The products of the plant systems analysis task are

1. a list of the assumptions made for the analysis;
2. a list of the different event tree conditions that require different fault trees for each frontline system;
3. a description of each system detailing the purpose of the system, the system configuration, system interfaces, instrumentation and control, testing and maintenance, applicable technical specifications, how the system operates, and assumptions used in the analysis of the system;
4. fault trees for each frontline system for each of the success criteria specified on the event trees;
5. fault trees for each support system developed in the context of each frontline system it supports;
6. information regarding location, generic type, and applicable test procedures for components involved in each failure event;

7. an identification of further component failure rate data needs, if any; and
8. a list of basic events with definitions and (after completion of Reliability Data Assessment task) generic and plant-specific quantifications.

To include preparation of the system models for a concurrent or subsequent evaluation of environmental effects, the system models will contain information regarding component location and susceptibility to the environmental effects of interest, e.g., earthquake, fire, or flooding, beyond that mentioned in item 6. It is strongly urged that information of this type be encoded within the component name or provided on separate tables correlating event names with applicable information.

Particular care should be taken in documenting the basic events of the fault trees. In some studies, it is difficult to discover the meaning or the probability of an event, given only its identifier; tables of event definitions are generally supplied, but sometimes in a form which necessitates exhaustive searching to find an item of interest. This will be true, for example, if there is no relation between the event name and its placement in the table. It should be straightforward, without exhaustive searching, to

- find the definition of an event name, and its probability;
- find all event names which relate to a particular component;
- find plant-specific event names which are instances of events from the supplied generic data base;
- find plant-specific event names which are subevents of events from the generic data base.

At a minimum, for example, one could tabulate basic events separately for each system, and order the events lexicographically within each system. Then, given an event naming convention which incorporates component type information, a user could fairly straightforwardly locate (say) all EMD pump failure events within the service water system. However, better schemes can no doubt be devised by the teams performing the studies.

This should also be undertaken with other task products in mind. It is extremely beneficial to coordinate certain products in order to facilitate cross-reference. For example, a great deal of comparison will be made between the basic event tables, the FMEA tables, the tables giving locations of components, etc. The usefulness of a study depends a great deal on how easy it is to go back and forth; of course, great emphasis should be placed on making it convenient to go from the fault trees to the tables, and from one sheet of the fault trees to another.

4.3 Human Reliability Analysis (HRA)

4.3.1 Purpose

This section provides guidance on the treatment of human errors in assessing plant safety and documenting HRA results in a PSA. The objective of this section is to provide sufficient latitude to allow use of the many emerging HRA methods available to the analyst, while still providing sufficient guidance on documenting HRA results to make them scrutable and comparable to other PSAs using different HRA methods. It is recognized that there is no strong consensus in the HRA community on the best methods to use in risk assessments. Accordingly, this section should not be viewed as limiting the use of new HRA methods as they are developed and evaluated; rather, this section establishes standards of documentation on the HRA methods, including intermediate results, which should broadly apply to any HRA method chosen by the utility.

4.3.2 Scope

This section covers the analysis of all human acts identified during the course of risk assessment as being of concern. The recommended approach consists of successively more detailed analysis of these acts. The level of detail applied to the analysis of a particular set of human errors is dependent on the sensitivity of risk to the probabilities of those errors. That is to say, the human errors that are considered in the most detail are those which most impact risk if their probability is high. If a particular error has been identified but, even with a high probability, would not significantly affect risk, it is not considered further. In order to identify those errors which may have such an impact on risk, a screening process is recommended that determines the importance of a human error from the potential contribution of each error to risk of core damage (Section 6.3). The objective of the screening process is to optimize the use of resources by focussing attention on potentially risk-significant events. As a result, the sensitivity of the screening process can vary depending upon these factors. Subsequent to the screening process, each important human error is assigned a plant specific probability by an HRA specialist. The human error probability assigned is then used in the broader analysis of the overall sequence and, ultimately, risk.

4.3.3 Process Considerations

The process by which HRA was integrated with the overall risk assessment in a PSA should be thoroughly documented. There are many means of integration available; a good example is discussed in Systematic Human Action Reliability Procedure (SHARP) (EPRI-NP-3583). SHARP is an acceptable process for this integration. The SHARP report discusses specific documentation requirements for each step in the procedure which are summarized below.

Step 1 - Definition. The objective of this step is to assure that key human interactions are included in the logic structures (i.e., event and fault trees) of the system analysis. Generally, the HRA specialist receives the sequences to be analyzed after they were initially developed by hardware-oriented specialists. If practical, an HRA specialist should provide input to the initial definition of accident sequences to be

considered. If not, the HRA specialist should comprehensively review each sequence for potential human errors. Desirable documentation of this step includes (1) the human actions explicitly considered, (2) the human actions implicitly considered, and (3) a description of the review of operating history which was conducted. Any human errors which the HRA specialist identifies as important, but do not appear in the event or fault trees, should be fully discussed.

Step 2 - Screening. The objective of this step is to reduce the number of human errors considered in the final analysis to a manageable number. The level of screening is dependent on the size of the HRA staff and budget. Suitable documentation of this step includes (1) the method of screening used, (2) the quantitative screening values used and how they were chosen (3) the important errors carried forward for more detailed analysis, and (4) a list of all errors dropped from further consideration. Acceptable screening processes are discussed in EPRI NP-3583 and in Section 6.3.

Step 3 - Breakdown. The objective of this step is to amplify (to a practical degree) the qualitative description of each key human error identified in Step 2 in order to develop sufficient information to quantify the probability for each error. Background for this step may include (1) the nature of plant staff interviews, (2) what plant personnel were interviewed, (3) operation history reviewed, and (4) results of reviews (e.g., control room reviews). Each human error considered should be described as comprehensively as practicable.

Step 4 - Choice of Method. The objective of this step is to identify and select the most appropriate method for analysis of each of the human errors considered in Step 3. Suitable documentation for this step includes a complete discussion of the reasons for selected methods. If a method other than those presented in Table 4.1 is used, a complete set of references for that representation should be provided in the PSA.

Table 4.1a HRA Methods

Method	References
Confusion Matrix	NSAC/60
Direct Numerical Estimation	NUREG/CR-3688
Influence Diagrams	Phillips et al.
LER-HEP Method	NUREG/CR-3519
MAPPs	NUREG/CR-3626
MSF Model	NUREG/CR-3837, -2211
OATs/Time Reliability	NUREG/CR-3010
Paired Comparisons	NUREG/CR-3688
SLIM-MAUD	NUREG/CR-3518, -4016
THERP	NUREG/CR-1278, -2254

Step 5 - Method of Integration. The objective of this step is to integrate any models derived from methods selected in Step 4 into the logic structures of the overall risk analysis. Suitable documentation for this step includes (1) the specific factors that lead to modification of the logic structures and (2) recovery actions which were considered. It is important that changes made in the logic structures of the risk assessment be fully discussed.

Step 6 - Quantification. The objective of this step is to assign the probabilities of success and failure for each of the errors included in the risk analysis. Documentation requirements for this step are outlined in the next section.

Step 7 - Documentation. The objective of this step is to produce a traceable description of the overall process used to develop the quantitative estimates of human error probabilities (HEPs) used in the risk assessment. This documentation should be part of the final risk assessment document as outlined in Section 7 of this report.

4.3.4 Quantification of Human Error Probabilities (HEPs)

In PRAs done to date, many methods for estimating HEPs have been used. In addition, there are many emerging methods, several of which have been developed and evaluated by NRC. In this section, generic as well as method-specific documentation requirements are discussed. These requirements should not be viewed as biasing the choice for or against any specific methods. Basically, any method chosen should be documented sufficiently to allow meaningful review and comparison to other methods which are used, and possible later revision of the treatment, undertaken in light of plant modifications or new information.

4.3.4.1 General Requirements for Documentation of HRA Results

There are many methods currently in use and under development for assessing the human reliability component of safe nuclear power plant operation. This guide does not endorse any specific methods for use in HRA and it is expected that Table 4.1 will be updated periodically. However, it is necessary that any HRA method which is used in a PSA be well documented so that the results of the analysis are scrutable and comparable to other PSAs. In addition, sufficient information must be provided so that later revisions can be made based on plant modifications or new information.

Four general classes of HRA methods have been identified: (1) expert judgment, (2) performance process simulation, (3) performance data analysis, and (4) dependence calculations. Many existing methods represent a mix of these classes so that the specific methods discussed in Section 4.3.5 are not classified according to this taxonomy. However, by describing the type of documentation required in a PSA for each class of methods, any alternative method can be used and documented properly by determining the particular mix of these classes it represents. Each class of HRA methods is discussed below.

4.3.4.2 Expert Judgment

Expert judgment is a widely used tool in many parts of risk assessment besides HRA. Methods for expert estimation of human error or equipment failure probabilities range from individual desk-top judgments (e.g., "engineering" judgment) to highly structured and facilitated group estimation techniques (e.g., SLIM-MAUD). The elements of these processes which should be documented when used include:

- The specific human errors analyzed using this type of method.
- The background of the expert(s) making the judgment, and the facilitator if one is used, in terms of education and experience.
- The size and composition of any groups and, if they interact during the process, the nature of the interaction.
- The judgment process. If it is a structured technique describe the structure and process.
- Any assumptions or models used in the structure or process which play a role in determining the final probability estimates.
- A complete set of references used in developing the specific expert judgment method used in the PSA.

4.3.4.3 Performance Process Simulation

Performance process simulation includes all models or simulations which involve representation of the psychological or physical processes occurring during the human error under consideration. To the extent that any HRA method uses process simulation, it should be fully described. The elements of performance process simulation methods that should be documented when used include:

- The specific human error tasks analyzed using this type of method.
- The particular process being simulated and how the simulation was developed.
- The inputs the HRA specialist put into the simulation in order to make it address each error analyzed in this manner.
- The structural process aspects of the simulation that facilitate determination of HEPs from the simulation.
- Any factors that were subsequently considered by the HRA specialist in assigning the HEPs that are used in the overall risk assessment.
- A complete set of references used in developing the specific simulation used in the PSA.

4.3.4.4 Performance Data Analysis

Analysis of performance data can provide information useful in determining HEPs. If performance data are analyzed documentation should include:

- The specific human errors that were analyzed using this type of method.
- The source of the performance data analyzed and, when appropriate, a description of the database and why it was selected.
- The assumptions and algorithms used to derive HEPs from the data.
- Any factors that were subsequently considered by the HRA specialist in assigning the HEPs used in the overall risk assessment.
- A complete set of references used in developing the specific performance data analysis technique used in the PSA.

4.3.4.5 Dependence Calculations

Dependence calculations in risk analysis generally take the form of predicting conditional failure probabilities for redundant components in a safety system assuming that one has already failed. These conditional probabilities are then used to calculate the probability of a complete system failure. For any dependency calculation documentation should include:

- A list of all systems for which dependence calculations were made.
- The assumptions and specific model used to generate the conditional failure probabilities for components in each system analyzed using this method.
- The input data used as input to the model and how they were selected.
- The independent and conditional failure probabilities for each component in every system analyzed.
- A complete set of references used in developing the specific dependency calculation used in the PSA.

Important aspects of dependence arise, particularly in response to "external" events, such as earthquakes, fires, and floods, etc. In addition to the expected opportunities for human error associated with "internal" failure and accident scenarios, such events may stimulate substantial further degradation of operator performance via spurious instrumentation and other information signals in the control room, by toxic and other noxious environmental effects and by general perturbation of the operational and maintenance environment.

Such phenomena should be treated in a similar way to that defined above, with appropriate reference to the disturbances listed in Sections 9, 10, and 11.

4.3.5 Method Specific Documentation

There are many different HRA methods which have been either (1) used in currently available PRAs, (2) developed and evaluated for use in PRAs, or (3) both. Eleven such methods are discussed in this section along with recommended documentation for each. It must be recognized that many of these methods contain elements of two or more of the classes of methods described in the previous section. As a result, no attempt is made to classify these methods.

4.3.5.1 Confusion Matrix

The confusion matrix (NSAC/60, 1984) is a method that identifies potential operator errors stemming from incorrect diagnosis of an event. For example, it can be used to identify the potential for an operator to conclude that a small LOCA has occurred, when it is actually a steam line break. This method provides a rational method for identifying operator actions which stem from the wrong response to an off-normal plant condition. As such, it is particularly useful in Step 5 of the SHARP procedure which identifies potential system interactions and result in modification of the risk assessment logic structures.

Documentation should include:

- A list of the possible misdiagnoses and subsequent operator actions under consideration which could give rise to system interactions from operator diagnostic errors.
- The confusion matrix developed for each diagnosis and operator action which was represented in a confusion matrix.
- A list of the misdiagnoses which are determined not to potentially cause system interaction, and why they were viewed this way.
- Any probabilities that were assigned to diagnostic errors and how they were chosen.

4.3.5.2 Direct Numerical Estimation

The method of direct numerical estimation (NUREG/CR-3688) is a structured expert group judgment technique (i.e., psychological scaling). A list of human errors is given to a group of experts who assign a best estimate probability of error and associated uncertainty bounds. Subsequently, the error rates and uncertainty bounds are combined using the geometric mean to arrive at a final estimate of the HEP and associated uncertainty bounds.

Documentation should include:

- A complete list of human errors considered by the expert group.
- A description of the composition of the expert group used, including the size of the group and the backgrounds of the individuals involved.
- A description of the training and background of the facilitator instructing the expert group.

- The raw data which were generated by the group (i.e., individual estimates for each error considered).
- A complete list of the final probability estimates and associated uncertainty bounds derived from the group data.

4.3.5.3 Influence Diagrams

The Influence Diagram method (Phillips et al., 1985) is a structured expert group technique in which a graphical representation of the possible dependence between various outcomes is used to derive probabilistic estimates of those outcomes.

Documentation should include:

- A list of all errors analyzed using this method.
- A description of the composition of the expert group used, including the size of the group and the backgrounds of the individuals involved.
- A description of the training and background of the facilitator instructing the group.
- The actual influence diagrams developed by the group.
- All weights assigned to each occurrence in the influence diagrams.
- All factors considered in assigning those weights.

4.3.5.4 LER-HEP Methodology

The LER-HEP method (NUREG/CR-3519) is a means of analyzing field data to estimate HEPs. It involves considering available data on specific human errors committed in a plant which are similar to those being considered in the risk assessment. The application of the method used in NUREG/CR-3519 is to the Licensee Event Report (LER) file so it is called the LER-HEP method. For each error analyzed using this method, an error rate is derived by dividing the number of errors reported which were closely similar to the error being analyzed by the estimated number of opportunities for that specific type of error. That rate is then used as a basis for estimating the HEP used in the risk assessment.

Documentation should include:

- A list of all human errors analyzed using this method.
- The source of field data used (e.g., LER file, I&E reports, etc.).
- Assumptions used to group reported errors to represent the error being analyzed.
- Analyses used to determine the number of opportunities for each type of error to occur.

- The counts, opportunities, and resultant rates for each error analyzed.
- Any modifications of the rates to estimate the HEPs.

4.3.5.5 Maintenance Personnel Performance Simulation (MAPPS) Model

MAPPS model (NUREG/CR-3626) is a task-oriented, computer-based model for simulating actual processes in maintenance activities. It includes environmental, motivational, task, and organizational variables which affect human performance and yields information such as predicted errors, personnel requirements, areas of maintainer stress and fatigue, performance time, and required maintainer ability levels for any corrective or preventive maintenance actions.

Documentation should include:

- A list of the maintenance tasks analyzed using this method.
- A list of the subtasks used for each error analyzed.
- The input variables specified for each error analyzed and how they were selected.
- The assumptions used in analyzing the output of the method and how final probability values for use in the overall risk assessment were determined.
- Any uses of the output of the method to assist in any other part of the risk assessment.

4.3.5.6 Multiple Sequential Failure (MSF) Model

The MSF model (NUREG/CR-3837) is principally used to determine the level of dependency introduced by maintenance, testing, and calibration activities on safety systems which incorporate redundancy. It is a mathematical model which modifies the independent failure probability of any single component by considering that a component with which it is redundant has already failed. This allows calculation of the conditional failure probabilities of redundant components in order to more realistically determine the overall system failure probability.

Documentation should include:

- A list of all systems which were analyzed using this method.
- The sources of independent failure probabilities for the components involved.
- The dependency data which was analyzed.
- The dependency factors (i.e., the value of k) used in each calculation and how they were determined.

- The system failure probability for each system analyzed, and the specific conditional failure probabilities for each component in the system.

4.3.5.7 Operator Action Tree (OAT) - Time Reliability Correlation

The Operator Action Tree (OAT) - Time Reliability Correlation method (NUREG/CR-3010) is specifically designed to estimate HEPs for actions which require decisionmaking on the part of the plant operator. It employs two steps: (1) the development of an operator action tree which reflects the specific actions which may be taken by an operator faced with a particular decision, and (2) a time reliability correlation which relates the time available for action to the likelihood of an error.

Documentation should include:

- A list of all human errors analyzed using this method.
- The operator action tree used to develop the errors.
- The specific time reliability curves used and how they were developed.
- The critical considerations in determining the time available for each action.
- A list of any weighting factors used to modify the HEPs used in the risk assessment.

4.3.5.8 Paired Comparisons

The paired comparisons method (NUREG/CR-3688) is a structured group expert judgment method in which a list of human errors under considerations are systematically compared in pairs. By combining the judgments of the group of experts, the errors are arranged by order of likelihood of occurrence. If assessed probabilities are available for several of the human errors considered, they can be used as "anchor points" to assess the probabilities of other errors on the list.

Documentation should include:

- A list of all human errors analyzed using this method.
- The expert tables generated during the pairwise comparisons.
- The final ranking of the human errors considered.
- A list of the specific anchor points, their sources, and scaling factors used to determine probabilities for other errors analyzed.
- A description of the composition of the expert group used, including the size of the group and the backgrounds of the individuals involved.
- A description of the training and background of the facilitator instructing the expert group.

4.3.5.9 Success Likelihood Index Method/Multi-Attribute Utility Decomposition (SLIM-MAUD)

SLIM-MAUD (NUREG/CR-3518) is a structured group expert judgment method that is facilitated using a computer terminal to classify, rate, and weight HEPs. It involves a specific process by which each error considered is put into separate classes depending on their degree of similarity. Then the errors in each class are analyzed according to the factors which are perceived by the expert group to affect performance. The group weights these factors to arrive at an index value for each error analyzed which is then converted into an HEP to be used in the risk assessment.

Documentation should include:

- A list of all human errors analyzed using this method.
- A description of the composition of the expert group used including the size of the group and the backgrounds of the individuals involved.
- The errors analyzed according to the final classifications assigned by the group.
- A list of the factors considered for each error and the relative weight each factors was assigned.
- The final index values and the calculated HEP for each error considered.

4.3.5.10 Technique for Human Error Rate Prediction (THERP)

THERP (NUREG/CR-1278) is a method which is used to estimate HEPs for each error considered in a risk assessment. It provides error probabilities for numerous generic tasks, and describes the process used to modify these rates depending on the specific performance shaping factors (PSFs) involved in the task being analyzed. THERP also provides a method for estimating dependencies introduced into redundant systems by human activities.

Documentation for specific human errors should include:

- A list of all human errors analyzed using this method.
- All human action trees used and all input used in constructing those trees (e.g., procedures).
- A list of the generic human error probabilities used to determine a base error rate for each human error considered.
- For each error, a list of all PSFs considered and the considerations that went into scaling the generic probability to represent each error.

Documentation of dependence calculations should include:

- A list of all systems which were analyzed using this method.

- The event trees used to identify complete and partial failure combinations.
- The high, medium, or low dependence level assigned to each system and the resultant conditional failure probabilities.
- The reasons for selecting high, medium, or low dependence for each system.
- The results of any sensitivity analyses conducted during the analysis.

4.4 Special Tasks

The special tasks described below are supportive to the event tree/fault tree methodology described in Sections 4.1 and 4.2 but require iteration with tasks discussed in other sections of this guide (e.g., quantification tasks).

4.4.1 Impact of Physical Processes on Logic Tree Development

The purpose of this section is twofold: 1) to give recognition to physical processes and phenomena which should be incorporated into the development of the part of the accident sequences leading to core damage, and 2) to provide guidance on the linkage of the accident sequences event trees to containment event trees with the expectation that the latter would be developed at NRC or would be the subject of future analysis by the utilities.

4.4.1.1 Impact of Physical Phenomena on Accident Sequences

The current scope of these studies includes determination of the core damage frequency and the identification of the operability of active containment systems. Physical phenomena occurring after core melt will be studied later by NRC, and need not be treated at present, but it is important to recognize the impact on engineered safety features and their support systems of accident environmental conditions. Therefore, the ability of the relevant pieces of equipment to withstand accident conditions must be assessed as part of the studies.

Examples of points which are to be considered are the following:

1. The potential for containment failure prior to core meltdown should be addressed. A sudden depressurization of the containment building during an accident could lead to vaporization of recirculation water and potential pump cavitation and damage. For present purposes, it will be assumed that pumps will not be operable after such an event unless analysis is provided which demonstrates operability under these conditions.

2. An assessment should be made of the impact of blowdown forces associated with a loss-of-coolant accident on equipment survivability and containment integrity. Insights and information developed from the relevant regulatory issues should be used in this assessment. Containment atmosphere temperature and pressure should be assessed in a manner consistent with operability of containment safeguards for the particular accident initiator. For example, if the initiator is station blackout and if the containment safeguards require

ac power, then they should be given to accident initiators involving support systems to the containment safeguards.

3. Transients which may lead to the violation of the reactor coolant system pressure boundary should be identified. For example, an assessment should be made of system failures and/or conditions that could lead to vessel failure by pressurized thermal shock. Similarly, initiators which could lead to steam generator tube rupture events should be examined. In addition, the possibility of breaching the PWR reactor coolant pressure boundary following a range of ATWS conditions should be considered. Relevant to these issues is information developed by programs addressing generic issues A-3, A-4, A-5, A-9, and A-49, and by the plants' revised accident analyses performed in response to the TMI Action Plan (Appendix A and Section 7).

The current scope does not include a level of physical analysis adequate to distinguish between a damaged core and a melted core. It is left as an option to include such analysis.

4.4.1.2 Linkage of Accident Sequence Event Trees With Containment Event Trees

It is expected that, when the containment analysis of core damage sequences is performed by NRC for the plants selected for PSA studies, the formalism will be based on the approach presented in the Reactor Safety Study (WASH-1400). Thus, analysts working under the present guidelines are encouraged to develop their accident sequences in a manner that facilitates this linkage.

4.4.2 Qualitative Dependence Analysis

Dependent events are those that are correlated with other events. This in general means that the probability with which a dependent event might occur will depend on whether the other events on which it depends have already occurred. Since a probabilistic risk assessment study is mainly interested in the existence of adverse dependences, a dependence between faults is usually meant to imply that the occurrence of one fault is positively correlated with the occurrence of other faults.

4.4.2.1 Purpose

The purpose of the qualitative dependence analysis task is twofold. First, it should identify the existing dependences in the design of a nuclear power plant; and second, it should provide the right framework for incorporating these dependences into the quantitative estimation of the risk. Identification of dependences is extremely important not only for avoiding an underestimate of the risk, but because it points out the weak points of the design and by doing so provides the single most effective way for reducing the risk and by doing so provides the single most effective way for reducing the risk by appropriate design changes. The search for dependences must involve hardware dependence as well as human-coupling between failures.

4.4.2.2 Scope*

A serious attempt to model failure dependence and systems interaction is crucial to PSA studies. Shortly, NRC will endorse a methodology for this subtask to be used in the studies. Pending such a development, this guide requires that (1) qualitative information developed in this subtask be presented as a basis for further work in the area, (2) functional and human-interaction dependences be shown on the tree and quantified as part of the results, and (3) a limited study be done of the sensitivity of core damage frequency to certain failure dependences (Section 6.5.4).

In general, the classification of dependences can be based on the causative factor of the dependence (i.e., the nature of the "coupling" between faults) and on the complexity of the devices that are involved (i.e., system, redundant train, subsystem, component). Such a classification is useful because some methods more efficiently identify and/or model specific types of dependences than other methods. On the basis of the nature of the causative factor, dependences may be placed in the following three categories**

Type 1 Functional Dependences: Dependences among devices that are due to the sharing of hardware or to a process coupling. Shared hardware refers to the dependence of multiple devices on the same equipment. An illustration of shared hardware is the dependence of both the LPCI and RHR systems upon the same pumps in a BWR. By a process coupling we mean that the function of one device depends directly or indirectly on the function of another. A direct dependence exists when the output of one device constitutes an input to another. An indirect dependence exists whenever the functional requirements of one device depend on the state of another. An illustration of a direct process coupling in a BWR is the dependence of the low pressure ECCS upon the automatic depressurization system if the high pressure system should fail during a transient or a small LOCA. An illustration of an indirect process coupling is the increased flow rate requirements of a pump whenever another pump running in parallel fails. Possible direct process couplings between devices include electrical, hydraulic, pneumatic, and mechanical connections.

Type 2 Physical Dependences: Dependences that couple two devices through a common environment or environmental conductor(s). Most dependences of this type involve devices sharing a spatial domain which allows an extreme environmental condition to affect these devices simultaneously. Such extreme environmental conditions can be generated either externally to the plant by phenomena such as earthquakes, flood, airplane crashes, or other missiles; or internally to the plant by fires, explosions, pipe breaks, etc. It should be emphasized that proximity is not the only

*A useful and extended description and taxonomy of failure dependence and systems interactions may be found in Reference 7.

**In the following definitions, the term device is used in a generic sense to mean system, train, subsystem, or component.

"environmental" coupling inducing physical dependences. A ventilation duct, for example, might provide an environmental coupling among devices located in seemingly decoupled locations. In addition, radiation or electromagnetic couplings are two other forms of coupling not directly associated with a common spatial domain. Examples of "physical" dependences resulting in adverse system interactions are the Browns Ferry-1 fire and the postulated Hosgri earthquake at Diablo Canyon. More specifically, at Diablo Canyon, a charging pump suction line could be "spatially coupled" with a crane monorail during a seismic event resulting in a loss of the charging pump suction.

Type 3 Human-interaction Dependences: Dependences introduced by human actions. We can distinguish between two types: those based on cognitive behavioral processes and those based on procedural behavioral processes (see also Section 4.3.1). Cognitive human errors can result in multiple faults once an event has been initiated. An illustration of cognitive error is the turning off of the HPIS by an operator after failure to correctly diagnose the state of the plant (as occurred during the TMI-2 accident). Dependences due to procedural human errors include multiple maintenance errors which result in dependent faults with effects that may not be immediately apparent. An illustration of multiple faults due to a procedural human error is the failure to reopen the discharge valves in all redundant trains of an auxiliary feedwater system after a test or maintenance act (as also happened in the TMI-2 accident).

It should be emphasized that the above three types of dependences are not mutually exclusive. Thus, a dependence that exists between one device that provides a cooling function and devices that operate within the domain cooled by the first could be characterized either as a functional dependence (i.e., indirect process coupling since the failure probability of the latter devices depends on whether they operate in a coolable environment and hence on the state of the former device) or as a physical dependence, since they are associated with a common spatial domain.

Further classification of the dependences can be based on the complexity of the devices involved, e.g., system, train, subsystem, component. Here, a component is defined as a device that does not need to be further resolved into finer constituents (for the purpose of the PSA) and where subsystems, trains, and systems are collections of components of varying degrees of complexity. (See also Section 4.2 on the limit of resolution of fault trees.) The exact definition of subsystems, trains, and systems is usually plant specific; for the purposes of this section, we will refer to anything that consists of more than two components as a system. We can therefore distinguish between dependences among systems and among components. Combining the classification of dependences based on the nature of the causative factor with the classification based on the complexity of the devices, we finally distinguish six types of dependences.

1.1 System Functional Dependences

1.2 System Physical Dependences

1.3 System Human-Interaction Dependences

2.1 Component Functional Dependences

2.2 Component Physical Dependences

2.3 Component Human-Interaction Dependences

The following two subsections describe methods for identifying and modeling of the above-mentioned types of dependences.

4.4.2.3 Assumptions, Methods, and Procedural Steps

4.4.2.3.1 Identification of Dependences

Qualitative dependence analysis is called out separately in this guide in order to give the subject special emphasis, not because it is to be performed separately from fault tree analysis. Indeed, identification of dependences is the essence of the fault tree development subtask.

The identification of dependences should be based on a complete and thorough understanding of the plant, and should draw heavily from the existing operating experience of the particular plant as well as other plants. There is no well-defined technique for the identification of dependences. However, the Office of Nuclear Reactor Regulation is about to define and subsequently implement systems interaction regulatory requirements and guidance for light water reactors. The techniques and procedures developed under this program should eventually be integrated with PSA procedures in the area of dependence identification. At present, there are three somewhat different approaches under consideration by the Systems Interaction Program:

1. The method outlined in the remainder of this section, consisting of a combination of Event tree, Fault tree, and Failure Modes and Effects Analysis techniques¹ (hereafter FT/FMEA).
2. The "digraph-matrix analysis" which is currently being developed and documented.²
3. The methodology used by PASNY in its study of Indian Point Unit 3.³

These differ in their choice of analytical tools, and in their respective emphases on different elements of the process, but all are aimed at encouraging a systematic approach which will foster reliable coverage of the proper ground, and will encourage consideration of the right questions as the analysts go about their work. By now, it is clear that digraph-matrix analysis produces cutsets, just as fault tree analysis does; beyond details of code versatility and/or efficiency, there is no fundamental reason to expect important differences between a digraph analysis and a fault tree analysis. If the bulk of the PSA is being carried out with fault tree methods, there is little incentive to consider recasting the problem in digraph form, particularly since the fault tree approach has proven its effectiveness. The remainder of this subsection discusses identification of dependences according to the FT/FMEA approach. As noted above, certain essential features will be seen to transcend the particular choice of logic model.

The essential features of the approach are:

1. initially, to define a fairly coarse level of resolution (corresponding to the segment level), but
2. to model all dependences of frontline systems on support systems at this resolution.

For each segment, one performs an FMEA.

The purpose of this analysis is to determine the different failure modes of the various systems (components) and the potential effects of these failures on other systems. For each system (component), a Failure Modes and Effects list like the one shown in Figure 4.1 should be generated. Every failure mode identified should be included along with the causative factor(s), the effects of the failure on other systems, and the indication available to the operator for the existence of the failure. The failure modes of the system should include, in addition to total failures, partial failures corresponding to degraded operation or failure modes which correspond to the delivery of an excess of the service provided or controlled by the system. To determine the effect on other systems, the Dependence Tables (see Section 3) should be used. It should be emphasized, however, that the search for possible effects of a certain system failure should not be limited to the systems with which the former is associated through the dependence tables. In assessing the indication available to the operator for a systems failure, special care should be given to whether the provided indication is sufficient to unambiguously specify the particular failure mode of the system. A special note should be made if one type of indication covers several failure modes.

The list of failure modes is next rearranged in such a way that the functional failure modes appear first, then the physical, and finally the human errors. Any failure modes having the same causative factor, the same effect on all other systems, and the same indication to the operator should be grouped into one failure mode.

The column of operator's indications should be searched to identify identical or similar indications that correspond to different failure modes of the system. A special note should be made if such cases are actually identified.

The development of the Failure Modes and Effects lists should draw heavily from the existing operating experience of the particular plant, as well as other plants.

After completing the FMEA for each system, all the causative factors are combined to form a single list of generic causative factors (such a list for "physical" failure modes is given in Table 4.1). This list includes next to each generic cause, the systems subject to the corresponding failure mode (see Figure 4.2).

The completed lists of failure modes are also searched for identifying operator's indications that could be generated by faults in different systems.

SYSTEM: ...				
	FAILURE MODE	CAUSATIVE FACTOR	FAILURE EFFECTS	OPERATOR'S INDICATION FOR FAILURE
1				
2				
•				
•				
•				

Figure 4.1 List of failure modes for a given system (train, subsystem, component).

	GENERIC CAUSATIVE FACTORS	SYSTEM THAT CAN BE AFFECTED
1		FLS ₁ , SS ₂ , SS ₃ . . .
2		
•		
•		
•		

Figure 4.2 List of generic causative factors and corresponding systems (trains, subsystems, components).

Table 4.1b Extreme "Environmental Conditions"

(Generic Causes of Dependent Failures)

Excerpted from the ANS/IEEE PRA Procedures Guide (NUREG-2300)

Extreme Condition (Generic Cause)	Example of Source	Environmental Channel
1. Impact	Pipe whip, water hammer, missiles, structural failure, earthquakes	Common location, hydraulic coupling, common structural base
2. Vibration	Machinery in motion, earthquake	Common structural base
3. Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuits	Common location, ventilation ducts
4. Moisture	Condensation, pipe rupture, rainwater, floods	Common location, ventilation ducts, hydraulic coupling
5. Pressure	Explosion, out-of-tolerance system changes (pump overspeed), flow blockage	Common location, ventilation ducts, hydraulic coupling
6. Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from control system	Common location, ventilation ducts
7. Electro-magnetic interference	Welding equipment, rotating electric machinery, lightning, power supplies, transmission lines	Spatial proximity to source
8. Radiation	Neutron sources and charged-particle radiation	Spatial proximity to source
9. Corrosion or other chemical reaction	Acid, water, or chemical attack	Common location, ventilation ducts, hydraulic coupling
10. Conductive Medium	Conductive gases	Common location, ventilation ducts

Next, fault trees are constructed. The resulting model is not detailed, but in principle, it correctly reflects the functional dependences. It is now feasible to obtain leading order cutsets for the fully-linked problem, i.e., one and two element cutsets for systems or for accident sequences, in terms of supercomponent (segment-level) fault trees.

It is essential that analysis of mitigating systems' failure be properly conditioned on the character of the initiating event. A number of things can be done to accomplish this:

1. A fault tree for transient initiators is recommended. This will include a number of events corresponding to failure of certain normally operating support systems, which serve both normal plant operation and accident mitigation.
2. It is useful to explicitly display certain conditions on the fault trees, such as presence of an SI signal, availability of offsite power, etc.
3. Failure modes appropriate to different conditions must be distinguished. Following some initiators, service water pumps may trip and be required to restart; following others, they may not trip in the first place.

The initial search for functional dependences is complete when the segment-level plant model has been debugged and the results have been surveyed. It is noted that significant qualitative results are expected at this stage, long before detailed modeling is complete.

With the functional model now in hand, guidance can be provided to the searches for physical dependences, including spatially-coupled interactions, and humanly coupled interactions. In particular, it is noted that a complete set of results from a purely functional model tells the analyst which groups of multiple events should be searched for physical or human coupling. These searches are discussed below.

4.4.2.3.2 Further Search for Dependences

All the dependences identified during the various phases of the FMEA should be listed separately and reported according to the reporting requirements of Section 7. These dependences should also be properly included in the logic models (see Section 4.2 and Section 6) in order to correctly evaluate their impact on the level of risk. Further search for dependences should be performed for each type of dependence as follows:

Functional Dependences

All functional dependences should in principle be identified at the FMEA phase and/or included in a correctly drawn fault tree. A fault tree should contain, in particular, all the shared-hardware and direct-process-coupling types of dependences. Additional functional dependences could be identified if the basic events in the fault trees are further decomposed to simpler events. The level of resolution in a fault tree depends on whether the

analyst believes that a dependence could possibly exist at lower levels and on the relevant significance of such dependences.

Physical Dependences

A search of physical dependences generally consists of generating minimal cutsets and examining whether the elements of these sets are susceptible to the same generic causative factor and in addition are connected by an "environmental" conductor that will allow such a dependence to be created by a single source. Computer-aided search procedures have been developed for this purpose and are described in Section 3.7.3.9 of the ANS/IEEE PRA Procedures Guide. In applying these techniques, the information generated during the FMEA and put in the form of generic causative factors list (Figure 4.2) is extremely useful. Special caution should be exercised if codes that generate minimal cutsets using cutoff probabilities are employed, in order to avoid missing important dependences contained in the rejected cutsets.

For certain physical dependences the search within minimal cutsets can be combined with the PASNY approach of identifying "targets" and "sources" for these interactions. If critical combinations of "targets" to be examined during "walk throughs" are defined on the basis of the min cutsets, then the efficiency of the "walk through" procedure will improve substantially.

Human-Interaction Dependences

The state-of-the-art for identifying problem-solving and/or procedural based human dependences is still under development (see also Section 4.3.1). Techniques are generally based on task analyses on the information collected from FMEAs and on plant walk throughs. Problem-solving human interactions could be identified by examining the cutset elements and establishing the possibility that one of the failures could induce a human action that will result in one or more failures contained in the same cutset. The failure mode lists developed during an FMEA (Figure 4.2) will be helpful at this point. A search is made in the list of generic causative factors (see Figure 4.2) to determine whether human errors constitute a generic causative factor for more than one fault in the cutset. If this is the case, an analysis is made to assess whether the same human error (or a string of consecutive human errors) can cause the occurrence of these faults. The "operator's indication" column of the failure mode lists (see Figure 4.2) should be useful at this point. The information contained in these columns helps in assessing the possibility that the operator could misinterpret the available indications of a particular failure mode and respond improperly. Procedural human interactions can be identified in a similar way. Again, elements of the same cutset are searched to establish whether one or more events are subject to the same or related procedural actions.

4.4.2.3.3 Incorporation of Dependences Into the Logical Models

In addition to being identified, dependences should also be incorporated correctly into the logic models so that their effect on the level of risk can be appropriately estimated.

In general, dependences can be incorporated at any stage in the analysis, but depending on the particular type of dependence and on the specific method

applied (e.g., large event trees/small fault trees versus small event trees/large fault trees) some methods of incorporation are more efficient than others. Below, we examine each of the six types of dependences and comment on the methodologies of incorporating them into the logic models.

1. System Functional Dependences: These dependences may be included in the event trees.

Depending on the size of the event tree (i.e., whether it includes more than the frontline systems--see Section 4.1), an increasing number of functional dependences can be included and in the limit all the identified system dependences can be included in the event tree. In that case, the fault trees corresponding to the headings of the event trees are completely independent (from functional dependences). An alternative method is that of fault tree linking (see Section 4.2, and Section 6) where the events of an accident sequence of the systemic event tree are linked together under an "AND" gate and a large fault tree is developed.

2. System Physical Dependences: Dependences that result from a common generic factor that constitutes an initiating event can, in certain cases, be incorporated into the event trees. Other types of physical dependences can be incorporated in the fault trees.
3. System Human Interactions: These dependences are usually of the cognitive type and are best modeled in the event trees or at the top level of the system fault trees (see Section 4.3.1).
4. Component Functional Dependences: Some component functional dependences are inherently included in the fault trees. The effect of other component dependences (such as indirect process coupling) on the top event probability can be treated parametrically. Section 6.5.4 of this guide addresses the issue of the quantitative treatment of dependences.
5. Component Physical Dependences: Such dependences are best incorporated in the fault trees. The computer-aided methods described in Subsection 3.7.3.9 of the ANS/IEEE PRA Procedures Guide can be used to identify possible dependences.
6. Component Human Interaction Dependences: Such dependences are usually procedural in nature and are best incorporated in the fault trees (see Section 4.3.1).

4.4.2.3.4 Incorporation of Dependences in the Event Trees

The inclusion and treatment of dependences in the event trees have been discussed in Section 4.1. An extended discussion of the treatment of dependences in large event trees is presented in the ANS/IEEE PRA Procedures Guide (Section 3.7.3.3).

4.4.2.3.5 Incorporation of Dependences in the Fault Trees

The inclusion of functional dependences in the fault trees has been discussed in Section 4.2.

4.4.2.4 Regulatory Issues Related to the Qualitative Dependence Analysis Task

The qualitative dependence analysis task addresses most of the concerns of Unresolved Safety Issue A-17 "System Interactions." A number of additional regulatory issues are related to this task and are discussed in Appendix A (Table A.3). The procedural steps for the identification of dependences described in this section can also be used in addressing the relevant regulatory issues. Table 4.2 presents these regulatory issues along with the corresponding type of dependences. In addition, Table 4.3 identifies inputs and outputs that would be required if the issues were addressed in the PSA study.

Table 4.2 Regulatory Issues Related to Qualitative Dependence Analysis

Regulatory Issue Title	NRC Program	Type of Dependence To Be Considered
1. Shared Systems	SEP-II, 4.9	a) System functional dependences b) Physical dependences c) Human-interaction dependences
2. Support Systems:		a) System functional dependences b) Human-Interaction dependences
a) Emergency AC power	SEP-III, 4.8.1	
b) Emergency DC power	SEP-III, 4.8.2	
c) Control and actuation systems	SEP-III, 5.1 and	
d) Decay heat removal	GI-A-47	
e) Service and cooling systems	SEP-III, 4.2.1, 4.2.2 and GI-A-45	
f) Ventilation systems	SEP-III, 4.3 SEP-III, 4.4	
3. a) Isolation of high and low pressure systems AND b) Passive mechanical failures	SEP-III, 4.6 GI, B-58	Component functional dependences
4. Pipe break effects	SEP-III, 7.1.2	a) System physical dependences b) Component physical dependences
5. Risk Assessment - System Interaction	TMI-II.C.3 or GI, A-17	

Table 4.3 Input and Output of Dependence Analysis Task for Regulatory Issues

Regulatory Issue Title	Input	Output
1. Shared Systems	<ul style="list-style-type: none"> - Identify all shared systems in multiple units station. - Identify common locations or other environmental links of systems used in different units. - Identify test and maintenance procedures which affect system serving different units. Look for non-staggered operations - Include dependences on relevant FT, ET. 	<ul style="list-style-type: none"> - Documentation of all discovered dependences. - Documentation of impact of shared systems on core damage probability and weak points, if any.
2. Support Systems: ac, dc, DHRS Control, Actuation, SW, Ventilation	<ul style="list-style-type: none"> - In the process of FT, ET development task, review any added system or equipment to identify the dependences on these support systems in particular. 	<ul style="list-style-type: none"> - System and components appearing on FT and ET will all have an indication of which support system they depend on, if any. - Document components discovered and their significance.
3. Isolation of High and Low Pressure Systems	<ul style="list-style-type: none"> - Identify those components that have a potential to lead to the following, if failed: (1) LOCA outside containment, (2) initiate an event with loss of mitigating systems, (3) change system success definition as a result of flow diversion. 	<ul style="list-style-type: none"> - Document components discovered and their effect on core damage probability.

Table 4.3 (Continued)

Regulatory Issue Title	Input	Output
4. Pipe Break Effects	<ul style="list-style-type: none"> - Identify important cutsets leading to core damage. - Identify locations of systems and components dominating these cutsets. - Review these locations for possible pipe break impacts. 	<ul style="list-style-type: none"> - Documentation results and their risk significance.
5. Risk Assessment System Interaction	<ul style="list-style-type: none"> - Documentations of all the above four sub-tasks. 	<ul style="list-style-type: none"> - Document impact of Dependence Analysis on risk. - Comments on adequacy of Dependent Analysis methodologies used.

References

1. R. Youngblood et al., "Fault Tree Application to the Study of Systems Interactions at Indian Point 3," NUREG/CR (Draft) (1984).
2. H. P. Alesso, I. Sacks, and C. F. Smith, "Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies at Selected LWR's," Lawrence Livermore National Laboratory, NUREG/CR-2915 (1983).
3. "Power Authority of the State of New York--Indian Point 3 Nuclear Power Plant Systems Interaction Study," Ebasco Services, Inc., 1981.
4. "Interim Reliability Evaluation Program: Phase II Procedure and Schedule Guide: Draft-Revision-2," USNRC, Sept. 1981.
5. A. J. Buslik, I. A. Papazoglou, and R. A. Bari, "Review of Systems Interaction Methodologies," USNRC Report NUREG/CR-1896, Jan. 1981.
6. J. J. Lim et al., "Systems Interactions: State-of-the-Art Review and Methods Evaluation," NUREG/CR-1859 (Jan. 1981).
7. K. N. Fleming et al., "Application of PRA Methods to the Systems Interaction Issue," PLG-0284 (April 1984).
8. D. D. Carlson et al., "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728 (July 1982).
9. "PRA Procedures Guide," American Nuclear Society and Institute of Electrical and Electronics Engineers, NUREG/CR-2300 (1983).
10. K. N. Fleming and A. Mosleh, "Common Cause Data Analysis and Implications in System Modelling," Paper 3, "Proceedings of the ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications," February 24 - March 1, 1985, San Francisco, Calif. (EPRI).
11. K. J. Voska and J. N. O'Brien, "Human Error Probability Estimation Using Licensee Event Reports," NUREG/CR-3519 (July 1984).
12. A. I. Siegel et al., "Maintenance Personnel Performance Stimulation (MAPPS) Model: Summary Description (Vol. 1)," NUREG/CR-3626.
13. P. K. Samanta et al., "Multiple Sequential Failure Model: Evaluation of and Procedure for Human Error Dependency," NUREG/CR-3837 (Draft) (March 1985).
14. P. K. Samanta and S. P. Mitra, "Modeling of Multiple Sequential Failures During Testing, Maintenance, and Calibration," NUREG/CR-2211 (Dec. 1981).
15. R. E. Hall et al., "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," NUREG/CR-3010 (Nov. 1982).
16. M. K. Comer et al., "Generating Human Reliability Estimates Using Expert Judgment (Vol. 1)," NUREG/CR-3688 (Nov. 1984).

17. D. E. Embrey et al., "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment (Vol. 1)," NUREG/CR-3518.
18. E. Rosa et al., "Application of SLIM-MAUD: A Test of an Interactive Computer-Based Method for Organizing Expert Assessment of Human Performance and Reliability," NUREG/CR-4016 (Draft) (March 1985).
19. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278 (Aug. 1983).
20. B. J. Bell and A. D. Swain, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants," NUREG/CR-2254 (Nov. 1981).
21. "Oconee PRA," Vol. 4, Appendix C, NSAC/60 (June 1984).
22. L. D. Phillips, P. Humphrey, and D. E. Embrey, "Appendix D: A Socio-Technical Approach to Assessing Human Reliability (STAHR)." In D. Selby, Pressurized Thermal Shock Evaluation of the Calvert Cliffs Unit 1 Nuclear Power Plant. Research Report on DOE Contract 105840R21400, Oak Ridge National Laboratory, Oak Ridge, TN (1985)
23. L. D. Phillips and D. E. Phillips, "Appendix E: Quantification of Human Actions by STAHR." In D. Selby, ibid.

5. RELIABILITY DATA ASSESSMENT AND PARAMETER ESTIMATION

5.1 Purpose

The purpose of the task is to assess point values and corresponding uncertainties for the parameters necessary for the quantification of accident sequences. These parameters characterize the probabilities of the constituent events of the accident sequences and are estimated from experiential (historical) data utilizing statistical techniques. Thus, this task identifies existing relevant historical information and defines methods to transform it into probability statements about the events of interest.

The objective of the parameter estimation task can be divided into the following:

1. identifying pertinent sources of experiential data;
2. extracting relevant data from these sources;
3. selecting appropriate models that provide the probabilities of the events of interest;
4. obtaining estimates of the parameters in the probability models.

5.2 Scope

The data base developed must support all the quantification requirements of the models chosen to represent each of the events in each accident sequence. The data base must therefore provide point estimates and appropriate uncertainty measures for each of the parameters of the models proposed. The constituent events of each accident sequence can be divided into three categories:

1. Those relating to the initiation of the accident sequence, i.e., initiating events.
2. Those relating to the way individual system elements respond to an initiating event, i.e., component basic events.
3. Those relating to the way individual systems or system elements are affected by human errors, i.e., human error basic events.

5.3 Inputs and Outputs

The inputs (from other tasks) and the outputs from (to other tasks) the Data Assessment task are given in Tables 5.1 and 5.2, respectively. The tasks which provide inputs are

- 3.0 plant familiarization,
- 4.0 accident sequence definition,
- 6.0 accident sequence quantification.

Table 5.1 Reliability Data Assessment Task Relationships: Inputs

Inputs From Other Tasks	Uses in This Task
1. Frontline systems and support systems identification and physical/operational boundary definition (plant familiarization task).	Identifies systems and components and their operational requirements so that test, maintenance, demand and exposure calculations can be made.
2. List of initiating events grouped according to common mitigating requirements (plant familiarization task).	Identifies initiating events in the groups for which frequency evaluations are needed.
3. Basic event identification (accident sequence definition task).	Identifies component failure basic events and test and maintenance basic events requiring quantification.
4. Human error event identification (accident sequence definition task).	Identifies human error events which need further analysis to establish their probabilities.
5. List of events for which plant-specific quantification is required (baseline evaluation).	Identifies initiating events, components, and human errors for which plant-specific data analysis is required.

The inputs provided are

1. systems identification,
2. initiating event groupings and their constituents,
3. component basic event identification,
4. human error event identification,
5. list of events for which plant-specific quantification is required.

The use to which each of these inputs is put in the task is given in Table 5.1.

The outputs of the task are

1. a list of grouped initiating events and their plant-specific frequencies, and, if appropriate, recovery times and associated probabilities;

2. a table of generic and plant-specific component failure rates, test and maintenance frequencies, and associated unavailabilities;
3. a table of generic and plant-specific human error rates;
4. detailed human error analysis for selected events.

The uses to which each of these outputs is put in other tasks are given in Table 5.2.

The required output data elements and the suggested presentation format for these outputs are given in Section 5.8. In addition to the inputs shown, other information is required to allow for the data assessment. Since this external information is not generated by other tasks, it is discussed here. These informational needs are discussed in Sections 5.5. to 5.7. Intermediate outputs, generated exclusively for use within this task, are also discussed in Section 5.4.

5.4 Assumptions, Methods, and Procedural Steps

The reliability data assessment and parameter estimation task is concerned with the analysis of three major categories of data:

1. Initiating event data.
2. Component failure and repair data.
3. Human error data.

For each of the major categories the following subtasks are distinguished.

1. Event definition and interface with other tasks.
2. Data sources and data gathering.
3. Model and parameter selection.
4. Estimation technique application.

In the first subtask, the analyst familiarizes himself with the particular event of interest and establishes appropriate lines of communication and interfaces with the analysts of the relevant subtasks both in the accident sequence definition task (Sections 3 and 4) and in the quantification task (Section 6).

In the second subtask the sources of appropriate failure data are established and the gathering of the data is performed.

In the third subtask, the models that describe the stochastic behavior of events of interest are selected by reviewing the models employed in the accident delineation task (Sections 3 and 4) and the quantification task (Section 6) and by making appropriate assumptions consonant with available data.

Table 5.2 Reliability Data Assessment Task Relationships: Outputs

Products	Other Tasks Using Products
1. Initiating event frequencies and appropriate recovery times for each initiating event group.	Accident sequence quantification; used to quantify accident sequence frequencies.
2. Generic component failure and repair probabilities	Accident sequence definition; provides guidance as to the level of resolution that is supported by the data.
2.1 Component failure rates and corresponding hardware unavailabilities.	
2.2 Component test, repair, and maintenance frequencies and corresponding unavailabilities.	
3. Plant-specific component failure and repair probabilities.	Accident sequence quantification; used in quantification of fault trees.
3.1 Component failure rates and corresponding hardware unavailabilities.	
3.2 Component test, repair, and maintenance frequencies and corresponding unavailabilities	
4. Event-related human error rates.	Accident sequence definition; used at the systemic event tree construction or at the fault trees at a top-event level.
5. Detailed failure/human error rates for selected events.	Accident sequence quantification; used in quantifications of dominant sequences.

In the fourth subtask, the estimation technique (for the parameters defined in the third subtask) is applied, and the parameters that must be inferred from experiential data are estimated along with associated measures of uncertainty. The estimation techniques selected for use are Bayesian techniques with flat "noninformative" priors which generally give numerical results similar to classical statistical techniques.

5.5 Initiating Events

The data sources and the technique for assessing the plant-specific frequencies are described in Appendix H. The data used in this assessment should, however, be verified, supplemented, and updated by searches and analyses of the plantspecific events reported in the NRC Grey Books, Operating Experience Summaries, and the Licensee Event Reports. The procedural steps for the quantification of the initiating events are described in the following subsections.

5.5.1. Initiating Event Definition

The task of initiating event quantification starts with the output of the Determination of Initiating Event Groups subtask of the Plant Familiarization Task discussed in Section 3. Typically, grouping of the individual transients selected is based on the expected plant response. Each group includes a number of transients with identical event tree sequence responses. To complete this step successfully, it is very important that the rationale for a particular grouping of transients be well understood, because such an understanding (which implies review of the plant design and strong interface with the team that developed the initiating event grouping) will facilitate the identification of the various ways each initiating event group could be caused for the plant being analyzed. For example, in a plant that has instrumentation which trips the main feedwater pumps upon high water level in any steam generator, such events will be listed as trips due to high steam generator level. These trips are important for the quantification of the Loss-of-Feedwater transient, however, since they result in such a condition. This understanding is especially important for the correct classification of transients that are found in plant records with a description not listed specifically in the original listing of initiating events.

5.5.2 Data Sources, Parameter Selection, and Parameter Estimation

For the initiating event frequencies, the subtasks of data gathering, parameter selection, and parameter estimation have been performed for the user. The generic initiating event frequencies are given in Appendix G. The plant specific initiating event mean frequencies to be used along with associated uncertainty information are given in Appendix H; the plants are grouped into categories according to initiating event frequency behavior. When propagating uncertainties, the initiating frequency distribution is assumed to be a gamma distribution. The gamma shape and scale parameters are also given in the table.

Appendix H describes the data sources, parameters, and parameter estimation techniques used to generate the values in Table H.1. The initiating event frequency is assumed to be constant with time and, to account for plant-to-plant variations, it is modeled as being a random variable with an assumed

probability distribution whose parameters are estimated from the initiating event frequency data.

5.6 Component Data

The procedural steps for the analysis of plant-specific component failure data are described in the following subsections.

5.6.1 Component Basic Event Definition

Component data analysis has as its objective the modeling of component failure, component repair, and component test and maintenance. The definition of what constitutes a component failure requires the specification of the failed component (the component boundary) and the specification of the mode of failure of the component. This specification delineates the component boundary assumed (e.g., command faults not included), and establishes a unique component number for identification. The mode of failure is given as an undesirable state of component performance (e.g., unavailable on demand). This combined information defines the component failure event (e.g., Pump SIAPCS 01-Unavailable on Demand).

Component repair and component test and maintenance are analyzed with respect to how often and how long they render a component inoperable, which component or components are impacted, and whether the action occurs during online operation or during shutdown. Only online repair and test and maintenance are of concern in calculating probabilities of accidents which can occur during full power plant operation. However, the offline activities can be important if accident probabilities are to be estimated for other modes of operation. Under the present scope, only full power operation will be analyzed (see Section 1.2).

5.6.2 Plant-Specific Data Sources and Data Gathering

Although many nuclear power generating stations have established rather extensive operating and maintenance data collection systems, and although some of these systems have been computerized since the time the plants began operating, very few stations have data systems designed specifically for providing data for use in a risk assessment. The PRAs previously performed have had to depend on a combination of sources of plant-specific information to provide the raw material for the construction of a plant-specific data base to support a PRA. These sources include plant design, operating, and maintenance records and procedures which should be made available to the PRA data analysts. The names utilized to refer to these records differ from plant to plant, but a representative listing of record types and their content is given in Table 5.3.

The basic data to be collected from these records are summarized in Table 5.4. Further descriptions of data collection activities and the data which can be extracted from plant records are given in Chapter 5 of the IEEE/ANS PRA Procedures Guide (NUREG-2300).

The availability, accessibility and effective usability of plant failure information of all kinds is greatly facilitated by reliance on, and conformity

Table 5.3 Plant-Specific Data Sources

General Record Type	Specific Names	Content
1. Design Drawings	P&IDs, Process Drawings, Electrical Drawings, Fire Zone Drawings	Type, population, identification, location, and functional as well as physical interface of equipment in the plant.
2. Operating Records	Operator (Control Room) Logs, Monthly Status Reports, Licensee Event Reports	Chronological reporting of events occurring during operation in various levels of detail, and various reporting scopes.
3. Plant Systems Specification	System Identification list, System Operability Matrix	Identification of system names, functions, and boundaries, and identification of which systems are operable during which plant modes.
4. Equipment Records	Equipment Lists, Parts Lists	Type, population, functional name, and system assignment of each component.
5. Maintenance Records	Maintenance Logs, Maintenance Work Requests, Maintenance Requests, Job Orders	Date, Name, Type, and Identification of component and system requiring maintenance action, Problem Observed, & Action Taken.
6. Test Records	Periodic Test Reports, Plant Test Procedures, Plant Test Schedule, (Master Surveillance Schedule)	Procedures, Schedule, Reporting of tests, and Identification of Components requiring test.
7. Calibration Records	Calibration Reports, Calibration Cards, Calibration Procedures	Same as above.

Table 5.4 Basic Data to be Extracted from Plant Records

Component failure data	Time to component failure and Failure Mode.
Component repair data	Durations of component repair including detection time and any waiting time.
Component test data	Times of test and test duration times.
Component maintenance data	Times of maintenance and maintenance duration times.

with, the LER Sequence Coding and Search Procedure (SCSP). This has recently been introduced by NRC/AEOD and ORNL/NSIC (see NUREG/CR-1928, February 1981), and describes in computer-readable and computer-searchable format the sequence of events described in the LER. It embodies a consistent, comprehensive, and industry-wide categorization of the components and systems involved, which is also to be used by the individual utilities, INPO, and equipment manufacturers as part of the NPPD System.

This type of systematic codification is of clear significance and utility in the execution and analysis of a PSA. In particular it provides (i) historical component and systems data in an unequivocal way; and (ii) clearly defined accident (sub)sequences and potential initiators based on actual plant behavior.

In the long term, too, this type of material will be available and readily usable (i.e., consistent and intercomparable) on a generic and industry-wide basis.

5.6.3 Model and Parameter Selection

The models of interest in this subtask are those describing the stochastic failure behavior of the components of the various systems. In general, these models estimate the probability that a component will not perform its intended function and they depend on the mode of operation of the system to which the components belong. To assure uniformity in the present studies, the models to be used are briefly described in the following paragraphs.

(i) Standby Systems - The reliability measure of interest for standby systems is their unavailability on demand. In the current state of the art it is assumed that the unavailability of a standby system can be reasonably approximated by the use of fault trees (or other logic model) where the component time-averaged unavailabilities are used as the probabilities of the basic events. We can distinguish three types of components of standby systems:

a) Periodically Tested Standby Components - These components are usually in a standby mode and they are tested periodically. If during a test they are found failed, they are repaired. In addition, the components may be subject to periodic scheduled maintenance. For these components there are five kinds of contributions to the component unavailability: hardware failure; unavailability due to test; unavailability due to unscheduled repair; unavailability due to scheduled maintenance; and unavailability due to interfacing maintenance. Formulas for these unavailabilities are given in Table 5.5. Their derivations can be found in various reliability references. The basic assumption here is that component failure times have an exponential distribution. The parameters that must be estimated from experiential data are the standby failure rate, the mean time to repair (unscheduled repairs), and the mean time of online maintenance actions. The estimation techniques are described in the subsequent section.

b) Untested Standby Components - If a standby component is not tested, then the average availability is given by the formula presented in Table 5.5. In this formula, T_p is the fault exposure time, i.e., the time during which a failure can occur and the state of the component is unknown. If the component is really never tested, T_p is set equal to the life of the plant (40 years). However, it often happens that the component is indirectly tested or renewed. For example, if the system to which the component belongs is called upon to operate, the state of the untested component might be detectable (operating or failed) when the system is demanded. In that case the mean fault exposure time for the untested component is the mean time to challenge the system to which it belongs. In other cases the component may be replaced every time some other tested component is replaced. In this case the mean fault exposure time is approximately equal to the mean time to failure of the tested component (see also Section 5.6.3 of the ANS/IEEE PRA Procedure Guide, NUREG-2300).

c) Continuously Monitored Components - Some components, although they belong to standby systems, are continuously monitored. This is equivalent to assuming that a failure is detectable as soon as it occurs and repair starts immediately. The formula for the average unavailability for such components is given in Table 5.5.

(ii) Online Systems - For online systems, the reliability characteristic of interest is generally the probability that the system will fail to operate successfully for a given period of time T_M (mission time). In the current state of the art it is assumed that the failure probabilities and unavailabilities of an online system can be approximated by the use of fault trees (or other logic models) where the component unavailabilities at time T_M are used as the probabilities of the basic events. The failures of operating components are assumed again to follow an exponential distribution with an operating failure rate λ_0 instead of a standby rate. For systems which change phases from standby to operating, both standby and operating failure contributions must be treated. The treatment of these multiphase systems is given in various references. Online systems contain two general types of components, nonrepairable components and repairable components.

a) Nonrepairable Components - These are components that can not be repaired once failed. The failure probability for such components is given in

Table 5.5 Component Unavailability Expressions for Standby Systems

Component Type/ Unavailability Mode	Time-Averaged Unavailability Expression	Parameter Definition	Data Requirements for Parameter Estimation
1. Tested Standby Components			λ_S
1.1 Hardware Failure	$1 - \frac{1 - e^{-\lambda_S T}}{\lambda_S T}$	λ_S : Standby failure rate T : Component Test Period	• Number of observed Failures
1.2 Test Outage	$\frac{\tau}{T} q_0$	τ : Average test duration q_0 : Override unavailability (if applicable) obtained from system analysis	• Total component standby time _____ • _____ τ • Observed test durations _____ • _____
1.3 Repair Outage	$\lambda_S T_R$	T_R : Mean time to repair	
1.4 Scheduled Maintenance	$f_m T_m$	f_m : Scheduled maintenance frequency (includes interface maintenance) T_m : Mean time of scheduled maintenance action	T_R, T_m • Observed individual times for repair and maintenance, respectively, including detection and wait time

Table 5.5 (Continued)

Component Type/ Unavailability Mode	Time-Averaged Unavailability Expression	Parameter Definition	Data Requirements for Parameter Estimation
		λ_s : Standby failure rate	T_p
2. Untested Standby Component	$1 - \frac{1 - e^{-\lambda_s T_p}}{\lambda_s T_p}$	T_p : Fault Exposure Time	Inferred from re- placement times of com- ponent due to other failures or if not replaced, then assume $T_p = 40$ years
3. Monitored Standby Component	$\frac{\lambda_s T_R}{1 + \lambda_s T_R}$	T_R : Mean time to repair	

Table 5.6. The parameter λ_0 (operating failure rate) is estimated in a completely analogous way to the other failure rates mentioned above.

b) Repairable Components - These are components that can be repaired once failed. The modeled unavailability for such components is given in Table 5.6.

5.6.4 Estimation of Component Failure, Repair, Test, and Maintenance Parameters

The following subsections describe the approaches which are to be used to estimate component failure rates, mean times to repair, test frequencies, average test times, maintenance frequencies, and average maintenance times. Techniques are also given for estimating the parameters of a repair distribution for those applications where the probability of failure to complete repair in a given time period is required.

(i) Component Failure Rate Estimation

The parameter to be estimated is either the standby failure rate λ_s or the operating failure rate λ_0 of the exponential distribution. The level of component specificity (i.e., components assumed to have the same failure rates) and the component failure modes which are to be used in the present studies are those defined for the generic component failure data base given in Appendix C. If a plant-specific data base is lacking, the data in Appendix C should be used. Otherwise, the steps for estimating the plant-specific standby failure rates λ_s are as follows:

1. Identify the component population whose failure history is to be used to estimate the assumed common component failure rate.
2. Identify the time period during which the component failures are to be counted.
3. In the component population, count the total number of failures and the total component standby time T for the time period.
4. Estimate the plant-specific mean failure rate λ_s as

$$\lambda_s = \frac{N}{T} .$$

This is the mean of the posterior distribution when the failure rate is treated as a random variable and when a noninformative prior distribution is used. This estimate is also the usual classical statistics estimate obtained under a Poisson model (maximum likelihood).

5. For an uncertainty description associated with λ_s , use a gamma distribution with the shape and the scale parameters set equal to N and T , respectively. The gamma density function $g(\lambda_s)$ is given as

Table 5.6 Component Unavailability Expressions for Online Systems

Component Type/ Unavailability Mode	Time-Averaged Unavailability Expression	Parameter Definition	Data Requirements for Parameter Estimation
1. Nonrepairable Component	$1 - e^{-\lambda_0 T_M}$	λ_0 : Operating Failure Rate T_M : Mission Time (obtained from success requirement)	$\frac{\lambda_0}{n}$ <ul style="list-style-type: none"> • Number of observed Failures • Total time-to-Failure
2. Online Repairable Component	$\frac{\lambda_0 T_R}{1 + \lambda_s T_R}$	T_R : Mean Time to Repair	T_R <ul style="list-style-type: none"> • Observed individual times for repair

$$g(\lambda_s) = \frac{\lambda_s (\lambda_s T)^{N-1} e^{-\lambda_s T}}{(N-1)!} .$$

This gamma distribution is to be used in propagating failure rate uncertainties as described in Section 6.3.

The same procedure is to be used in estimating operating failure rates λ_0 where operating failure and operating times are used in place of standby failures and standby time.

If there are no recorded failures ($N = 0$), the failure rate distributions in Appendix C are to be used as a prior, and a posterior will be computed utilizing the likelihood ($e^{-\lambda_s T}$) of having zero failures.

(ii) Repair Time Estimation

For a collection of N repair times t_1, \dots, t_N , the average repair time T_R is estimated as

$$T_R = \frac{1}{N} \sum_{i=1}^N t_i .$$

The repair times t_i should include detection plus any wait times. For reliable estimates, N should be larger than 10. If there are less than 10 samples available, the generic values in Appendix D should be used.

If a repair time distribution is required, then as a crude model, an exponential distribution for the time of repair can be used with the mean repair time estimated as T_R . It is important to identify any inaction time t_0 during which repair is unlikely or unable to be performed because of the time required for detection and repair initiation. This inaction time can have large effects and can compensate for the crudeness of the exponential model (as compared to the lognormal, say). The exponential density $f(t)$ for the repair time accounting for an inaction time t_0 is

$$f(t) = \frac{1}{T_R} e^{-\frac{(t-t_0)}{T_R}} .$$

When t_0 is incorporated, then any wait or detection times do not need to be included in the estimation of T_R used in the density $f(t)$.

(iii) Test Frequency Estimation

The estimation of actual test frequency, or, equivalently, the actual average time between surveillance tests, can be made when testing is more frequent than that specified in the tech specs and it is desired that credit be taken for the extra testing. The average time between tests T is estimated as

$$T = \frac{1}{N} \sum_{i=1}^N T_i .$$

Where T_i is times between tests, the sample of T_i should be random and not be biased toward high or low values of T_i s. The number of tests N should be at least 10 and the most recent test history should be used. If fewer than 10 samples are available, then the generic values given in Appendix E should be used.

(iv) Average Test Time Estimation

The average test duration time τ is estimated as

$$\tau = \frac{1}{N} \sum_{i=1}^N \tau_i ,$$

where τ_i is the individual test duration times and N is the total number of tests in the sample. For reliable estimates, N again should be larger than 10; otherwise the generic data in Appendix E should be used.

(v) Maintenance Parameter Estimation

The estimation of maintenance frequency and maintenance duration estimation is similar to that used for test times. If T is the estimate of the average time between maintenance and T_i is the individual times between maintenance, then

$$T = \frac{1}{N} \sum_{i=1}^N T_i .$$

Also

$$f_m = \frac{1}{T}$$

where f_m is the corresponding estimate of the maintenance frequency. If T_m is the estimate of the average maintenance duration time and t_i is the individual maintenance duration times, then

$$T_m = \frac{1}{N} \sum_{i=1}^N t_i ,$$

where N is the total number of maintenance times on the sample. The samples for T_i and t_i should again be random.

5.7 Human Error Data

The tools that may be used in the Human Reliability Analysis (HRA) segment of the PSA process are discussed in Section 4.3 of this report. That section describes ten analytic tools which have been used in PSAs or endorsed for use by NRC. Alternative tools, other than those described, can be used and generic documentation requirements for any HRA tool provided.

5.8 Documentation of the Data Analysis Performed

The plant-specific data analyses which are performed must be clearly documented. The documentation should contain the basic data used in the estimation as well as the final estimates obtained. The sources of the data should also be clearly identified to allow possible reevaluation if desired. With regard to format of presentation, the initiating event frequencies should be grouped together followed by the failure rate evaluations, the repair evaluations, the test evaluations, and finally the maintenance evaluations. In each evaluation, a summary of the final estimates should be given in tabular form, followed by a listing of the raw data. The raw data should be in the same order as the final estimates.

5.8.1. Initiating Events

The results of the initiating event quantification may be reported in tabular form as indicated in Figure 5.1.

The first column indicates the designation selected for the event group in the study and contains a short description of the generic definition of the group in terms of mitigation response similarities.

The second column indicates the individual event types included in the group for the study.

The third column contains the total number of events which have occurred at the plant under study for each event group.

The fourth column indicates the baseline value used in the analysis (from Appendix G).

The fifth column gives the plant-specific mean frequency and the parameters of the gamma distribution that describe the uncertainties.

The sixth column gives the point estimate and distribution characteristics for the recovery time.

The last column is reserved for comments and observations.

If additional occurrences to those included in EPRI-2230 have been identified, a separate table with a detailed description of the events should be supplied.

5.8.2 Component Basic Events

The component failure rate quantification may be reported in a tabular form as indicated in Figure 5.2.

The first two columns contain a description of the component, its boundary, and the failure mode.

The next two columns summarized the plant-specific data used in the estimation.

The following three columns report the characteristics of the plant specific distribution.

The last two columns contain the generic point value and relevant comments, respectively.

Similar tables should be supplied for repair, test, and maintenance duration and frequency.

Separate tables reporting the raw data used in the quantification should also be supplied.

5.8.3 Human Error Events (Procedural Errors)

The results of the human error quantification may be reported in tabular form as indicated in Figure 5.3.

The first two columns indicate the event designation used and a short description of the task and the task context.

The third and fourth columns provide the nominal HEP(s) and ranges which were chosen to best represent the task generically, and the source(s) from which they came.

The fifth and sixth columns provide the HEP point value and range used in the study and the justification for any deviation from the nominal value.

The seventh column provides a place for comments and observations and a place to systematically designate the task type in terms of its essential action content and its situational context (e.g., normal operation/omission error/maintenance/written procedure provided/check off required/ Short list ≤ 10 items).

COMPONENT DESCRIPTION AND FAILURE MODE	PLANT-SPECIFIC					SCALE PARAMETER	SHAPE PARAMETER	GENERIC POINT VALUE	COMMENTS
	COMPONENT BOUNDARY	NUMBER OF FAILURES	TOTAL TIME	MEAN VALUE					
1) <u>System:</u> <u>Safety Injection</u> <u>Component Type:</u> <u>Safety Inj. Pumps</u> <u>Failure Mode:</u> <u>Fail During Oper.</u>	Including Driver w/o Command Faults	0	4.6 (1) hours					2(5)/ hours	N-1205 Alternating System.

Figure 5.2 Example of data table for component hardware failure.

Human Error Events (Procedural)

Event Designation	Event Description	Nominal HEP	Data Source	HEP Assigned to Event	Justification for Deviation	Comments Designation (selection basis for HEP)
X2239H	Failure to restore Manual valve 2239 after test of pump	.001 (.0005 to .005)	NUREG/CR1278 Item 1, Table 20-15 Item 2, Table 20-20	.0005 (.0001 to .0008)	Plant Procedures require full operational test after maintenance before system can be returned to operational status. Valve position clearly indicated by Test.	Failure to restore value given written procedure (Normal Op/Omission/Maint/Written Procedures/Checkoff/Shortlist)
RT45234	Failure to Observe high temp. in primary system analog meter, limit band shown during normal operation	.001	ORNL Simulator Data on Plant XYZ-2	.0005 (.0002 to .001)	Plant operator training stresses the identification of this event	Oak Ridge tests taken on new operators working on simulator which was not identical to their plant. (Normal/ Op/Omission/Operational/Ck.Read/w.limits)

Figure 5.3 Example of data table for procedural human errors.

6. ACCIDENT SEQUENCE QUANTIFICATION

This section addresses the process by which the accident sequences are quantified and ranked by importance. The section is partitioned into five subsections, or tasks, as follows:

- Section 6.1: Accident Sequence Boolean Equations
- Section 6.2: Accident Sequence Binning
- Section 6.3: Sequence Quantification
- Section 6.4: Importance and Sensitivity Analyses

The products resulting from completing these tasks are:

- Dominant accident sequences and the dominant cut sets for these sequences.
- Minimal cut sets for systems involved in these sequences.
- Binning of all accident sequences.
- Point estimates for the dominant accident sequences.
- Estimate of the core damage frequency.
- Plant-specific error bounds on frequencies of dominant accident sequences and on the core-damage frequency.
- Importance measures for accident sequences, systems, cut sets, and components.
- Sensitivity studies showing effects of dependences and human errors.
- Engineering insights into systems, components, and procedures that most affect risk.

These products are all considered to be reportable end products resulting from conducting the PSA; specific subsections describe in greater detail the results which are to be reported and which constitute the above products.

Figure 6.1 pictorially represents the flow of information into the tasks of this section, between tasks, and the resulting task products.

6.1 Accident Sequence Boolean Equations

6.1.1 Purpose

One of the main objectives of PSA studies is to produce system and accident logic models which can be used in later analyses. The purpose of this task is to obtain reduced Boolean equations for each accident sequence as defined in the event trees. The Boolean equation for an accident sequence at a

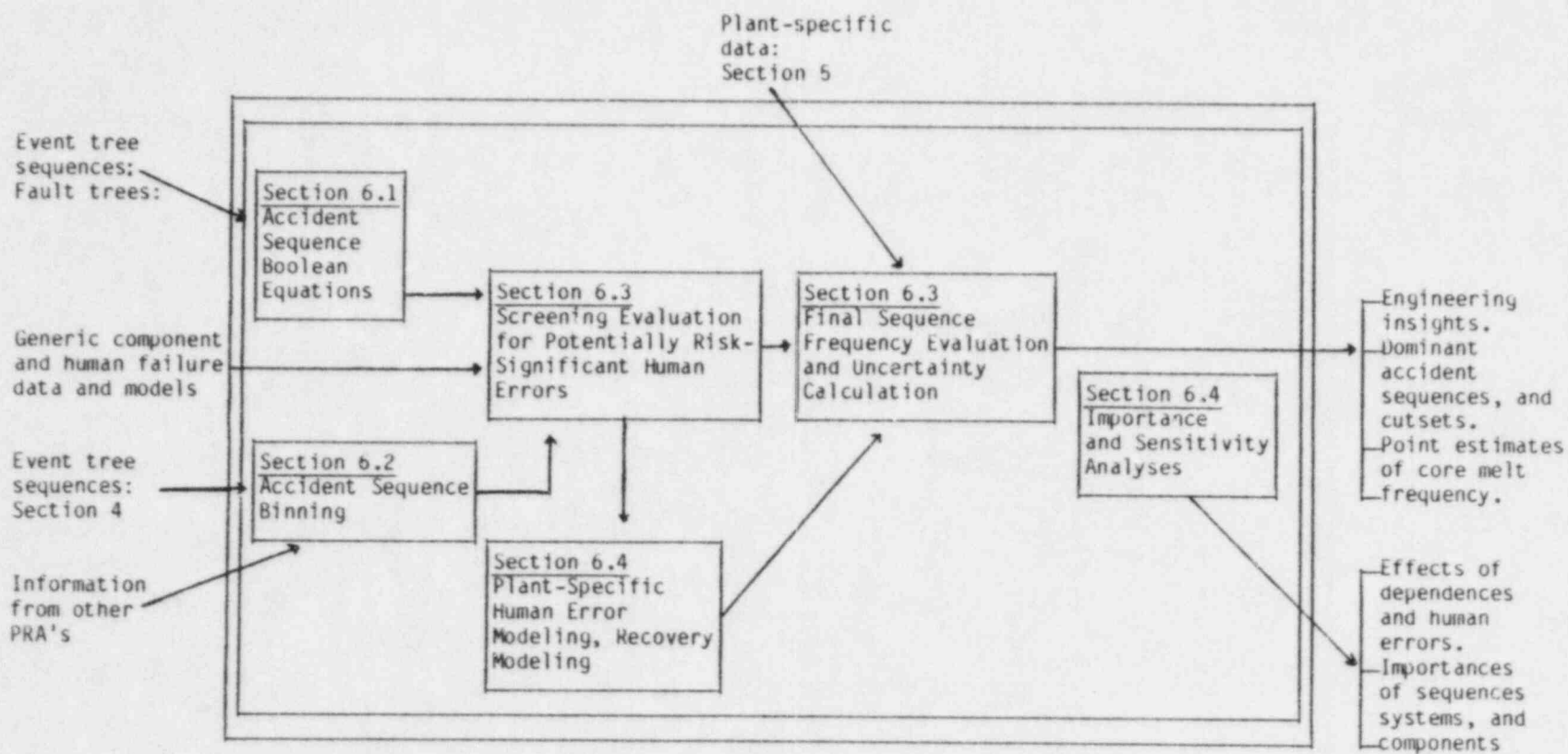


Figure 6.1 Information Flow Block Diagram.

component level contains combinations of component failures, i.e., the cutsets, that result in the accident sequence.

The reduced Boolean equation for each accident sequence, i.e., the accident sequence minimal cutsets, provides the qualitative structure for probabilistic quantification of that accident sequence.

6.1.2 Scope

This task includes obtaining reduced Boolean equations for each accident sequence. Included in this task are considerations for treating dependent faults (i.e., coupled faults), elimination of cutsets that may represent violation of procedures (e.g., concurrent maintenance that would result in outage of both trains of a two-train system), and the impact of system successes (in an accident sequence involving both system failures and successes) on the allowable cutsets in that sequence. Also included are considerations for development of independent subtrees (i.e., "modules" or "supercomponents").

6.1.3 Inputs

Inputs to the Boolean reduction task are the systemic event trees from Section 4.1; the accident sequences in terms of system failures and successes defined on these event trees; and the Boolean equations (system minimal cutsets) representing system failure for each system from Section 4.2. If the fault tree linking method is used, a formal Boolean reduction for each accident sequence is needed. The Boolean expression for an accident sequence must properly reflect the successes of those systems which are designated in the particular sequence as having succeeded.

6.1.4 Methods and Assumptions

Dependences of various types present special requirements for the reduction of event tree sequences. These requirements exist no matter which of the two event tree methods is used (large event tree method or large fault tree method). The large event tree method essentially requires that the dependences among systems be treated and displayed on the event tree, as part of the event tree construction process. The large fault tree linking method requires that the dependences be treated as part of a Boolean reduction process to obtain Boolean reduced equations for each small event tree sequence. In both cases, reduced Boolean equations are required for the sequence quantification process, and these equations must correctly reflect the various types of dependences between systems.

There are several types of dependences among systems that result in a requirement to Boolean reduce event tree accident sequences when the fault tree linking method is used. These dependences include

1. Single component faults that would fail more than one system or portions of more than one system (shared individual faults).
2. Dependences caused by shared support system trains.
3. Dependences caused by support systems embedded in other support and frontline systems.

4. Dependence loops caused by mutual dependence of support systems on each other (dependency loops).
5. Dependences caused by the requirement to distinguish between early and late system failures.

Dependences of these types can be treated by either the large event tree method or the large fault tree method. The treatment of dependences of types 1, 2, 3 by these methods is discussed in the IEEE/ANS PRA Procedures Guide, on pages 3-77ff and 6-13ff. One should note that in the large fault tree approach, where a large fault tree is obtained for an accident sequence by linking "top events" for each system together by an "AND" gate, the chance of missing a dependence is reduced provided events are labeled identically on the different fault trees corresponding to the different systems and provided the Boolean manipulations are carried out meticulously. If credit is given in a particular sequence, cutsets must properly reflect this.

When the large event tree method is used, it is important that there are no dependences which are overlooked and not treated explicitly in the event tree. If there is a component which is common to two systems, and this is not noted, then incorrect quantification will result. It is not absolutely necessary that all dependences be explicitly displayed on the event tree. If two systems have a common component not displayed explicitly on the event tree, then fault tree linking can be used for those two systems. In any event, when the large event tree method is used, a clear description of the procedure should be given to ensure no overlooked common events between systems, and the documentation should be such that this aspect of the calculation can be easily verified.

Early Versus Late System Failure

Often accident consequences depend on whether a particular frontline system fails early in the progress of an accident, or later, after the accident has been partially mitigated. Thus, it is required to treat both early and late failures of the systems. In some cases, the early failure of a system precludes any situation for which the system will be called upon later. This specific type of dependence is expressed on the event tree by not branching on late failure for those branches that include early failure of the same system. However, support systems can also fail early or late (resulting in early or late failure of frontline systems). In some cases, it is possible to have event tree sequence cut sets that include both early and late failures of support systems. These cut sets should be excluded from sequences where both early and late frontline system failure is not possible. An accepted method of accomplishing this is to express the late failure of a support system as the Boolean product, "system fails late" and "system succeeds early." The reductions will then correctly account for combinations of early and late failure in this case. The IEEE/ANS PRA Procedures Guide and the IREP Procedures Guide further discuss dependence and operational considerations in constructing event trees.

Requirements for Modularization

The complexity of the Boolean reduction process of the event trees increases geometrically with the number of terms (cutsets) in the individual

fault trees making up the sequences. A process by which the complexity can be reduced is to define independent subtrees, or modules, which contain multiple primary faults. The Boolean equation for the fault tree is then written in terms of the individual subtrees rather than in terms of the primary events. Since each independent subtree in general consists of more than one primary event, the resulting Boolean equation in terms of subtrees will contain considerably fewer terms than the Boolean equation written in terms of primary events. Thus, modularization of fault trees using independent subtrees can significantly reduce the complexity of the Boolean reduction process.

The objective in the modularization process is to combine as many primary faults as possible into independent subtrees. This process must be accomplished with caution, however. It is required that each subtree be entirely independent of every other subtree. If a primary fault appears as a fault in more than one system, it is itself defined as an independent subtree. Collections of faults that appear in more than one system as independent subtrees must be given the same name in each system in which they appear. Again the IEEE/ANS PRA and IREP procedures guides further discuss modularization considerations.

Requirements for a Boolean Reduction Code

The process of Boolean reduction of all event tree sequences is a significant effort, often underestimated in conducting a risk analysis. The Boolean reduction process is also a mechanical one which lends itself to a computerized solution. Several computer programs exist which are capable of accomplishing the Boolean reduction of event tree sequences. A computer code is required for this process, for the following reasons:

- Boolean reduction of event tree sequences by hand requires inordinately large amounts of time and resources.
- Boolean reduction by hand would generally increase considerably the chance of obtaining incorrect or incomplete cut sets.

It is emphasized that the requirement for defining independent subtrees remains and may be necessary even though a code will be used for the mechanics of the Boolean reduction process. All of the codes are limited by the number of terms that they can accept. Codes capable of performing Boolean reduction are listed in Appendix D and are discussed in the IEEE/ANS PRA Procedures Guide.

Incorporation of Initiating Events

The quantification of accident sequences requires incorporation of the frequency of the initiating event. For the small event tree/large fault tree method, the initiating event is a simple multiplier to each sequence on the event tree and no special manipulations need be done on the accident sequences. However, care must be exercised to assure that any dependences between the initiating event and the system failures and successes have been reflected in the accident sequence cut sets.

For the large event tree/small fault tree method, the accident sequences should be coalesced into those that would be used in the small-event-tree/

large-fault-tree method for discussion and display purposes. The treatment of the initiating event frequency then corresponds to that of the fault tree linking method. It is important that the accident sequences be displayed in terms of the initiating event and combinations of frontline system failures and successes, as well as in terms of the sequences which appear directly on the large event tree. Refer to the IREP and IEEE/ANS PRA procedure guides for further discussions.

6.1.5 Products

The products of this task are the reduced Boolean equations corresponding to each accident sequence, for each systemic event tree. These Boolean equations consist of the following parts:

- Initiating event as the beginning event of each event tree sequence.
- Reduced Boolean equation corresponding to combinations of component failures for each event tree sequence, reflecting the system successes designated in the sequence. (This may be expressed in terms of combinations of module successes and failures, where each module is an independent subtree of component successes or failures. The definition of each module in terms of components must be explicitly given.)

In the reporting format, the event tree sequence should be given in terms of system failure and success, and then the corresponding combinations of component failures and successes should be listed.

Table 6.1 Accident Sequence Boolean Equations Inputs and Outputs

Inputs	Outputs
1. Systemic event trees; identifying accident sequences in terms of system successes and failures (from Section 4.1)	1. Qualitative representation of accident sequence cut-sets in terms of component and human faults.
2. Fault tree Boolean equations (from Section 4.2)	

6.2 Accident Sequence Binning

6.2.1 Purpose

The purpose of this task is to assign event tree sequences to bins as a first cut indication of accident sequence severity. It is expected that NRC will build on the results of PSA studies to examine in-plant and ex-plant consequences of core damage events. To do this, it is necessary to characterize core damage accident sequences according to the overall physical state of the plant to which each accident sequence leads; and as a practical matter, it is extremely useful to group together in "bins" those sequences whose plant

states are sufficiently alike to justify analysis of the sequences together as a group. This binning process will serve as an initial step in the selection of those accident sequences which may, in some subsequent evaluation process, be analyzed in detail with a core meltdown code such as MARCH or MELCOR.

6.2.2 Scope

All accident sequences should be uniquely assigned to a bin. The scope of this subtask therefore includes (1) bin definition, with due regard to previous studies, and (2) assignment of accident sequences to bins.

6.2.3 Inputs

Input to this task includes the event tree sequences identified in Section 4.1. Also, information from external sources should be useful in constructing the bins and for their assignment to release categories. Several examples of the binning process are available in the risk assessments that have been performed to date. These include the Zion and Indian Point Probabilistic Safety Studies which provide examples for the Westinghouse 4-loop, dry containment PWR. The Probabilistic Risk Assessment for the Limerick Generating Station provides an example for the General Electric, Mark II containment and the GESSAR-II Probabilistic Risk 2 Assessment provides an example for the Mark III containment. Cybulskis et al. [Trans. Am. Nucl. Soc. 40 (1982)] give examples of binning procedures for the plants analyzed in the RSSMAP study, i.e., Babcock & Wilcox, dry containment, PWR; Combustion Engineering, dry containment PWR; Westinghouse ice condenser containment, PWR; General Electric, BWR6, Mark III Containment. Finally, the Big Rock Point Probabilistic Risk Assessment provides an example for a plant of a vintage design.

6.2.4 Methods and Assumptions

Binning is a general method of simplifying and making tractable the evaluation of the large number of accident sequences which arise from the event trees developed for the plant. A good discussion of the binning procedure is given in Chapter 7 of the IEEE/ANS PRA Procedures Guide (NUREG/CR-2300). The concept is quite simple: a bin is a set of accident descriptors which facilitate grouping or categorizing of those accident sequences having similar physical responses in the plant.

The definition of the accident bins should be determined by considering the following accident sequence characteristics:

- Initiating Events
 - LOCA (including steam generator tube rupture and interfacing LOCA)
 - Transients
 - Vessel rupture
- Functionability of reactor protection system
- Functionability of ECCS

- Functionability of containment safeguards

For a particular reactor type (i.e., vendor, containment type, special design features), the above-mentioned functions can be translated into system failure and success descriptors in a manner which conveniently and sensibly suits the particular reactor. For example, containment safeguards, sprays, fan coolers, ice inventory, and suppression pool subcooling should be considered as system decompositions. The following specific considerations may aid the analyst in defining bins.

1. Early core damage vs late core damage (relative to time of scram)
2. Containment failed prior to or after core damage (both structural failure and isolation failure should be considered)
3. Containment bypass (those sequences of Event-V type)
4. LOCA with or without pressure suppression (BWR)
5. Pool is subcooled or saturated when core damage occurs (BWR)
6. Vessel pressure when core slump occurs
7. Availability of containment sprays
8. Availability of containment heat removal
9. Availability of ac power and recovery times
10. Condition of reactor cavity at vessel failure (water flooded or dry)

Table 6.2 Accident Sequence Binning Inputs and Outputs

Task inputs	Task Outputs
1. Event tree sequences in terms of system successes and failures (from Section 4.1)	1. Each accident sequence assigned to a bin
2. Binning information from external sources (from other PRAs)	2. Definition of descriptors which provide system and containment status for each bin

6.2.5 Products

After the bins are defined and accident sequences are grouped into bins, the analyst should provide a list of the bins and the accident sequences that they contain.

6.3 Sequence Quantification

6.3.1 Purpose

The primary purpose of sequence quantification is to evaluate the accident sequence frequencies using plant-specific data and including the possibility of recovery of component faults, human faults, and outages. The initial phase of the evaluation also serves as a screening calculation for human errors.

6.3.2 Scope

The calculation proceeds in two stages. In the first stage, accident sequence frequencies are calculated with no credit taken for post-accident correction of mispositioning or actuation faults, and using screening values for human error probabilities. This serves as a screening calculation for human errors; the results of this calculation are used to generate the list of important human errors, which are to be analyzed further as part of the Human Performance subtask. In the second stage, credit is taken for recovery of mispositioning or actuation faults on a cutset-specific basis.

6.3.3 Inputs

Inputs to the first stage of this task are the following:

- Reduced Boolean equations for each event tree sequence.
- Point values for initiating event frequencies.
- Component data base.
- List of human errors of potential concern, together with screening values.
- Output of the binning task.

Inputs to the second stage are the above, plus:

- Plant-specific human error probabilities
- Recovery Model.

6.3.4 Methods and Assumptions

6.3.4.1 Human Error Screening Calculation

The first phase of the quantification serves as a screening calculation for human errors. A list of human errors of potential concern is input to this calculation, together with screening values. Human errors which contribute significantly to core damage frequency ("important errors") are then studied further as part of the Human Performance subtask; errors which do not contribute significantly are not considered to warrant further study. The list of errors and the output list of important errors should be supplied, along with a detailed statement of the criterion of importance.

Preliminary point estimates of the frequencies of the accident sequences for the human error screening quantification are calculated by multiplying the point value unavailability estimate of each event tree sequence by the point value frequency estimate for the corresponding initiator. The unavailability of the event tree sequence is estimated by summing the point value unavailabilities of the component-level minimal cut sets for each sequence. The formulas used in the quantification of component faults and outages are described in Section 5.6. The quantification of human faults is described in Section 5.7.

The evaluation should be performed using means of the posterior plant-specific failure distributions and point estimates of the plant-specific operational data. Credit for post-accident recovery of actuation faults or of pre-accident mispositioning faults is not taken at this stage.

In practice, it may be convenient to perform the quantification concurrently with the sequence Boolean reduction, particularly when the large fault tree method is used, and a code is used to perform both the sequence Boolean reduction and sequence quantification. Appendix I describes several codes that perform both functions concurrently.

6.3.4.1.1 Truncation

In order to make sequence quantification practical, it may be necessary to truncate: to consider only those cutsets whose probability is above some cutoff, which is then called the truncation value. NUREG/CR-2728 suggests a truncation value of 10^{-9} for sequence cutsets, but allows for relaxation of this, provided that sequences of order 10^{-6} per year are not neglected.

While the benefits of truncation are undeniable, they are gained only at a price. It may be that the results of a calculation truncated at 10^{-9} will substantially exhaust the top event probability, but there is no fundamental law which guarantees this. Truncation is an approximation which may be excellent but which is generally uncontrolled. The NUREG/CR-2728 guidance should be adopted as a starting point, and if less conservative truncation is performed, a detailed discussion of the need for this should be provided.

6.3.4.2 Final Results Including Recovery

After plant-specific human error probabilities have been derived, the sequences can be requantified using these values. Generally, the results of such a calculation without credit for recovery will be conservative to the point of distorting the conclusions to be drawn. Unless particular accident sequences are negligible, or recovery is out of the question, it will be obligatory to consider recovery. Thus, after intermediate results have been obtained with plant-specific human error probabilities. The final results are obtained by applying an appropriate multiplicative factor to each cutset probability, in order to factor in the possibility that operator action will eliminate one of the faults in the cutset, and thereby prevent core damage. Preliminary guidance for this step was provided in NUREG/CR-2728, which has influenced the following discussion.

Post-accident recovery credit is taken for actuation faults or preaccident mispositioning faults, but generally not for repairs or for heroic

actions. Recovery credit is taken on a cutset-specific basis because the recovery probability of a given basic event depends on the particular scenario. One simple class of recovery models essentially relates the probability of a recovery to the cutset-dependent time which is available for accomplishing the act. Recovery acts which must take place outside the control room require more time than comparable acts within the control room, because personnel must go to remote locations. A model of this type is discussed in NUREG/CR-2728, and elements of this approach are incorporated into many of the techniques discussed in Section 4.3.

The generally large effect of recovery in shaping the final results means that the documentation of the recovery model and its application are also important. Elements of suitable documentation are called out in Section 4.3 (Human Reliability Analysis). Assessment of recovery is no more settled than other aspects of human behavior or, and it is feasible to prescribe the necessary documentation in useful detail beyond what is discussed in Section 4.3, but the general requirements given for documentation of human error probability should be understood to apply to recovery as well.

The output of this process is the following:

- A list of leading accident sequence cutsets quantified without recovery;
- A display, for each accident sequence, of each cutset for which recovery credit is taken, the probability of nonrecovery which has been assigned along with the event(s) which are being recovered, and the cutset probabilities before and after the recovery factor is applied;
- Documentation of the recovery model.

6.3.4.3 Uncertainty Evaluation

The uncertainty evaluation is to be performed using the plant-specific gamma posteriors for the initiating event frequencies and the component failure rates. Error ranges identified for human error rates and recovery probabilities are to be included by treating them as random variables with the defined uncertainty distribution (Appendix I). Human error rates for similar human errors should be treated as the same random variable; similarly, failure probabilities for similar components should be treated as the same random variable.

6.3.5 Products

Products resulting from completion of the final sequence quantification include point estimates of all accident sequence frequencies, of the core damage frequency, and of each bin frequency, before and after recovery credit is taken. An identification of the potentially dominant sequences in each bin is to be given by ranking the sequences in each bin according to their point value frequencies and preserving those that contribute 99% of the frequency in each bin. An overall ranking of the final accident sequences should also be carried out according to their point value frequencies, and those sequences constituting the top 99% of the core damage frequency are to be identified. For accident sequences that include failure to isolate the containment, the

analyst should provide the specific conditional probability to isolate containment as derived in the study.

For the final results, bar-chart plots should be presented which display the following:

- a. contribution to total core damage probability from the following categories:
 1. sequences with no containment cooling,
 2. sequences with substantial containment cooling,
 3. sequences that bypass the containment (Event V types);
- b. contribution to total core damage probability made up of:
 1. transients,

Table 6.3 Sequence Quantification Inputs and Outputs

<u>Screening Calculations</u>	
Task inputs	Task Outputs
1. Accident sequence Boolean expressions	1. Importance ranking of potentially risk-significant human errors for further study
2. Plant-specific failure data	
3. Screening probability values for human errors of potential concern	
4. Output of the binning task	
<u>Final Sequence Evaluation</u>	
All of the above, plus	1. Final point estimates for accident sequences frequencies, core damage frequency, and bin frequencies
5. Final plant-specific human error probabilities	
6. Recovery model	2. Ranking of accident sequences and estimation of dominant accident sequences
	3. Uncertainty characterization of the accident sequence frequencies, core damage frequency, and bin frequencies

2. large break LOCAs,
3. small break LOCAs.

Evaluation of uncertainty should cover the following results:

1. The overall core damage frequency.
2. The frequency of each bin.
3. The frequency of accident sequences contributing either to the top 99% of total core damage frequency or to the top 99% of any bin.

Regardless of how the calculation is performed, the mean and median values should be given, together with sufficient information about the distribution to allow the user to estimate any desired probability interval. For example, if parameters of a probability distribution are fitted to calculated moments of a sequence frequency, then the parameters should be presented. If a simulation is performed, a table should be presented which gives frequencies corresponding to cumulative percentiles of 99, 95, 90, 80, . . . , 10, 5, and 1.

6.4 Importance and Sensitivity Analyses

6.4.1 Purpose

This task is divided into two parts, the importance evaluations and the sensitivity analyses. The purpose of the importance evaluations is to identify the important accident sequences, system failures, and component failures and human errors with regard to core damage frequency. The importance evaluations are presented in a hierarchical fashion to allow tracing from the important accident sequence to the important system failure (or failures) in the accident sequence to the important component failures or human errors contributing to the system failure.

The purpose of the sensitivity analyses is twofold: (1) to determine how sensitive the core damage frequency is to possible dependences among component failures and among human errors; (2) to address those assumptions suspected of having a potentially significant impact on the results. These assumptions are generally in areas where information is lacking and heavy reliance must be placed on the analyst's judgment. Sensitivity analysis can then be accomplished by substituting alternative assumptions for conservatisms and evaluating their individual impacts on the results. If, in the case of failure dependences, significant sensitivities are exhibited, the analyst should describe what conditions, precautions, and actions are in place to help ensure against them.

6.4.2 Scope

The importance evaluations consist of the calculation of two importance measures. The first measure is the usual fractional contribution to the core damage frequency or to the system unavailability and is sometimes called the Fussell-Vesely importance measure. The second measure is the change in core melt frequency or system unavailability when the contributor's failure

probability is set equal to one. This second measure, called here the degradation ratio,* is useful when analyzing effects of assumed failures, e.g., component allowed-downtime analyses.

The sensitivity analyses of potential component dependences consist of identifying minimal cutsets, some or all of whose components are potentially susceptible to dependences because of defined identified characteristics. A relatively high dependent failure probability is then assumed. If the use of this high dependent failure probability results in a significant change in the core damage frequency, then precautions, actions, or conditions are to be described which serve to reduce the potential dependence. The sensitivity analysis of potential human error dependences entails identification of minimal cutsets containing multiple human errors and then a description of defenses, management controls, or conditions which serve to reduce the potential dependence.

The following sections describe the methodology which is to be used and the specific products of the importance and sensitivity analyses.

6.4.3 Methodology for the Importance Evaluations

The fractional contribution, or Fussell-Vesely importance measure, should be computed for every initiator, for every accident sequence, for every frontline and support system, and for the top 20 Boolean reduced cutsets (event tree minimal cutsets). The importance for these contributors should be calculated with regard to the core damage frequency. In addition, the importance should also be calculated for the top 20 contributors to every frontline and support system; in calculating these contributors, only component unavailabilities and human error probabilities should be considered for the top 20 ranking. If common cause events have been postulated to account for presumed coupling between nominally distinct failures, the importance of these events should also be calculated as if they were component importances. The importance for these component and human error contributions should be calculated with respect to the system probability characteristic appearing in the accident sequence frequency, which is generally the system unavailability.

Generally, it will be necessary to calculate the importances for more than 20 contributors to ensure that the top 20 are indeed identified. The data to be used for these importance calculations are the plant-specific point values. Chapter 6 of the IEEE/ANS Procedures Guide and the IREP Procedures Guide discuss the calculations involved in determining the importance values.

The second measure of importance, the degradation ratio, is computed by calculating the core damage frequency or system unavailability with the failure assumed given and dividing by the reference (unconditional) frequency or unavailability value. These degradation ratios should be computed for every frontline and support system with regard to the resulting changes in core damage frequency. If the system contains minimal cutsets which are common to other systems, then the implication of the assumed system failure on the unavailabilities of these other systems must be taken into account. This

*The degradation ratios are also termed "risk achievement ratios" in other NRC work.

accounting of shared minimal cutsets is handled by using standard Boolean and conditional probability techniques.

As additional importance calculations, the top 20 degradation ratios on the core damage frequency from assumed important component failures and human errors should be calculated. The ratios are calculated by assuming that the component unavailability or human error probability is unity and then determining the ratio of the resulting core damage frequency to the reference frequency. Finally, the top 20 ratios for every frontline and support system unavailability from assumed component failures and the top 20 ratios for assumed human errors should be determined.

It again will be generally necessary to calculate more than 20 impact ratios to ensure that the top 20 are indeed obtained. The data to be used for these degradation ratio calculations are again the plant-specific point values.

6.4.4 Methodology for the Sensitivity Analyses

The sensitivity analyses consist of three parts: sensitivity analyses of potential component failure dependences, of potential human error dependences, and of major assumptions recognized by the analyst to be overly conservative (see also Section 4.3.3 and Section 4, Ref. 7).

Component Failure Dependence Analyses

The sensitivity analysis prescribed here is intended to explore, among other things, the type of modeling incompleteness for which beta factors are intended to compensate.

As a first step, a search is conducted for areas which are sensitive to coupling between hardware failures. Searches for sensitivity to dependence are carried out on a system-by-system basis, so it is feasible to explore each system in more depth than would be the case if entire accident sequence cutsets were searched. The process of truncation may discard cutsets which seem unimportant if no coupling is assumed, but which are important in the presence of coupling; therefore, truncation in the following searches should be as conservative as possible.

Plant-specific failure data are to be used in the following calculations. The following assessment should be performed for each frontline system and each support system, for each distinct set of mission success requirements arising from distinct accident sequences.

1. A new top event (failure) expression should be formed for the system under study. For frontline systems, the top event should reflect the mission success requirement under study, and it should be conditioned on (a) complete support system success, and (b) the initiating event, except that where (a) and (b) conflict, only (b) should apply. For support systems, the top event is failure of any pair of redundant trains which supports any pair of redundant frontline system trains. In the case of either frontline or support systems, the unavailability corresponding to these new system top events should be calculated and presented.

2. Each top event expression should be searched for dependence-suspect minimal cutsets (DSMCS). DSMCS are minimal cutsets containing failures of components, of which two or more have a common property which renders them susceptible to dependent failures. (Note that all components in the cutset do not have to have the common property, but only two or more.) DSMCS affected by the following types of coupling are to be identified:

- a. between components in the same location (same room);
 - b. between components which are periodically tested using identical testing procedures (these are components actually tested, and not merely reconfigured during testing);
 - c. between components of the same generic type, where generic type is defined by the classifications used in the generic data base supplied in this guide (e.g., motor-operated valves).
3. Each DSMCS should be requantified as follows:
- a. identify the highest failure probability among the coupled events;
 - b. set the product of the remaining coupled failure probabilities equal to 0.1.
4. For each type of coupling, the pertinent DSMCS should be presented, together with their respective new and old quantifications; the ratio change in system unavailability (referred to that assessed in (1) above) should also be presented.
5. Whenever the effect of a given coupling on a given system is substantial (greater than a factor of 2 in system unavailability), the corresponding change in the frequencies of the affected core damage sequences should be presented, along with a discussion of precautions, actions, or conditions existing in the subject plant which serve to reduce the potential dependence.

Single failures in any of the systems should also be tabulated and discussed separately. The discussion should give the defenses or conditions reducing the contribution of these events to system unavailability.

Human Error Dependence Analyses

The human error dependence sensitivity analyses should be performed in a manner similar to the component dependence sensitivity analyses. The dependence-suspect minimal cutsets which should be identified are those containing multiple human errors, of any type. The minimal cutset can also have component failures contained in it; it is the fact that it contains multiple human errors that renders it suspect. Rather than being requantified, these dependence-suspect minimal cutsets must be analyzed and a description given of the precautions, management control, or conditions which serve to eliminate significant dependences among the human errors in the cutsets. These discussions should be prepared in a tabular format, with the dependence-suspect cutsets ordered according to number of human errors involved.

Major Conservative Assumptions

Assumptions recognized by the analyst as being overly conservative are to be replaced by more realistic ones, and the resulting impact on the core damage frequency is assessed.

6.4.5 Products

The products of the importance analyses are:

1. The Fussell-Vesely importances for every accident sequence, for every frontline and support system, and for the top 20 event tree minimal cutsets. These importances are to be calculated with respect to the core damage frequency.
2. The Fussell-Vesely importances for the top 20 contributors to every frontline and support system.
3. Degradation ratios for every frontline and support system on core damage frequency.
4. Degradation ratios of the top 20 component contributors to core damage frequency.
5. Degradation ratios of the top 20 human error contributors to core damage frequency.
6. Degradation ratios of the top 20 component contributors to every frontline and support system.
7. Degradation ratios of the top 20 human error contributors to every frontline and support system.

The products of the component failure sensitivity analyses are

1. the dependence-suspect minimal cutsets, for each system, for each distinct mission,
2. the resulting changes in system unavailability and core damage sequence frequencies, where the changes are substantial (greater than a factor of 2),
3. a description of the defenses or conditions which serve to eliminate the dependences for these sensitive minimal cutsets.
4. a tabulation and discussion of single failures of each system.

The products of the human error sensitivity analyses are

1. the dependence-suspect minimal cutsets,
2. a description of the defenses, management controls, or conditions which serve to eliminate the human error dependences in the dependence-suspect minimal cutsets.

The format of reporting these results should be structured to allow straightforward review.

The products of the conservative assumption sensitivity analysis should be presented in a tabular form, and contain the conservative assumption, the realistic alternative, the impact on the core damage frequency, and a brief description of the rationale and data to support the realistic assumption.

Table 6.4 Importance Analysis Inputs and Outputs

Task Inputs	Task Outputs
1. Dominant accident sequence cutsets (from Section 6.4)	1. Fussell-Vesely importance (referred to overall core damage frequency of a) each initiator b) each accident sequence c) each frontline and support system d) 20 most important core damage cutsets e) 20 most important component failures f) 20 most important human errors
2. Boolean expressions for failure of frontline and support systems	2. Degradation ratios (referred to overall core damage frequency) of a) each frontline and support system b) 20 component failures having largest degradation ratios c) 20 human errors having largest degradation ratios
3. Plant-specific failure data	3. For each frontline and support system, for each distinct mission: a) system unavailability b) Fussell-Vesely importance of 20 most important cutsets c) Fussell-Vesely importance of 20 most important component failures d) Fussell-Vesely importance of 20 most important human errors e) Degradation ratios for each of the 20 most important component failures f) Degradation ratios for each of the 20 most important human errors

Table 6.5 Sensitivity Analysis Inputs and Outputs

Task Inputs	Task Outputs
1. Boolean expressions for accident sequences	1. Component Failure Sensitivity Analysis: Dependence suspect minimal cutsets, for each system, for each distinct mission; where the change in system unavailability from a given type of coupling is more than a factor of 2, the effect of that coupling on core damage frequency should be presented.
2. Boolean expressions for failure of frontline and support systems	Description of defenses or conditions which serve to eliminate the dependences for these sensitive minimal cutsets.
3. Information regarding component locations	Tabulation and discussion of single failures for each mission.
4. Information regarding component testing procedures	2. Human Error Sensitivity Analysis: Dependence-suspect minimal cutsets, for each system, for each distinct mission
5. Classification of each component generic type	Description of defenses, management controls, or conditions which serve to eliminate the dependences between the human errors in the suspect minimal cutsets.
6. Analyses bearing on mission success criteria	3. Conservative Assumption Sensitivity Analysis: Tabulation of conservative assumptions, realistic alternatives, effects on core damage frequency of adopting realistic alternatives, accompanied by a description of the rationale and available data supporting the realistic assumption.
7. Plant-specific failure data	

7. DISPLAY AND INTERPRETATION OF RESULTS

After the tasks discussed in Section 6 have been completed, it remains to suitably display the results of the study and to communicate insights gained from the enterprise. It is the purpose of this section to recapitulate the guidance given in Sections 3 through 6 and to provide some additional remarks on how to interpret the results.

7.1 Documentation of a PSA

There are several needs to be met by the documentation of a PSA study.

- . The study must communicate its essential results to the community of reactor safety specialists.
- . The study must lend itself to high-level peer review.
- . The study must permit detailed technical review, including substantial recalculation.
- . The study must lend itself to extensions or adaptations of its basic models; it must be possible to build on the study.

This guide has prescribed a number of outputs of various tasks. These intermediate results are of great value, and are to be included in the report. For convenience, these are summarized in Table 7.2.

Regarding the structure of the overall presentation of the report, a number of useful suggestions are contained in a forthcoming EPRI report, "Documentation Design for Probabilistic Risk Assessment". The general EPRI approach is adopted here, with modifications which adapt the format and content of the reports to the specific needs of PSA studies. The report should contain three major divisions:

1. a summary, which communicates the essential results and methodology at a level which is useful to a wide audience of reactor safety specialists and which is adequate for high level peer review;
2. a main report, which contains an "integration" of the entire study, detailed descriptions of the tasks, and the detailed conclusions, presented in sufficient detail to support (together with its appendices) a detailed technical review;
3. a collection of appendices, which contain detailed computations and blocks of information supporting models and analyses presented in the main report.

The following subsections discuss each of these major divisions in more detail. Portions of the following discussions have been taken verbatim from the above-cited EPRI report.

7.1.1 Summary of a PSA

The purposes of the summary are to communicate the project's motivations, objectives, and scope of the report and the essential methods, results, and conclusions of the study to interested parties, and to do this in a way which meets the needs of a high-level peer reviewer. The summary should contain sections on report organization, scope, methods, and display and interpretation of results. These will be discussed individually below.

A unique feature of PSA studies is the baseline evaluation: the quantification of the plant-specific model with generic failure probabilities. A PSA study therefore carries within it a comparison of the plant-specific results with a "baseline" whose design is identical to the subject plant but whose failure probabilities are generic. Thus, while comparison of the subject plant with other plants should play an important role in the discussion of the results, a discussion of the relation between the baseline evaluation and the plant-specific evaluation should appear even more prominently.

7.1.1.1 Report Organization

In addition to providing an overview of the report's organization, this section should contain an index relating sections of the summary to sections of the main report:

Summary Report Section	Corresponding Main Report Section(s)	Comments
S.4.3 Fault Tree	M.4.1 Fault Tree Methods M.4.2 System Fault Trees M.9.1 Linking of Fault Trees	Appendix A.9 contains complete fault trees and fault summaries

This guide prescribes the inclusion of a number of task outputs as part of the report. The section on report organization should give the location of each such output.

7.1.1.2 Scope

Treatment of scope should include the following:

- the objectives of the PSA, which will include, but not be limited to, those mentioned in this guide;
- the major tasks of the PSA;
- a summary of where (in the main report and in the summary) the tasks and subtasks are treated;
- a description of the PSA team;
- a description of the steps taken to monitor technical quality as the study was performed (e.g., external review at major milestones).

7.1.1.3 Methods

Methods for some tasks (notably basic event quantification) are prescribed in this guide, but most are not. The methods section should discuss the following:

- The methods used to perform each task and each subtask defined in this guide, along with whatever additional tasks are defined by the report. The descriptions should suffice to permit a high-level peer reviewer to assess the adequacy of the methods for the purposes of PSA studies of this program. Where possible, use should be made of material in the IEEE/ANS guide. Advances in the state of the art should be described. If special techniques were evolved in the process of performing the study, these should be discussed in a separate subsection.
- Activities undertaken to assure completeness of the models, with special attention devoted to the initiating events, the identification of failure modes associated with each event tree heading, and the identification of dependences.

In addition, the text should direct the reader to those portions of the main report which contain information on the above points.

7.1.1.4 Display and Interpretation of Results

The presentation of results has been explicitly covered previously. Certain points bear special emphasis:

- A narrative description of each of the dominant accident sequences noted above should be provided. This narrative should briefly discuss the nature of the initiating event and of the additional system failures involved in the sequence (their impact on the maintenance of plant critical safety functions). The major contributing failures associated with each system failure should be presented. Any significant dependences between the events involved in the sequence should be discussed.
- Regardless of the methods and terminologies used in the study, the display of results in the summary should include a presentation of the dominant accident sequences in terms of the standardized event nomenclature given in Appendix J. In general, unless the study happens to have chosen the standardized scheme, the summary will contain a detailed discussion which relates the study's nomenclature to the standard nomenclature, and will contain a table recasting each of the study's dominant accident sequences into the standard notation.
- The tabulations of dominant accident sequences must allow a determination of the source of that sequence and the constituent elements of that sequence. This will entail sequence narrative descriptions which reference sections in the Main Report relating to the source event tree, relevant fault trees, and failure rates associated with contributing events. For example:

SEQUENCE: A B C (Frequency = $1 \times 10^{-6}/\text{yr}$)

Initiating Event "A" entails a small steam line break outside of containment. A more detailed description of initiating events A is found in Section 2.2.1 of the Main Report. The event tree developed for "A" is presented and discussed in Section 5.3 of the Main Report.

System B is designed to [...]. A more detailed description of System B can be found in Section 4.3 of the Main Report and additional information related to its response to "A" is presented in Section 5.3. An important dependency between the occurrence of "A" and the performance of System B was identified to be [...]. A more detailed discussion of this interaction is presented in Section 13.3.1.

The fault tree for System B is presented in Section 4.3.2. The major contributing cutsets (conditional upon "A") are

$$\begin{aligned}(C_1, C_2) &= (1.0 \times 10^{-2}) (5.0 \times 10^{-2}) = 5 \times 10^{-4} \\(C_1, C_3) &= (1.0 \times 10^{-2}) (1.0 \times 10^{-2}) = 1 \times 10^{-4} \\&= 6 \times 10^{-4}\end{aligned}$$

[Both baseline and plant-specific results should be presented.]

C_1 is the failure of valve xyz to open on demand. C_2 is the failure of the operator to notice this failure and manually open the valve. C_3 is the failure of the switch which allows manual opening of the valve. These failure events are discussed in more detail in Section 4.3.2 of the Main Report and Appendix A.6. The failure probabilities for C_1 , C_2 , and C_3 are discussed in Section 4.3.2 (Fault Trees) and Section 7.8 (Failure Data) of the Main Report.

- Modularized logic trees depicting major contributors to system failure can be a valuable aid to the high-level peer reviewer, in conjunction with the discussion format recommended above for dominant accident sequences. This is not a substitute for presentation of the actual trees used in the study, but is simply a pictorial method of representing the conclusions. This type of documentation is encouraged.
- A "road map" from the dominant accident sequences to the relevant sections of the main report should be provided in tabular form. For example (this is only an example; actual headings will differ):

Sequence	Initiating Event	Event Tree	System Descriptions	System Interactions	Fault Trees	Fault Data
ARC	2.2.1	5.3	4.1 (A)	13.3.1	4.1 (A)	7.8
			4.2 (B)		4.2 (B)	7.9
			4.3 (C)		4.3 (C)	

- Importance measures and system unavailabilities pertinent to the issues tabulated in Table 7.1 should be summarized.

Interpretation

At this point in the report, a vast amount of information will have been summarized. It is therefore appropriate to

- discuss the relation between the baseline evaluation and the plant specific evaluation;
- compare the subject plant's dominant sequences with those of comparable plants that have been studied, highlighting differences in assumptions between studies and, where appropriate, quantitatively characterizing the effect of credible changes in the modeling assumptions;
- reflect on the results in light of existing plant-specific regulatory issues.

The special reporting requirements mentioned in Table 7.1 should be dealt with in a separate subsection. Many of the products called for in Table 7.1 actually appear as products of various different tasks; however, an integrated discussion of these issues should be provided in one place, as part of the Interpretation section.

Consideration of a broader range of regulatory issues is optional. Suggestions are given in Appendix A. It is useful to discuss existing or pending regulatory requirements in light of the results being presented in the study, and to show how they have influenced the conduct of the PSA.

7.1.2 Main Report of a PSA

This segment, together with the Appendices, provides the information necessary for the detailed technical review. The inputs and outputs of the various tasks defined in this guide are a major constituent of the main Report. Roughly speaking, the summary of a PSA corresponds to the main report of WASH-1400 or an IREP study, and the main report of a PSA corresponds to the appendices of WASH-1400 or an IREP study; but the main report of a PSA is expected to do a thorough job of elucidating the connections between different parts of the report. Subsections of the main report are discussed below.

7.1.2.1 Integration Section

This section presents the overall organization of the project. It includes

- the objectives and scope of the project;
- a description of the structure of the study, in terms of tasks and subtasks, and inputs and outputs of each. Most of this is prescribed in this guide, but the study should be self-contained;
- an annotated cross reference between chapters of the main report and those of the appendices.

7.1.2.2 Task Description

This portion of the report describes each task in depth. Following are portions of the EPRI prescription for documenting the inputs and methods for each task.

7.1.2.2.1 Input Data for Each Task

- The information requirements of each task should be summarized. The source of each input should be defined (i.e., which inputs come directly from other tasks in the study, which are generated through iterative loops with other tasks, which originate outside the study).
- Inputs generated outside the study should be given either in the main report with specific sources cited, or in the appendices. Inputs generated within the study as outputs of other tasks are to be given in any case (see Table 7.2).
- The limitations of the available information and data bases should be discussed. The applicability of the sources to the general requirements of the task should be evaluated with respect to their effect on the quality of the task output; shortcomings of the baseline data base should be discussed in a separate subsection.

7.1.2.2.2 Methods for Each Task

This guide allows considerable latitude in choice of methodology for several of the tasks. In several areas (notably human error), advances in the state of the art are expected. Treatments of the methodology are therefore necessary not only in order that the reports be self-contained, but also because of the current pace of development in PRA.

Treatments of the methodology for each task should cover the following.

- The general methodology should be outlined; comparisons to the IEEE/ANS PRA procedures guide should be made.
- Inherent limitations of the methodology or practical constraints encountered during implementation should be defined and discussed.
- The impact of these limitations and/or constraints on the quality of the output of the task should be discussed.
- If the methodology is new or varies significantly from past applications, benchmarking of the methodology should be provided or referenced. This should be discussed in the course of interactive review.
- If computer codes are used, users' manuals should be referenced and a brief discussion of the code consistent with the above items should be provided. Any new validation and verification process should be referenced. Codes not generally available should be provided to NRC as part of the appendices. Input decks for computer calculations should be provided, both in printed form and in machine-readable forms (e.g., magnetic tape), as part of the appendices.

- The uncertainties associated with the limitations of the methodology should be quantified to the extent necessary to support the decision making goals of the PSA. This is particularly true for the special regulatory issues highlighted in Table 7.1

7.1.2.2.3 Products of Each Task

The view adopted here is that the products of each task are "results" of the PSA which compare in importance with the final core damage frequencies. Nominally, each task is a stepping stone on the path to the final answer; but for future users of the model, the intermediate results of the various tasks are as important as the contents of the results section. Moreover, clear presentation of intermediate steps is a prerequisite to a successful detailed technical review.

Products of the various tasks and subtasks are listed in Table 7.2. Generally, each product which is an input to another task should be reported in a form which is both scrutable and consistent with the input requirement.

Certain of the required outputs cannot usefully be printed as part of the report (or can be printed only by particular computer codes in particular formats). An example of this is the task output "Boolean equations for each accident sequence of each systemic event tree." With all events developed down to basic component failures, such an expression is so large as to be useless. In such a case, it is appropriate to provide an abbreviated version in print (e.g., a few leading terms), and a machine-readable version on magnetic tape. The goal is to permit users of the study to make use of products which have been generated at great cost.

"Credibility" Section

The final section of the main report brings together in one location those aspects of input, methods, or results known to be key factors in the ultimate credibility of the PSA results and conclusions. This section should include:

- Results of sensitivity studies prescribed in Section 6, along with other such studies which may have been performed.
- Summary description of activities directed at assuring completeness of initiating event list.
- Summary description of activities directed at assuring completeness of system failure modes or causes.
- Summary description of activities directed at identifying all inter-system dependences.
- Summary description of activities undertaken to assure technical quality (e.g., interactive review).
- Summary description of limitations and constraints associated with input data and methodologies and their impact on PSA results.

- Summary comparison of reported results with those of previously published PRAs.
- Summary description of advances in the state-of-the-art.

7.1.3 Appendices of a PSA

The appendices are a repository of material whose bulk and level of detail are such that its inclusion in the main report is unwarranted. It may also turn out that in the particular case of PSA, there are categories of material unsuitable for general release, by virtue either of their proprietary nature or of a low probability of users other than NRC requiring access to the material. Earlier in this section, it was mentioned that input decks for all computer calculations should be provided in the appendices, and that any codes used which are not generally available should also be provided.

Examples of other information which should be provided are the following. These appeared as inputs to the Fault Tree Development subtask or the Plant Familiarization task.

- Plant Technical Specifications
- System descriptions of the type used in plant/operator training manuals
- As-built system drawing
- Electrical one-line drawings
- Control and actuation circuitry drawings
- Emergency, test, and maintenance procedures
- Analyses in support of mission success criteria

Additionally, substantial information will be gathered in the course of the plant-specific reliability data assessment. This includes such items as (Table 5.3)

- operator logs, monthly status reports, LERs
- maintenance logs
- test records
- calibration records

It is not the present intention of this guide to demand all the above regardless of its usefulness, but rather to establish the principle that the more information there is in the appendices, the greater the ultimate usefulness of the PSA. In general, if something has been deemed useful enough in the first place to gather for the PSA, it is worth including in the appendices unless it is easily found in the open literature.

References

1. Von Herrmann, J. L., Parkinson, W. J., and Leaver, D. E., "Documentation Design for Probabilistic Risk Assessment", EPRI RP-2171, (Draft, 1983).

Table 7.1 Special Reporting Requirements for Selected Regulatory Issues

No.	Regulatory Issue Title	NRC Program	PSA RELATED AREA*	COMMENTS
1.	ATWS	GI, A-9	ET, FT	Report importance measures of relevant accident sequences and associated systems.
2.	Station blackout	GI, A-44	ET, FT, SI, HE	Report importance measures of accident sequences involving station blackout and special system interactions and human errors consideration.
3.	Shutdown decay heat removal	GI, A-45 SEP-4.2.1 SEP-4.2.2 TMI, II.E.3.2	ET, FT, SI, HE	Report importance measures of accident sequences involving loss of decay heat removal capability. Report identified system interactions and human errors.
4.	Auxiliary feed-water system evaluation	TMI, II.E.1.1 TMI, II.E.1.2	FT	Report importance measures and system unavailability.
5.	ECCS reliability	TMI, II.E.2.1 TMI, II.K.3 (17) GI, B-61	FT	Report importance measures and system unavailability.
6.	Service and cooling water systems	SEP-III, 4.3	FT, SI	Report importance measures and system unavailabilities. Report identified dependences (system interactions).
7.	Ventilation systems (space coolers)	SEP-4.4 or TMI, II.K.3 (24)	FT, SI	Report importance measures and system unavailabilities.
8.	Reactor core isolation system (BWR)	SEP-3.2	FT	Report importance measures and system unavailability.

(*) ET = Event Trees
 FT = Fault Trees
 SI = Qualitative Importance Analysis
 HE = Human Errors

Table 7.1 (Continued)

No.	Regulatory Issue Title	NRC Program	PSA RELATED AREA*	COMMENTS
9	Emergency power supply for pressurizer (PWR) - Relief valves and - Block valves - Level indicators - Heaters	TMI, II.E.3.1 & TMI, II.6.1	FT	Report importance measures and system unavailability. Also report relationship with #2 of this list.
10	Pressurized thermal shock (PTS)	GI, A-49	ET	Report importance measures of accident sequences leading to PTS.
11	Long-term program plan for updating of procedures	TMI, I.6.9	ET, FT	Summarize procedure changes made during or because of the PSA.
12	System interactions	GI, A-17 SEP-4.9 SEP-4.6 SEP-5.1 SEP-7.1.2		Report all identified system interactions along with their importance measures.

Table 7.2 Task Outputs to be Provided with Reports*

Task	Subtask	Section in Guide	Output
Plant familiarization	Determination of function/system relations	3.4.1	List of frontline systems List of support systems Dependence tables or diagrams
	Determination of initiating events	3.4.2	List of LOCA break sizes List of interfacing system LOCAs List of LOCAs which affect mitigating systems List of transients applicable to the subject plant, including both generic and plant-specific transients List of transients initiated by support system faults faults which affect mitigating systems
	Determination of mitigating system requirements	3.4.3	Table giving LOCA mitigating systems, their success criteria, and reference to supporting documentation for success criteria. (Supporting documentation for success criteria less conservative than FSAR should be supplied in the Appendices.) Table giving transient mitigating systems, etc.
	Determination of initiating event groups	3.4.4	List of grouped LOCA initiating events List of grouped transient initiating events
	Review of operational data for multiple failures	3.4.5	List of events from NRC survey which are possible at subject plant Summary of how each pertinent multiple failure is reflected in the plant model or sensitivity study (available only at conclusion of study)

*This is a tabulation of task products which are to be supplied as part of the report. Some products are labeled "optional"; products not specifically labeled optional are required. In addition to these task products, certain other information is to be provided. This is discussed in Section 7.1. Not all of these products can usefully be printed (see Section 7.1.2.2.3).

Table 7.2 (Continued)

Task	Subtask	Section in Guide	Output
	Survey of regulatory	3.4.6	List of regulatory issues pertinent to subject plant [OPTIONAL]
Accident sequence definition	Event tree development	4.1	Functional event trees for LOCAs Systemic event trees for LOCAs Functional event trees for transients Systemic event trees for transients Documentation of dependences between function or systems which are displayed by omitted branch points in event trees Descriptions accompanying each event tree
	Fault tree development	4.2	List of assumptions made in the analysis List of different event tree conditions requiring different fault trees for each frontline system Description of each system giving system purpose, system configuration, system interfaces, instrumentation and control, testing and maintenance, applicable technical specifications, how the systems operate, and assumptions used in the analysis Fault trees for each frontline system, for each success criterion specified on event trees Fault trees for each support system developed for each supported frontline system List of component failure data needed (beyond those already available) List of basic events with definitions and (after completion of reliability data assessment task) generic and plant-specific quantification [FUTURE] For each component, information regarding its location and susceptibility to environmental effects

Table 7.2 (Continued)

Task	Subtask	Section in Guide	Output
			[FUTURE] For each system, tables relating dependences of each train and major component on each other and on other systems
	Human performance analysis (Note that recovery is treated in the baseline evaluation)	4.3.1	<p>List of human errors and screening probabilities for each</p> <p>List of ordered human errors based on importance</p> <p>List of potentially important human errors to be further analyzed</p> <p>List of sequence-specific human errors, quantified by plant-specific analysis, together with analysis and documentation for each risk-significant human error</p> <p>Explanation or documentation of methodology used in the plant-specific analysis</p>
	Qualitative dependence analysis	4.3.3 (cf.Fig.4.3) (cf.Fig.4.4)	<p>Failure modes and effects analyses for all frontline and support systems</p> <p>List of generic causative factors</p>
	Regulatory issues to qualitative dependence analysis [OPTIONAL]	4.3.3.4 (cf.Tab.4.5)	<p>Documentation of all discovered dependences (shared systems)</p> <p>Documentation of impact of shared systems on core damage probability and weak points, if any</p> <p>Documentation of component having potential to:</p> <ol style="list-style-type: none"> 1) cause LOCA outside containment 2) initiate an event with loss of mitigating systems 3) cause flow diversion affecting system success <p>Study of pipe break effects:</p> <ol style="list-style-type: none"> 1) identify importance core damage cutsets 2) identify locations of dominant systems and components 3) review these locations for possible pipe break impacts 4) document results and their risk significance

Table 7.2 (Continued)

Task	Subtask	Section in Guide	Output
Reliability data assessment and parameter estimation		5	
		5.8.1	Initiating events, frequencies (baseline and plant specific), recovery times and associated probabilities
		5.8.2	Component failure rates (baseline and plant specific), test and maintenance frequencies, and associated unavailabilities
Accident sequence quantification	Accident sequence	6	
	Boolean equations	6.1	Boolean equations for each accident sequence of each systemic event tree
	Accident sequence binning	6.2	Definitions of sequence bins: system and containment status for each bin Assignment of each sequence to a bin
	Sequence quantification	6.3	Importance ranking of potentially risk-significant human errors based on screening calculation Display, for each accident sequence, of each cutset before and after credit is taken for post-accident correction of misposition or actuation faults; indication of which faults are readily correctable, time available, and probability of failure to correct. Full documentation of recovery model. Point estimates of all accident sequence frequencies, core damage frequency, frequency of each accident sequence bin Ranking of accident sequences and assessment of dominance of accident sequences
	Uncertainty of plant-specific results	6.3.4	Characteristics of probability distribution of a) overall core damage frequency b) frequency of each accident sequence bin c) frequencies of accident sequences contributing to either the top 99% of total core damage frequency or the top 99% of any bin

Table 7.2 (Continued)

Task	Subtask	Section in Guide	Output
	Importance and sensitivity analyses	6.4	
	Importance	6.4.3,6.4.5	<p>List of important human errors for further study, together with specification of criterion of importance</p> <p>Display, for each accident sequence, of each cutset before and after credit is taken for post-accident correction of misposition or actuation faults, with indication of which faults are readily correctable and what is the probability of failure to correct</p> <p>Point estimates for all accident sequence frequencies, core damage frequency, and bin frequencies</p>
	Component sensitivity	6.4.4,6.4.5	<p>Dependence-suspect minimal cutsets, for each system, for each distinct mission; where change in system unavailability from a given type of coupling is more than a factor of 2, effect of that type of coupling on core damage frequency should be presented</p> <p>Description of defenses or conditions which serve to eliminate the dependences for these sensitive minimal cutsets</p> <p>Tabulation and discussion of single failures for each system</p>
	Human error sensitivity	6.4.4,6.4.5	<p>Dependence-suspect minimal cutsets, for each system, for each distinct mission</p> <p>Description of defenses, management, controls, or conditions which serve to eliminate the dependences between the human errors in the suspect minimal cutsets</p>

Table 7.2 (Continued)

Task	Subtask	Section in Guide	Output
Display and interpretation	Conservative	6.4.4,6.4.5	Tabulation of conservative assumptions, realistic alternatives, effects on core damage frequency of adopting realistic alternatives, accompanied by a description of the rationale and available data supporting the realistic assumption
		7	Comparison of plant-specific with baseline results Comparison of plant-specific results with other PRAs Comparison of baseline results with other NREP studies, if possible Presentation of special reporting requirements [OPTIONAL] comment on regulatory issues in Appendix A in light of plant-specific results

APPENDIX A

Treatment of Regulatory Issues

The objective of this appendix is to briefly outline the relationships and possible interactions of PSA and various regulatory issues as reflected in PSA. With the exception of some special reporting requirements outlined in Section 7 of this guide, the discussions in this appendix refer to optional tasks that could aid in the integration of several aspects of selected regulatory issues into a PSA study. Given the currently defined scope of PSA and the existing state of the art of probabilistic risk assessments as well as the technical resolution of some regulatory issues, the contents of this appendix are not to be interpreted as implying any additional requirements (beyond those outline in the main body of the guide) for a PSA study.

Several ongoing NRC programs include a number of safety-related issues which are applicable to operating plants. A number of these issues include aspects that strongly interact or overlap with items addressed (directly or indirectly) in a PSA study. These relationships fall into three major categories:

- (i) Information developed during the technical resolution of a regulatory issue could affect the results of a PSA study.
- (ii) The PRA model of a plant provides the means for assessing the risk significance of a regulatory issue or more specifically of a particular design or procedures change suggested for its resolution (i.e., implementation of a technical resolution).
- (iii) Information developed from the performance of a PSA study could provide part of the input necessary for the technical resolution of a regulatory issue.

A review of the (over 330) regulatory issues included in three major NRC programs

- (a) Systematic evaluation Program (SEP) Phase III,
- (b) Generic Issue program GI), and
- (c) TMI Action Plan (TMI)

identified 195 issues as addressable by PSA in its presently defined scope. These issues were further reduced by identifying the top 100 issues believed to have a more potentially significant impact on core damage frequency. The 100 issues were regrouped to eliminate overlapping between the three major NRC programs mentioned above and divided into three categories described below:

1. Issues That Can Provide Significant Input to a PSA

The regulatory issues in this category exhibit the issue - PSA relationship (i) mentioned above. Important information has been generated and documented as a result of the programs for the resolution of these issues. This

information can potentially affect the results of a PSA study and should, therefore, be considered for inclusion in the study. This category consists of issues that are "technically resolved" or that are very close to a technical resolution. It should be noted that "technical resolution" does not mean "implementation," and that inclusion of relevant information in the PSA study does not imply explicitly or implicitly any requirement for implementation.

The issues in this category are given in Table A.1, along with the relevant NUREG reports (or drafts). In addition, the issues in Table A.1 have been divided into groups according to the area of the PSA study that they affect. Examples of such issues are the ATWS issue (GI-A9, NUREG-0460) which affects the frequency of the initiating events and system success criteria and probability; and the DC - Power Supply issue (GI-A30, NUREG-0666) which affects the fault tree development of various systems.

2. Issues That Can Benefit From PSA Without Being Specifically Addressed

The regulatory issues in this category exhibit the issue - PSA relationships (ii) and/or (iii) mentioned above. These issues can benefit from a completed PSA study without requiring special modeling considerations or expansion of the currently defined scope in any way. These issues are given in Table A.2. Examples of such issues are the Upgrading of Operator Training (TMI-I.A.2), the Feedback of Operation Experience (TMI, I.C.5), and Integrated SEP Assessment (SEP-III, item 8).

3. Issues That Can Benefit From a PSA Study If They Are Specifically Addressed

The regulatory issues in this category exhibit the issue--PSA relationships (ii) and (iii) mentioned above. Several of these issues involve accident sequences or systems which are included in a PSA study. For others, additional modeling is required in the sense that additional accident sequences, failure modes, or components should be considered. All these issues require some type of additional effort to be included in the analysis or to identify their impact on the core damage frequency. Examples of issues in this category are the Containment Emergency Sump Performance (GI - A.43); the Swing Bus Design in BWR-4 (SEP-III, 4.8.3); and the Power supply to Pressurizer Relief Valves and Block Valves (TMI, II.G.1). A complete list of these issues is given in Table A.3, along with the areas of the PSA study that they affect. The incorporation of the relevant issues into a plant-specific PSA study is optional. One exception to this rule is the special reporting requirements outlined in Section 7 of this guide.

References

1. D. Ilberg and I. A. Papazoglou, On the Relationship between Regulatory Issues and Probabilistic Risk Assessments, BNL report, June 1984.

Table A.1 Issues of the NRC Ongoing Programs Which Can Provide Information Significant to the Conduct of the PSA Studies

A. <u>Issues affecting the determination of initiating events and their frequency:</u>	
<div>ISSUE TITLE</div>	<div>NRC PROGRAM</div>
1. Severe Weather Characteristics (Tornadoes, Snow, Ice Loads, Extreme Temp., Lightning, etc.). [Loss of offsite power and its duration]	SEP, 2.2.1
2.a Reactor Vessel Integrity. .b Reactor Vessel Material Toughness. .c Pressurized Thermal Shock. [Potential for reactor vessel failure]	SEP, 3.1 GI, A-11 GI, A-49
3. Steam Generator Tube Integrity. [Tube rupture coincident with LOCA]	GI, A-3, A-4 A-5
4. Classification of Systems. [Small LOCA frequency]	SEP, 4.1
5. Fracture Toughness of Steam Generator and Reactor Coolant Pump Supports (NUREG-0577). [Potential for a LOCA and coincident failure of mitigating systems]	GI, A-12
6. ATWS (NUREG-0460) [Frequency of initiating events]	GI, A-9
7. Evaluation of B/W plants-Feedwater Transients [where review is complete, it can be utilized in PSA]	TMI, II.E.5.1
8. B/W Reactor Transient Response (response to anticipated transients from ICS and NNI) (Vendor Reports)	TMI, II.E.5.2
B. <u>Issues affecting the determination of mitigating system requirements:</u>	
<div>ISSUE TITLE</div>	<div>NRC PROGRAM</div>
1. Short-Term <u>Accident</u> and Procedure Review.	TMI, I.C.1
2. Research on Small Break LOCAs and Anomalous Transients.	TMI, II.E.2
3.a Orders of B/W Plants (Item 20). .b Final Recommendations of B and O Task Force (e.g., recommendations 28, 29, 31, 44).	TMI, II.K.2 TMI, II.K.3
4.a ATWS (NUREG-0460). .b B/W Reactor Transient Response (response to anticipated transients from ICS and NNI) (Vendor Reports).	GI, A-9 TMI, II.E.5.2

Table A.1 (Continued)

<p>C. <u>Issues affecting the development of accident sequences event trees:</u></p> <p style="text-align: center;"><u>ISSUE TITLE</u></p> <ol style="list-style-type: none"> 1. The four issues listed under B above. [Analyses of plant response under transients and accidents] 2.a Mark II Containment Pool Dynamic Loads Long-Term Program (NUREG-0808). .b Determination of Safety Relief Valve Pool Dynamic Loads and Temperature Limits (NUREG-0802 draft). [LOCA with subsequent loss of ECCS heat sink] 3. Research on Phenomena Associated With Degraded Core. [Information useful to determine whether an event sequence should be considered leading to core melt] 	<p style="text-align: center;"><u>NRC PROGRAM</u></p> <p>GI, A-8</p> <p>GI, A-39</p> <p>TMI, II.B.5</p>
<p>D. <u>Issues affecting the fault trees (qualitatively and/or quantitatively):</u></p> <p style="text-align: center;"><u>ISSUE TITLE</u></p> <ol style="list-style-type: none"> 1. Revision of IE Inspection Program (more direct verification). [Surveillance tests and maintenance activities] 2. Short-Term Accident and Procedures Review. [Procedure changes resulting from post/TMI reviews] 3. Auxiliary Feedwater System Evaluation. [Factor into PSA AFW reliability analysis if already performed] 4.a Orders on B/W Plants (recommendations 9, 13, 14, 16, 19). .b Final Recommendations of B and O Task Force. (E.g., recommendations 1, 2, 3, 5, 7, 12, 16, 17, 18, 19, 21) 5. Adequacy of Safety-Related dc Power Supplies. [Information produced in GI resolution should be considered (NUREG-0666)] 6. Containment Emergency Sump Performance (NUREG-0897 draft, NUREG/CR-2403). [Information produced in GI resolution should be considered] 	<p style="text-align: center;"><u>NRC PROGRAM</u></p> <p>TMI, I.B.2.1</p> <p>TMI, I.C.1</p> <p>TMI, II.E.1.1</p> <p>TMI, II.K.3</p> <p>TMI, II.K.3</p> <p>GI, A-30</p> <p>GI, A-43</p>

Table A.1 (Continued)

7. Ice Condenser Containment.	GI, B-54
8. Passive Mechanical Failures.	GI, B-58
9. Review of (N-1) Loops Operation. [If other than full power operation is included in NREP scope]	GI, B-59
E. <u>Issues affecting reliability data assessment and parameter estimation:</u> <u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
1. Operational Safety Data Analysis. [Published data summaries of LERs for pumps, control rods, diesel generators, valves, and penetrations]	TMI, I.E.3
2. Information on Operating Experience - Foreign.	TMI, I.E.7
3. Human Error Rate Analysis.	TMI, I.E.8
F. <u>Issues affecting the analysis of human performance:</u> <u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
1.a Control Room Design Improved Instrumentation Research.	TMI, I.D.5
.b Accident Monitoring Instrumentation.	TMI, II.F.1
G. <u>Issues affecting the analysis of system interaction:</u> <u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
1. System Interaction.	TMI, II.C.3
2. Adequacy of Safety-Related dc Power Supplies. [Information produced in GI resolution (NUREG-0666)]	GI, A-30
H. <u>Issues Producing General Overall Guidance:</u> <u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
1. IREP	TMI, II.C.1

Table A.2 Issues for Which PSA Perspective is Gained Without Being Specially Addressed by PSA

<u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
Shift Technical Advisor.	TMI, I.A.1.1
Upgrading of Operator and Senior Operator Training and Qualifications.	TMI, I.A.2.1
Revise Scope and Criteria for Licensing Exams.	TMI, I.A.3.1
Operator Licensing Program Changes.	TMI, I.A.3.2
Long-Term Training Simulator Upgrade.	TMI, I.A.4.2
Loss of Safety Function Due to Personnel Error.	TMI, I.B.1.3
Regional Evaluations.	TMI, I.B.2.3
Procedures for Feedback of Operating Experience.	TMI, I.C.5
Operational Safety Data Analysis. [Plant-specific data evaluation produced in PSA study]	TMI, I.E.3
Reporting Requirements for Reactor Operating Experience	TMI, I.E.6
Human Error Rate Analysis. [Some original analyses produced in course of PSA study]	TMI, I.E.8 TMI, I.E.8
Quality Assurance, Expansion QA List.	TMI, I.F.1
Site Evaluation of Existing Facilities. [PSA provides PSA phase I for a site-specific full PSA study]	TMI, II.A.2

Table A.2 (Continued)

<u>ISSUE TITLE</u>	<u>NRC PROGRAM</u>
Training for Mitigating Core Damage.	TMI, II.B.4
Rulemaking Proceeding on Degraded Core Accidents.	TMI, II.B.8
Reliability Engineering (Guidance on Reliability Assurance).	TMI, II.C.4
Decay Heat Removal - Alternative Concepts Research.	TMI, II.E.3.4
Study of Control and Protection Action Design Requirements [How much, automatic initiation of ESF]	TMI, II.F.4
Classification of Instrumentation, Control, and Electrical Equipment.	TMI, II.F.5
Upgrade Licensee Emergency Support Facilities.	TMI, III.A.1.2
Liquid Pathway Radiological Control.	TMI, III.D.2.3
NRC Safety Decision Making.	TMI, IV.E
Improvement of Safety Rulemaking Procedures.	TMI, IV.G
Develop NRC Policy Statement on Safety.	TMI, V.1
Event Categorization.	GI, B-3
Locking Out of ECCS Power Operator Valves.	GI, B-8
Criteria for Safety-Related Operator Actions.	GI, B-17
Assessment of Failure and Reliability of Pumps and Valves.	GI, C-11
Integrated Assessment.	SEP, Phase III.8

Table A.3 Issues of NRC Ongoing Programs for Which Treatment by PSA Will Provide Risk Significance Insight or Input to Their Resolution Programs

A. Key to Symbols

- | | |
|-----------------------------------|---|
| 1) Plant Familiarization: | a = Functions, systems and their relations
b = Determination of initiating events
c = Success criteria of mitigating systems
d = Review of operational data for multiple failures |
| 2) Accident Sequences Definition: | ET = Event tree development
FT = Fault tree development |
| 3) Special Tasks: | HE = Treatment of human performance
SI = Treatment of system interactions (Qualitative Dependence Analysis) |
| 4) Relation with NREP: | (ii) = The PRA model of a plant provides the means for assessing the risk significance of the issue

(iii) = Information developed in the PRA study could help the technical resolution of the regulatory issue |

B. Notes

- (+) Some aspects of these issues are included in the present scope of a PSA study. Special reporting requirements exist for these issues. [See Section 7]

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION				ACCIDENT SEQ.				SPECIAL TASKS:	
			a	b	c	d	ET	FT	HE	SI	(ii) (iii)	
1	Reactor coolant pressure boundary Leakage Detection	SEP-III, 3.2 (SEP-II, V-5)		b				FT			+	1)Compare piping leakage probability to RCP seal failure probability. 2)Determine whether it needs be considered in the fault tree analysis. 3)Document risk significance of this issue.
2	Water Hammer	GI, A-1 (SEP II, V-13)		b			ET	FT			+	1)Familiarization with past events (NUREG/CR-2059). 2)Include relevant branches on ET and FT. 3)Use bounding assumptions for incurred damage. 4)Document impact on plant risk (bounds).
3	Pressurized Thermal Shock (+)	GI, A-49					ET		HE		+	1)Identify important event sequences leading to pressurized overcooling of pressure vessel. 2)Assess the effect of operating procedures & the potential for operator errors on the potential frequency of these events. 3)Document results of these tasks. 4)Document significance of these sequences relative to core melt prob.

1) Compare piping leakage probability to RCP seal failure probability.
2) Determine whether it needs be considered in the fault tree analysis.
3) Document risk significance of this issue.

1) Familiarization with past events (NUREG/CR-2059).
2) Include relevant branches on ET and FT.
3) Use bounding assumptions for incurred damage.
4) Document impact on plant risk (bounds).

1) Identify important event sequences leading to pressurized overcooling of pressure vessel.
2) Assess the effect of operating procedures & the potential for operator errors on the potential frequency of these events.
3) Document results of these tasks.
4) Document significance of these sequences relative to core melt prob.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM Issues Mainly Related to Initiating Events & Event Sequences	RELATED PSA AREAS							RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS	
			PLANT FAMILIARIZATION				ACCIDENT SEQ.					SPECIAL TASKS:
			a	b	c	d	ET	FT	HIE			
4.a	Isolation of High & Low Pressure Systems (+) - High Pressure/Low Pressure Interface Requirements for Isolation - RHR Interlock Requirements	SEP-III, 4.6 (SEP-II, V-11.A) (SEP-II, V-11.B)	a	b		d	ET	FT	HIE	SI	+	1) Include these issues in the plant familiarization subtasks. 2) In developing ET & FT, consider LOCA outside containment & CMF of redundant trains of safety systems (e.g., flow diversion). 3) Consider human factors surveillance & maintenance. 4) Document both the results of the tasks & the general risk significance.
4.b	Isolation of Low Pressure Systems Connected to the Reactor Coolant Pressure Boundary	61, B-63										
5.a	Feedwater System Transients	SEP-III 7.4 (SEP-II, XV-1)	b				ET				+	1) Assess frequency of these transients in particular plant. 2) Use bounding assumptions for possible impact (thermal shock, SE tube rupture). 3) Document general risk significance of this issue & potential modifications to reduce challenges.

1) Include these issues in the plant familiarization subtasks.
 2) In developing ET & FT, consider LOCA outside containment & CMF of redundant trains of safety systems (e.g., flow diversion).
 3) Consider human factors surveillance & maintenance.
 4) Document both the results of the tasks & the general risk significance.

1) Assess frequency of these transients in particular plant.
 2) Use bounding assumptions for possible impact (thermal shock, SE tube rupture).
 3) Document general risk significance of this issue & potential modifications to reduce challenges.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS	
			PLANT FAMILIARIZATION				ACCIDENT SEQ.				SPECIAL TASKS:
			a	b	c	d	ET	FT	IE	SI	(11) (111)
5.b	Issues Mainly Related to Initiating Events & Event Sequences										
	Evaluation of B/W Plants-Feedwater Transients	IMI, II.E. 5.1									
6	Reactor Coolant System Vents	IMI, II.B.1	b				ET	FT			+ 1) Estimate failure probability of vents 2) Include vents in ETs & FTs & differential between sequenced for which it is beneficial & those caused by its inadvertent failure. 3) Document risk reduction contribution of reactor coolant system vents implementation.
7	ATWS (+)	GI, A-9	a	b			ET	FT			+ 1) Familiarization with information developed in course of the resolution of this issue (NUREG-0460). 2) Include specific fixes proposed for the plant when developing event trees & fault trees. 3) Document risk reduction potential of plant-specific fix implementation.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS					RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS
			a	b	c	d	ACCIDENT SEQ. ET FT	SPECIAL TASKS: HIE SI	(II) (III)	
1	Issues Related to Power Supply									
	Adequacy of Offsite Power Systems (+)	GI, A-35				d	ET FT		+	1) Review plant-specific experience. 2) Assess probability of loss of offsite power for various time periods. 3) Consider offsite power system reliability when evaluating following issues. 4) Document risk significance of loss of offsite power for various durations.
2	Emergency Power Supply to ESEs (+)									1) Review plant-specific experience of diesel failures. 2) Assess diesel-generator system reliability including support systems, status information in control room, maintenance, etc.
2.a	Emergency AC Power Systems 1) Diesel Generators 2) App.k, Electrical Inst. & Control (EIC) Review	SEP-III, 4.8.1 (SEP-II, VII.2) (SEP-II, VI.7.C.1)								3) Review dependences of ESF on EIC & include in the reliability analysis single failures that can fail redundant ESFs. 4) Document risk significance of the reliability of emergency power to ESFs.
2.b	Diesel Reliability	GI, B-56								
2.c	Swing Bus Design BUR4	SEP-III, 4.8.3 (SEP-II, VII.7)								1) Review dependences in swing bus automatic transfer circuitry. 2) Include dependences

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS					RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS			
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:				
			a	b	c	d	ET	FT	IE		SI	(ii)	(iii)
	Issues Related to Power Supply												
3	Emergency dc Power Systems:(+) 1)dc power system bus voltage monitoring & annunica- tion	SEP-III, 4.8.2 (SEP-II, VIII.3.B) (SEP-II,VI .7.C.1)	a			d		FT			SI	+ +	& modifications per- formed in ac power re- liability analysis. 3)Document impact of swing bus on ac power reliability (& impact of fixes). 1)Review plant-specific experience of dc power failures. 2;Use input from GI,A-30 resolution. 3)Assess dc power system reliability including support systems, inter- facing loads, mainte- nance, communication,etc. 4)Document adequacy of status information to the oper. & risk signifi- cance of dc power system.
4	Station Blackout(+)	GI,A-44						ET				+ +	1)Use information devel- oped by the above tasks. 2)Use reliability anal- ysis of non-ac driven systems (turbine, dedicated diesels, etc.). 3)Include event sequences of station blackout. 4)Document prob. of melt- down due to station blackout by all signifi- cant event sequences & identify existing weak points (list most import- ant cut sets for this issue).

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREA						RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS	
			PLANT FAMILIARIZATION				ACCIDENT SEQ.				SPECIAL TASKS:
			a	b	c	d	ET	FT			
	Issues Related to Power Supply										
5	Non-Safety Loads on Class 1E Power Sources	GI, A-25						FT	+		1) Include fault trees prepared for the ac & dc power systems discussed above. 2) Document risk significance of this issue.
6	Power Supplies for Pressurizer Relief Valve, Block Valves, & Level Indicators. (+)	IMI, II. G.1						FT	+		1) Include relevant FTs. 2) Document risk significance of this issue.
7	Emergency Power for Pressurizer Heaters (Reliability of natural circulation). (+)	IMI, II. E.3.1						FT	+	+	1) Include relevant FTs. 2) Document reliability for use in decay heat removal system reliability analyses.

Table A.3 (Continued)

			RELATED PSA AREA								RELATIONSHIP WITH PSA		
SEQ. NO.	TITLE ISSUE	NRC PROGRAM	PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:			COMMENTS ON POSSIBLE TASKS	
			a	b	c	d	ET	FT	HE	SI	(ii) (iii)		
	Issues Mainly Related to Control & Protection Systems												
1	Reactor Protection System & ESF Isolation (++)	SEP-III, 5.1				d		FT		SI	+	1) Include SI study & document results on dependences if found, & their risk significance.	
1.a	Isolation of RPS From Non-Safety Systems	(SEP-II, VII.1.A)											
1.b	ESF Control Logic & Design (dependences review)	(SEP-II, VII.2)											
2	RPS & ESF Testing:	(SEP-III, 5.2)				d		FT	HE		+	1) Document adequacy of test scope & frequency as revealed from the NREP study.	
2.a	Testing of Reactor Trip System & ESF, Including Time Testing	(SEP-II, VI.10.A)											
2.b	ECCS Actuation System (testability & adequacy)	(SEP-II, VI.7.A.3)											

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION				ACCIDENTY SEQ.		SPECIAL TASKS:				
			a	b	c	d	ET	FT	HE	SI		(ii)	(iii)
	Issues Mainly Related to Control & Protection Systems												
3	Safety Implication of Control Systems (++)	G1,A-47	a	b				FT	HE	SI	+	+	1)Evaluate SG overfill transient (PWR) & reactor overfill transient (BWR) which result from control system failures. 2)Evaluate control system failures leading to reactor overcooling transients (input to pressurized thermal shock). 3)Evaluate (all other) significant event sequences. 4)Document results of control system implications & risk significance of these.
3.a	FMEA on B/W ICS Systems	TMI,II.K.2 (9)											
3.b	Procedures to Control AFW Independent of ICS	TMI,II.K.2 (2)											
3.c	Several Items of List	TMI,II.K.3											

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS								RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:		(ii)	(iii)	
			a	b	c	d	ET	FT	HE	SI			
	Issues Mainly Related to Decay Heat Removal Systems												
1	Cooldown & Long-Term Heat Removal Capability (+)												
1.a	Shutdown Systems (RIIR reliability-cooldown with safety grade equipment & single failure)	SEP-III, 4.2.1 (SEP-II, V. 10.B)	a	b	c	d	ET	FT	HE	SI	+	+	1)Familiarization should cover all safety & non-safety systems that can be used to remove decay heat. 2)ETs for full power operation as well as for modes 2-5 operations (hot standby hot & cold shutdown, etc.) may be developed. 3)This task addresses plant as is, & FTs should be developed on the basis of existing systems procedures, surveillance, safety grade classification, etc.(CCW,ESW,AFW, UHS & also other systems may be considered). 4)Document reliability of: -cooldown -cold shutdown for various time periods a)using safety grade equipment b)using applicable equipment
1.b	RIIR Shutdown Requirements	GI,A-31											

1)Familiarization should cover all safety & non-safety systems that can be used to remove decay heat.
 2)ETs for full power operation as well as for modes 2-5 operations (hot standby hot & cold shutdown, etc.) may be developed.
 3)This task addresses plant as is, & FTs should be developed on the basis of existing systems procedures, surveillance, safety grade classification, etc.(CCW,ESW,AFW, UHS & also other systems may be considered).
 4)Document reliability of:
 -cooldown
 -cold shutdown for various time periods
 a)using safety grade equipment
 b)using applicable equipment

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION a b c d				ACCIDENT SEQ. T FT		SPECIAL TASKS: HE SI			(ii) (iii)	
	Issues Mainly Related to Decay Heat Removal Systems												
1.c	Shutdown Electrical Inst. & Control (Reactivity Control Systems & Shutdown Cooling Systems).	SEP-III,4.2.2 (SEP-II, VII.3)	a	b	c	d		FT	HE	SI	+	+	5)Document additional surveillance & procedures for non-safety-grade systems, if upgraded reliability is required. 1, 2, 3, as above. 4)Document reliability of: -cooled from outside the control room(remote shutdown & cooldown) -cooldown using safety grade equipment -cooldown using non-safety-grade equipment 5)As above & whether additional automatic initiation may be effective.
1.d	Further Staff Consideration of Need for Diverse Decay Heat Removal Method Independent of SGs (PWR).	TMI,II.K.3.(8)									+		1)Document the need, based on risk significance gained in the study of the above issues.
2	Shutdown Decay Heat Removal Requirements	GI,A-45											

Table A.3 (Continued)

			RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
SEQ. NO.	TITLE ISSUE	NRC PROGRAM	PLANT FAMILIARIZATION a b c d				ACCIDENT SEQ. ET FT		SPECIAL TASKS: HE SI			(ii) (iii)	
	Issues Mainly Related to Decay Heat Removal Systems												
2.a	Assess Adequacy of DHRS in "Existing" LWR's	(GI,A-45 & TMI,II.E. 3.2 TMI,II.E. 3.3)	a	b	c	d	ET	FT	HE	SI	+	+	1)Subtask 2a is equivalent to task 1 above. 2)Document which DHRS system or function requires improvement, if any, for all relevant modes of operations. 3)Provide general risk significance on proposed modifications if any required.
2.b	Develop Means to Improvements of DHRS	(As above)									+		

1) Subtask 2a is equivalent to task 1 above.
 2) Document which DHRS system or function requires improvement, if any, for all relevant modes of operations.
 3) Provide general risk significance on proposed modifications if any required.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:				
			a	b	c	d	ET	FT	HE	SI		(ii)	(iii)
	Issues Related to Safety System Relia- bility Analysis												
1	Auxiliary Feedwater System Ev- aluation(+)	TMI,II.E. 1.1											1)Perform AFW reliability analysis. 2)Compare to reliability allocation goal of SRP 10.4.9
1.a	Reliability Analysis	TMI,II.E. 1.1	a	b	c	d		FT	HE	SI	+	+	3)Document results & proposed modifications with their risk reduc- tion significances.
1.b	Initiation & Flow (Automatic	TMI,II.E. 1.2				d		FT	HE		+		4)Evaluate impact of automatic initiation in terms of risk signifi- cance. 5)Review reliability of control & actuation to AFW & verify that no single failure depend- ences exist & no inter- ference with manual corrective action.
2	ECCS Re- liability (+)												1)Perform ECCS reliabi- lity analysis 2)Include experience with ECCS actuation
2.a	Reliance on ECCS	TMI,II.E. 2.1	a			d		FT	HE	SI	+	+	3)Document results: a)Reliability b)Modification if re- quired & their signifi- cance
2.b	Allowable ECCS Equip- ment Out- age Periods	GI,B61(TMI II.K.3(17)				d		FT					c)Allowable ECCS equip- ment outage periods.

Table A.3 (Continued)

			RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
SEQ. NO.	TITLE ISSUE	NRC PROGRAM	PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:				
			a	b	c	d	ET	FT	HE	SI		(ii) (iii)	
	Issues Related to Safety System Reliability Analysis												
3	Service & Cooling Water (+) Systems	SEP-III,4.3 (SEP-II,IX.3)	a			d		FT	HE	SI	+	+	1)Perform System reliability analysis. 2)Include consideration of separation, water makeup, interfaces with other systems. 3)Document results, proposed modifications if required & risk significance.
4	Ventilation Systems (+)	SEP-III,4.4											1)Include ventilation system in ETs & FTs development.
4.a	Containment Heat Removal	(SEP-II,IX-5)						FT			+	+	2)Perform an SI analysis of space coolers failure.
4.b	Room Coolers (space coolers)	(SEP-II,IX-5;TMI,II.K.3(24))								SI			
5.a	Containment Isolation System	SEP-III,7.2 (SEP-II,VI-4)	a				ET	FT			+		1)Perform system reliability analysis. Include sump lines, fluid system penetration isolation after refueling or purging operation, etc.
5.b	Isolation Dependability	TMI,II.E.4.2	a				ET	FT		SI			2)Include containment isolation in ETs & FTs. 3)Perform analysis of isolation initiating signals & control & verify their redundancy diversity & reliability.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED 'PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:			(ii)	(iii)
			a	b	c	d	ET	FT	HE	SI			
	Issues Related to Safety System Relia- bility												
6	Containment Emergency Sump Performance	GI,A-43					ET	FT			+	1)Include system on ETs and FTs. 2)Use information pro- duced in GI resolution. 3)Document risk signifi- cance of sump failure due to its potential failure modes(entrained air,vortexing,losses, blockage by debris)	
7	Hydrogen Control Measures & Effects of Hydrogen Burns on Safety Equipment	GI,A-48					ET	FT		SI	+	1)Include dependence of safety equipment on hydrogen burns for rel- evant accident sequen- ces. 2)Provide bounding cal- culation with/without this effect. 3)Document potential risk significance of this effect.	
8	Reactor Core Isola- tion Cool- ing System (BWR) (+)	SEP-III,3. 3 (SEP-II,V. 9)					ET	FT			+	+	1)Include this system on small break LOCA & transients ETs. 2)Assess system reliabil- ity. 3)Assess impact of sys- tem on risk reduction. 4)Document results & upgraded surveillance & outage procedures if up- grading required.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION a b c d				ACCIDENT SEQ. ET FT		SPECIAL TASKS: HE SI			(ii) (iii)	
	Issues Related to Safety System Relia- bility												
9	Ice Conden- ser Con- tainment (PWRs)	GI,B-54					ET	FT			+	1)Include ice inventory availability where rel- evant on ETs & FTs. 2)Assess availability of ice inventory. 3)Document risk signifi- cance of issue & sur- veillance requirements if upgrading is needed.	
10	Review of (N-1) Loop Operation in BWRs & PWRs	GI,B-59	a	b	c		ET	FT	HE	SI	+	+	1)Evaluate frequency of (N-1) loop operation. 2)Include changes in most affected ETs & FTs for this mode of opera- tion. 3)Assess allowable per- iods of (N-1) loop opera- tion without affecting core melt probability in a significant manner. 4)Document results.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED TO PSA						RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS		
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:			(ii)	(iii)
			a	b	c	d	ET	FT	HE	SI			
	Issues Related to Sub-Systems & Components Reliability Analysis												
1	Recirculation Loop Isolation (BWRs) (Surveillance required recirc. pumps & discharge valves)	SEP-II, 4.7.2 (SEP-II, III.10.C)						FT			+	1) Include this in FTs development & quantification. 2) Document risk significance of this issue.	
2	Coolant Loop Isolation Valve Closure (PWR)	SEP-III, 4.7.3 (SEP-II, VI.7.C.3)						FT			+	1) Include the isolation valve failure modes on the relevant FTs. 2) Document risk significance of this issue.	
3	BWR CRD Mechanical Failure (Collet Housing)	GI, B-48						FT			+	1) Include collet housing cracking failure mode in the relevant FTs. 2) Document risk significance of collet housing failure.	
4	Improved Reliability of Target-Rock Safety Relief Valves	GI, B-55						FT			+	1) Include these specific valves on relevant FTs. 2) Use plant-specific data for their failure rate as much as possible. 3) Document risk significance of this issue.	

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREA							RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS	
			PLANT FAMILIARIZATION				ACCIDENT SEQ.					SPECIAL TASKS:
			a	b	c	d	ET	FT	HE			
1	Automatic ECCS Switch over	SEP-III.4. 7.1 (SEP-II, VI.7.B)							FT	HE	+	1)On event sequences where ECCS switchover is included, identify other cognitive-type require- ments for operator inter- vention. 2)Estimate reliability of ECCS switchover as is & if more automation is used. 3)Estimate time gained for the other cognitive- type operator actions & their impact, if more automations are used in switchover. 4)Document benefit of automatic switchover, if it exists, in terms of reduced core melt prob- ability.
2	Long-Term Program Plan for Updating of Procedures (+)	IMI, I.C.9							FT	HE	+	1)Document any upgrading of procedures found to be beneficial in course of study.
3.a	Safety Sys- tem Status Monitoring	IMI, I.D.3							FT	HE	+	1)Verify that important systems & valves, in term of contribution to core melt probability, have an adequate status indication.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS								RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:		(ii)	(iii)	
			a	b	c	d	ET	FT	HE	SI			
	Issues Related to Human Performance Analysis (require such an analysis or can benefit from)												
3.b	Relief & Safety Valve Position Indication	TMI, II.D.3											2) Quantify benefits of adding safety system status monitoring in control room. Take into account operator corrective actions.
3.c	Operability status of Safety Systems & ESF Valves	(TMI, II.K. 1 items 5, 10)											3) Document benefits if such exist, & list systems & equipment that should be considered for status monitoring.
4.a	Plant Safety Parameter Display Console	TMI, I.D.2					ET	FT	HE	SI	+	+	1) Perform a cognitive human performance analysis for significant event sequences. 2) Identify plant safety parameters & type of instrumentations which have a potential to reduce errors.
4.b	Additional Accident Monitoring Instrumentations	TMI, II.F.1											3) Review procedures for recovery from conditions leading to inadequate core cooling.
4.c	Identification of & Recovery from Conditions Leading to Inadequate Core Cooling	TMI, II.F.2											4) Document results of this task, & its risk significance.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS							RELATIONSHIP WITH PSA	COMMENTS ON POSSIBLE TASKS	
			PLANT FAMILIARIZATION				ACCIDENT SEQ.		SPECIAL TASKS:			
			a	b	c	d	ET	FT	HE	SI	(II)	(III)
4.d	Issues Related to Human Performance Analysis (require such an analysis or can benefit from)											
	Describe R. V. Level Indication for Automatic Manual Initiation of Safety Systems	IMI, II.K.1 (23)										

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM Issues Mainly Related to System Interaction	RELATED PSA AREAS					RELATIONSHIP WITH PSA		COMMENTS ON POSSIBLE TASKS
			PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET FT	SPECIAL TASKS: HE SI			(II) (III)		
3.c	Pipe Break Effects on Structures	SEP-III, 7.1.3 (III.5.B)								
4	Passive Mechanical Failures (+)	GI, B-58		FT	SI			+	+	1) Using SI methodology identify those valves in which passive failure could be more important than in other valves. 2) Include those valves on FIs. 3) Assess the level of the passive failure rates at which they have an impact on core damage probability.

APPENDIX B

TQA Plan Discussion and Exemplification

B.1 General Considerations

The "technical quality" of a PSA involves not only its intrinsic technical content, but also its formal structure, its consistency with its objectives, its tractability for possible applications, and its scrutability and perspicuity. Thus, both the correct and orderly execution and the disciplined and systematic conduct of the PSA are needed to ensure its technical quality, and "TQA" cannot, therefore, be regarded as a purely retrospective or simply formal activity. When PSAs are carried out with such an integrated form of QA, their results may be considered on individual, comparative, and unified bases, and so can contribute to a more comprehensive and deeper understanding of the characteristics of both individual plants and plants as a whole, and thus allow enhanced intra- and inter-plant perspectives and insights.

The purpose here is to exemplify the specifications and requirements for a typical TQA program which could be used in the production of a plant-specific PSA. The references cited below (B.6), as well as a number of others, give adequate definitions, descriptions, and qualitative requirements to serve as a resource base for developing a TQA program. This section gives more specific recommendations for establishing a TQA program, and describes the particulars for verifying its credibility.

The major requirements and characteristics of a PSA have been outlined in Section 2.2. The associated and integrated TQA program sets up the formal framework (i.e., standard guidelines, verifying checks, and recommended practices) to guarantee that the estimates so produced will satisfy this aim, will be quantitatively, qualitatively, and conceptually correct, and will be in a scrutable and perspicuous format.

The reviewers will thus be able to determine the bases for the quantitative estimates, and to examine their underlying assumptions. Compatibility of the various methods should be verified and assured, particularly in regard to external events.

The reviewers can then assume (and verify) that the calculations involved have no fundamental or significant errors, and are consistently performed with the best methods and computational tools available. They will be able to duplicate (as necessary or desired) the calculations used to establish the risk estimates, and to examine and confirm the conditions under which expert judgment was used to assess more subjective factors in the risk estimate.

The above is not an inflexible condition. The use of TQA procedures and controls clearly entails additional costs and resource commitments for the PSA, and these increases should be commensurate with the anticipated use of the analyses. For example, an analysis which is to be used for order of magnitude assessments such as those needed for project prioritization and schedule planning, requires less stringent TQA procedures and guidelines than one used to provide technical support for utility evaluation of a generic issue or a suggested regulatory modification. In view of the many intended

uses for PSA models and results, the associated TQA program ought to be sufficiently flexible to be applicable to work which is "safety related" and documented as such in the regulatory record of the licensee. It must, however, be emphasized that this flexibility refers mainly to the formal aspects of the TQA program. Those features of TQA which are integral with the substantive work of the PSA apply across the board.

This guide offers substantial detail in terms of the required form and substance of the output of a plant specific PSA (see subsection 2.2.1). The TQA program ensures that these requirements are met and that the results will be accurate, scrutable, and reproducible. Three areas which require standard guidelines and verification (authentication) are as follows:

1. Personnel: A general discussion of personnel requirements for PSA has been given in subsection 2.2.2. The important TQA requirements include those for demonstrating project team adequacy. A crucial feature must be the recognition by the PSA project team of the role and importance of TQA, and the TQA program must therefore, in turn, be adapted to needs, desires, and orientation of the (qualified) PSA team. The TQA sub-organization which implicitly or explicitly accompanies the PSA activity must, therefore, be thoroughly coordinated with it, without, however, being completely amalgamated with it. Some personnel overlaps may be permitted, provided that they do not involve "conflict of interest."

2. Technical Work: Probabilistic estimates can be made using a variety of approaches, models, and calculational methods. When the assumptions for application, conditions for decision, and classification and data manipulation are included, the result is an almost unlimited set of possible varied calculations between projects. The TQA program is not intended to circumscribe the associated technical scope and methods of execution. It is, however, a fundamental requirement of the TQA program to describe the technical basis for the project in sufficient detail (and with enough clarity) to be verified by interested reviewers.

3. Documentation: The major documentation of a PSA is usually thought to be the project report. While this report can provide a substantial amount of information, it does not necessarily establish a clear path by which calculations can be checked and verified. If it did, it would probably be useless as a communication tool. This guide describes reporting requirements and recommendations for reporting format. The TQA program provides a basis for ensuring that the accuracy of the data and the calculations are supported and can be verified in such a way that reviewers can clearly identify the nature of any disagreements.

B.2 Formal TQA Requirements

1. A published procedure which describes, in detail, the organization of the PSA project, including the key participants, the models, calculational procedures and codes used, and the basis for internal checks and reviews. Since this document authenticates the ensuing work, it should typically be of the form shown in B.3 below, filed with the responsible reviewers, and retained by the project group. It should be updated by published revisions as modifications in the calculational procedure are introduced. As well as describing the methods for calculating risk estimates, this

procedure will indicate the treatment of missing information and references, non-repeatable results, and unclear (or ill-defined) assumptions. By following the so described procedures, the reviewers should be able to repeat and check all fundamental calculations performed in the PSA.

2. A TQA organization which performs checks and verifications of calculations made on the project is responsible for identifying additional calculational and documentation requirements, and resolves TQA concerns during the course of the project. This organization need not be large: a single coordinator may be designated for the project. The crucial point is that internal reviews and checks be made by qualified staff who are different from those persons performing the "project" calculations, and that the project results be formally accepted by key members of the project organization. The basis for establishing the TQA organization, together with the associated responsibilities and technical duties should be described in the initial PSA project procedure. A model for such an organization and the required experience levels is given in B.4 below. It should be noted that the TQA activities tend to "punctuate" the general flow of the PSA; therefore, they should be planned to do this in a strategically and tactically efficient the economical manner (see the remarks in 2.2.1). Further, it may be noted that these activities are in the nature of an internal interactive review: their extension to external review is discussed in section 2.4.
3. A defined set of analytical tools and computational programs which are to be used on the project. The basis for the acceptance of computer codes should be stated, referenced, or agreed on in advance with responsible reviewers. Calculational tools and this basis for use in the PSA must be fully defined in the project procedures.
4. A calculational file which documents the calculations, supporting data, and underlying calculational assumptions used in the production of risk estimates. This file provides the only complete record of project results which is available at a later use to fill in missing information and to verify the progress of calculations made on the project. Because of the huge amount of data and information involved, it may not be feasible to store it completely. However, the input data sets must be included or referenced, with deviations and changes explained (justified). Revisions should be scrutable and explained. For example, in a fault tree analysis, the supporting system description should be given, together with dependence and intertie diagrams, included failure modes and their rationale, quantifying data and manipulation techniques, output cutsets and value uncertainty measures, and sensitivity data. Changes should be identified clearly as inserts or overlays if previous versions of the calculations have been released. Finally, the check and verification record should be shown to establish responsibility and ~~verification~~ for meeting additional information needs of the reviewers. ~~This file~~ should be tailored to make the significant information most accessible. Brief presentations of assumptions, data, and results at the front would be helpful (but are not mandatory). To the extent possible, the calculational file should include the relevant computer files in a form amenable to the resolution of calculational errors and questions regarding assumptions and data. The PSA report is intended to communicate and the calculational file should

support the the communication in a reasonably complete and accessible way. Computational file specifications are given in B.5.

B.3 TQA Plan Procedure

This section outlines the form and content of the published procedure which describes the organization and operation of the TQA activity. Several preliminary remarks are in order:

- This document is to be current and up-to-date (i.e., a so-called "living" document).
- It should be filed initially with the Project Organization, the Review Organization, and the Regulatory Agency (if separate).
- It should be updated (and the revisions appropriately distributed), whenever
 - substantive changes are made;
 - major submittals are made; and
 - at regular predetermined intervals.
- If all the criteria described below are met, the document itself need not be subject to further review.
- The activities described are to be completed on a published schedule coordinated with determined major submittal dates.

Explanatory comments are included below where further clarification seems desirable.

B3.1 Project Scope

B3.1.1 Overall Mission: This section establishes the utility's concept of the purpose which the PSA is to serve, and its relation to regulatory, operational and other requirements.

B3.1.2 Specific Objectives: Here consideration should be given to particular objectives of the PSA (e.g., streamlined technical specifications, altered LCOs, etc.) in order to focus the assessors' and reviewers' attention, and enhance the clarity and credibility of the final result.

B3.2 Project Organization and Staffing

B3.2.1 Project Level Functional Requirements: This section defines the technical coordination requirements at the project engineer level, to enable the proper direction and management needed for the successful execution of the PSA. Multiple responsibilities may be assigned to a single individual, but all functions identified should be manned by utility personnel or contracted surrogates. The designated individuals will have "sign-off" authority on calculations and documentation, and a report will be produced for each category.

At a minimum these coordination categories should include the following:

- systems design - involving plant design knowledge of systems and operator safety, systems performance analyses, maintenance and testing requirements, systems interactions and dependences, and "as-built" vs. documented differences.
- plant operational data - involving the collection, assimilation, analysis and use of plant data to support the PSA calculations (including operational data, scrams, outages, LCOs, "trending", etc.).
- plant specific PSA models - this includes responsibility for all probabilistic models and calculations intended to reflect the risk profile for the plant considered.
- thermal hydraulics and containment physics - this comprises all calculations of minimum success criteria and containment performance associated with various accident sequences.
- computational tools - this involves responsibility for the procurement, coordination, integration and validation of all computer software used to perform calculations and to store models and data used in the PSA, and for maintaining the calculational file and the capacity for subsequent and ongoing calculations by the utility.
- TQA - this function is responsible for submitting and updating the project plan and for all project review activities (except code validation), as well as for resolution of documentation and calculational file-related problems with the reviewers (and other users of the PSA). (See also B3.5 below.)

B3.2.2 Staffing: The utility will submit the expected staffing for the key functional positions with the guidance already provided. This staff is to appear (i.e., sign-off) on all official acceptance sheets for the project.

B3.2.3 Management and Reporting Interfaces: The utility will identify the management hierarchy and other specifics which define the overall project control and validation, and the various organizational interactions both within the utility and with outside contractors, if any.

B3.2.4 Training: The utility will identify the process by which (a) all the project staff described in B3.2.2 and B3.2.3 above are familiarized with the project objectives, responsibilities and procedures, and (b) technology transfer is made to the extent needed to ensure total utility involvement in the execution of the PSA and capability to use the results properly.

B3.3 Methodology

B3.3.1 Specific Techniques and Elements of Project Methodology

- Basis for probabilistic analysis methods (e.g., ET/FT, "G0", other models)
- Scope and emphasis

- Flow chart emphasizing accountability for different types of calculations.

B3.3.2 Assessment of Adequacy of Specific Models and Calculations

- Treatment of dependencies in event sequences
- Identification of major contributors
- Identification of contributors in GO models
- Treatment of interactions

B3.3.3 Functional Information Requirements for Methodology

- Flow charts

B3.3.4 Computational Tools

B3.3.5 Maintenance and Utilization Tools (including data-base query systems) This is optional for future utility applications.

B3.4 Documentation

B3.4.1 Reporting Requirements

- Document types and purposes
- TQA requirements

B3.4.2 Calculational File (see B.5)

- Contents (types of calculations)
- Organization
- Maintenance for TQA

B3.5 TQA Organization

B3.5.1 TQA Objectives

B3.5.2 TQA Methods

- types of PSA information generated;
- manner of information generation, checking and maintenance;
- software (algorithms and processing routines) validation and utilization;
- checking of software data.

B3.5.3 TQA Responsibilities

- key participants
- functional activities (responsibility matrix) (see B.4)
- communications (to ensure that information is correctly handled internally and that the key functional responsibilities have sufficient current information available to perform their tasks)

B.4 Responsibility Matrix

This section indicates in a schematic way, i.e., in the form of a matrix, the relation between the project staff and the activities and documents with which they are involved. This format enables a clear and immediate view of what is (or should be) going on, and serves to identify gaps, overlaps, and tenuous or illogical connections.

The rows of this "responsibility matrix" list the various project participants as described in Section B3.2 above, i.e.,

TQA Manager/Coordinator
Project Engineer 1

Project Engineer n
Checker 1

Checker m
Functional Coordinator 1

Functional Coordinator k
PSA Project Manager
Responsible Utility Manager
etc.

The columns of this matrix list the various activities and documents involved, i.e.,

data acquisition
data revision
model construction
analytic calculation
computer calculation
plans

schedules
reports
etc.

The matrix entries then describe what (if anything) a given participant does in relation to a given activity. A partial example is given in the table (matrix below). For reasons of space the entries are coded by letters, which are described below.

	<u>System</u> <u>Calc.</u>	X	<u>Data Acq.</u>	<u>Report</u>	<u>System</u> <u>Schedule</u>	X
QA Mgr.				G		
Proj. Engr. 1	B		A			
.						
.						
Checker 2	C					
.						
.						
Coord. Engr. 3	D			E		
.						
.						
PSA Mgr.				F	I	
Utility Mgr.				H	I	

A: obtains appropriate data
 B: performs calculation
 C: checks data and calculation
 D: verify compatibility with
 E: prepares partial report
 F: integrates partial reports
 G: reviews and modifies report
 H: stays awake at presentation
 I: discusses schedule revision

B.5 Calculational File Requirements

B5.1 Types of Information Covered

- hard copy data bases
- data bases stored as computer files
- model descriptions
- analysis calculations
- computer printouts

B5.2 Acceptance Requirements

- calculation file documentation cover sheet, as follows:
 - document title, data and version
 - document author and checker (if applicable)
 - type of calculation (cf. B1.3)
 - purpose of calculation (cf. B1.3.3)
 - brief description, including changes from previous versions

- other calculations referenced, used or related
- input data used, if not contained in calculation
- "signature ladder", including project engineer

B5.3 File Organization

- description of organization
- identification of how base line calculation and sensitivity data have been separated
- description of file maintenance

B.6 References

1. IEEE/ANS Procedures Guide, NUREG/CR-2300.
2. IREP Procedures Guide, NUREG/CR-2728.
3. Probabilistic Risk Assessment (PRA) Reference Document, NUREG/CR-1050 (September 1984).
4. Reliability and Risk Analysis Methods Research Plan, NUREG/CR-1093 (September 1984).
5. G. Kolb et al., Risk Methods Integration and Evaluation Program Plant, SANDIA (February 1984).
6. B. J. Bell and A. D. Swain, A Procedure for Conducting HRA for NPP, SANDIA/NUREG/CR-2254 (August 1983).
7. G. Hannaman et al., Systematic Human Action Reliability Procedure, NUS/EPRI-NP 3583 (June 1984).
8. D. Okrent et al., On PRA Quality and Use, DE-83013138/ALO-1017/UCLA ENG 8269 (October 1982).
9. S. Eide et al., Approach to the Assurance of Technical Adequacy of LWR Probabilistic Risk Assessments, Energy Incorporated/EPRI RP 2171-2 (July 1983).
10. W. J. Parkinson et al., An Intensive Peer Review for Probabilistic Risk Assessment, Delian/NSAC 67 (March 1984).
11. J. S. Christians and Z. J. Janik, Quality Engineering Programme in the Design Process, IAEA/SM-253/66 (June 1966).
12. G. Apostolakis et al., On Quality, Peer Review and the Achievement of Consensus in Probabilistic Risk Analysis, Nuclear Safety 24 (November 1983) p. 792f.

APPENDIX C

Component Failure Rates

C.1 Generic Failure Rate Values

This generic data base was generated from the estimates produced by a two-day Reliability Data Workshop held at NRC in April 1982. The workshop brought together experts in data analysis and risk assessment; participants represented the NRC, the electric utilities, national laboratories, and nuclear consulting firms. For each component failure mode a nominal failure rate value and an error factor representing an approximate 90% upper bound value and an approximate 10% lower bound value were generated.* These expert-generated failure rates and error factors and those given in the IREP users guide (NUREG/CR-2728) were combined to yield the baseline failure data given in this guide. The following procedure was used:

1. For a given component failure mode, the maximum nominal value was selected from the two sources, and the maximum error factor was selected.
2. The selected nominal value was then multiplied and divided by the selected error factor to obtain defined upper 90% and lower 10% bounds.
3. A truncated loguniform distribution (i.e., flat on a log scale) was fitted to the two bounds, and a mean value was then calculated.
4. The mean value of the truncated loguniform and the minimum and maximum bounds are given in Table C.1 which defines the baseline data base to be used for PSA.

It should be noted that for most components, the expert-generated values and the IREP values agreed with one another. Where there was disagreement, either in nominal failure rate or in error factor, then, in general, the disagreement was a factor of 3 or less. The generic values generated in the above manner are conservatively biased and have the largest assigned error factor where there was disagreement.

The truncated loguniform which is used to describe the uncertainty in the failure rate is flat on the log scale and has no implied most-likely value as does the lognormal (in the log scale). The truncated loguniform can also be viewed as a truncated noninformative prior which is used in Bayesian analysis and which generally gives similar numerical results to a classical statistics treatment when the range is interpreted as a classical confidence interval.

Finally, it should be noted that no attempt is made to describe plant-to-plant variability by the loguniform which is used. The loguniform is simply a crude measure of the uncertainty associated with an estimated generic failure rate value which is meant to represent an industry-average failure rate.

*Oswald et al., Generic Data Base for Data and Models Chapter of the NREP Guide, EGG-EA-5887, June 1982.

C.2 Use of the Data Table

The mean values in Table C.1 (rounded to one significant figure) are to be considered generic point estimates. If m, l denote the natural logarithms of the maximum and minimum values M and L , respectively, then the median and means values of the loguniform are given by the expressions

$$\text{Median } \lambda_{50} = \exp \left[\frac{m+l}{2} \right],$$

$$\text{Mean } \bar{\lambda} = (M-L)/(m-l) .$$

A loguniform distribution is simulated by first selecting a random number z uniformly between 1 and m and then taking the exponential (e^z).

C.3 Shortcomings of the Data Table

In all likelihood, modification of this table (C.1) will be necessary from time to time, both because of new insights gained from operational experience and because of difficulties encountered in applying the table. NRC will periodically review the need for modification of the table. Problems in application can beneficially be discussed in the course of the interactive review process, and should in any case be brought to the attention of NRC.

Table C.1 Generic Component Failure Rates (All Values per Hour)

Component and Failure Modes	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
1. Pumps				
1.1 Motor driven				Pump and motor; excludes control circuits.
1.1.1 Failure to start	2E-7	1E-5	5E-5	
1.1.2 Failure to run, given start	2E-6	1E-4	5E-4	
1.1.2.1 Extreme environment	6E-5	3E-3	2E-2	Considered as interface with heavy chemical environment such as concentrated boric acid.
1.2 Turbine driven				Pump, turbine, steam and throttle valves, and governor.
1.2.1 Failure to start (includes under and over speed)	2E-6	1E-4	5E-4	
1.2.2 Failure to run, given start	8E-6	2E-5	1E-4	
1.3 Diesel driven				Pump, diesel, lube oil system, fuel oil, suction and exhaust air, and starting system.
1.3.1 Failure to start	2E-7	1E-6	5E-5	
1.3.2 Failure to run, given start				
2. Valves				Catastrophic leakage or "rupture" values assigned by engineering judgment; catastrophic leakage assumes the valve to be in a closed state, then the valve fails.
2.1 Motor operated				
2.1.1 Failure to open	2E-7	1E-5	5x10 ⁻⁵	
2.1.2 Failure to remain open	8E-8	2E-7	1E-6	
2.1.3 Failure to close	2E-7	1E-5	5E-5	
2.1.4 Internal leakage (catastrophic)	1E-10	1E-7	7E-7	
2.2 Solenoid operated				
2.2.1 Failure to operate	8E-7	2E-6	1E-5	
2.3 Air/fluid operated				
2.3.1 Failure to operate	2E-7	1E-5	5E-5	
2.4 Check Valves				
2.4.1 Failure to open	8E-8	2E-7	1E-6	
2.4.2 Failure to close	6E-7	2E-6	1E-5	

Table C.1 (Continued)

Component and Failure Modes	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
Valves (continued)				
2.4.3 Internal leakage				
2.4.3.1 Minor	6E-8	3E-6	2E-5	
2.4.3.2 Catastrophic	1E-10	1E-7	7E-7	Valve initially closed, then failed.
2.5 Vacuum breakers				Applies only to BWRs.
2.5.1 Failure to open	2E-8	6E-8	4E-7	
2.5.2 Failure to close	2E-8	6E-8	4E-7	
2.6 Manual valves				
2.6.1 Failure to operate	8E-8	2E-7	1E-6	Failure to operate is dominated by human error; rate is based on one actuation per month.
2.7 Code safety valves				Applies only to PWRs; premature opening covered under initiating events.
2.7.1 Failure to open	3E-6	6E-7	4E-5	
2.7.2 Failure to close, given open	8E-6	2E-5	2E-4	
2.8 Primary safety valves				Applies only to BWRs.
2.8.1 Failure to open	8E-6	2E-5	2E-4	
2.8.2 Failure to close, given open	8E-6	2E-5	2E-4	
2.9 Relief valves				
2.9.1 Failure to open				
2.9.2 Failure to close, given open				
2.10 Stop check valves				
2.10.1 Failure to open				
3. Switches				Where torque/limit switches are used as part of pumps/valves, switch failure rate.
3.1 Torque				
3.1.1 Failure to operate	8E-6	2E-7	1E-6	

Table C.1 (Continued)

Component and Failure Modes	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
Switches (continued)				
3.2 Limit				
3.2.1 Failure to operate	8E-7	6E-6	4E-6	
3.3 Pressure				
3.3.1 Failure to operate	8E-8	2E-7	1E-6	
3.4 Manual				
3.4.1 Failure to transfer	2E-8	1E-6	5E-6	
4. Other				
4.1 Circuit breaker				
4.1.1 Failure to transfer	2E-7	1E-5	5E-5	
4.1.2 Spurious trip	6E-7	3E-5	2E-4	
4.2 Fuses				
4.2.1 Premature open	6E-8	3E-6	2E-5	
4.3 Buses				
4.3.1 All modes	6E-10	3E-8	2E-7	
4.4 Orifices				WASH-1400 data; no alternative data available.
4.4.1 Failure to open				
4.4.1.1 Plug	3E-7	6E-7	4E-6	
4.4.1.2 Rupture	6E-10	3E-8	2E-7	
4.5 Transformers				
4.5.1 All modes	3E-7	6E-7	4E-6	

Table C.1 (Continued)

Component and Failure Modes Other (continued)	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
4.6 Emergency diesel (complete plant)				Engine frame and associated moving parts, generator coupling, governor, static exciter, output breaker, lube oil system, fuel oil, suction and exhaust air, starting system; excludes starting air compressor and accumulator, fuel storage, load sequencers, and synchronizers. Failure to start is failure to start, accept load, and run for 1/2 hour; failure to run for more than 1/2 hour, given start.
4.6.1 Failure to start	3E-5	6E-5	4E-4	
4.6.2 Failure to run, given start (emergency conditions)	6E-5	3E-3	2E-2	
4.7 Relays				Assumes out-of-spec cell replacement.
4.7.1 Contacts fail to transfer (open or close)	2E-8 6E-8	1E-6 3E-6	5E-6 2E-5	
4.7.2 Coil failure (open or short)				
4.8 Time delay relays				
4.8.1 Premature transfer	2E-8	1E-6	5E-6	
4.8.2 Fails to transfer	2E-7	1E-5	1E-5	
4.8.2.1 Bimetallic				
4.9 Battery power system (Wet Cell)				
4.9.1 Fails to provide proper output	8E-7	2E-6	1E-5	
4.10 Battery charger				
4.10.1 Failure to operate	3E-7	6E-7	4E-6	
4.11 DC Motor generators				
4.11.1 Failure to operate	6E-8	3E-6	2E-5	
4.12 Inverters				
4.12.1 Failure to operate	3E-5	6E-5	4E-4	

Table C.1 (Continued)

Component and Failure Modes	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
Other (continued)				
4.13 Wires (per circuit)				
4.13.1 Open circuit	2E-7	1E-5	5E-5	
4.13.2 Short to ground	2E-8	1E-6	5E-6	
4.13.3 Short to power	6E-10	3E-8	2E-7	
4.14 Solid state devices				
4.14.1 High power applications	6E-8	3E-6	2E-5	
4.14.2 Low power applications	6E-8	3E-6	2E-5	
4.15 Terminal boards				
4.15.1 Open circuit	6E-9	3E-7	2E-6	Values given are <u>per terminal</u> .
4.15.2 Short to adjacent circuit	6E-9	3E-7	2E-6	
4.16 Dampers				
4.16.1 Failure to operate	2E-7	1E-6	5E-5	
4.17 Air coolers				
4.17.1 Failure to operate	3E-6	6E-6	4E-5	
4.18 Heat exchangers				
4.18.1 Tube leak (per tube)	6E-11	3E-9	2E-8	
4.18.2 Shell leak	6E-8	3E-6	2E-5	
4.19 Strainer/filter				
4.19.1 Plugged	6E-7	3E-5	2E-4	For clear fluids; contaminated fluids or fluids with a heavy chemical burden should be considered on a plant-specific basis.

For other component failure modes use the values given in the IREP users guide.

APPENDIX D

Generic Repair Times

For a given component, the generic repair time is taken to be the maximum allowed unscheduled downtime given in the plant technical specification (tech spec). The particular technical specifications should be referenced in the section of the report documenting the repair time values which were used.

The conservative prescription given above is expected to be modified shortly as a result of substantial NRC staff activity directed towards characterizing the relationship between allowed outage time and mean outage time.

APPENDIX E

Generic Surveillance Test Intervals and Test Duration Times

The surveillance test interval to use for a periodically tested component is taken to be the value specified in the plant tech specs. The average test duration for the surveillance test is taken to be the maximum allowed scheduled downtime given in the plant technical specification. These test interval and test duration definitions can also be used for the plant-specific evaluation when actual reliable data on surveillance test characteristics are not obtainable. For evaluations of accident probabilities during steady state operation, the test intervals and durations should be used only for those tests performed online while the plant is operating. The particular technical specifications should be referenced in the section of the report that documents the test interval and duration values used.

APPENDIX F

Generic Maintenance Intervals and Maintenance Duration Times

The generic frequency of unscheduled maintenance actions is taken to be ten times the baseline failure rate. The average time between unscheduled maintenance actions is the inverse of the maintenance frequency. This definition of the maintenance frequency is equivalent to the assumption that minor component failures requiring maintenance actions (incipient failures) have a frequency of occurrence which is an order of magnitude higher than the catastrophic failure frequency. The generic maintenance duration time is taken to be the unscheduled allowed downtime. The particular technical specifications should again be referenced in the section documenting the maintenance parameter values that were used.

The prescription above may be modified shortly as a result of a broad NRC Staff inquiry into the character of maintenance outages.

APPENDIX G

Initiating Event Frequencies

This Appendix provides point values and associated probability density functions for the frequencies of various accident initiators. The initiators have been divided into two groups pertaining to BWRs and PWRs and given in Tables G.1 and G.3, respectively. Point values of the frequencies and associated uncertainties are given in Tables G.2 and G.4 for both BWRs and PWRs, respectively. The tables give the mean value, the variance and the median value for each transient initiator. The mean value is to be used as point value. The probability density function (pdf) that characterizes each transient initiator will be approximated with a gamma pdf given by

$$g(f|a,b) = \frac{(bf)^{a-1} \cdot e^{-bf}}{\Gamma(a)} \cdot b \quad (G.1)$$

where a, b are the parameters of the gamma distribution expressed in terms of the mean (m) and variance (v) as

$$a = \frac{m^2}{v}, \quad b = \frac{m}{v} \quad (G.2)$$

and $\Gamma(a)$ is the gamma function defined as

$$\Gamma(a) = \int_0^{\infty} f^{a-1} e^{-f} df \quad (G.3)$$

The derivation of the point values and the corresponding uncertainties was based on the methodology described in Reference G.1 and on the data base given in Reference G.2.

Frequencies (point values and uncertainties) for groups of initiators are obtained by appropriate summation of the frequencies of the individual events in each group.

References

1. I. A. Papazoglou et al., "Bayesian Analysis under Population Variability with an Application to the Frequency of Anticipated Transients in Nuclear Power Plants."
2. A. S. McClymont and B. W. Poehlman, "ATWS: A Reappraisal Part 3: Frequency of Anticipated Transients," EPRI Interim Report NP-2230, January 1982.

Table G.1 BWR Transient Categories

Category	Title
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 Stream 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

Table G.2 Generic Frequencies for BWR Transient Initiators

Int.	BWR Transient Categories	Mean	Variance	Median
1	Electric Load Rejection	7.0 E-1	1.9 E-1	5.7 E-1
2	Electric Load Rejection with Turbine Bypass Valve Failure	1.1 E-2	4.7 E-4	5.2 E-3
3	Turbine Trip	1.2 E+0	5.9 E-1	9.2 E-1
4	Turbine Trip with Turbine Bypass Valve Failure	1.1 E-2	4.7 E-4	5.2 E-3
5	Main Stream Isolation Valve Closure	5.7 E-1	2.0 E-1	4.3 E-1
6	Inadvertent Closure of One MSIV (Rest Open)	2.1 E-1	3.4 E-2	1.5 E-1
7	Partial MSIV Closure	1.2 E-1	1.2 E-2	8.1 E-2
8	Loss of Normal Condenser Vacuum	4.8 E-1	1.0 E-1	3.9 E-1
9	Pressure Regulator Fails Open	1.8 E-1	2.7 E-2	1.2 E-1
10	Pressure Regulator Fails Closed	1.7 E-1	2.8 E-2	1.1 E-1
11	Inadvertent Opening of a Safety/Relief Valve (Stuck)	2.5 E-1	4.8 E-2	1.7 E-1
12	Turbine Bypass Fails Open	6.1 E-2	3.0 E-3	4.5 E-2
13	Turbine Bypass or Control Valves Cause Increase Pressure (Closed)	4.8 E-1	1.4 E-1	3.6 E-1
14	Recirculation Control Failure-Increasing Flow	2.5 E-1	4.7 E-2	1.8 E-1
15	Recirculation Control Failure-Decreasing Flow	1.3 E-1	1.4 E-2	8.4 E-2
16	Trip of One Recirculation Pump	8.8 E-2	6.2 E-3	6.5 E-2
17	Trip of All Recirculation Pumps	2.1 E-2	5.0 E-4	1.3 E-2
18	Abnormal Startup of Idle Recirculation Pump	1.4 E-2	8.0 E-2	7.2 E-5
19	Recirculation Pump Seizure	1.1 E-2	4.7 E-4	5.2 E-3
20	Feedwater-Increasing Flow at Power	1.8 E-1	2.6 E-2	1.2 E-1
21	Loss of Feedwater Heater	4.0 E-2	1.2 E-3	2.8 E-2
22	Loss of All Feedwater Flow	1.3 E-1	1.1 E-2	1.0 E-1
23	Trip of One Feedwater or Condensate Pump	1.7 E-1	2.4 E-2	1.2 E-1
24	Feedwater-Low Flow	5.8 E-1	1.7 E-1	4.5 E-1
25	Low Feedwater Flow During Startup or Shutdown	2.3 E-1	3.5 E-2	1.7 E-1
26	High Feedwater Flow During Startup or Shutdown	7.5 E-2	3.8 E-3	5.7 E-2
27	Rod Withdrawal at Power	2.1 E-2	5.2 E-4	1.3 E-2

Table G.2 (Continued)

Int.	BWR Transient Categories	Mean	Variance	Median
28	High Flux Due to Rod Withdrawal at Startup	9.7 E-2	6.7 E-3	7.2 E-2
29	Inadvertent Insertion of Rod or Rods	1.4 E-1	1.6 E-2	9.6 E-2
30	High Flux Due to Rod Withdrawal at Startup	9.7 E-2	6.7 E-3	7.2 E-2
31	Loss of Offsite Power	1.2 E-1	6.0 E-3	9.2 E-2
32	Loss of Auxiliary Power (Loss of Auxiliary Transformer)	1.1 E-1	4.7 E-4	5.1 E-3
33	Inadvertent Startup of HPCI/HPCS	1.1 E-1	4.7 E-4	5.2 E-3
34	Scram Due to Plant Occurrences	4.7 E-1	1.7 E-1	3.3 E-1
35	Spurious Trip Via Instrumentation, RPS FAULT	1.3 E+0	6.1 E-1	1.1 E+0
36	Manual Scram - No Out-of-Tolerance Condition	8.1 E-1	4.4 E-1	5.9 E-1
37	Cause Unknown	1.4 E-1	1.9 E-2	9.3 E-2

Table G.3 PWR Transient Categories

Category	Title
1	Loss of RCS Flow (1 Loop)
2	Uncontrolled Rod Withdrawal
3	CRDM Problems and/or Rod Drop
4	Leakage from Control Rods
5	Leakage in Primary System
6	Low Pressurizer Pressure
7	Pressurizer Leakage
8	High Pressurizer Pressure
9	Inadvertent Safety Injection Signal
10	Containment Pressure Problems
11	CVCS Malfunction - Boron Dilution
12	Pressure/Temperature/Power Imbalance-Rod Position Error
13	Startup of Inactive Coolant Pump
14	Total Loss of RCS Flow
15	Loss or Reduction in Feedwater Flow (1 Loop)
16	Total Loss of Feedwater Flow (All Loops)
17	Full or Partial Closure of MSIV (1 Loop)
18	Closure of All MSIV
19	Increase in Feedwater Flow (1 Loop)
20	Increase in Feedwater Flow (All Loops)
21	Feedwater Flow Instability - Operator Error
22	Feedwater Flow Instability - Misc. Mechanical Causes
23	Loss of Condensate Pump (1 Loop)
24	Loss of Condensate Pumps (All Loops)
25	Loss of Condenser Vacuum
26	Steam Generator Leakage
27	Condenser Leakage
28	Miscellaneous Leakage in Secondary System
29	Sudden Opening of Steam Relief Valves
30	Loss of Circulating Water
31	Loss of Component Cooling
32	Loss of Service Water Systems
33	Turbine Trip, Throttle Valve Closure, EHC Problems
34	Generator Trip or Generator Caused Faults
35	Total Loss of Offsite Power
36	Pressurizer Spray Failure
37	Loss of Power to Necessary Plant Systems
38	Spurious Trips - Cause Unknown
39	Auto Trip - No Transient Condition
40	Manual Trip - No Transient Condition
41	Fire Within Plant

Table G.4 Generic Frequencies for PWR Transient Initiators

Int.	PWR Transient Categories	Mean	Variance	Median
1	Loss of RCS Flow (1 Loop)	4.4 E-1	1.3 E-1	3.2 E-1
2	Uncontrolled Rod Withdrawal	2.0 E-2	3.2 E-4	1.3 E-2
3	CSDM Problems and/or Rod Drop	6.1 E-1	3.1 E-1	4.2 E-1
4	Leakage from Control Rods	2.3 E-2	5.0 E-4	1.6 E-2
5	Leakage in Primary System	1.1 E-1	1.1 E-2	7.3 E-2
6	Low Pressurizer Pressure	3.1 E-2	6.5 E-4	2.3 E-2
7	Pressurizer Leakage	9.6 E-3	1.5 E-4	6.0 E-3
8	High Pressurizer Pressure	2.8 E-2	5.5 E-4	2.0 E-3
9	Inadvertent Safety Injection Signal	5.4 E-2	2.3 E-3	4.0 E-2
10	Containment Pressure Problems	1.0 E-2	1.8 E-4	5.9 E-3
11	CVCS Malfunction-Boron Dilution	3.6 E-2	8.3 E-4	2.7 E-2
12	Pressure/Temperature/Power Imbalance-Rod Position Error	1.5 E-1	2.2 E-2	1.0 E-1
13	Startup of Inactive Coolant Pump	4.8 E-3	5.7 E-4	2.3 E-3
14	Total Loss of RCS Flow	2.8 E-2	5.4 E-4	2.0 E-2
15	Loss or Reduction in Feedwater Flow (1 Loop)	1.8 E+0	9.2 E-1	1.5 E+0
16	Total Loss of Feedwater (All Loops)	1.8 E-1	3.0 E-2	1.1 E-1
17	Full or Partial Closure of MSIV (1 Loop)	2.3 E-1	4.8 E-2	1.5 E-1
18	Closure of All MSIV	3.0 E-2	6.6 E-4	2.1 E-2
19	Increase in Feedwater Flow (1 Loop)	6.4 E-1	3.3 E-1	4.4 E-1
20	Increase in Feedwater Flow (All Loops)	1.6 E-2	3.0 E-4	1.0 E-2
21	Feedwater Flow Instability - Operator Error	1.8 E-1	3.2 E-2	1.1 E-1
22	Feedwater Flow Instability - Mechanical Cause	2.0 E-1	4.0 E-2	1.3 E-1
23	Loss of Condensate Pumps (1 Loop)	1.0 E-1	9.8 E-3	6.8 E-2
24	Loss of Condensate Pumps (All Loops)	4.8 E-3	5.7 E-4	2.3 E-3
25	Loss of Condenser Vacuum	2.3 E-1	4.2 E-2	1.7 E-1
26	Steam Generator Leakage	3.7 E-2	8.0 E-4	2.7 E-2
27	Condenser Leakage	5.3 E-2	2.6 E-3	3.8 E-2

Table G.4 (Continued)

Int.	PWR Transient Categories	Mean	Variance	Median
28	Miscellaneous Leakage in Secondary System	8.8 E-2	5.9 E-3	6.4 E-2
29	Sudden Opening of Steam Relief Valves	3.9 E-2	8.9 E-4	3.0 E-2
30	Loss of Circulating Water	6.3 E-2	2.7 E-3	4.7 E-2
31	Loss of Component Cooling	1.5 E-2	8.8 E-2	5.1 E-5
32	Loss of Service Water System	1.0 E-2	1.8 E-4	5.9 E-3
33	Turbine Trip, Throttle Valve Closure, EHC Problems	1.6 E+0	6.6 E-1	1.3 E+0
34	Generator Trip or Generator Caused Fault	4.1 E-1	8.3 E-2	3.2 E-1
35	Total Loss of Offsite Power	1.3 E-0	6.4 E-3	1.1 E-1
36	Pressurizer Spray Failure	3.8 E-2	7.8 E-4	2.9 E-2
37	Loss of Power Necessary to Plant Systems	1.1 E-1	1.1 E-2	7.5 E-2
38	Spurious Trips - Cause Unknown	1.3 E-1	1.4 E-2	9.5 E-2
39	Auto Trip - No Transient Condition	1.2 E+0	6.4 E-1	9.8 E-1
40	Manual Trip - No Transient Condition	5.8 E-1	3.0 E-1	3.9 E-1
41	Fire Within Plant	2.3 E-2	4.3 E-4	1.6 E-2

APPENDIX H

Plant-Specific Frequencies for the Initiating Events

H.1 Purpose

The purpose of this appendix is to describe the procedure for assessing frequencies and associated uncertainties for the initiating events (see Section 5.5). Plant-specific values for the frequencies of the various initiators are provided in Reference 5. These values were based on the information contained in an EPRI report¹ with the exception of the loss-of-offsite-power initiator for which References 2 and 3 were used.

The values provided in this appendix notwithstanding, the data in the above-mentioned reports should be verified, supplemented, and updated by searches and analyses of the plant-specific events reported in the NRC Gray Book, Operating Experience Summaries and the Licensee Event Reports.

H.2 Model and Parameter Selection

The parameters of interest here characterize the occurrence and the recovery of the initiating events.

Occurrence: It is assumed that each initiating event occurs randomly according to a Poisson random process. Such a process is characterized by its intensity; i.e., the frequency with which such events occur (which is estimated from experiential data).

Recovery: For certain initiators, it is very important to assess, in addition to the frequency of occurrence, its duration. The duration of an initiating event is equal to the time necessary to restore the associated equipment to service (recovery time).

The recovery from an initiating event is treated as a random process. The recovery time is then a random variable. Experience to date indicates that the gamma or lognormal families of probability density functions (pdf) adequately describe the random character of the recovery time. As a gross model of the recovery time distribution, an exponential distribution can be used with an associated inaction time. The model can also be used for repair times of components, and the comments given in Section 5.6.4 (ii) apply here.

H.3 Estimation Technique

A point estimate and appropriate uncertainty measures for the frequency of the initiating events can be derived from the number of occurrences of the event and the total time during which these occurrences have been observed. Regardless of the particular estimation technique selected, these are the raw data of interest.

Since, for most of the operating plants and certainly for new plants, individual accident initiators are relatively infrequent, the data are insufficient to provide a base for a reliable estimation. The need exists, therefore, to incorporate, in the analysis, data from other plants (generic). Such

an incorporation should be systematic, however, to avoid "penalizing" plants that exhibit low frequencies or give undue credit to plants that are characterized by high frequencies. The estimation technique described here is a Bayesian technique that allows for plant-to-plant variability. This method is described in References H.4, and H.5, and the application includes the following steps.

a. Selection of Plant Population - For each accident initiator the plants that are expected to exhibit similarities are grouped to provide the "plant population." This grouping depends on the particular accident initiator. For some initiators a grouping according to the plant type (PWR or BWR) could suffice. For others, like loss of main feedwater, a distinction among manufacturers (e.g., Westinghouse, CE, and B&W for PWRs) is more suitable. Finally, other groupings such as grouping the loss of offsite power by regional Reliability Councils could be appropriate.

b. Assessment of Prior Distribution - The technique calls for the assessment of prior distributions for certain parameters. This technique is equivalent to assessing a prior distribution for the frequency of the initiator that characterizes the plant population. The priors that were used were effectively flat on a log scale over a wide range of values (three to four orders of magnitude). For example, in the derivation of the loss of offsite power frequencies provided here, this prior was practically uniform in a log-scale range $10^{-3}/\text{yr}$ to $10/\text{yr}$.

c. Use of the Prior Distribution and the Experiential Data According to the Proposed Technique - The goal of this phase of the analysis is to assess plant-specific distributions as well as a distribution that characterizes the population as a whole.

For operating plants the corresponding plant-specific distribution is to be used. For new plants (for which it is reasonable to assume that they belong to the particular group), the population distribution is to be used.

The parameters relevant to the recovery of an initiating event that must be estimated depend upon the specific distribution assumed. Regardless of the selected estimation technique, the data upon which the estimation can be based consist of the times to recovery of the observed occurrences of the initiating event.

Here, again, the remark on the adequacy of plant specific data for a reliable estimation of a recovery time is valid. For this reason the same technique, outline above for the frequency of occurrence, should be used to account for information from other similar but not identical plants.

H.4 Data Sources and Data Gathering

The data necessary for the initiating event parameter estimation consist of the times between occurrences of the events of a specific kind and, if recovery is of interest, of the corresponding recovery times. Because of the Poisson assumption for the occurrence of the initiating events, the total number of occurrences and the total time of plant operation are sufficient instead of the individual times between occurrences. For the recovery, however, since the underlying random process and hence the sufficient statistic are not

yet well established, the individual repair time are necessary. The major source of data for initiating events is an EPRI report.¹ The data in this report should, however, be verified, supplemented, and updated by searches and analyses of the plant-specific events reported in the NRC Grey Books, Operating Experience Summaries and the Licensee Event Reports.

References

1. "Anticipated Transients," EPRI NP-2230.
2. "Loss of Off-Site Power at Nuclear Power Plants: Data and Analysis," EPRI NP-2301, March 1982.
3. R. F. Scholl, Jr., "Loss of Off-Site Power Survey Status Report," Rev. 3, Report of the Systematic Evaluation Program Branch, Division of Licensing, U. S. Nuclear Regulatory Commission.
4. S. Kaplan, "On a Two Stage Bayesian Procedure for Determining Failure Rates from the Experiential Data," PLG-0191, 1982.
5. I. A. Papazoglou et al., "Bayesian Analysis Under Population Variability with an Application to the Frequency of Accident Initiating Events in Nuclear Power Plants," BNL-NUREG-31794, Aug. 1983.

APPENDIX I

COMPUTER CODES FOR ACCIDENT SEQUENCE EVALUATION

It will be necessary, for practical purposes, to select and utilize one or more computer codes to perform the Boolean evaluations and probability quantifications. A number of codes and code packages to perform PRA are currently available. Many of these are described in both Appendix C and Chapter 6 of NUREG/CR-2300. The codes described in Chapter 6 of that document are divided into four general groups: qualitative analysis; quantitative analysis; dependent failure analysis; and data analysis. Brief descriptions of the codes in the first three groups are presented in tables which are reproduced here, for the readers convenience, as Tables I.1, I.2 and I.3. More complete descriptions of the codes in all four groups are contained in NUREG/CR-2300.

Selection of the code(s) to be used is a decision that may be influenced by many factors:

- computer facilities available,
- staff expertise,
- objectives of the analysis,
- state of documentation of codes considered,
- compatibility of qualitative and quantitative evaluation codes with each other and with other analyses planned.

The last point is of particular importance because the selection of a code for the quantitative evaluation should not be made independent of code selection for the qualitative evaluations. In fact, some of the code packages, e.g., MOCUS-SUPERPOCUS and PREP-KITT, were designed to use the output from the qualitative evaluation.

No specific codes or code packages can be recommended for the reasons described above. All the codes have advantages and disadvantages which the user must consider as they apply to his particular needs and qualification. Any code used, however, must have complete documentation, as must any modifications made to a code for a particular evaluation.

Qualitative Analysis Codes

Qualitative analysis codes are used to compute minimal cutsets and/or minimal path sets for a fault tree, or to perform a Boolean reduction of the fault tree. The various codes which have been developed to perform this type of analysis differ significantly in their capabilities, limitations, and special features, as shown in Table I.1.

Two points related to qualitative analysis codes are noteworthy. The first is that minimum cut sets are used as inputs by several codes that perform quantitative analysis and dependent failure analysis. Second is that there are two methods of calculating minimum cut sets: a rigorous

deterministic approach based on Boolean algebra principles, and the Monte Carlo approach.

Quantitative Analysis Codes

Quantitative analysis codes are used to compute point estimates of the probabilities of system fault tree top events and to identify the dominant cut sets and their probabilities. Some of these codes also have the capability to compute other types of quantitative results, such as importance measures, sensitivity, and/or uncertainty analysis, and time-dependent unavailability, as shown in Table I.2.

In general, these codes can be divided into two major groups: the classical codes, which require the input of minimum cutsets (from an internal computation or a qualitative analysis); and the "direct evaluation" codes, which do not utilize or compute cutsets to evaluate the top event.

Dependent Failure Analysis and Other Codes

Codes for dependent failure analysis, shown in Table I.3, are used to assist in the effort to identify minimal cutsets of the system susceptible to a single common cause mechanism. Several other more specialized codes described in NUREG/CR-2300 are also available to assist in data analysis, particularly for updating of Bayesian data.

Uncertainty Analysis Codes

Uncertainty analysis codes are used to propagate uncertainties through the PRA models. Monte Carlo simulation or moments methods are generally used when the parameters are treated as random variables in the Bayesian approach employed here. Chapters 6 and 12 of the IEEE/ANS PRA Procedures Guide describe various codes that can be used for these calculations.

Table 1.1 Computer Codes for Qualitative Analysis

Code	Input	Checking of input errors	Limit on number of gates or events	Types of gates	Limit on number or size of cut sets ^a	Method of generating cut sets ^a	Other outputs	Fault-tree truncation	Other features	Type of computer, language, and availability
ALLCUTS	8-character alphanumeric names, control information, basic event probability, fault-tree description	Through auxiliary program BRANCH	Up to 175 primary events and 425 gates	AND OR	Up to 1000 cut sets can be calculated	Top-down successive Boolean substitution	Cut sets in specified probability range, cut set and top-event probability	Minimal cut sets, probability	Fault-tree plotting option	IBM 360/370 CDC 7600 Fortran IV
FATRAM	8-character alphanumeric names, control information, fault-tree description	Y.N.		AND OR		Top-down successive substitution with gate coalescing option	Minimal cut sets up to specified order	Minimal cut sets	--	CDC Cyber 76 Fortran IV Available from EG&G Idaho
FTAP	8-character alphanumeric names, control information, fault-tree description	Yes, very extensive		AND OR K-of-N NOT		Top-down, bottom-up, and Nelson method (prime implicants)	Minimal cut sets and prime implicants	Minimal cut sets	Independent subtrees automatically found and replaced by module	IBM-370, CDC-7600 Fortran IV Available from Operations Research Center, U.C. Berkeley
GRAP	Interactive graphics fault-tree input, failure rates	Yes	Up to 600 primary events or gates	AND OR		Similar to algorithm used in FTAP	Probabilities of cut sets and top event	Minimal cut sets	On-line tree construction by interactive terminal	CDC Cyber 750 Fortran IV Available from Babcock & Wilcox
NOCUS	8-character alphanumeric names, control information, fault-tree description	Yes, very extensive		AND OR INHIBIT	Minimal cut sets of up to order 20 can be generated	Top-down successive Boolean substitution	Path sets	Minimal cut sets	Cut sets can be automatically punched on cards or on-line data sets for use by KITT or SUPERPOCUS	IBM 360/370 CDC-7600 Fortran IV Available from Argonne Software Center
PL-MOD	79-character alphanumeric names, control information, fault-tree description, failure data	Yes	None; computer storage capacity limiting factor	AND OR NOT K-of-N	None	Bottom-up modularization and decomposition of fault tree into its finest modular representation	Probability of top event, time-dependent characteristics of top event, minimal cut sets, uncertainty for top event	Minimal cut sets	Option of not generating minimal cut sets for quantifying fault tree	IBM 360/370 PL/I Available from Argonne Software Center
PREP	8-character alphanumeric names, control information, fault-tree description	Yes, very extensive	2000 primary events and 2000 gates	AND OR INHIBIT	Minimal cut sets of up to order 10 can be generated	Combinatorial testing	--	No	Minimal cut sets can be automatically punched on cards or on-line data sets for use in KITT or SUPERPOCUS	IBM 360-370 CDC 7600 Fortran IV Available from Argonne Software Center

Table 1.1 (Continued)

Code	Input	Checking of input errors	Limit on number of gates or events	Types of gates	Limit on number or size of cut sets ^a	Method of generating cut sets ^a	Other outputs	Fault-tree truncation	Other features	Type of computer, language, and availability
SETS	16-character alphanumeric names, user's program, failure data, fault-tree description	Yes, very extensive	8000 events (gates and primary events together)	AND OR INHIBIT PRIORITY Exclusive or special	None	Top-down Boolean substitution, but user's program can be designed for any other method	Probability of minimal cut sets, prime implicants	Yes, based on both cut-set order and probability	Automatic fault-tree merging and plotting; on-line data sets can be stored on tapes for use in other runs; independent subtrees can be obtained to simplify cut-set generation	CDC-7600 Fortran IV Available from Argonne Software Center
SIFTA	10-character alphanumeric names, control information, failure data, fault-tree description	Yes, very extensive		AND OR K-of-N	No cut sets generated	Pattern-recognition technique to reduce structure of tree; numerical simulation to calculate probabilities	New structure of tree after reduction; probability of top event	Independent branches of tree with small probability can be truncated	Trees with multiple top events are handled; merging of fault trees possible; fault trees can be plotted	HP-1000 Available from Atomic Energy Control Board, Ottawa, Canada
TREEL and MISCUP	8-character alphanumeric names, control information, fault-tree description	Yes, very extensive		AND OR INHIBIT		Top-down successive Boolean substitution	Path sets	Minimal cut sets	Minimal sets of intermediate gates can be determined	CDC-6400 Fortran IV Available from Operations Research Center, U.C. Berkeley
WAMCUT and WAMCUT II	10-character alphanumeric names, control information, failure data, fault-tree description	Yes, very extensive	1500 primary events and 1500 gates	AND OR NOT NOR NAND ANOT CNOT K-of-N	Up to 2000 minimal cut sets of any order can be generated	Bottom-up Boolean substitution; WAMCUT-II finds independent subtrees, replaces them by pseudo-component, then uses top-down Boolean substitution	Probabilities of minimal cut sets and top event; first and second moments of minimal cut sets and top event	Yes, based on both cut-set order and probability	Plot option; minimal cut sets of intermediate gates can be generated	CDC-7600, IBM-370 Extended Fortran IV available from EPRI

^aOr prime implicants.

Table 1.2 Computer Codes for Quantitative Analysis

Code	Input	Quantitative calculations	Importance calculation	Uncertainty analysis	Other features	Type of computer, language, and availability
BOUNDS	Reduced system equations or minimal cut sets, primary-event failure data	No	No	Two moments of minimal cut sets and top event calculated by mathematical approach	Multiple system functions with multiple data input description can be handled; Johnson-type distribution can be fitted to top event	IBM 360/370 Fortran IV Available from UCLA
DPD	Reduced system equation, primary-event failure data	No	No	Combines two histograms at a time to achieve the histogram; log-normal can be handled automatically	A Bayesian updating of capability allows distributions to be updated	CDC 7600 Fortran IV Available from Pickard, Lowe and Garrick, Inc.
FRANTIC and FRANTIC II	Reduced system equation or minimal cut sets, primary-event failure data	Time-dependent calculation; nonrepairable, monitored, and periodically tested primary events are handled	No	Uncertainty analysis for failure rates in conjunction with time-dependent calculation	Human-error and dependent-failure contributions can be modeled; FRANTIC-II can handle time-dependent failure rates and incorporates effect of renewal on aging	IBM 360/370 Fortran IV Available from Argonne Software Center
GO	GO chart* and fault-tree failure data	Only time-independent calculations for gates and top event; nonrepairable or periodically tested primary events are handled	No	No	Cut sets for selected gates and probability truncation of cut sets up to order 4	CDC 7600 Fortran IV Available from EPRI
IMPORTANCE	Minimal cut sets, primary-event failure data	Top-event point-estimate probability or unavailability	The following importance measures can be calculated: Birnbaum, criticality, upgrading function, Fussell-Vesely, Barlow-Proschan, steady-state, Barlow-Proschan, sequential contributory	No	Cut sets and primary events can be ranked on basis of each importance measure	CDC 7600 Fortran IV Available from Argonne Software Center
KITT-1 and KITT-2	Minimal cut sets supplied directly or by MOCUS or PREP; primary-event failure data	Time-dependent unavailability for primary events, minimal cut sets, and top event; failure rate, expected number of failures, and unreliability for top event and minimal cut sets	Fussell-Vesely importance calculations for primary events and minimal cut sets	No	KITT-2 allows each component to have unique time phases and thus failure and repair to vary from phase to phase	IBM 360/370 CDC 7600 Fortran IV Available from Argonne Software Center
MOCARS	Minimal cut sets or reduced system equation, primary-event failure data	No	No	Similar in method to SAMPLE, but handles exponential, Cauchy, Weibull, Pearson type IV, and empirical distributions	Microfilm plotting of output distribution. Kolmogorov-Smirnov goodness-of-fit test on output distribution possible	CDC Cyber 76 Fortran IV Available from Argonne Software Center
PROSA-2	Reduced algebraic function for system representation, failure data	No	No	Similar in method to SAMPLE, but can also handle any distribution in the form of a histogram, truncated normal, and beta distribution	Input parameters can be correlated; no sorting necessary to obtain top-event histogram	IBM 370 Fortran IV Available from Argonne Software Center

Table 1.2 (Continued)

Code	Input	Quantitative calculations	Importance calculation	Uncertainty analysis	Other features	Type of computer, language, and availability
FUFD	Reduced algebraic function for system representation, failure data	No	No	Distribution of primary events propagated up to top event, for which mean, variance, and third and fourth moments about the mean are calculated	--	CDC 7600 Fortran IV Available from Babcock & Wilcox
BALLY	Fault-tree description, control information, failure data	Average unavailabilities and failure frequencies calculated for top event; time-dependent calculation possible through use of minimal cut sets	Code CRESSEX in BALLY can perform important calculations	Uncertainty analysis is possible by using minimal cut sets obtained by BALLY. Normal, lognormal, Johnson, extreme value-I, Weibull, gamma, and exponential distributions are handled	Up to 1500 components and 2000 gates can be handled. Minimal cut sets can be determined using either a simultaneous or analytical way	IBM 360/370 Fortran IV
RAS	Fault-tree description or minimal cut sets; failure and repair rates	Time-independent unavailability, expected number of failures, and frequency of top event	No	No	Phased-mission analysis possible; if fault tree is input, minimal cut sets will be calculated	CDC 7600 Fortran IV Available from Argonne Software Center
SAMPLE	Minimal cut sets or reduced system equation, primary-event failure data	No	No	Monte Carlo simulation. Three types of distributions can be used for primary event: uniform, normal, and lognormal	Used in the Reactor Safety Study	IBM 360/370 Fortran IV Available from Argonne Software Center
SPASH	Fault tree or reduced system equation, component failure data	No	No	Similar in method to BOUNDS, but SPASH can work in conjunction with WAMCUT	--	CDC 7600 Fortran IV Available from EPRI
STADIC	Reduced system equation, primary-event failure data	No	No	Similar in method to SAMPLE, but has an efficient method of sorting probabilities obtained in each trial; can handle normal, lognormal, log-uniform, and tabular input distributions	Up to 10 system equations and up to 75 different variables can be used in each system equation	PRIM UNIVAC 1180 CDC 7600 Fortran IV Available from General Atomic Company
SUPERFOCUS	Minimal cut sets, component failure data, time at which calculations are performed	Time-dependent unavailability, reliability, and expected number of failures for minimal cut sets and top event	Yes	No	Minimal cut sets are ranked on the basis of importance; cut sets can be read directly from MOCUS or PREP	IBM 360/370 CDC 7600 Fortran IV Available from Dept. of Nuclear Engineering, University of Tennessee
WAM-BAM	Fault-tree description, primary-event failure data	Point unavailability calculation for top event and intermediate gates; no time-dependent analysis possible	No	No	Extensive error checking possible through WAM; probability truncation of fault tree; sensitivity analysis possible by using WAM-TAP preprocessor instead of WAM	CDC 7600 Fortran IV Available from EPRI

a. OZ chart (see Section 3.6.3) is a chart that resembles a schematic of system primary events and their relations via a set of 16 Boolean operators.

Table I.3 Computer Codes for Dependent-Failure Analysis

Code	Input	Method of common-cause analysis	Other features	Type of computer, language, and availability
BACFIRE	Cut sets, component susceptibilities, location of components, and susceptibility domains	Cut sets are examined for possible common generic causes or links between all components in a cut set; cut sets that are common-cause candidates are printed	Has same features as COMCAN, but allows use of multiple locations for basic events such as pipes and cables	IBM 360/370 Fortran IV Available from Dept. of Nuclear Engineering, University of Tennessee
COMCAN	Cut sets, component susceptibilities, location of components, and susceptibility domains	Cut sets are examined for possible common generic causes or links between all components in a cut set	Cut sets that are common-cause candidates can be ranked by significance of common-cause failure output	IBM 360/370 Fortran IV Available from Argonne Software Center
COMCAN II	Fault tree, component susceptibilities, location of components, and susceptibility domain	Same as COMCAN	FATRAM is used to generate cut sets before common-cause analysis; other features are similar to those of COMCAN	CDC 7600 Fortran IV Available from Argonne Software Center
MOCUS-BACFIRE	Fault tree, component susceptibilities, location of components and susceptibility domain	Same as BACFIRE	Similar to BACFIRE, but does not need cut-set input: cut sets are generated by MOCUS and automatically passed to BACFIRE	IBM 360/370 Fortran IV Available from Dept. of Nuclear Engineering, MIT

Table I.3 (Continued)

Code	Input	Method of common-cause analysis	Other features	Type of computer, language, and availability
SETS	Fault tree	Adds generic causes and links to fault tree; cut sets that include one or more generic causes are obtained and identified as common-cause candidates	Can handle large fault trees and can identify partial dependency in cut sets; attractive features of SETS as cut-set generator justify use for dependent-failure analysis	CDC 7600 Fortran IV Available from Argonne Software Center
WANCOM	Fault tree with susceptibilities added	Uses modularization and SETS to more effectively identify cut sets that are either containing critical events, critical random events, significant common-cause events, or to describe common-cause sets for each random failure	Can identify common total or partial links between components of fault tree; can handle very large fault trees	CDC 7600 Fortran IV Available from Science Applications, Inc.

APPENDIX J

Standardized Accident Sequence Nomenclature

J.1 OBJECTIVES

Section 7.1.1.4 of this guide calls for presentation of the dominant accident sequences in terms of the standardized nomenclature presented in this appendix. The aim of establishing a standard nomenclature for accident sequences is to provide reviewers and users of PSA studies with a

- concise,
- clear,
- understandable, and
- intercomparable

representation of important accident sequences of different nuclear reactor plants. At the same time, this nomenclature must be able to accommodate important features of present and future PRAs without requiring substantial reworking of their results or methods.

The nomenclature should thus be able to

- adapt to plant-specific and PRA-specific differences;
- include special factors deemed significant by NRC or the utilities or both;
- treat more detailed definitions elicited by improved methods and extended regulatory and safety needs;
- take account, where appropriate, of physical, functional, and operational plant conditions; and
- handle existing results.

J.2 GENERAL FORMULATION

In order to embrace the results of existing concurrent PRAs and the general (though variable) terminology common in this field, it is desirable to establish a nomenclature which rests on the triad of initiators I_i , frontline systems F_j , and accident physical characteristics bins Z_k , which are largely, but not exclusively, determined by containment and consequence phenomena. This approach is adopted here. Although optional, inclusion of binning is important not only for the insight it provides about the accident sequences, but also for its utility in carrying the Level 1 PRAs further to Levels 2 and 3.

The present system is typical of PRA nomenclature schemes in that it includes initiators and frontline system failures, but it is somewhat untypical

in that it excludes support system failures (notably electric power failures) and certain other events which appear in the nomenclature of some PRAs. It will be seen below that there is scope within the present system for adding certain details of interest to the primary sequence identifier; but it is felt that standardization is easiest and clarity is greatest if the primary sequence identifier is kept as simple as possible, and suppression of support system failures contributes to these goals.

The general formulation of this nomenclature is set out below, together with some explanatory comments. The following section lists the suggested specific definitions for the I_i , F_j , Z_k . (Since the nomenclature is constructed to allow expansion and extension, the lists are not to be considered exhaustive.) The notation I_i , F_j , Z_k is used here (in this section) for purposes of discussion only: the actual notation listed in Section K.3 uses wherever possible the more familiar (and in a historical sense more suggestive) letters associated with previous studies.

The primary accident sequence identification is simply

$$\boxed{I_i F_j \text{--} F_m Z_k} \quad (*)$$

which represents an accident sequence initiated by the initiator I_i , involving the failure of the frontline systems $F_j \dots F_m$ and "belonging" to the bin Z_k .

The more detailed (optional) format for an accident sequence is as follows:

$$\begin{aligned} &I_i \dots F_j \dots \text{---} F_m \dots Z_k \dots \\ \text{or} \\ &I_i(\dots) F_j(\dots) \text{--} F_m(\dots) Z_k(\dots) \end{aligned}$$

The additional indices or bracketed dots " \dots " represent additional information which serves to qualify and elaborate the primary identifiers I_i , F_j , Z_k , based on the specific plant PSA, and on the particular sequence. This information, when available, will always add useful detail to the classification, but may not be necessary for the preliminary review, except in certain plant specific cases or unusual circumstances. Typical information of this kind is briefly discussed following the individual lists.

Those frontline system failures F_n which are deterministically related to preceding failures F_j , or to the initiator I_i need not be included in the primary identification (*). They may however be usefully displayed, if the situation is not immediately obvious, in the more detailed general (indexed or bracketed) format.

J.3 NOMENCLATURE

Because of the objectives and requirements discussed above, the suggested nomenclature listed below is, at the first level, as general as possible, and

relies as far as possible on functional and operational characteristics. This allows ready comparison between the analyses of plants whose specific initiators and frontline systems might have rather different quantitative engineering descriptions. These differences in detail could be included in the additional indices (or brackets) if desired and available.

1. Initiators I_i

LOCA initiators are qualitatively determined by the associated coolant inventory loss, but the particular definitions in terms of either geometric (break size) or mitigating function requirements tend to be plant specific depending on both design and operational considerations. It is nevertheless convenient to divide them into three classes, and the index or bracket format described above should be used to indicate the specific details.

A Large LOCA: For example, a breach of the RCS resulting in a pressure drop calling for the activation of the low pressure (high flow rate) ESF mitigation system. In many PRAs such initiators are defined by the breach area, e.g., greater than 1 ft². This, or other critical characteristics, should be identified as indicated.

S₁ Medium LOCA: For example, a breach of the RCS which results in a (lower) pressure drop which calls for high pressure (low flow rate) ESF mitigation: often characterized by breach areas between 0.55 ft² and 1 ft². Again, the geometric and functional characteristics should be identified.

S₂ Small LOCA: For example, a small breach of the RCS, with a low enough flow rate that it can be controlled by non-ESF systems, e.g., charging pumps. The geometry and mitigation should be identified.

A more detailed (or finer) subdivision could be used if desired.

This terminology is exemplary rather than definitive. It is essential that the geometric and functional details be provided to clarify the plant specific variations.

V Interfacing System LOCA: This is a LOCA leading to bypassing of containment.

T. Loss of Off-site Power transient.

T Other transients $i \neq 1$.

The primary index i may be used to identify particular transients such as turbine trips, loss of main feedwater, and others that may apply. In a number of cases, transient initiators, followed by one or other frontline system failures, result in LOCA conditions, which in turn lead to exactly the same further behavior (sequences) as engendered by the corresponding A or S_i. From the point of view of the quantitative contribution to the CDF (core damage frequency) it is adequate and convenient to lump these with the corresponding S-sequences. However, considering some aspects of plant intercomparability and operational and functional insight it is important to note the genesis of such contributions. This may be done by applying the indexing (or bracketing)

method described above to the S-sequence, e.g., $S_1(T_1F_2)$, denoting that the medium LOCA S_1 was generated by the transient induced sequence $T_1F_1F_2$. In particular, such identification should always be given in the case of transient induced LOCAs and in the case of LOOP initiated by in-plant phenomena.

2. Frontline System Failures

For historical and engineering reasons it appears desirable to distinguish somewhat the proposed nomenclature for PWR and BWR plants. (It would however be possible to develop a single non-overlapping system if required.)

(a) PWR

C failure of containment spray system.

For those systems with different success criteria for which operation of the injection and recirculation can be appropriately distinguished the index i , should be used to distinguish the corresponding failures, viz.

C_i Failure of containment spray injection system

C_r Failure of containment spray recirculation system

The same type of notational distinction should be adopted for those other systems listed below for which it is appropriate.

G Failure of the containment heat removal system

D Failure of the low pressure emergency core cooling system

K Failure of the reactor protection system

L Failure of the auxiliary feedwater system

M Failure of the power conversion system

N Failure of the secondary system steam relief valves

Q Failure of the PORVs to reclose after opening

R Massive rupture of the reactor vessel

U Failure of high pressure core cooling system

Y Failure of reactor building cooling system

This classification is slightly more expanded and somewhat more rationalized than the familiar RSS version. For example, the old TMLB' (from the RSS) now might appear as $T_1(\Xi)$, where the symbol " Ξ " represents failure to recover electric power within a (defined) specific time. Other extended or bracket information could include

- functional and operational peculiarities;

- the system success criteria and associated support systems failure;
and
- specific failure mode information.

(b) BWR

K The failure of reactor protection system

The following indices should be used to identify the particular distinct failure modes:

- m mechanical operation
 - e electrical activation
 - a alternate rod insertion
 - s standby liquid control system
 - t timely scram.
- L Failure to limit reactor vessel high water level
- M Failure of overpressure protection system
- P Failure of RVs to reclose after opening

The primary index n may be used to indicate the number of SORVs involved.

- Q Failure of the feedwater system to provide core make-up water
- R Failure of recirculation pump trip
- R_f Failure of recirculation pump trip and feedwater runback
- V Failure of low pressure

Indices may be used to identify distinct aspects of such failure. However, the indices i and r should be reserved for the injection and recirculation phases.

- U Failure of high pressure core cooling system.

(Again with appropriate [defined] indices.)

- W Failure of containment heat removal system
- X Failure of depressurization system
- X_i Failure to inhibit depressurization

Similar remarks to those made regarding PWRs apply to additional index (or bracket) information.

(c) Binning

Binning is defined by important common characteristics of the accident sequence, with special reference to the effects on containment integrity and leakage and ultimate release. This information is usually implicit (and sometimes even explicit) in the partial sequence

$$I_i \cdot F_j \cdot \dots F_m \cdot \dots$$

especially if the indexed (or bracketed) information is complete. Even in this case, it will be desirable to display the most significant bin features; in general, the detailed (index or bracketed) information may not appear in the accident sequence listing in complete form, and it then becomes important to include at least the more critical aspects of the binning in the sequence definitions. At a minimum, each sequence should include the following, as appropriate:

- Z_e Early core damage relative to time of reactor scram
- Z_{\bullet} Late core damage relative to time of reactor scram
- Z_p Containment failure (of whatever kind) prior to core damage
- Z_a Containment failure (of whatever kind) after core damage.

The following additional features (as well as others not listed here), which to a degree recapitulate implicit information in the partial accident sequences, are also candidates for inclusion in the binning information, viz.

- Containment Bypass (those sequences of Event-V type)
- LOCA with or without pressure suppression (BWR)
- Pool is subcooled or saturated when core damage occurs (BWR)
- Vessel pressure when core slump occurs
- Availability of containment sprays
- Availability of containment heat removal
- Availability of AC power and recovery times
- Condition of reactor cavity at vessel failure (water-flooded or dry)

D.4 Recapitulation

The scheme outlined above has the following properties:

- it displays the accident sequences in a relatively familiar form;

- it embraces both more comprehensive and/or more detailed formulations, without requiring either extensive translation, or loss of clarity;
- it allows the embodiment of more specific equipment, functional, and operational data as permitted or required by available data; and
- it can be used and reviewed at a variety of levels depending on the needs of the reader.

NRC FORM 335 (2-84) NRCM-1102 3201, 3202		U.S. NUCLEAR REGULATORY COMMISSION		1. REPORT NUMBER (Assigned by TIDC, and Vol. No., if any) NUREG/CR-2815 BNL-NUREG-51559 Vol. 1, Rev. 1	
2. TITLE AND SUBTITLE Probabilistic Safety Analysis Procedures Guide Sections 1 - 7 and Appendices					
3. LEAVE BLANK					
4. DATE REPORT COMPLETED MONTH: July YEAR: 1985					
5. AUTHOR(S) R.A. Bari, A.J. Buslik, N.Z. Cho, A. El-Bassioni, J. Fragola, R.E. Hall, D. Ilberg, E. Lofgren, J. O'Brien, I.A. Papazoglou, P.K. Samanta, T. Teichmann, W. Vesely, A. Unione, R.W. Youngblood					
6. DATE REPORT ISSUED MONTH: August YEAR: 1985					
7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS Brookhaven National Laboratory Upton, New York 11973					
8. PROJECT/TASK/WORK UNIT NUMBER					
9. FUNDING GRANT NUMBER A-3758					
10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include 2a Code) Division of Safety Technology Office of Nuclear Reactor Regulation U.S. Nuclear Regulatory Commission Washington, DC 20555					
11. TYPE OF REPORT Final Technical					
12. SUPPLEMENTARY NOTES					
13. ABSTRACT (200 words or less) A procedures guide for the performance of probabilistic safety assessment has been prepared for interim use in the Nuclear Regulatory Commission programs. It will be revised as comments are received, and as experience is gained from its use. The probabilistic safety assessment studies performed are intended to produce probabilistic predictive models that can be used and extended by the utilities and by NRC to sharpen the focus of inquiries into a range of issues affecting reactor safety. This first volume of the guide describes the determination of the probability (per year) of core damage resulting from accident initiators internal to the plant (i.e., intrinsic to plant operation) and from loss of off-site electric power. The scope includes human reliability analysis, a determination of the importance of various core damage accident sequences, and an explicit treatment and display of uncertainties for key accident sequences. The second volume deals with the treatment of the so-called external events including seismic disturbances, fires, floods, etc. Ultimately, the guide will be augmented to include the plant-specific analysis of in-plant processes (i.e., containment performance). This guide provides the structure of a probabilistic safety study to be performed, and indicates what products of the study are valuable for regulatory decision making. For internal events, methodology is treated in the guide only to the extent necessary to indicate the range of methods which is acceptable; ample reference is given to alternative methodologies which may be utilized in the performance of the study. For external events, more explicit guidance is given.					
14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS Probabilistic Risk Analysis Analysis Procedures					
15. AVAILABILITY STATEMENT Unlimited					
16. SECURITY CLASSIFICATION (This page) Unclassified (This report) Unclassified					
17. NUMBER OF PAGES					
18. PRICE					

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300

FOURTH CLASS MAIL
POSTAGE & FEES PAID
USNRC
WASH D C
PERMIT No G 87