NUREG/CR-2815
BNL-NUREG-51559

Probabilistic Safety Analysis Procedures Guide

Prepared by I. A. Papazoglou, R. A. Bari, A. J. Buslik, R. E. Hall, D. Ilberg,
P. K. Samanta, T. Teichmann, R. W. Youngblood/BNL
A. El-Bassioni/USNRC
J. Fragola, E. Lofgren/SAI, Inc.
W. Vesely/BCL

Brookhaven National Laboratory

**Prepared for
U.S. Nuclear Regulatory
Commission**

GPO Printed copy price: $6.50

NUREG/CR-2815
BNL-NUREG-51559

Probabilistic Safety Analysis Procedures Guide

Manuscript Completed: September 1983
Date Published: January 1984

Prepared by
I. A. Papazoglou, R. A. Bari, A. J. Buslik, R. E. Hall, D. Ilberg,
P. K. Samanta, T. Teichmann, R. W. Youngblood, Brookhaven National Laboratory
A. El-Bassioni, U.S. Nuclear Regulatory Commission
J. Fragola, E. Lofgren, Science Applications, Inc.
W. Vesely, Battelle Columbus Laboratories

Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN A3382

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 guide addresses the determination of the probability (per year) of core damage resulting from accident initiators internal to the plant and from loss of offsite electric power. The scope includes analyses of problem-solving (cognitive) human errors, a determination of importance of the various core damage accident sequences, and an explicit treatment and display of uncertainties for the key accident sequences. Ultimately, the guide will be augmented to include the plant-specific analysis of in-plant processes (i.e., containment performance) and the risk associated with external accident initiators, as consensus is developed regarding suitable methodologies in these areas. This guide provides the structure of a probabilistic safety study to be performed, and indicates what products of the study are essential for regulatory decision making. 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.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES

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 PRAs can be extremely valuable in the area of reactor safety, but it is also widely felt that PRAs 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 PRA are still evolving in some areas. Second, a wide variety of methodologies and assumptions have been used in different PRAs, 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). In the hope of providing a more intelligible body of results for purposes of interplant comparison, a "baseline evaluation" of the plant model is to be provided, along with the plant-specific evaluation. The baseline evaluation is the quantification of the plant-specific model with generic data; comparison of baseline evaluations for different plants will allow NRC and others to distinguish the effects of design differences from the effects of other variations. 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 PRA 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, and D. H. Worledge for making draft reports of EPRI work available to us.

1.0 INTRODUCTION

The overall objective of this guide is to provide NRC and the nuclear industry with a basis for the construction of a risk management model that can be used in a cost-effective manner 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,

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 research 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 chose not to treat the risk from external initiating events in this guide. 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 has decided to include external events by augmenting this guide at a later date.

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 meltdown 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 required 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. Nor are they required to do thermal-hydraulic plant transient analysis which would yield core or component thermal conditions.

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

- Includes internal initiating events other than internal fires, floods, etc.
- Includes accidents initiated only from full power operation.
- Does not require detailed mechanistic analysis of plant behavior.
- Does not require initiating events due to natural and energetic phenomena such as earthquakes, tornadoes, fires, floods, explosions, etc. However, the loss-of-offsite power initiator is included within the study scope.
- Does not require 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.
- Treatment of cognitive human errors: In addition to modeling of procedural errors, cognitive-based human performance is included in this guide.
- 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 will be required to report specific products of their studies.

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 employed in different studies. Clearly, to be useful for the purposes described in Section 1.1, the results of PSA studies must be easily assimilable by the community of reactor safety specialists. In particular, they must lend themselves to comparison with each other. It must 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.
- In addition to the fully plant-specific calculation, the guide calls for a "baseline evaluation" of core damage frequency. In the baseline evaluation, generic data supplied here are used to quantify the ac-

cident sequences defined for the subject plant. The result of this calculation is not necessarily expected to be representative of a given plant's likelihood of core damage; rather, since baseline evaluations for all plants are carried out with the same data, comparison of baseline evaluations for different plants is expected to provide insight into design differences. The baseline evaluations are a kind of sensitivity study: individually, they highlight the effect of different failure probabilities on a given plant's likelihood of core damage; collectively, they highlight the effect of design differences between plants.

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 Baseline Evaluation

The baseline evaluation is to be performed with generic failure probabilities given in Appendix C. Additionally, the sensitivity study prescribed in Section 6.5.4 is defined in terms of the baseline data base. However, for purposes of the plant-specific evaluation and the systems interaction studies, the level of resolution of the fault tree may very well differ from that of the baseline data base. Therefore, the fault trees should be so constructed as to lend themselves to quantification at different levels. For example, diesel driven pump failure appears in the data base, and the "Remarks" column indicates that this event includes failures of the pump, diesel, lube oil system, fuel oil, suction and exhaust air, and starting system. It may well be desirable to develop this event in finer detail; if this is done, the tree should still contain an event "diesel-driven pump failure to start," which can be unambiguously correlated with event 1.3.3 in Table C.1 of Appendix C.

1.3.1.2. 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.

1.3.1.3. 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.

1.3.1.4. Systems Interaction Studies

In its present form, this guide uses only indirectly the products of the systems interaction study. Essentially, the study is used to ensure that functional dependences have been correctly included in the models. However, NRC will shortly issue guidelines for system interaction studies; at that time, more direct use of the products will be made, and more specific guidance will

be given. Spatial coupling, for example, will assume more importance than seems to be the case, and the process of gathering information about failure modes of components should reflect this.

1.3.1.5. External Events

Earthquakes and other external catastrophes are beyond the present scope of this program. However, extension of the scope to include such accidents is expected. For example, vulnerability of components to seismic events must ultimately be assessed. Since substantial information about components is being gathered under the present scope, it may save effort to anticipate studies of external events now, by gathering this type of information at the same time. Additionally, such features as passive failures will assume greater significance in the fault trees when the scope is broadened, and effort may be saved in the long run if these are included now rather than retrofitted later.

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 Familiarization

This task describes how the analysis team becomes familiar with the plant design and information related to it. The analysts will become familiar with operation and administrative procedures. They will also gather together plant and site-specific information to be used in the accident sequence definition task. This task closely follows the plant familiarization process discussed in the IREP Procedures Guide. This task includes a specification of the initiating events to be considered. Events relevant to current licensing and regulatory issues are incorporated. Frontline systems and support systems are defined.

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. 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 post-accident 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.

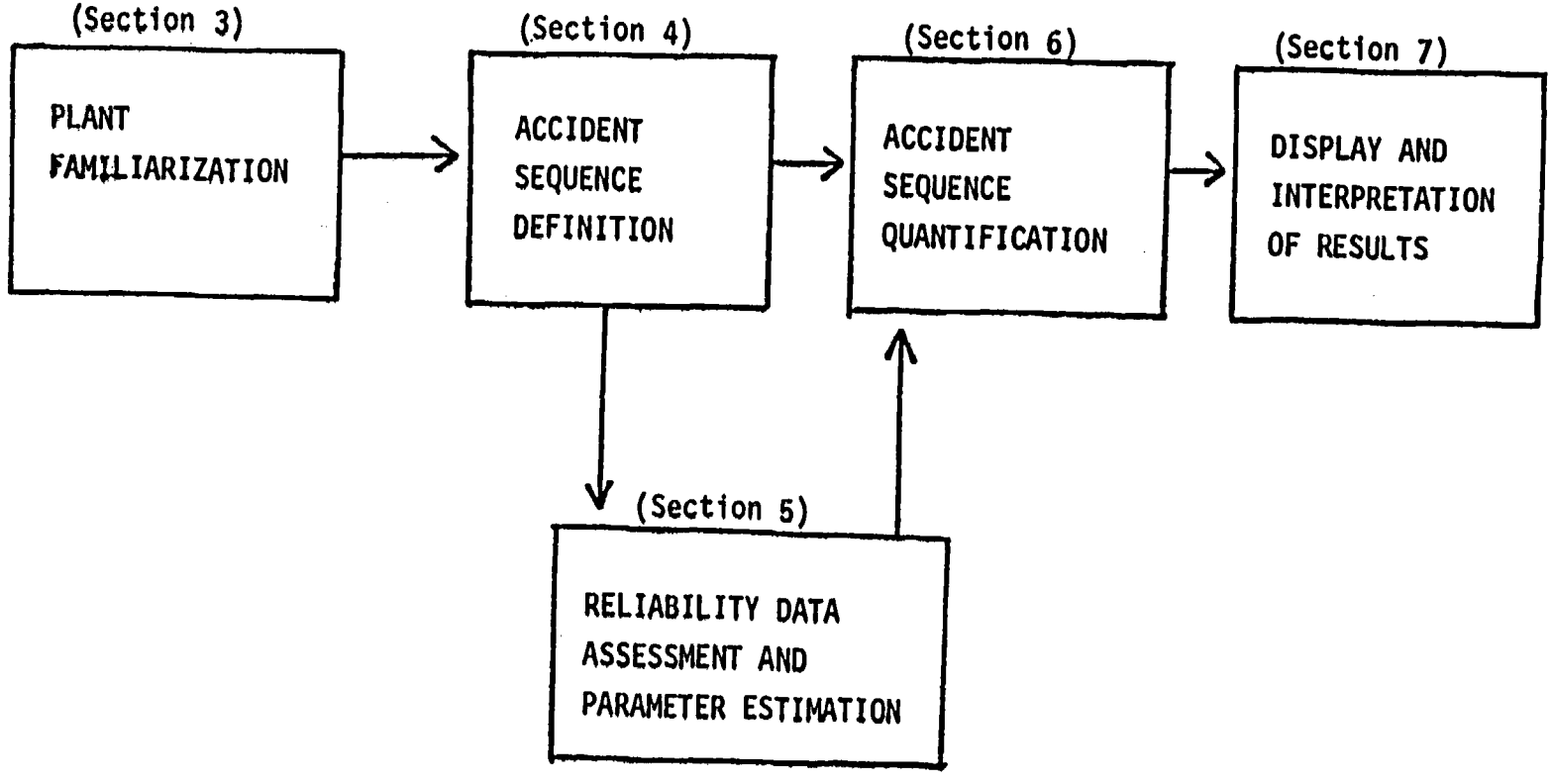

Figure 1.1 Major PSA Tasks

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 PSA study. This task consists of five main subtasks: generation of Boolean Equations for Accident Sequences; accident sequence classification; baseline evaluation; plant-specific evaluation; 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.

2.0 PSA ORGANIZATION AND MANAGEMENT

2.1 Management Goals

Discussions of how to organize and manage a PSA are given in the IEEE/ANS Procedures Guide (NUREG/CR-2300) and in the IREP Procedures Guide (NUREG/CR-2728). Among these documents one can find helpful guidance on topics such as the expertise and composition of the analysis team, schedules and manpower estimates by task, reporting, documentation of results, and assurance of technical quality. These are important for a successful PSA study and the documents will be helpful to those who are to manage the particular PSA studies.

The PSA studies will undergo review by NRC and its consultants. Therefore, to facilitate the review process, it is important that the PSA studies be clearly written with assumptions clearly stated, methods amply documented, data straightforwardly presented, and supporting tools (such as computer codes) readily available for examination.

Assurance of technical quality is of great importance to any PSA. The managers and analysts of these studies should follow the guidance given in the above-mentioned documents as part of their internal management of the study. Particular attention should be given to assuring that

1) the PSA is conducted in a manner that is commensurate with the objective and scope chosen for this program;

2) reviews are obtained from various perspectives and at various key times during the course of the study.

2.2 Interactive Review

This section discusses the benefits of interactive review, and suggests an overall approach. Interactive review is a cooperative undertaking by the analyst group and NRC, with the goal of enhancing the usefulness of the PSA under review. The timing and depth of the review for any particular study must be coordinated between the analyst group and 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 baseline evaluation. This guide prescribes the baseline evaluation in as much detail as is feasible, given the kind of flexibility that is encouraged for this program; however, it is unclear that this prescription alone will be able to achieve the kind of intercomparability of analyses that is sought in the baseline evaluations. Intercomparability is an attribute which should be assessed carefully by persons outside the team which is performing the study. Another area deserving special emphasis 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 PSA 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.

3.0 PLANT FAMILIARIZATION

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.

An overall familiarity with all aspects of the plant is necessary for at least one member of the team, to help avoid errors occurring at the interfaces between tasks. It is essential to have plant operations experience represented in the analysis team.

3.2 Scope

Under the present scope, PSAs will determine the frequency of core damage and the operability of containment systems and will quantitatively handle only internal initiating events, except for loss of offsite power. 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 certain qualitative information useful for a later extension to external events, fires, and floods, as well as for systems interaction studies.

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. The plant familiarization 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 this task 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

This information is, of course, best utilized with the help of the plant personnel who are involved in the study. 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.

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.

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).

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

Transients are identified. The standard list of transients in EPRI-NP-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).

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 PSA 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 must ultimately be confronted by PSA studies. At present, they are within the scope of the Qualitative Dependence Analysis subtask. Guidance in this area is forthcoming as a result of the resolution of the unresolved Safety Issue A-17 (Systems Interaction). At present, development of these scenarios is optional, although it is pointed out elsewhere in this guide how PSA studies can beneficially anticipate extensions to this and other areas.

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

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

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. Under present guidelines, only those dependent failures explicitly modeled on the fault trees and event trees are included in the estimates of core damage frequency; beta-factor methods or Marshall-Olkin specializations (see, e.g., NUREG/CR-2300, Rev. 1, p.3-90 ff.) are not to be used. It is left to the sensitivity studies to address the effect of possible coupling between failures beyond that which is explicitly modeled. In this way, one gains some insight regarding the relative importance of certain classes of coupled failures, without burdening all the quantitative results for core damage

frequency with the uncertainties associated with parametric methods. But the explicit modeling in the studies must be correspondingly thorough, if the core damage frequency is not to be signficantly underestimated.

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 MULTSTRCRUD 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 why it is out of scope; and if out of scope, 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].

4.0 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 4.3.2, discussing the impact of physical processes on logic tree development, also supplies input to this task. In certain cases, where operator errors of a cognitive nature are placed in the systemic event trees, Section 4.3.1 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.

Ultimately, both a baseline evaluation and a plant-specific evaluation of the model are required. It is inherent in the baseline evaluation that the prescription of it dictates a level of resolution of the fault tree. However, it is not the intent of this guide to constrain the plant-specific model to this level of resolution. The fault trees should be developed in such a way as to permit quantification at a level corresponding to the baseline data, as well as quantification at the level chosen for the plant-specific analysis, which will reflect considerations of (1) dependence and common-cause analyses, (2) the character of the plant-specific data base, and (3) the plant-specific failure modes not covered in the baseline data.

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.

Environmental common causes, e.g., fire, dust, ice, etc., are not at present treated in a comprehensive manner.* Other commonalities such as manufacturing deficiencies and installation errors are also not treated comprehensively. However, they are addressed in Section 6 under Sensitivity Analysis. Finally, factors describing "other" unspecified causes of system failure are not to be included as part of the analysis.

Although the explicit modeling of dependent failures is currently limited to the above, the information base which is developed should be substantially broader than this limitation would suggest. There are two major reasons for this.

1) 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.

---

*This is a temporary assumption until the scope of qualitative dependence analysis (see Section 4.3.3) is determined by NRR/NRC.

2) It is very likely that the scope of this task will soon be extended to include environmental effects (earthquake, fire, flood, etc.) and associated passive failures, and that the scope of the systems interaction task (qualitative dependence analysis) will soon be completed. This will require much additional information, which can be gathered and presented together with that portion which is immediately necessary for the purposes listed here.

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 Familiarization (Section 3)
3.	System success criteria.	
4.	System dependence diagrams.	
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 Information (Licensee)
13.	System descriptions.*	

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

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 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.

---

*Some normal operating procedures may also be required.

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 offsite 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.

Extension to External Events

The current scope of these studies does not include the analysis of external initiators. A very limited consideration of these events is included in the discussion of physical dependences (Section 4.3.3). However, NRC plans to include analysis of external initiators in the future. The analyst should recognize that much of the information needed for the analysis of these events can be collected during the plant familiarization phase. Information gathered in the effort described above in Section 4.2.2 and in Section 4.3.3 should be put in a format that is readily applicable to any future studies. With these extensions in mind, the analyst may choose to enhance future usage and

versatility of the plant models by incorporating the impact of external initiators now. His discussion should strike a balance between the benefits of the additional information and modeling requirements on the one hand, and their associated cost on the other.

Segmentation

If desired, an approach where piping and wiring are segmented may be used. This approach is described in the IREP Procedures manual on p. 64ff.

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.

If the scope of this task is expanded 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.

If the scope of this task is expanded to include consideration of potential systems interaction, an additional product will result which consists of tables of dependence information for each system relating the dependences of each train and major component to each other and to other plant systems.

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 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).

4.3.1 Human Performance Analysis

4.3.1.1 Purpose

The purpose of this section is to provide guidance for the treatment of human errors. At present, the level of consensus in the PRA community regarding the treatment of human errors does not justify the prescription of any extant methodology for use in detailed plant-specific calculations; some latitude is therefore allowed in the treatment of human errors in the plant-specific results. However, in the interests of scrutability and verifiability, a screening procedure is prescribed here, which will display all human errors identified as being of potential concern, and will show which were found to be risk-significant.

4.3.1.2 Scope

This task covers the analysis of all human acts identified during the course of a risk assessment as being of potential concern. The approach therefore addresses both procedural and post-accident problem-solving types of human behavior.* The suggested technique, which is depicted in Figure 4.1, consists of a successively more detailed analysis of events. The level of analysis selected for an individual event is determined by the sensitivity of

*For a description of procedural and problem-solving (cognitive) behavior, see the bibliography in Appendix B of this document.

risk to its probability. First, an attempt is made to identify human errors of potential concern, primarily from a consequence-oriented perspective, in which an event probability is considered only grossly in terms of event credibility. Next, the risk sensitivity of each credible human error is assessed by means of the first phase of the baseline evaluations (Section 6.3): preliminary core damage frequencies are calculated using screening values for each credible human error, and generic failure probabilities for hardware failures. The importance of a human error is determined from the contribution to core damage of the cutsets in which it appears. Finally, detailed plant-specific quantification is undertaken for each identified important human error.

4.3.1.3 Input and Output

4.3.1.3.1 Introduction

When the event trees and the fault trees are developed, the man-machine interface is addressed. Since an evaluation of the potential for human error and its effects on the system can be a driving force at both stages of the analysis, it is essential to use a systematic approach to include the human. This section addresses the inputs and outputs required to perform the needed analysis, as suggested in Section 4.3.1.4. The analyst should note that the methodology presented here requires an integrated human performance evaluation and systems analysis team. In addressing the completeness question, the systems analysts and the human performance analysts will iteratively exchange information as the analysis proceeds; but the iterative ties between the human performance evaluation and the fault trees and event trees will not be presented here, since they could involve many stages and should evolve depending on the team assembled and the management review philosophy. Instead, we will address the basic input and output as shown in Table 4.1.

4.3.1.3.2 Input

The human performance analysis task requires the identification of events within the plant that relate to human behavior. These events are extracted from the Accident Sequence Definition within the event tree and fault tree analysis. These events, together with sufficient information to justify the assignment of screening values, are input to the screening calculation. From the

Table 4.1

Human Performance Analysis Task Relationships - Input and Output

Input	Uses In This Task	Output
(Accident Sequence Definition) included in the event trees and fault trees	Identifies human acts of potential concern and their operational and situational environment so that probability calculations can be made	List of categorized human errors and screening probability values for each
Initial screening probability values for both procedural & cognitive acts & detailed procedural data tied to specific events (Rel-	Screening quantification of human errors for sensitivity evaluation & for detailed quantification of risk-significant human errors	List of ordered human errors based on risk contribution
Ordered list of human errors (Accident Quantification)	Identification of human errors for which closer scrutiny is required to reduce conservatism & to narrow the uncertainty	List of potential risk-significant human errors to be further analyzed
Plant design information, operations, & maintenance procedures, plant walk through, operator talk through (Plant Familiarization)	Identification of design, operational, and procedural information which allows for correct nominal human error probabilities assignment & for deviations from nominal values to be recognized	List of sequence-specific quantified human errors, along with analysis & documentation for each risk-significant human error
Input	Uses in baseline evaluation	Output
Recovery Model [NUREG/CR-2728]	Quantification of all accident sequences using generic baseline data, screening values for human errors, and IREP recovery model	Baseline results

screening calculation, a list of risk-significant human errors is generated, which is input (along with other information) to the process of deriving plant-specific, sequence-specific values for each error. These final values are input to the plant-specific accident sequence quantification task.

4.3.1.3.3 Products

Following is a list of material to be supplied as part of the report:

1. a list of human errors together with their screening values (the input to the screening calculation);

2. a list of the human errors which emerge from the screening calculation as being important with an indication of which sequences are affected by each of the errors listed;

3. a catalog of the sequence-specific, plant-specific errors quantified for the plant-specific calculation, along with analysis and documentation of information pertinent to each error;

4. explanation or documentation of methods used in the plant-specific analysis.

The screening calculation is the first phase of the baseline calculation. It is discussed more fully in the section on the Accident Sequence Quantification Task, and its full output is provided as part of the output of that task. Item 2 above is an index of the human error contribution to the screening calculation.

In addition to the above output products, the human performance analysis produces input to the accident sequence quantification and uncertainty/ sensitivity tasks.

4.3.1.4 Assumptions and Methods

4.3.1.4.1 Introduction

The methodology presented in this section attempts to address human performance by incorporating numerical predictions of the probability of error, success, recovery, and multiple or dependent errors in a manner that is consistent with the requirements of the event tree and fault tree approach used in the risk assessment. The methodology covers both procedural errors (which occur with greater frequency but usually have lower consequence) and cognitive

or problem-solving errors (which occur with less frequency but usually have greater consequence). The approach suggested for procedural errors is fairly well established, but because of the state of the art in the treatment of problem-solving errors, only general guidelines for their detailed analysis are offered.

It is adequate to apply a staged analysis to human error events, in which a simple screening of most of the events is performed first, and a detailed analysis is subsequently performed only for those human errors of major importance. This approach should save time for the human factors specialists by allowing more of the analysis to be conducted by a knowledgeable engineer. For more details on the concept of a screening technique, see NUREG/CR-2728 and the results of the IREP studies.

4.3.1.4.2 Approach

The approach suggested for this task is divided into two parts. The first part addresses procedural errors. This type of behavior was modeled in WASH-1400 using the THERP technique. The second part addresses problem-solving errors. These events are characterized by extended mediational or decision-type activities, and for the most part have not been addressed in past PRAs. The approach is briefly described below.

a. Procedural Events Modeling: Recommended Practice

Most of the actions taken by a human in operating or maintaining a nuclear power plant can be described as procedural. The procedure might be externalized (i.e., a written step-by-step list) or internalized (i.e., based upon an acquired skill). These actions include normal operational tasks and responses to expected transients. Procedural errors become increasingly important as single errors (such as the inadvertent closing of one valve) become coupled in multiple or dependent errors. In these cases, the Human Error Probability (HEP) is incorporated into the model at the fault tree event level, with the initial identification of the procedural errors having usually been made by the fault tree analyst and reviewed by the human factors specialist.

As Figure 4.1 shows, after a credible event has been identified and categorized as procedural, it is assigned a screening HEP value from Section 4.3.1.4.3. These screening values are high enough that all errors having any

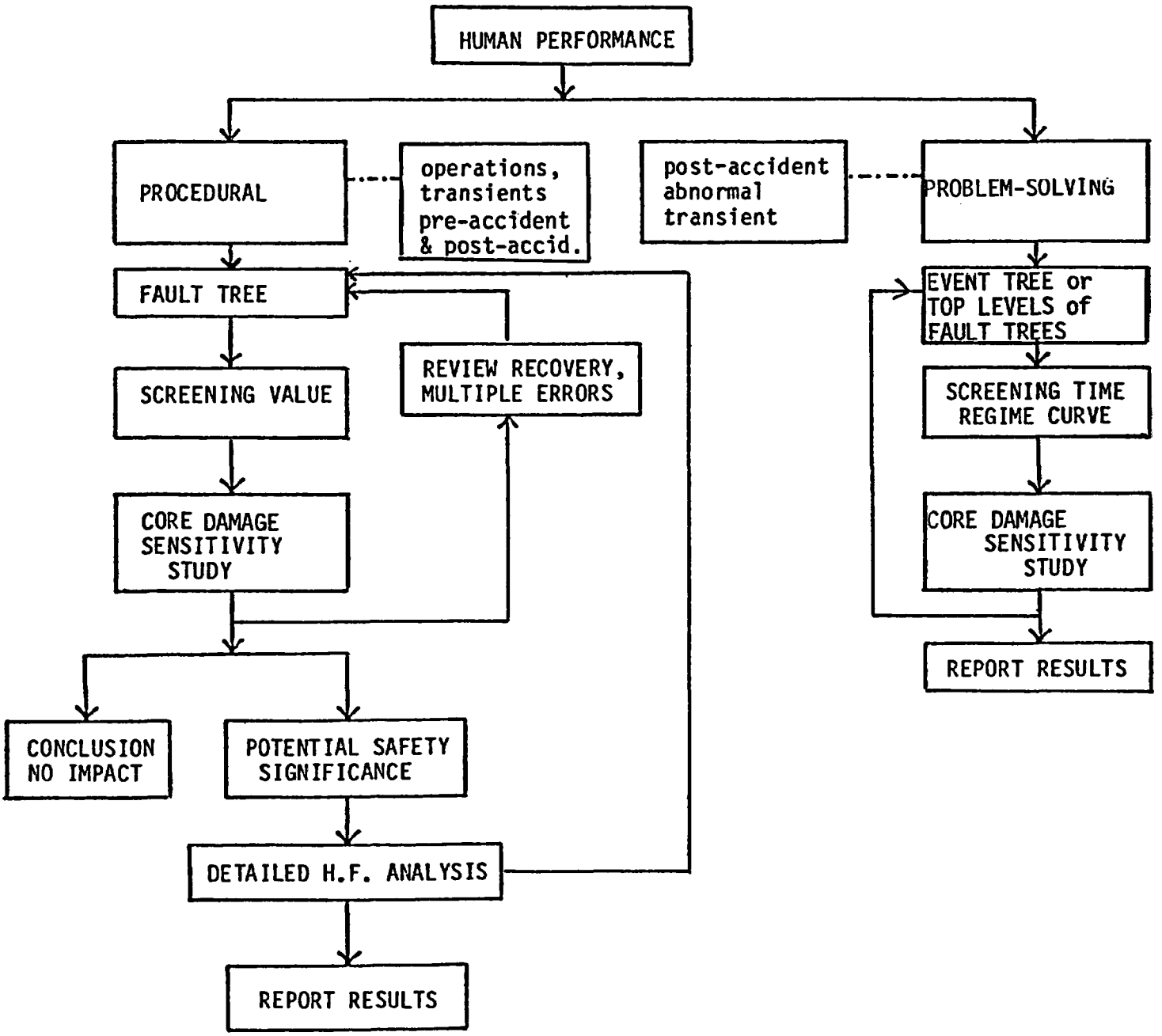

Figure 4.1 Illustrative framework for inclusion of human performance in probabilistic risk assessment.

reasonable system impact are identified, but low enough that extremely low impact events will be eliminated before the detailed analysis. With the procedural errors identified and the screening HEPs assigned, initial sequence quantification is performed to determine the risk significance of the error. This approach to selecting the risk-significant procedural events allows for a significant reduction in the number of human actions that need detailed analysis, and also allows for feedback to the fault trees. This feedback can include the effect of pre-accident recovery and multiple errors, and can produce bounds on the effects of relevant Performance Shaping Factors (PSFs). Those procedural errors which are found not to be contributors to core damage should be cataloged with reference to the applicable fault tree to allow for review.

Those procedural errors which seem to be important require a more detailed human factors review to understand the actual man-machine interface and thereby allow for the assignment of more realistic HEPs. One discussion of various ways of quantifying human error can be found in "Critical Review and Analysis of Performance Models Applicable to Man-Machine Systems Evaluations," by R. Pew, S. Baron, C. Fechrer, and D. Miller, 1977 (Bolt Beranek and Newman Inc., Report No. 3446, prepared under contract F44620-76-C-0029 for the Air Force Office of Scientific Research, Report No. AFOSR-TR-77-0520.) In addition, a review of the record of the IEEE Workshop on Human Factors and Nuclear Safety, held September 1981, should prove beneficial. As an illustration, two different approaches to quantifying the probabilities of multiple errors are presented in NUREG/CR-1278 (also NUREG/CR-2254) and NUREG/CR-2211. The level of depth required in the analysis of procedural errors can be reviewed by consulting NUREG/CR-2728 and the output of the IREP Studies. However, the field is undergoing rapid development, and the analysts should review the current literature for available models and data that may apply to their analysis. In the plant-specific calculation, the analysts should attempt to acquire and utilize data from the plant undergoing study, rather than generic data.

For this portion of the analysis, the recommendations are understandably less stringent as to the specific approach to be taken, in order to allow the analyst to take advantage of advances in the state of the art. But in the choice of procedural model and sources of specific data, the analyst must ensure that the analysis can be audited. In addition to the data output format

given in Section 5.5, a detailed report of the specific approaches taken must be provided. The report must clearly show how the input data, the model chosen, and the output values are related for each important human error.

b. Post-Event Problem-Solving Modeling: Recommended Practice

The emphasis on problem-solving errors as dominant contributors to risk - and on problem-solving processes as important elements of recovery actions - is a fairly recent development. Thus, although this area clearly must be addressed, the present state of the art does not permit a detailed prescription for such analyses. However, this section outlines a reasonable approach for dealing with problem-solving errors of omission. This approach has the following important advantages: once the important errors of omission are identified, the process of quantifying them is simple and reproducible, and readily lends itself to sensitivity studies. Ultimately, it is essential to address problem-solving errors of commission; while the ingredients necessary for such a study are not all present here, it is hoped that this approach will provide useful input to such a study. At present, it is important to recognize the omission from the studies of errors of commission.

Problem-solving errors are identified either in the event tree or at the topmost level of the fault trees. This high visibility makes problem-solving events easily identifiable and available for future analysis. Also, as the state of the art in modeling problem-solving behavior is advanced further, the risk impact of problem-solving errors can be evaluated in more detail.

As with procedural errors, credible problem-solving errors should be assigned screening HEP values to allow dominant contributors to be identified and documented. A simplistic screening model is illustrated in Figure 4.2. This approach assumes that the essential aspect of problem-solving behavior can be represented by a time-oriented phased model. This approach assumes that the decision time available is a major factor controlling correct decision making, and that it is to some degree uncoupled from the other factors (such as the skill level of the individuals, and their training). It is at least uncoupled enough that these other factors can be regarded as perturbations of the model, rather than reason for constructing a new model. Further justification for the application of a time-phased reliability model for decision errors along with examples can be found in the references given in Appendix B.

In the use of the model, problem-solving situations are investigated and the time available for decision making is established. This time does not include the annunciation or prompting time (the time it takes for the information to become available to the operator), or the time required to take action. With this decision time known, screening values for the HEPs can be assigned to the error. These values can be used in the initial quantification, as in the case of procedural errors, to identify problem-solving errors that are involved in dominant sequences. For the plant-specific calculation, it is left to the analyst to select a method for going further in establishing the HEP. There appears to be no single endorsable method available at present. However, whatever approach is chosen must be applied in an auditable fashion, as described above for procedural errors. It should be understood that the approach given here is recommended only as an interim solution to allow the analyst to include potentially important man-machine interactions that have not been addressed in the past. Recently, it has been recognized that the capability to model problem-solving errors is relatively poor in comparison to the important role they play in human performance; therefore, numerous domestic and foreign research programs have been initiated in the area. The analyst should keep abreast of ongoing work, since some of these programs may bear fruit in the near future.

4.3.1.4.3 Screening Data

Screening values for human error are given in Table 4.2 and Figure 4.2. Procedural errors are defined as those errors occurring within a procedural framework ("within procedures where a series of steps are followed in a regular order"). Problem-solving errors are defined as those errors committed in situations which lie outside the procedural framework ("out of" procedures), or situations which call for a nontrivial diagnosis of the plant condition.

Screening values for problem-solving errors, shown in Table 4.2 and Figure 4.2, have been categorized in time regimes with appropriate error bounds. For the screening quantification, only the nominal values will be used. Values are also given in Table 4.3-2 for procedural errors under two general conditions: (a) recovery is still possible at the point of error, (b) recovery is no longer possible. The screening values for problem-solving errors represent the best guess probability of error as a function of decision time. Here, decision time is the time available for the operator to take action given that an

event has occurred, less the time for the mechanical annunciation of the event and less the actual time required to take the action decided on. The recommended values are applicable only to problem-solving errors that are in response to existing abnormal transient or accident conditions.

4.3.2 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.

4.3.2.1 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,

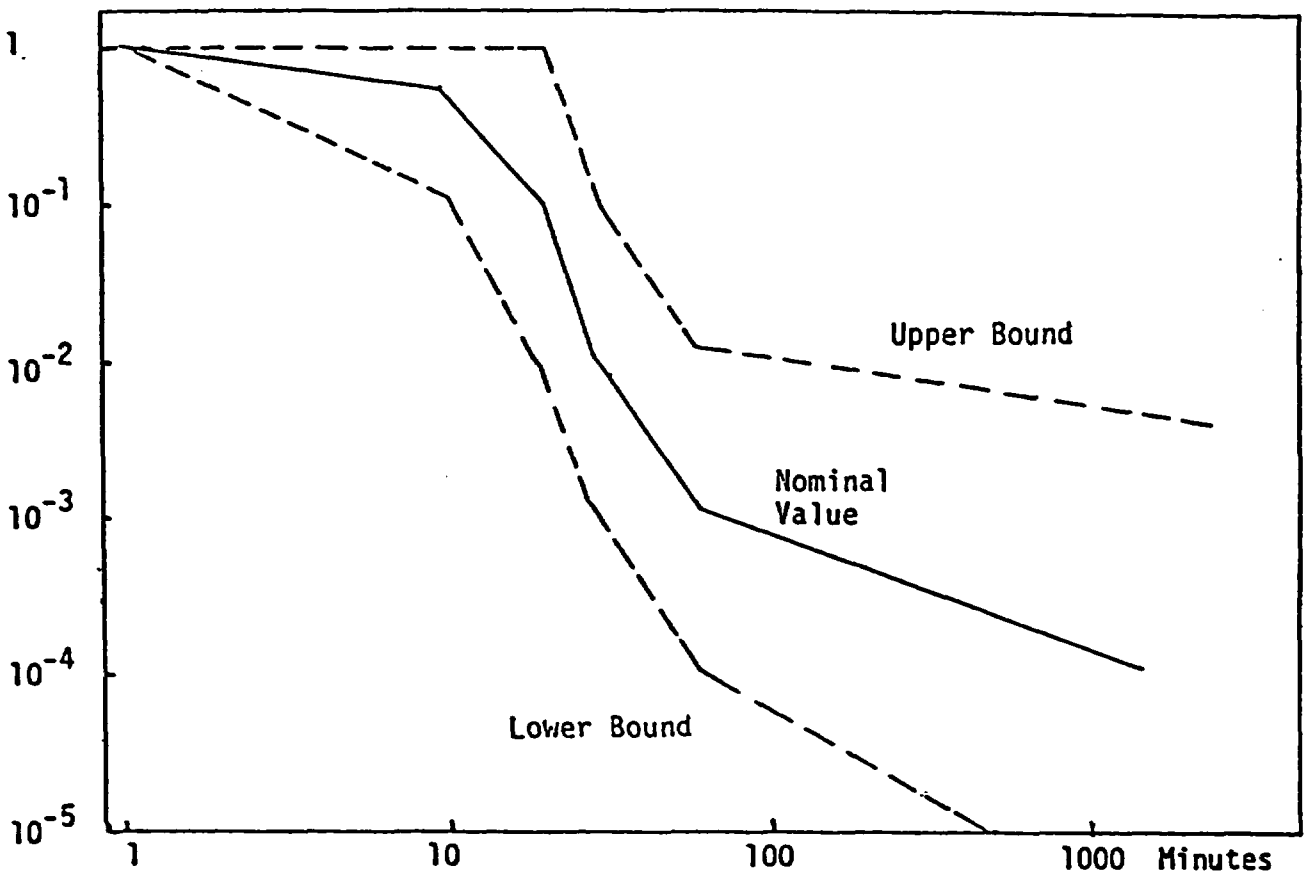

Figure 4.2 Problem-solving human error probability vs time - screening values.

Table 4.2 Human Error Probability: Screening Values

Problem-solving

Time	Nominal Value	Error Factor
<1 min.	1	---
10 min.	5E-1	5
20 min.	1E-1	10
30 min.	1E-2	10
60 min.	1E-3	10
1500 min.	1E-4	30

Procedural Errors

Nominal Value	Error Factor
1E-3 (With Recovery)	3
1E-2 (Without Recovery)	3

if the initiator is station blackout and if the containment safeguards require ac power, then they should be assumed to be failed during the accident; also, particular attention 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.

4.3.2.2 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.

4.3.3 Qualitative Dependence Analysis

Dependent events are those that are influenced by the occurrence of 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 alredyu occurred. Since a probabilistic risk assessment study is mainly interested in the existence of adverse dependences, a dependence betwen faults is usually meant to imply that the existence or occurrence of one fault increases the probability of occurrence of other faults.

In order to obtain an operational procedure for ascertaining the existence of a dependence, denote the event "a particular fault occurs" by A and the event that "another fault occurs" by B. Then, if the joint probability of these events is denoted by Pr(A•B), a dependence exists if

$$Pr(AB) \neq Pr(A)Pr(B);$$

an adverse dependence exists if

$$Pr(AB) > Pr(A)Pr(B).$$

4.3.3.1 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 by appropriate design changes. The search for dependences must involve hardware as well as human-dependent failure and errors. A result of hardware independence does not indicate the same status for the human.

4.3.3.2 Scope

A full treatment of the subject of failure dependence or systems interaction is beyond the present state of the art. On the other hand, a serious attempt to model failure dependence and systems interaction is ultimately 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

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

as earthquakes, flood, airplane crashes, or other missiles; or internally to the plant by fires, explosions, pipe breaks, etc. It should be emphasized that spatial coupling is not the only "environmental" coupling inducing physical dependences. A ventilation duct, for example, might provide an environmental coupling among devices located in seemingly spatial 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 section line could be "spatially coupled" with a crane monorail during a seismic event resulting in a loss of the charging pump section.

Type 3 Human-interaction Dependences: Dependences introduced by human actions. We can distinguish between two types: those based on cognitive behavioral processes processes and those based on procedural behavioral processes. (see also Section 4.3.1). Dependences due to cognitive human errors result in multiple dependent faults once the event has been initiated and during the actual development of an accident and can be considered dynamic. 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 and equipment positioning and calibration errors which result in multiple 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 (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 and 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.

4.3.3.3 Assumptions, Methods, and Procedural Steps

4.3.3.3.1 Identification of Dependences

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 search for and identification of dependences. The Office of Nuclear Reactor Regulation is developing, however, a Systems Interaction Program which proposes to define and subsequently implement systems interaction regulatory requirements and guidance for light water reactor plants. The techniques and procedures developed under this program should eventually be integrated with the PRA 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 combination of Event tree, Fault tree, and Failure Modes and Effects Analysis techniques.[1]

2) The "digraph-matrix analysis" which is currently being developed and documented.[2]

3) The methodology proposed by PASNY for application to the Indian Point Unit 3 plant.[3]

The main difference between these approaches is that while the first approach exclusively employs failure-oriented techniques, the second and third approaches combine failure-oriented techniques with success-oriented techniques. Thus, the "digraph-matrix" analysis combines event trees with success-oriented diagrams while the PASNY approach uses success-oriented diagrams in combination with fault trees.

The first approach addresses all three types of dependences (i.e., functional, physical, and human). The "digraph-matrix analysis" addresses functional dependences. Finally, the PASNY methodology addresses functional and physical dependences. It should be emphasized that the process of identifying dependences is not an isolated step in the performance of a PRA study, but it is an essential part of and should be performed in parallel with the development of the logic models.

In the first of the three approaches mentioned above, the strategy for identification of dependences is to perform Failure Mode and Effects Analyses (FMEA) at various levels of component resolution and to search for dependences within strings of events with undesired consequences (i.e., accident sequences at a system level and minimal cut sets at a component level). Depending on the level of resolution at which it is performed, FMEA appears in the literature under different names. If it is performed at a system level, it is called Interactive Failure Modes and Effects Analysis, Cascade Failure Analysis, or Gross Hazard Analysis. At a component level it is usually called Failure Mode and Effects Analysis.

Failure Modes and Effects Analysis

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 4.3. 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.

SYSTEM: ...,

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

Figure 4.3 List of failure modes for a given system (train, subsystem, component).

	GENERIC CAUSATIVE FACTORS	SYSTEMS THAT CAN BE AFFECTED
1		FLS_1, SS_2, SS_3 . . .
2		
.		
.		
.		

Figure 4.4 List of generic causative factors and corresponding systems (trains, subsystems, components).

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 4.3). This list includes next to each generic cause, the systems subject to the corresponding failure mode (see Figure 4.4).

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

4.3.3.3.2 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 cut sets 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 4.4) 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 4.4) will be helpful at this point. A search is made in the list of generic causative factors (see Figure 4.4) 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 4.4) should be useful at this point. The information contained in these columns helps in assessing the possibility

Table 4.3 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.	Electromagnetic interference	Welding equipment, rotating electrical 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 agent attack	Common location, ventilation ducts, hydraulic coupling
10.	Conductive Medium	Conductive gases	Common location, ventilation ducts

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.

4.3.3.3.3 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).

4.3.3.3.4 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).

4.3.3.3.5 Incorporation of Dependences in the Fault Trees

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

4.3.3.4 Regulatory Issues Related to the Qualitative Dependence Analysis Task

The qualitative dependence analysis task addresses most of the concerns of Generic 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 4.4 presents these regulatory issues along with the corresponding type of dependences. In addition, Table 4.5 identifies inputs and outputs that would be required if the issues were addressed in the PSA study.

References

1. I. A. Papazoglou and B. Atefi, A Methodology for Identification and Evaluation of System Interactions, BNL-NUREG/CR to be issued.

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, June 14, 1982 (Draft).

3. "PASNY" Methodology for Systems Interaction.

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-1901, Jan. 1981.

6. J. J. Lim et al., Systems Interactions: State-of-the-Art Review and Methods Evaluation, NUREG/CR-1859, Jan. 1981.

Table 4.4

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 GI-A-47	
d) Decay heat removal	SEP-III, 4.2.1, 4.2.2 and GI-A-45	
e) Service and cooling systems	SEP-III, 4.3	
f) Ventilation systems	SEP-III, 4.4	
3. a) Isolation of high and low pressure systems AND	SEP-III, 4.6	Component functional dependences
b) Passive mechanical failures	GI, B-58	
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 4.5

Input and Output of Dependence Analysis
Task for Regulatory Issues

Regulatory Issue	Input	Output
1. Shared Systems	- 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 nonstaggered operations. - Include dependences on relevant FT, ET.	- 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	- In the process of FT, ET development task, review any added system or equipment to identify the dependences on these support systems in particular.	- System and components appearing on FT and ET will all have an indication of which support system they depend on, if any. - Document dependences found and their significance.
3. Isolation of High and Low Pressure Systems	- 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.	- Document components discovered and their effect on core damage probability.

Table 4.5 (Continued)

Regulatory Issue	Input	Output
4. Pipe Break Effects	- Identify important cut sets leading to core damage. - Identify locations of systems and components dominating these cut sets. - Review these locations for possible pipe break impacts.	- Document results and their risk significance.
5. Risk Assessment-System Interaction	- Documentations of all the above four sub-tasks.	- Document impact of Dependence Analysis on risk. - Comments on adequacy of Dependent Analysis methodologies used.

5.0 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.

Two estimates for the probability of the events in these categories are required. First an evaluation of the accident frequencies using generic failure data is performed as a baseline calculation. Then a plant-specific evaluation is performed as the best representation of the plant's actual risk (see also Sections 6.3 and 6.4).

For the baseline calculation, the estimates for the various parameters are obtained from the generic data base provided in Appendices C to G. Plant-specific estimates are obtained according to the procedural steps described in this Section.

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.

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, their baseline frequencies, 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.

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.

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 2.1 Component failure rates and corresponding hardware unavailabilities. 2.2 Component test, repair, and maintenance frequencies and corresponding unavailabilities.	Accident sequence definition; provides guidance as to the level of resolution that is supported by the data.
3. Plant-specific component failure and repair probabilities. 3.1 Component failure rates and corresponding hardware unavailabilities. 3.2 Component test, repair, and maintenance frequencies and corresponding unavailabilities.	Accident sequence quantification; used in quantification of fault trees.
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.

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.

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.

The baseline evaluation of the event trees and fault trees will utilize the generic data given in the guide and hence will not entail any data analysis per se. It will require, however, the assessment of the basic event probabilities as described in Section 5.6.3 below. The plant-specific evaluation will entail data analysis of plant-specific records. Hence, the subtasks described in this section have as their objective the analysis of plant specific data to obtain plant-specific accident probabilities. These four subtasks are further described in the following sections.

5.5 Initiating Events

The initiating event frequencies to be used for both the baseline and the plant specific evaluations are supplied as part of this guide. 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 plant-specific 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 baseline 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. Recovery from the initiating events (e.g., recovery of main feedwater or recovery of offsite power) will not be assumed for the baseline evaluation. The probability of recovering from the initiating event will, however, be included in the plant-specific evaluation. The estimation of the plant-specific recovery probabilities is similar to that for the component repair times discussed in subsection 5.6.4.

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).

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.

The availability, accessiblity and effective usability of plant failure information of all kinds is greatly facilitated by reliance on, and conformity 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, Tp 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 unavailablity for such components is given in Table 5.5.

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	o Number of observed Failures o Total component standby time
1.2. Test outage	$\frac{\tau}{T} q_o$	τ: Average test duration q_o: Override unavailability (if applicable) obtained from system analyses	τ o Observed test durations
1.3. Repair outage	$\lambda_s T_R$	T_R: Mean time to repair	T_R, T_m
1.4. Scheduled Maintenance	$f_m T_m$	f_m: Scheduled maintenance frequency (includes interface maintenance) T_m: Mean time of scheduled maintenance action	o Observed individual times for repair and maintenance, respectively, including detection and wait time

TABLE 5.5 (Continued)

Component Unavailability Expressions for Standby Systems

Component Type/ Unavailability Mode	Time-Averaged Unavailability Expression	Parameter Definition	Data Requirements for Parameter Estimation
2. Untested Standby Component	$1 - \frac{1-e^{-\lambda_s T_p}}{\lambda_s T_p}$	λ_s: Standby failure rate T_p: Fault Exposure Time	$\frac{T_p}{}$ Inferred from replacement times of component 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

Component Unavailability Expressions for Online Systems

Component Type/ Unavailability Mode	Time-Averaged Unavailability Expression	Parameter Definition	Data Requirements for Parameter Estimation
1. Nonrepairable Component	$1-e^{-\lambda_o T_M}$	λ_o: Operating Failure Rate T_M: Mission Time (obtained from success requirement)	$\frac{\lambda_o}{T_R}$ • Number of observed Failures • Total time-to-Failure
2. Online Repairable Component	$\frac{\lambda_o T_R}{1 + \lambda_o T_R}$	T_R: Mean Time to Repair	Observed individual times for repair

(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_o 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 5.6. The parameter λ_o (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_o 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. 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

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

This gamma distribution is to be used in propagating failure rate uncertainties as described in Section 6.4.

The same procedure is to be used in estimating operating failure rates λ_o 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 baseline 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 $t_1,\ldots t_N$, the average repair time T_R is estimated as

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

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 baseline 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_o 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_o is

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

When t_o 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_is. 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 baseline 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 baseline 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 state of the art in the collection and presentation of human error data to support a risk assessment lags that for the other events discussed here (cf. Section 4.3.1 and Appendix B for discussion). For the problem-solving errors, there are no recognized sources of "standard" information. For the procedural errors, only one recognized source of generic information is in general use, Chapter 20 of NUREG/CR-1278. Even this source has several shortcomings, arising primarly from the lack of reproducibility of the results obtained due to subjective interpretations of the analyst. The reproducibility can be improved if the reasons for the choice of the nominal HEP are systematically derived from a review of the behavioral (action dependent) and situational (contextual dependent) content of the postulated event, and clearly documented. If deviations from the nominal are postulated, they should be clearly identified and the justification for the deviations must be documented.

For the reasons stated, there are no "models" in the usual mathematical-statistical sense for the development of individual human error probabilities. Although psychological models for behavior do exist, they are for the most part unvalidated and are only now being applied to the development of human

error probabilities. For this reason, the data given are either empirically derived or clinically based, or are based upon the clinical modification of empirically derived data. Section 4.3.1 describes the procedures that are to be used in assessing human error probabilities, including the application of the data in NUREG/CR-1278.

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 frequence.

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 $\leq$ 10 items).

EVENT GROUP DESIGNATION & DESCRIPTION	EVENTS INCLUDED IN GROUP	TOTAL EVENT OCCURRENCES IN PLANT HISTORY	GENERIC FREQUENCY	PLANT-SPECIFIC FREQUENCY			RECOVERY TIMES		COMMENTS
				MEAN VALUE	SCALE PARAMETER	SHAPE PARAMETER	MEAN VALUE	DISTRIBUTION PARAMETERS	

Figure 5.1. Example of data table for initiating event quantification.

COMPONENT DESCRIPTION AND FAILURE MODE	PLANT-SPECIFIC						GENERIC POINT VALUE	COMMENTS
	COMPONENT BOUNDARY	NUMBER OF FAILURES	TOTAL TIME	MEAN VALUE	SCALE PARAMETER	SHAPE PARAMETER		
1) System: Safety Injection Component Type: Safety Inj. Pumps Failure Mode: Fail During Oper.	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.

6.0 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: Baseline Evaluation
- Section 6.4: Plant-Specific Evaluation
- Section 6.5: Importance and Sensitivity Analyses

The products resulting from completing these tasks are:

- Dominant accident sequences and the dominant cutsets for these sequences.
- Minimal cutsets for systems involved in these sequences.
- Binning of all accident sequences.
- Baseline and plant-specific point estimates for the dominant accident sequences.
- Baseline and plant-specific 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, cutsets, 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.

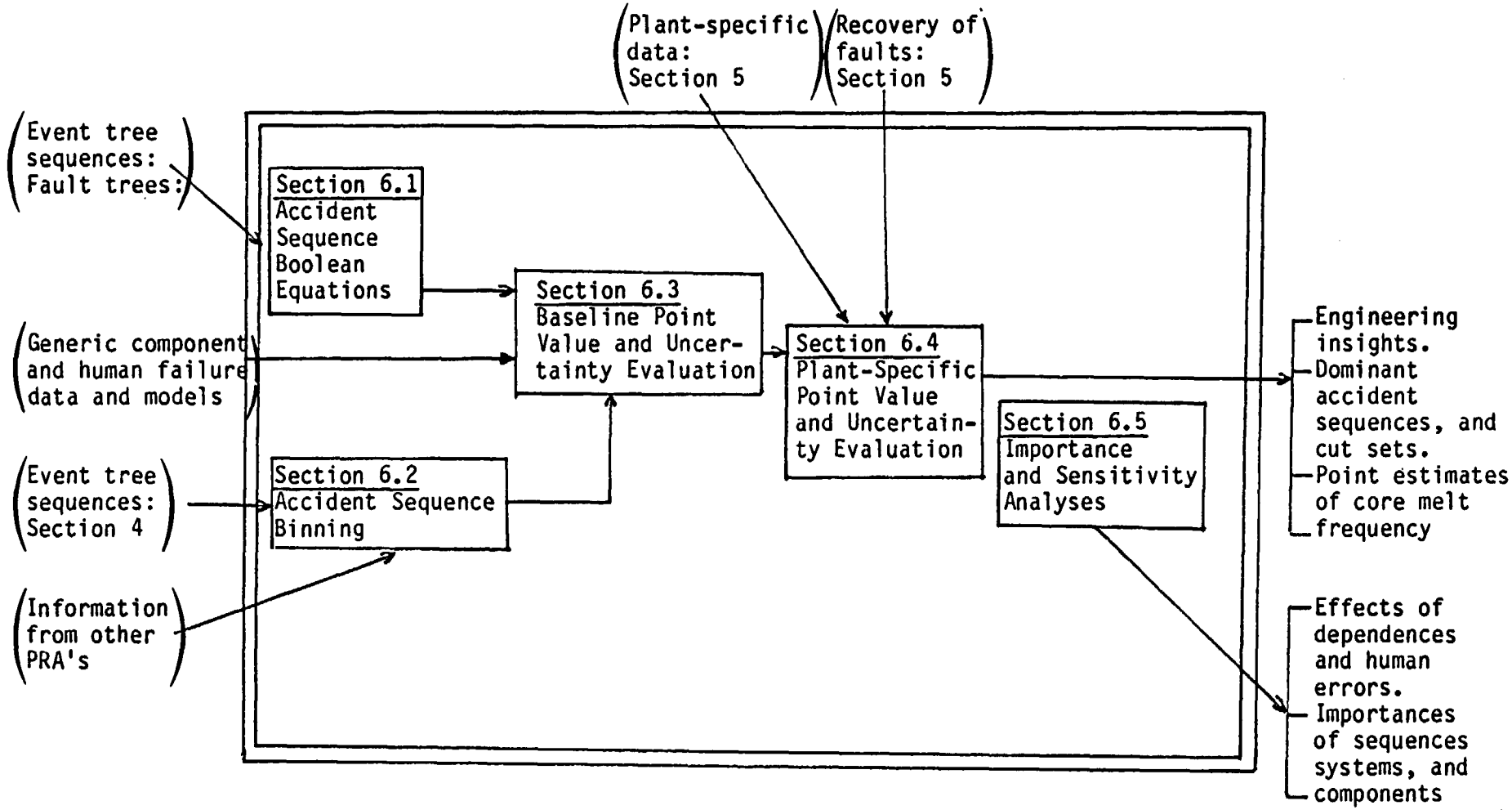

Figure 6.1 Information Flow Block Diagram.

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 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 cut sets) 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.

Dependence Loops

Dependence loops arise when there is a circular dependence of support systems on each other. An example is a diesel generator that depends on component cooling water, while the component cooling water system depends on the diesel generator during a loss-of-offsite-power accident. Proper modeling should take advantage of conditionalities to avoid circular logic.

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 (cut sets) 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 J 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.

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.

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)	

6.2.3 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

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

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)

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 Baseline Evaluation

6.3.1 Purpose

The purpose of the baseline evaluation is to obtain a point estimate of the accident sequence frequencies and core damage frequency using the baseline data set. The baseline evaluation provides generic perspective and insights into the risk impact of plant-to-plant design differences. This perspective, of course, incorporates the assumptions implicit in the baseline data base. The baseline evaluation also serves as an aid in identifying important human errors on which attention must be focused in the plant-specific evaluation.

The baseline calculation is, however, inadequate for plant-specific decision making, in that it does not account for certain plant-to-plant differences which the plant-specific evaluation does incorporate.

6.3.2 Scope

All event tree sequences are to be included in the baseline quantification. The baseline quantification should be conducted using baseline component failure data, screening values for human errors, and defined baseline values for plant operational data such as test periods and times, maintenance frequencies, and outage times. The baseline 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. 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; the resulting final accident sequence frequencies are then reported as the baseline calculation.

6.3.3 Inputs

Inputs to this task are the following:

- Reduced Boolean equations for each event tree sequence
- Point values for initiating event frequencies
- Baseline component data base
- List of human errors of potential concern, together with screening values
- Baseline defined operational data, including test periods and outage times, maintenance frequencies, and outage times
- Recovery model [NUREG/CR-2728]
- Output of the binning task

6.3.4 Methods and Assumptions

6.3.4.1 Preliminary Baseline Results Without Recovery (Human Error Screening Calculation)

The first phase of the baseline calculation also 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 quantification should be performed using point baseline values for (mean) the initiating event frequencies, point baseline values (mean) for the component failure rates, screening values for human error probabilities, and defined baseline values for the operational data (test and maintenance times etc.). The baseline data base to be used for the quantification is given in Appendices C to G. 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 J 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 Baseline Results Including Recovery

The final baseline 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. The guidance for this step follows that of NUREG/CR-2728, portions of which are abstracted below.

Post-accident recovery credit is taken for actuation faults or pre-accident 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. The recovery model essentially relates the probability of a recovery to the cutset-dependent time which is available for accomplishment of it. Recovery acts which must take place outside the control room require more time than those which can be accomplished in the control room.

All of this is very similar to the screening approach used in Section 4.3.1 for problem-solving or cognitive errors; the difference is the following. The recovery acts discussed here are relatively simple corrections of such faults as a block valve having inadvertently been left closed; the basic event "block valve left closed" appears on the fault tree, and recovery

credit is applied only after the cutset is generated. The problem-solving errors addressed in Section 4.3.1 are involved in such situations as the need for the operator to depressurize a BWR following the failure of high pressure injection (see Appendix B); unlike the simple recovery acts discussed above, problem-solving errors of this type appear as basic events in the fault trees.

The output of this process is 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 events(s) which are being recovered, and the cutset probabilities before and after the recovery factor is applied.

6.3.4.3 Uncertainty Evaluation

A baseline uncertainty evaluation is optional. If desired, however, the baseline uncertainty evaluations should be performed using the loguniform distributions given for the component failure rates in Appendix C and the baseline gamma distributions for the grouped initiating event frequencies given in Appendix G. In performing the uncertainty evaluations, failure rates of similar components (e.g., two motor-operated valves) are to be treated as the same random variable. (This is the "coupled" uncertainty evaluation in WASH-1400.) Simulation codes are available which can perform these uncertainty evaluations or which can be simply modified to perform them; Chapter 6 of the IEEE/ANS PRA Procedures Guide discusses available codes. In the simulations, at least 1200 trials should be performed to ensure acceptable precision in the estimates. Moments methods can also be used; a truncated loguniform should be fitted to the first two calculated moments to generate the percentiles.

6.3.5 Products

Products resulting from completion of this task 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 baseline 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 baseline 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,

   2. large break LOCAs,

   3. small break LOCAs.

Evaluation of uncertainty in the baseline results is optional. If performed, it 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 cummulative percentiles of 99, 95, 90, 80, ..., 10, 5, and 1.

Table 6.3

Baseline Evaluation Inputs and Outputs

Task Inputs	Task Outputs
1. Reduced Boolean equations for each accident sequence	1. List of important human errors for further study, together with specification of criterion of importance
2. Initiating event frequencies	2. 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
3. Generic component data base	3. Point estimates for all accident sequence frequencies, core damage frequency, and bin frequencies
4. List of human errors of potential concern, together with screening values	4. Uncertainty characterization of the accident sequence frequencies core damage frequency, and bin frequencies (optional)
5. Recovery probabilities (NUREG/CR-2728)	

6.4 Plant-Specific Evaluation

6.4.1 Purpose

The purpose of the plant-specific evaluation is to reevaluate the accident sequences using plant-specific data and including the possibility of recovery of component faults, human faults, and outages.

6.4.2 Scope

All event tree sequences are again to be included in the plant specific evaluation. The plant-specific evaluation should be conducted using plant-specific component failure rate data; evaluated human error probabilities, including recovery; and plant-specific operational data.

6.4.3 Inputs

Inputs to this task include the Boolean-reduced equations (or equivalent representation), plant-specific data, and guidelines and data for assessing recovery of faults and outages.

6.4.4 Methods and Assumptions

Plant-specific calculations produce a plant-customized analysis as opposed to the standardized baseline calculation that was previously performed. The more detailed analysis is to include an assessment of the likelihood of recovery of faults and outages and a requantification of the sequences using plant-specific data.

The assessment of recovery should be performed for an entire cutset of the sequence. Thus, if a cutset consists of a pump failure and a valve maintenance outage, the assessment of recovery should address the recovery of the failure and the recovery of the outage. All assumptions that faults or outages can potentially be recovered should be explicitly justified on a case-by-case basis (i.e., for each case where some credit for recovery is given). The values used for failure to recover should be also be justified.

Point Value Evaluation

The point value evaluation should be performed in the same manner as for the previous baseline point value calculation where now the means of the

(posterior) plant-specific failure distributions are used, the reevaluated point estimates of the human error probabilities, including recovery, are used, and point estimates of the plant-specific operational data are used.

Uncertainty Evaluation

The uncertainty evaluation is to be performed as for the baseline calculation with the modification that the plant-specific gamma posteriors are used 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.

6.4.5 Products

The products of this task are the same as those from the baseline calculation where now the plant-specific data are used and recovery considered (Table 6.4). The same format should be used as for reporting the baseline calculation products.

6.5 Importance and Sensitivity Analyses

6.5.1 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

Table 6.4

Plant-Specific Evaluation Inputs and Outputs

Task Inputs	Task Outputs
1. Reduced Boolean equations for each accident sequence	1. Point estimates for all accident sequence frequencies, core damage frequency, and bin frequencies
2. Plant-specific failure data	2. Ranking of accident sequences and estimation of dominant accident sequences
3. Guidelines for assessing recovery of faults and outages	3. Uncertainty characterization of the accident sequence frequencies, core damage frequency, and bin frequencies
4. Plant-specific human error data (if available)	

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.

6.5.2 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.

---

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

6.5.3 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. 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 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.

6.5.4 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.

Component Failure Dependence Analyses

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 all redundant 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.

6.5.5 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 cut sets,

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 6.5

Importance Analysis Inputs and Outputs

Task Inputs	Task Outputs
1. Dominant accident sequence cutsets (from Section 6.4) 2. Boolean expressions for failure of frontline and support systems 3. Plant-specific failure data	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. 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. For each frontline and support system, for each distinct mission: a) system unavailability b) Fussell-Vesely importance of 20 most important cutsets c) Fussel-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 6.6 Sensitivity Analysis Inputs and Outputs

Task Inputs	Task Outputs
1. Boolean expressions for accident sequences 2. Boolean expressions for failure of frontline and support systems 3. Information regarding component locations 4. Information regarding component testing procedures 5. Classification of each component by generic type 6. Analyses bearing on mission success criteria 7. Plant-specific failure data	1. Component Failure Sensitivity Analysis: Dependence suspect minimal cut sets, 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. Description of defenses or conditions which serve to eliminate the dependences for these sensitive minimal cut sets Tabulation and discussion of single failures for each mission 2. Human Error Sensitivity Analysis: Dependence-suspect minimal cut sets, for each system, for each distinct mission Description of defenses, management controls, or conditions which serve to eliminate the dependences between the human errors in the suspect minimal cut sets 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

7.0 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 an NREP 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"[1]. 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 M.4.2 M.9.1	Fault Tree Methods System Fault Trees 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 K. 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 = $1x10^{-6}$/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

$(C_1, C_2) = (1.0x10^{-2})\ (5.0x10^{-2}) = 5x10^{-4}$
$(C_1, C_3) = (1.0x10^{-2})\ (1.0x10^{-2}) = 1x10^{-4}$
$6x10^{-4}$

[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 conjuction 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
ABC	2.2.1	5.3	4.1 (A) 4.2 (B) 4.3 (C)	13.3.1	4.1 (A) 4.2 (B) 4.3 (C)	7.8 7.9

- 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 sequnces 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 feedwater 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 familiar-izaton	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 initating 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 (Cont.)

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 functions 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 operates, 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

Table 7.2 (Cont.)

Task	Subtask	Section in Guide	Output
			[FUTURE] For each component, information regarding its location and susceptibility to environmental effects [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	List of human errors and screening probabilities for each List of ordered human errors based on importance List of potentially important human errors to be further analyzed List of sequence-specific human errors, quantified by plant-specific analysis, together with analysis and documentation for each risk-significant human error Explanation or documentation of methodology used in the plant-specific analysis
	Qualitative dependence analysis	4.3.3 (cf.Fig.4.3) (cf.Fig.4.4)	Failure modes and effects analyses for all frontline and support systems List of generic causative factors
	Regulatory issues to qualitative dependence analysis [OPTIONAL]	4.3.3.4	[cf.Table 4.5] Documentation of all discovered dependences (shared systems) Documentation of impact of shared systems on core damage probability and weak points, if any

Table 7.2 (Cont.)

Task	Subtask	Section in Guide	Output
			Documentation of component having potential to: 1) cause LOCA outside containment 2) initiate an event with loss of mitigating systems 3) cause flow diversion affecting system success Study of pipe break effects: 1) identify important 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
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		6	
	Accident sequence Boolean equations	6.1	Boolean equations for each accident sequence of each systemic event tree
	Accident sequence binning	6.2	Definition of sequence bins: system and containment status for each bin Assignment of each sequence to a bin

Table 7.2 (Cont.)

Task	Subtask	Section in Guide	Output
	Baseline evaluation	6.3	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 Point estimates of all accident sequence frequencies, overall core damage frequency, and bin frequencies, with credit taken for post-accident correction of misposition and actuation faults
	Uncertainty of baseline results [OPTIONAL]	6.3.5	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 or the top 99% of any bin
	Plant-specific evaluation	6.4	Point estimates of all accident sequence frequencies, core damage frequency, frequency of each accident sequence bin. Full documentation of post-accident recovery modeling Ranking of accident sequences and assessment of dominance of accident sequences
	Uncertainty of plant-specific results	6.4.4	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 (Cont.)

Task	Subtask	Section in Guide	Output
	Importance and sensitivity analyses	6.5	
	Importance	6.5.3,6.5.5	List of important human errors for further study, together with specification of criterion of importance 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 Point estimates for all accident sequence frequencies, core damage frequency, and bin frequencies
	Component sensitivity	6.5.4,6.5.5	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 Description of defenses or conditions which serve to eliminate the dependences for these sensitive minimal cutsets Tabulation and discussion of single failures for each system

Table 7.2 (Cont.)

Task	Subtask	Section in Guide	Output
	Human error sensitivity	6.5.4,6.5.5	Dependence-suspect minimal cutsets, for each system, for each distinct mission Description of defenses, management controls, or conditions which serve to eliminate the dependences between the human errors in the suspect minimal cutsets
	Conservative assumption sensitivity	6.5.4,6.5.5	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
Display and interpretation of results	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[1] 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 implictly 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. Issue 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 invlove 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 Relation of Regulatory Issues with a Probabilistic Risk Assessment Study, BNL report to be issued.

Table A.1

Issues of the NRC Ongoing Programs Which Can Provide Information Significant to the Conduct of the PSA Studies

A. Issues affecting the determination of initiating events and their frequency:	
ISSUE TITLE	NRC PROGRAM
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.	SEP, 3.1
.b Reactor Vessel Material Toughness.	GI, A-11
.c Pressurized Thermal Shock. [Potential for reactor vessel failure]	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. Issues affecting the determination of mitigating system requirements:	
ISSUE TITLE	NRC PROGRAM
1. Short-Term Accident 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).	TMI, II.K.2
.b Final Recommendations of B and O Task Force (e.g., recommendations 28, 29, 31, 44).	TMI, II.K.3
4.a ATWS (NUREG-0460).	GI, A-9
.b B/W Reactor Transient Response (response to anticipated transients from ICS and NNI) (Vendor Reports).	TMI, II.E.5.2

Table A.1 (Cont.)

C. Issues affecting the development of accident sequences event trees:	
ISSUE TITLE	NRC PROGRAM
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).	GI, A-8
.b Determination of Safety Relief Valve Pool Dynamic Loads and Temperature Limits (NUREG-0802 draft). [LOCA with subsequent loss of ECCS heat sink]	GI, A-39
3. Research on Phenomena Associated With Degraded Core. [Information useful to determine whether an event sequence should be considered leading to core melt]	TMI, II.B.5

D. Issues affecting the fault trees (qualitatively and/or quantitatively):	
ISSUE TITLE	NRC PROGRAM
1. Revision of IE Inspection Program (more direct verification). [Surveillance tests and maintenance activities]	TMI, I.B.2.1
2. Short-Term Accident and Procedures Review. [Procedure changes resulting from post/TMI reviews]	TMI, I.C.1
3. Auxiliary Feedwater System Evaluation. [Factor into PSA AFW reliability analysis if already performed]	TMI, II.E.1.1
4.a Orders on B/W Plants (recommendations 9, 13, 14, 16, 19).	TMI, II.K.3
.b Final Recommendations of B and O Task Force. (E.g., recommendations 1, 2, 3, 5, 7, 12, 16, 17, 18, 19, 21)	TMI, II.K.3
5. Adequacy of Safety-Related dc Power Supplies. [Information produced in GI resolution should be considered (NUREG-0666)]	GI, A-30
6. Containment Emergency Sump Performance (NUREG-0897 draft, NUREG/CR-2403). [Information produced in GI resolution should be considered]	GI, A-43

Table A.1 (Cont.)

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. Issues affecting reliability data assessment and parameter estimation:	
ISSUE TITLE	**NRC PROGRAM**
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. Issues affecting the analysis of human performance:	
ISSUE TITLE	**NRC PROGRAM**
1.a Control Room Design Improved Instrumentation Research.	TMI, I.D.5
.b Accident Monitoring Instrumentation.	TMI, II.F.1
G. Issues affecting the analysis of system interaction:	
ISSUE TITLE	**NRC PROGRAM**
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. Issues Producing General Overall Guidance:	
ISSUE TITLE	**NRC PROGRAM**
1. IREP	TMI, II.C.1

Table A.2

Issues for Which PSA Perspective Is Gained Without Being Specifically Addressed by PSA

ISSUE TITLE	NRC PROGRAM
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)

ISSUE TITLE	NRC PROGRAM
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 Signficance 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: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Initiating Events & Event Sequences									
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.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Initiating Events & Event Sequences												
4.a	Isolation of High & Low Pressure Systems (+) -High Pressure/Low Press. 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	HE	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	GI,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.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: IIE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	! COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Initiating Events & Event Sequences									
5.b	Evaluation of B/W Plants-Feedwater Transients	TMI,II.E.5.1								
6	Reactor Coolant System Vents	TMI,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: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Power Supply									
1	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 ESFs (+)									1)Review plant-specific experience of diesel failures. 2)Assess diesel-generator system reliability including support systems, status information in control room, maintenance, etc. 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.a	Emergency AC Power Systems 1)Diesel Generators 2)App.k, Electrical Inst. & Control (EIC) Review	SEP-III, 4.8.1 (SEP-II, VIII.2) (SEP-II, VI.7.C.1)								
2.b	Diesel Reliability	GI,B-56								
2.c	Swing Bus Design BWR4	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: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: IIE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Power Supply												& modifications performed in ac power reiability analysis. 3)Document impact of swing bus on ac power reliability (& impact of fixes).
3	Emergency dc Power Systems:(+) 1)dc power system bus voltage monitoring & annunication	SEP-III, 4.8.2 (SEP-II, VIII.3.B) (SEP-II,VI .7.C.1)	a			d		FT		SI	+	+	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, interfacing loads, maintenance, communication,etc. 4)Document adequacy of status information to the oper. & risk significance of dc power system.
4	Station Blackout(+)	GI,A-44					ET				+	+	1)Use information developed by the above tasks. 2)Use reliability analysis of non-ac driven systems (turbine, dedicated diesels, etc.). 3)Include event sequences of station blackout. 4)Document prob. of meltdown due to station blackout by all significant event sequences & identify existing weak points (list most important cut sets for this issue).

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREA: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	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. (+)	TMI, 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). (+)	TMI, 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)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREA: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	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 Actiatopm System (testability & adequacy)	(SEP-II, VI.7.A.3)											

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (11)	(111)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Control & Protection Systems												
3	Safety Implication of Control Systems (++)	GI,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: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Decay Heat Removal Systems												
1	Cooldown & Long-Term Heat Removal Capability (+)												
1.a	Shutdown Systems (RHR 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	RHR Shutdown Requirements	GI,A-31											

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. T FT	SPECIAL TASKS: HE SI	RELATIONSHIP WITH PSA (ii) (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to Decay Heat Removal Systems						5)Document additional surveillance & procedures for non-safety-grade systems, if upgraded reliability is required.
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	+ +	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)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	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 DHR system or function requires improvement, if any, for all relevant modes of operations.
2.b	Develop Means to Improvements of DHRS	(As above)									+		3)Provide general risk significance on proposed modifications if any required.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Safety System Reliability Analysis												
1	Auxiliary Feedwater System Evaluation(+)	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 reduction significances.
1.b	Initiation & Flow (Automatic)	TMI,II.E. 1.2				d		FT	HE		+		4)Evaluate impact of automatic initiation in terms of risk significance. 5)Review reliability of control & actuation to AFW & verify that no single failure dependences exist & no interference with manual corrective action.
2	ECCS Reliability (+)												1)Perform ECCS reliability 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
2.b	Allowable ECCS Equipment Outage Periods	GI,B61(TMI II.K.3(17)				d		FT					b)Modification if required & their significance c)Allowable ECCS equipment outage periods.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	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. 2)Include containment isolation in ETs & FTs. 3)Perform analysis of isolation initiating signals & control & verify their redundacy diversity & reliability.
5.b	Isolation Dependability	TMI,II.E.4.2	a				ET	FT		SI			

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: IIE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Safety System Reliability									
6	Containment Emergency Sump Performance	GI,A-43		ET	FT			+		1)Include system on ETs and FTs. 2)Use information produced in GI resolution. 3)Document risk significance 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 relevant accident sequences. 2)Provide bounding calculation with/without this effect. 3)Document potential risk significance of this effect.
8	Reactor Core Isolation Cooling 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 reliability. 3)Assess impact of system on risk reduction. 4)Document results & upgraded surveillance & outage procedures if upgrading required.

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Safety System Reliability									
9	Ice Condenser Containment (PWRs)	GI,B-54		ET	FT			+		1)Include ice inventory availability where relevant on ETs & FTs. 2)Assess availability of ice inventory. 3)Document risk significance of issue & surveillance 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 operation. 3)Assess allowable periods of (N-1) loop operation 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: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: IIE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Sub-Systems & Components Reliability Analysis									
1	Recirculation Loop Isolation (BWRs) (Surveillance required recirc. pumps & dischange 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: PLANT FAMILIARIZATION a	b	c	d	ACCIDENT SEQ. ET	FT	SPECIAL TASKS: HE	SI	RELATIONSHIP WITH PSA (ii)	(iii)	COMMENTS ON POSSIBLE TASKS
	Issues Related to Human Performance Analysis (require such an analysis or can benefit from)												
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 requirements for operator intervention. 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 probability.
2	Long-Term Program Plan for Updating of Procedures (+)	TMI,I.C.9						FT	HE		+		1)Document any upgrading of procedures found to be beneficial in course of study.
3.a	Safety System Status Monitoring	TMI,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: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	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)Document benefits if such exist, & list systems & equipment that should be considered for status monitoring.
3.c	Operability status of Safety Systems & ESF Valves	(TMI,II.K.1 items 5, 10)								
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. 3)Review procedures for recovery from conditions leading to inadequate core cooling. 4)Document results of this task, & its risk significance.
4.b	Additional Accident Monitoring Instrumentations	TMI,II.F.1								
4.c	Identification of & Recovery from Conditions Leading to Inadequate Core Cooling	TMI,II.F.2								

Table A.3 (Continued)

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

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: IIE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to System Interaction									
1	Risk Assessment-System Interaction (+)	TMI,II.C.3 (GI,A-17)	a	ET	FT	IIE	SI	+	+	1)Apply the SI methodology described in the PSA Procedure Guide to at least all systems indicated as "SI" in this table (dc, Diesel, Room Controls, RHR, ESW etc.) 2)Document dependences identified. 3)Include dependences in ETs & FTs. 4)Document: a)The impact on core melt probability of the dependences identified. b)Deficiencies in the proposed methodology based on the experience gained in the SI study.
2	Shared Systems (Multiple Units Station)(+)	SEP-III,4.9			FT		SI	+		1)Identify dependences due to shared systems. 2)Document dependences identified & their risk significance.
3	Pipe Break Effects:(+)									1)Identify most important cut sets to core meltdown probability. 2)Identify location of systems & components for most important cut sets. 3)Review these cut sets for the effects of pipe break if exist. 4)Document results & their risk significance.
3.a	Pipe Break Definition Criteria	SEP-III,7.1.1 (III.5.A)								
3.b	Pipe Break Effects on Systems & Components	SEP-III,7.1.2 (III.5.B)	a b c		FT		SI	+		

Table A.3 (Continued)

SEQ. NO.	TITLE ISSUE	NRC PROGRAM	RELATED PSA AREAS: PLANT FAMILIARIZATION a b c d	ACCIDENT SEQ. ET	ACCIDENT SEQ. FT	SPECIAL TASKS: HE	SPECIAL TASKS: SI	RELATIONSHIP WITH PSA (ii)	RELATIONSHIP WITH PSA (iii)	COMMENTS ON POSSIBLE TASKS
	Issues Mainly Related to System Interaction									
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 FTs. 3)Assess the level of the passive failure rates at which they have an impact on core damage probability.

APPENDIX B

Modeling of Procedural and Post-Event Problem-Solving Human Performance; A Suggested Interim Approach

When the human performance analysis is conducted, the study need not necessarily be carried out to a level of detail which is out of proportion to the precision of the end result. Thus, very detailed and manpower-intensive human factors analysis can be deemphasized. The present trend towards simpler treatments of human performance should allow more of the initial analysis to be conducted by knowledgeable engineers, rather than by human factors specialists, who are currently in short supply. This will allow the human factors specialists to concentrate on the areas of greatest potential risk. Moderation in the expected level of detail of the analyses is expected to improve their cost-effectiveness and their time-effectiveness; additionally, by not over-prescribing the analytical process, one encourages the application of new methodologies to those areas of human performance that are currently identified as important to safety. This is not to suggest that the present guide should endorse new unproven techniques, but rather that it should remain flexible so that current research in the area of human performance can be incorporated in a timely manner.

The proposed approach is directed toward two types of behavior. The first is procedural. This category of human responses consists of static behavior, which J. Rasmussen (Risø National Laboratory, Denmark) chooses to divide into a) rule-based, for response to documented procedures, and b) skill-based, for "acquired" responses. These belong to the area of potential human error that is most commonly included in a PSA. This type of behavior was modeled in WASH-1400 by the Technique for Human Error Rate Prediction (THERP). The procedural mode at a nuclear facility becomes increasingly important in proportion to the coupling between individual errors.

The reason that this "static" approach can be applicable for procedural behavior can be explained in terms of Swain's S-O-R (Stimulus-Organismic-Response) model (cf. Figure 3-1 in NUREG-1278). The applicability of the

approach hinges on the observation that for mechanical behavior the mediating activity or thinking process is of less importance, so that the model can be approximated by a simplified S-R model. This is not true for the second (organismic) type of behavior represented on Swain's figure (Figure 3-1 in NUREG/CR-1278), which will be called "problem-solving" in the present discussion. In fact, it is extended mediational activity that primarily distinguishes problem-solving behavior from the more mechanistic type. Problem-solving errors are now recognized as potentially dominant contributors to core degradation. After the initiation of an event, a single wrong decision, based on inadequate information, lack of training, or conflicting operator goals, can lead to a series of incorrect actions. This was highlighted at the 1981 IEEE Standards Workshop on Human Factors and Nuclear Safety.

The crucial required addition to the "static" model described above is a model of the thinking process. If the thinking process in its entirety were to be modeled, then the task would be indeed formidable and perhaps insurmountable. However, we do not need to model the entire process, but only the portion that deals with making correct decisions in nuclear power plant situations that could have an impact on core integrity. Additionally, the model needs only to predict the probability of an incorrect decision being made by a representative individual (or individuals). Finally, in the present state of the art, the model is only expected to predict the failure probability to within an order of magnitude or so.

This simplification greatly decreases the magnitude and complexity of the modeling task. In the past, some human reliability models have attempted prediction by trying to emulate sequences of human actions. While this type of modeling (rather than modeling the statistical performance of a representative group of hypothetical individuals responding to generalized situations) can obviously provide considerably greater insight into individual human behavior, it is an extremely ambitious and perhaps impossible task. Furthermore, while there is no doubt that this type of behaviorally oriented model is extremely useful in providing a structure for a statistically oriented model, there is considerable doubt as to its necessity for the task at hand.

If it is assumed that the essential portion of the more "dynamic" problem-solving model (which is to be constructed) is the portion which attempts to model the thinking process, then a reasonable approach would be to

concentrate on that portion. The method described here uses a time-oriented phased approach to isolate the thinking portion of the model. The approach assumes that the time available for a decision is one of the most important parameters determining the failure probability, and that it is to some degree uncoupled from the other factors (such as the particular situation at hand, the skill level of the individuals, and their training). It is at least uncoupled enough that these other factors can be treated as perturbations of the time-based model.

To isolate the thinking phase, the approach can be divided into time phases. This produces three phases for the decision process to be modeled, namely:

A. Signal Annunciation Phase - This signal detection phase is initiated at the time the system indicates to the operator, by whatever means available, that a possible problem exists. This indication may be given by a clear annunciation via an alarm, or by something as subtle as a visual walk-around survey of the control panel which provides the operator with the "feeling" that something may not be right. The annunciation phase continues through an operator's secondary review of the initial and alternative indications, and terminates when the operator is convinced he has or does not have a problem with the system.

B. Situation Analysis Phase - This phase begins at the time the operator is convinced he has a problem requiring his action. The phase includes all the activities associated with the thought process he goes through to determine where the problem is, what the problem is and what must be done about it, the amount of time he has to act, and finally precisely what action he must take. When he is convinced of the action he must take, the phase is terminated. In modeling this phase of behavior, the analyst attempts to identify operator actions that would mitigate the accident progression. The analyst does not attempt to identify and subsequently quantify those operator actions of commission that would aggravate the accident progression.

C. Operator Action/Intervention Phase - This phase begins with the operator initiating his intended course of action. It includes the performance

of all the subsidiary actions required to carry the intended course of action to its conclusion. This also includes the influence of the subsidiary actions required for recovery from errors.

From the above definitions, it is clear that the Situation Analysis Phase is where the screening activities will be concentrated. The effect of Phases A and C on the phase of interest, B, will be assumed to be dominated by the fact that time elapsing in these phases will be unavailable for the decision-making phase. This assumption is made because it is felt that the bulk of the probability of error in knowledge-based behavior lies in the decision-making process and, in fact, that the other probabilities are usually negligible by comparison. In those cases where these effects are believed not to be negligible, they should be estimated by application of a suitable version of the model used for the procedural errors.

The approach summarized above is being recommended for errors of omission, that is, for estimating the probability of failure to perform an action which is necessary for safety. Another type of error is known to be extremely important, namely, errors of commission, in which an act is performed which aggravates a given upset condition. It is believed that while the methodology discussed here is a useful starting point for consideration of errors of commission, substantially more analysis is necessary for a meaningful treatment of them. Ongoing work in this area is mentioned in references 5 and 6. At this writing, the existing work in the area does not justify official endorsement of any particular approach, beyond the above observation that the approach used here for errors of omission may provide useful input to an analysis of errors of commission; but ultimately, analyses which do not address this problem in some way will be considered incomplete.

Given these ground rules and assumptions, the objective of the screening model can be stated as follows:

It must provide an estimate (together with stated uncertainty bounds) of the probability that the responsible operators will fail to decide within the available time to perform an act which is essential for safety, given annunciation of the circumstances warranting the act.

The type of screening model which is recommended at this time to fit the PSA framework is statistical in nature rather than behavioral. This could be constructed from either a holistic or reductionistic perspective. Here, a holistic perspective is chosen so that the screening model is a statistical model of the probability of response to any accident, where individual accidents are "folded in," in accordance to the time available (after a successful annunciation) for decision making. A screening model is represented in Figure 4.2. The essential point is that the basic error probability has been expressed as a simple function of time. In the following example, this will be seen to result in a simple and easily reproducible calculation of the quantity of interest. The impact of considering slightly different assumptions will be seen to be easily assessed.

Example: Operator Actuation of ADS

In some BWR transient scenarios, the high pressure injection systems fail. In order to make use of the low pressure injection system, it is necessary to depressurize the reactor coolant system. This function is performed by the Automatic Depressurization System (ADS). In the scenarios considered, ADS actuation is an operator act because the drywell high pressure signal necessary (along with the low water-level signal) for the automatic initiation of the system is not present. A typical event tree for transients that cause MSIV closure is presented in Figure B.1.

Initially, it is assumed that failure occurs if the water level drops below the top of the core. This will occur 30 minutes after the initiating event if success of at least one of the injection systems has not been achieved by then.

The thinking interval is then given by the difference between 30 minutes (the total available time) and the sum of a) the time required for the cues to become available to the operator, and b) the time required for his actions to take effect: that is, the time required for ADS to reduce the pressure and for LPI to begin to inject. Let us assume that 8 minutes are required for the cues to materialize; this is the interval over which the information that no water is being injected becomes available. Let us further assume that 5 minutes are required for ADS to succeed and LPI to initiate. This leaves 17 minutes as the

thinking interval [30 - (8+5)]. For this thinking interval, one obtains from Fig. 4.2 the failure probability of approximately 0.15.

Possible modifications to this reasoning are easily taken into account. For some transients, the 30-minute time frame might be judged too long, while for others it is too short. If the definition of the top event is modified to be "uncovery of more than X% of the core", rather than "uncovery of the top of the core," the thinking interval will be 0.058. If the thinking interval is lengthened by this reasoning from 17 to 22 minutes, the answer will again be 8.1×10^{-3}. If the top event allows for 35 minutes, the cues are available after 3 minutes, and the time required for action to be effective is again 5 minutes, then the thinking interval is [35 -(3+5)] = 28, and the corresponding failure probability is approximately 0.015. Further examples are given in References 5 and 6.

Bibliography

Further justification for the application of a time-based reliability model in the prediction of human errors in decision making can be found in the following references (current examples are included):

1. A. D. Swain and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Fig. 17-2, NUREG/CR-1278, Oct. 1980.

2. Bolt, Beranek, and Newman, Inc, Evaluation of Proposed Control Room Improvement Through Analysis of Critical Operator Decisions, EPRI NP-1982, 1981.

3. G. W. Hannaman, Treatment of Operation Actions in the HTGR Risk Assessment Study, Report GA-A-15499, General Atomic Co., Dec. 1979.

4. Probabilistic Risk Assessment, Limerick Generating Station, Philadelphia Electric Co., Philadelphia, PA, April 1982.

5. J. Wreathall, Operation Action Trees, An Approach to Quantifying Operator Error Probability During Accident Sequences, NUS Report #4655, NUS Corp., July 1982.

6. R. E. Hall, J. Wreathall, and J. Fragola, Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation, NUREG/CR-1605, BNL-NUREG-51601, November 1982.

APPENDIX C

Component Failure Rate

C.1 Failure Rate Values for the Baseline Calculation

This appendix provides a data base for use in the baseline quantification of accident sequences. The baseline, or 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 baseline (generic) values generated in the above manner are conservatively biased and have the largest assigned error factor where there was disagreement.

---

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

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.

C.2 Use of the Data Table

The mean values in Table C.1 (rounded to one significant figure) are to be used to calculate a point estimate for the baseline calculation. 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

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

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

A loguniform distribution is simulated by first selecting a random number z uniformly between l 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 difficlties 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

BASELINE 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	5xE-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	2E7	1E-6	
2.4.2 Failure to close	6E-7	2E-6	1E-5	

TABLE C.1 (Cont.)

BASELINE COMPONENT FAILURE RATES (All Values per Hour)

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				Failure to operate is dominated by human error; rate is based on one actuation per month.
2.6.1 Failure to operate	8E-8	2E-7	1E-6	
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 (Cont.)

BASELINE COMPONENT FAILURE RATES (All Values per Hour)

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 (Cont.)

BASELINE COMPONENT FAILURE RATES (All Values per Hour)

Component and Failure Modes	Minimum Value (L)	Mean	Maximum Value (M)	Remarks
Other (continued)				
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				
4.7.1 Contacts fail to transfer (open or close)	2E-8	1E-6	5E-6	
4.7.2 Coil failure (open or short)	6E-8	3E-6	2E-5	
4.8 Time delay relays				
4.8.1 Premature transfer	2E-8	1E-6	5E-6	
4.8.2 Fails to transfer				
4.8.2.1 Bimetallic	2E-7	1E-5	1E-5	
4.9 Battery power system (Wet Cell)				Assumes out-of-spec cell replacement.
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 (Cont.)

BASELINE COMPONENT FAILURE RATES (All Values per Hour)

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				Values given are per terminal.
4.15.1 Open circuit	6E-9	3E-7	2E-6	
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				For clear fluids; contaminated fluids or fluids with a heavy chemical burden should be considered on a plant-specific basis.
4.19.1 Plugged	6E-7	3E-5	2E-4	

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

APPENDIX D

Baseline Repair Times

For a given component, the average repair time for the baseline calculation is defined to be the maximum allowed unscheduled downtime given in the plant technical specification (tech spec). The use of a maximum allowed downtime for the repair time is conservative since for most components the actual repair time will often be less than the maximum allowed downtime. These maximum allowed downtimes can also be used for the plant-specific evaluation when actual reliable repair time data are not available. The particular technical specifications should be referenced in the section of the report documenting the repair time values which were used for the baseline calculation.

APPENDIX E

Baseline Surveillance Test Intervals and Test Duration Times

For the baseline calculation, the surveillance test interval to use for a periodically tested component is the value specified in the plant tech specs. The average test duration for the surveillance test is defined 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 for the baseline calculation.

APPENDIX F

Baseline Maintenance Intervals and Maintenance Duration Times

For the baseline calculation, the frequency of unscheduled maintenance actions is defined 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 maintenance duration time to be used for the baseline calculation is defined 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 for the baseline calculation.

APPENDIX G

Baseline 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

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

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

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

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

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

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
Baseline 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
Baseline Frequencies for BWR Transient Initiators
(Cont'd)

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	Detected Fault in Reactor Protection System	9.8 E-2	9.1 E-3	6.6 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
Baseline 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	CRDM 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
Baseline Frequencies for PWR Transient Initiators
(Cont'd)

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-1	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 report[1] 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. In the first phase of NREP, 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}/yr to 10/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, outlined 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 statistics are not yet well established, the individual repair times 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

Human Error Data

For human errors of the procedural type, Chapter 20 of NUREG-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," is recommended.

The analyst should recognize that any event sequence sensitive to human error requires a detailed analysis on a case-by-case basis, and should include consideration of stress-level factors which may not always be totally or accurately represented by a time line. Additional information pertaining to human error probabilities is covered in Section 4.3.1 of this document.

APPENDIX J

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 J.1, J.2 and J.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, several of the code packages, e.g., the WAM series, 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 J.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 J.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 J.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 J.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	Yes		AND OR		Top-down sucessive 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
MOCUS	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 J.1 Computer codes for qualitative analysis (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 HAND ANOT ONOT K-of-N	Up to 2000 minimal cut sets of any order can be generated	Bottom-up Boolean substitution; WAMCUT-II finds independent subtrees, replaces them by pseudo-component, then uses top-down Boolean substitution	Probabilities of minimal cut sets and top event; first and second moments of minimal cut sets and top event	Yes, based on both cut-set order and probability	Plot option; minimal cut sets of intermediate gates can be generated	CDC-7600, IBM-370 Extended Fortran IV available from EPRI

[a]Or prime implicants.

Table J.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[a] 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 Argonee 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 J.2 Computer codes for quantitative analysis (continued)

Code	Input	Quantitative calculations	Importance calculation	Uncertainty analysis	Other features	Type of computer, language, and availability
PUFD	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
RALLY	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 RALLY can perform important calculations	Uncertainty analysis is possible by using minimal cut sets obtained by RALLY. Normal, lognormal, Johnson, extreme value-1, 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 simulative 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
SPASM	Fault tree or reduced system equation; component failure data	No	No	Similar in method to BOUNDS, but SPASM 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, log-normal, 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
SUPERPOCUS	Minimal cut sets, component failure data, time at which calculations are performed	Time-dependent unavailability, reliability, and expected number of failures for minimal cut sets and top event	Yes	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]A GO chart (see Section 3.6.3) is a chart that resembles a schematic of system primary events and their relations via a set of 16 Boolean operators.

Table J.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 J.3 Computer codes for dependent-failure analysis (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
WAMCOM	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 K

Standardized Accident Sequence Nomenclature

K.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 accomodate important features of present and future PSAs 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.

K.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 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 <u>primary</u> accident sequence identification is simply

$$\boxed{I_iF_j\text{--}F_mZ_k} \qquad (*)$$

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

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

$$I_i..F_j.. \text{ --- } F_m..Z_k..$$

<u>or</u>

$$I_i(..)F_j(..) \text{ -- } F_m(..)Z_K(..)$$

The additional indices or bracketed 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.

K.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 PSAs such initiators are defined by the breach area, e.g., greater than 1 ft^2. This, or other critical characteristics, should be identified as indicated.

S_1 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 ft^2 and 1 ft^2. Again, the geometric and functional characteristics should be identified.

S_2 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_1 Loss of Off-site Power transient.

T_i 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., $S_1(T_iF_1F_2)$, denoting that the medium LOCA S_1 was generated by the transient induced sequence $T_iF_1F_2$. 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 pressrue 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) specified time. Other extended or bracket information could include

- functional and operational peculiarities;
- the system success criteria and associated support systems failures; and
- specific failure mode information.

(b) BWR

K 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 emergency core cooling system.

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 untimate release. This information is usually implicit (and sometimes even explicit) in the partial sequence

$$I_i \cdot\cdot F_j \cdot\cdot \text{ --- } F_m \cdot\cdot \ ,$$

especially if the index (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

$Z_®$ 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)

K.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 (6-83) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1 REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG/CR-2815

2 Leave blank

3 TITLE AND SUBTITLE
PROBABILISTIC SAFETY ANALYSIS PROCEDURES GUIDE

4 RECIPIENT'S ACCESSION NUMBER

5 DATE REPORT COMPLETED
MONTH: September YEAR: 1983

6 AUTHOR(S)
R. A. Bari, A. J. Buslik, A. El-Bassioni, J. Fragola, R. E. Hall, D. Ilberg, E. Lofgren, P. K. Samanta, T. Teichmann, W. Vesely, R. W. Youngblood, I. Papazoglou

7 DATE REPORT ISSUED
MONTH: January YEAR: 1984

8 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Brookhaven National Laboratory
Upton, New York 11973

9 PROJECT/TASK/WORK UNIT NUMBER

10 FIN NUMBER
A-3382

11 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safety Technology
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

12a TYPE OF REPORT
Technical

12b PERIOD COVERED (Inclusive dates)

13 SUPPLEMENTARY NOTES

14 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 guide addresses the determination of the probability (per year) of core damage resulting from accident initiators internal to the plant, and from loss of offsite electric power. The scope includes analyses of problem-solving (cognitive) human errors, a determination of importance of the various core damage accident sequences, and an explicit treatment and display of uncertainties for the key accident sequences. Ultimately, the guide will be augmented to include the plant-specific analysis of in-plant processes (i.e., containment performance) and the risk associated with external accident initiators, as consensus is developed regarding suitable methodologies in these areas. This guide provides the structure of a probabilistic safety study to be performed, and indicates what products of the study are essential for regulatory decision making. 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.

15a KEY WORDS AND DOCUMENT ANALYSIS
Probabilistic Risk Analysis

Analysis Procedures

15b DESCRIPTORS

16 AVAILABILITY STATEMENT
Unlimited

17 SECURITY CLASSIFICATION (This report)
Unclassified

18 NUMBER OF PAGES

19 SECURITY CLASSIFICATION (This page)
Unclassified

20 PRICE
$

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

U.S. NRC
RRBR
P. BARANOWSKY
MAILSTOP 1130SS