NUREG/CR-2728

Interim Reliability Evaluation Program Procedures Guide

Sandia National Labs.
Albuquerque, NM

Prepared for

Nuclear Regulatory Commission
Washington, DC

Jan 83

NUREG/CR-2728
SAND82-1100
AN, RG, XA, 1S
Printed January 1983

Interim Reliability Evaluation Program Procedures Guide

David D. Carlson, Principal Investigator

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

NOTICE

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

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

1/2

BIBLIOGRAPHIC INFORMATION

NUREG/CR-2728

Interim Reliability Evaluation Program Procedures Guide,

Jan 83

David D. Carlson, Donald R. Gallup, Alan M. Kolaczkowski,
Gregory J. Kolb, and Desmond W. Stack.

PERFORMER: Sandia National Labs., Albuquerque, NM.
SAND-82-1100
Contract DE-AC04-76DP00789

SPONSOR: Nuclear Regulatory Commission, Washington, DC.
Office of Nuclear Regulatory Research.

Prepared in cooperation with Science Applications, Inc.

This document presents procedures for conducting analyses of a scope similar to those performed in Phase II of the Interim Reliability Evaluation Program (IREP). It documents the current state of the art in performing the plant systems analysis portion of a probabilistic risk assessment. Insights gained into managing such an analysis are discussed. Step-by-step procedures and methodological guidance constitute the major portion of the document. While not to be viewed as a 'cookbook', the procedures set forth the principal steps in performing an IREP analysis. Guidance for resolving the problems encountered in previous analyses is offered. Numerous examples and representative products from previous analyses clarify the discussion.

KEYWORDS: *Nuclear power plants, *Nuclear reactor accidents.

Available from the National Technical Information Service,
Springfield, Va. 22161

PRICE CODE: PC A07/MF A01

NUREG/CR-2728
SAND82-1100
AN, RG, XA, 1S, NTIS
Printed January 1983

Interim Reliability Evaluation Program Procedures Guide

David D. Carlson, Donald R. Gallup, Alan M. Kolaczkowski,
Gregory J. Kolb, and Desmond W. Stack
Sandia National Laboratories
Albuquerque, New Mexico 87185

E. Lofgren
Science Applications, Inc.
McLean, Virginia

William H. Horton, Peter R. Lobner
Science Applications, Inc.
La Jolla, California

Sandia Corporation
for the
U.S. Department of Energy

Prepared for
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A1241

Abstract

This document presents procedures for conducting analyses of a scope similar to those performed in Phase II of the Interim Reliability Evaluation Program (IREP). It documents the current state of the art in performing the plant systems analysis portion of a probabilistic risk assessment. Insights gained into managing such an analysis are discussed. Step-by-step procedures and methodological guidance constitute the major portion of the document. While not to be viewed as a "cookbook," the procedures set forth the principal steps in performing an IREP analysis. Guidance for resolving the problems encountered in previous analyses is offered. Numerous examples and representative products from previous analyses clarify the discussion.

Acknowledgments

The authors acknowledge the contribution of Joseph A. Murphy of the Nuclear Regulatory Commission for his direction and guidance in developing this report and for his comments on earlier drafts. We also wish to acknowledge Arthur C. Payne, Steven W. Hatch, Jack W. Hickman, and G. Bruce Varnado of Sandia National Laboratories, and Jonathan Young of Energy Incorporated for their review and comments. Ruby C. Cochrell is also acknowledged for her invaluable assistance in producing this report.

Contents

Contents (cont)

Contents (cont)

Contents (cont)

Interim Reliability Evaluation Program Procedures Guide

Part I. Performing and Managing an IREP Analysis

1. Introduction

The Interim Reliability Evaluation Program (IREP), sponsored by the Division of Risk Analysis of the Office of Nuclear Regulatory Research of the US Nuclear Regulatory Commission, consisted of an analysis of five plants. The first analysis was performed on the Crystal River Unit 3 nuclear power plant operated by Florida Power Corporation [1]. Motivation for the study was to determine whether a Babcock and Wilcox designed facility had any risk-significant peculiarities in light of the accident at Three Mile Island. The study was conducted by Science Applications, Inc. with assistance from several national laboratories and contractors under the direction of the Nuclear Regulatory Commission (NRC). A final report was prepared and submitted to the NRC in December 1981.

In the fall of 1980, IREP was expanded to include analyses of four more reactors:

Arkansas Nuclear One Unit One, operated by Arkansas Power & Light Company;

Browns Ferry Unit One, operated by the Tennessee Valley Authority;

Calvert Cliffs Unit One, operated by the Baltimore Gas & Electric Company; and

Millstone Unit One, operated by Northeast Utilities.

The objectives of these four analyses were to:

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

The four analyses were performed concurrently under the direction of Sandia National Laboratories by four teams in three locations consisting of personnel from Sandia National Laboratories, Idaho National Engineering Laboratory, the NRC, Battelle Columbus Laboratories, Science Applications, Inc., and Energy Incorporated. In addition, Arkansas Power & Light, Baltimore Gas & Electric, and Northeast Utilities provided people full time to participate in the program and to perform portions of the analysis.

The four teams were provided with a set of draft procedures to guide the analysis. These were supplemented with documents detailing methods which could be used. Because the procedures had never been utilized in total, some flexibility in approach was allowed among the teams. In general, however, the analyses were conducted under the guidelines set forth in the original procedures, although some variations in detail persisted.

One of the products sought from IREP was a revised set of procedures reflecting insights gained from performing the analyses and setting forth the manner for conducting similar analyses in the future. A concerted effort was exerted during the program to develop these insights. An independent review team consisting of experienced probabilistic risk assessment (PRA) analysts from NRC, Sandia National Laboratories, and Energy Incorporated periodically visited each of the teams. The team reviewed in detail the content of periodic status reports and the draft final reports.

In addition, insights and views were solicited from all participants in the program. The participants represented a diversity of experience and perspective. The IREP teams consisted of experienced PRA practitioners, experienced systems analysts with limited PRA experience, personnel from both the research and regulatory sides of NRC, utility engineers and operating personnel, and computational and human factors specialists.

This document incorporates the experience gained from the IREP analyses and sets forth procedures for future IREP analyses. It is divided into three parts. Part I, intended for management concerned with organizing and managing the performance of an IREP analysis, discusses what is involved in performing the analysis and presents representative manpower needs and schedule. Quality assurance is discussed as well as suggested reporting points.

Part II, intended for those performing the analysis, presents procedures for performing each major portion of the analysis. The study is broken down into seven major tasks. Part II presents an overview of each task describing the purpose, scope, information needs, and assumptions pertinent to performing the task. The relationship of each task to others is presented along with examples of the products resulting from the task. Procedures to be followed in performing each task constitute the major portion of Part II. Reporting recommendations for each task are also discussed.

Part III provides detailed descriptions of methods which could be used for various portions of the analysis. This part supplements the procedures presented in Part II. Given the procedures and the methods, the analyst should be able to perform an analysis which would be consistent with that performed on other plants.

2. Objectives, Scope, and Results of an IREP Analysis

The original IREP analyses were conducted with several objectives in mind. Some of these were discussed in the previous section. Future IREP analyses will satisfy the following objectives:

1. Identify the dominant accident sequences and their frequencies of occurrence for the subject plant.
2. Identify those plant features, e.g., hardware failures, human errors, procedural inadequacies, or test and maintenance outages, which are the most important to the likelihood of core melt.
3. Provide documented plant models for use in analyzing particular regulatory issues as they pertain to the plant analyzed.

There may well be additional objectives depending upon the desires of those undertaking the analyses or upon the interests of the regulatory agency.

Emphasis on the previous IREP analyses has been on the systems analysis portion of the risk assessment. In fact, neither the Crystal River study nor the subsequent four plant analyses investigated containment phenomenology to any great extent and did not evaluate accident consequences at all. The Crystal River study assigned release categories based upon previous studies; the four plant analyses also deduced release categories from previous studies, although in some cases supplemental plant-specific analyses were performed. Limited containment analyses were performed in IREP to provide additional perspective as to which of the most frequent core melt sequences would lead to potentially high consequence releases. This document does not discuss this process of limited containment analysis. Information on this is contained in Reference 2.

External hazards such as earthquakes and floods and certain internal hazards such as fires and internally-caused flooding were excluded from the IREP analyses. This was primarily due to limited development of methodology to treat these issues.

The IREP analyses, however, throughly investigated plant response to loss of coolant accidents and anticipated plant transients to ascertain the most frequent core melt sequences. Particular attention was paid to the role of support systems (such as ac and dc power, auxiliary cooling water systems, and ventilation) and to potential human errors in accident sequences. Within the scope of the program, plant systems were analyzed in great detail.

Common cause aspects were included explicitly in the modeling. The following common causes or dependencies were included:

- Initiating event -- system response interrelationships.
- Common support system faults effecting more than one front-line system or component.
- Coupled human errors associated with test and maintenance activities and in response to accident situations.
- Shared components among front-line systems.

Environmental common causes, e.g., dust, ice, fire, etc, were not included in the analyses. Other commonalities such as manufacturing deficiencies and installation errors were also not included. Finally, β factors

Interim Reliability Evaluation Program Procedures Guide

Part I. Performing and Managing an IREP Analysis

1. Introduction

The Interim Reliability Evaluation Program (IREP), sponsored by the Division of Risk Analysis of the Office of Nuclear Regulatory Research of the US Nuclear Regulatory Commission, consisted of an analysis of five plants. The first analysis was performed on the Crystal River Unit 3 nuclear power plant operated by Florida Power Corporation [1]. Motivation for the study was to determine whether a Babcock and Wilcox designed facility had any risk-significant peculiarities in light of the accident at Three Mile Island. The study was conducted by Science Applications, Inc. with assistance from several national laboratories and contractors under the direction of the Nuclear Regulatory Commission (NRC). A final report was prepared and submitted to the NRC in December 1981.

In the fall of 1980, IREP was expanded to include analyses of four more reactors:

Arkansas Nuclear One Unit One, operated by Arkansas Power & Light Company;

Browns Ferry Unit One, operated by the Tennessee Valley Authority;

Calvert Cliffs Unit One, operated by the Baltimore Gas & Electric Company; and

Millstone Unit One, operated by Northeast Utilities.

The objectives of these four analyses were to:

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

The four analyses were performed concurrently under the direction of Sandia National Laboratories by four teams in three locations consisting of personnel from Sandia National Laboratories, Idaho National Engineering Laboratory, the NRC, Battelle Columbus Laboratories, Science Applications, Inc., and Energy Incorporated. In addition, Arkansas Power & Light, Baltimore Gas & Electric, and Northeast Utilities provided people full time to participate in the program and to perform portions of the analysis.

The four teams were provided with a set of draft procedures to guide the analysis. These were supplemented with documents detailing methods which could be used. Because the procedures had never been utilized in total, some flexibility in approach was allowed among the teams. In general, however, the analyses were conducted under the guidelines set forth in the original procedures, although some variations in detail persisted.

One of the products sought from IREP was a revised set of procedures reflecting insights gained from performing the analyses and setting forth the manner for conducting similar analyses in the future. A concerted effort was exerted during the program to develop these insights. An independent review team consisting of experienced probabilistic risk assessment (PRA) analysts from NRC, Sandia National Laboratories, and Energy Incorporated periodically visited each of the teams. The team reviewed in detail the content of periodic status reports and the draft final reports.

describing "other" unspecified causes of system failure were not considered.

Given the limited scope of an IREP analysis, an assessment of risk in terms of a frequency-consequence curve or something similar is not possible. Rather, the results consist of an identification of the most frequent core melt sequences. Of perhaps greatest importance, the analysis provides insight into plant design and operation which allows potential weaknesses to be discerned and their relative importance assessed. These qualitative insights constitute the most meaningful products of the analysis.

Finally, the analysis results in a fairly complete model, within the scope of the program, of the possible sequences leading to core melt and of the systems, and their supporting systems, which are called upon to prevent such accidents. These models should prove valuable to the utility involved in the analysis by improving their understanding of their plant design and operation and as a tool for evaluating future design options. For the regulatory agency, these models provide an information base documenting current plant design and provide a starting point for the analysis of regulatory issues in the future.

3. IREP Methodology

An IREP analysis consists of seven major tasks. These are illustrated in Figure 3-1. This section discusses briefly each major task and the interrelationships among the tasks. More detailed information and procedures for conducting each task are presented in Part II of this document. The final portion of this section discusses information needs for the analysis.

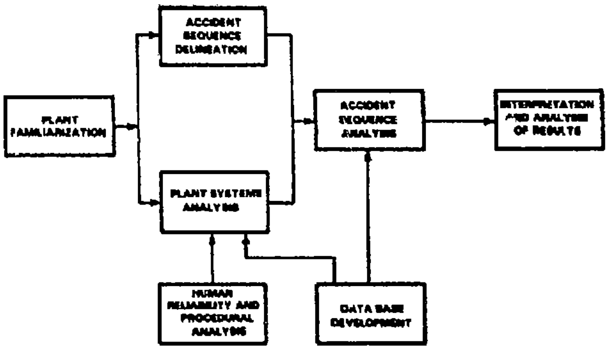

ACCIDENT SEQUENCE DELINEATION
PLANT FAMILIARIZATION
ACCIDENT SEQUENCE ANALYSIS
INTERPRETATION AND ANALYSIS OF RESULTS
PLANT SYSTEMS ANALYSIS
HUMAN RELIABILITY AND PROCEDURAL ANALYSIS
DATA BASE DEVELOPMENT

Figure 3-1. Major IREP Tasks

3.1 Plant Familiarization

The initial task of an IREP analysis is the development of familiarity with the plant and available information. This task forms the foundation for the development of plant models in subsequent tasks. Several products are achieved in this task:

1. A preliminary identification of initiating events (e.g., loss of coolant accidents, transients) to be included in the analysis.
2. An identification of functions to be performed for each initiating event to successfully prevent core melt or to mitigate its consequences.
3. An identification of plant systems which perform these functions (termed "front-line systems").
4. An identification of systems supporting front-line systems (termed "support systems").
5. Success criteria for each front-line system responding to each initiating event.
6. A grouping of initiating events into classes according to common responding systems and success criteria.

At the conclusion of this task, the number and type of event trees to be constructed and the systems to be modeled have been identified. Thus, the modeling effort in subsequent tasks has been clearly defined.

3.2 Accident Sequence Delineation

Accident sequences to be analyzed in the program are defined by constructing event trees for each initiating event group. Generally, separate event trees are constructed for each group. Each will be a unique tree with some difference in structure (otherwise, initiating event groupings have not been properly chosen).

In this task, both functional and system event trees are constructed. These reflect the functions to be performed following each initiating event class and the responding systems to each initiating event group as defined in the plant familiarization task. The event tree structure reflects functional and system interrelationships and aspects of accident phenomenology which could affect core conditions, system operation, and/or accident consequences.

At the conclusion of this task, models have been constructed reflecting all sequences to be assessed in the accident sequence analysis task.

3.3 Plant Systems Analysis

Nuclear power plant systems are generally complex collections of equipment. To conduct the risk assessment, the contributors to failure of each system must be identified and quantified. The models to facilitate this quantification used in IREP are system fault trees. The fault trees represent all ways in which a certain undesired event (termed the "top event") may occur.

Fault trees are constructed for each front-line system. They reflect the success criteria identified in the plant familiarization task. Each success criterion is transformed into a failure criterion which is the top event for a given fault tree. For example, if one out of two pump trains are required for system success, the top event of the fault tree becomes "both pump trains fail." Support system fault trees are developed in the context of the front-line systems they support. In a subsequent task, the support system trees are merged with the respective front-line system fault trees to reflect the ways, including support system faults, of achieving the undesired event.

The task interfaces with the human reliability and procedural analysis task and the data base development task. Human errors associated with test and maintenance activities and in response to accident situations are modeled in the fault trees. The fault trees are developed to a level of detail consistent with the data base utilized for quantifying failure probabilities.

The outputs of this task are detailed models for each event found in the event trees. These models provide a key element to the accident sequence analysis task.

3.4 Human Reliability and Procedural Analysis

This task involves an identification of potential human errors associated with failure to restore equipment to operability following test and maintenance activities and in response to accident situations. Test and maintenance procedures and practices are reviewed for each front-line and support system to identify which components are removed from service during the activity and which could potentially be erroneously left in an inoperable state following the activity. Procedures expected to be followed in responding to the accident situations modeled in the event trees are also identified and reviewed for possible sources of human errors which could affect the operability or functionability of responding systems.

These potential human errors constitute ways in which front-line and support systems may fail to perform and are incorporated into the appropriate system fault trees.

In addition, data are developed for human error failure rates. Upper bound estimates are used for initial calculations. For human errors expected to be significant in the analysis, best estimate human error probabilities are developed reflecting plant-specific characteristics.

3.5 Data Base Development

This task involves the development of a data base for quantifying faults other than human errors appearing in the system fault trees. A generic data base representing typical failure rates for nuclear components was developed for IREP and may be found in Part III of the guide. Data for the plant being analyzed, however, may differ significantly from industry-wide data. In this task, the operating history of the plant is reviewed to ascertain whether any plant components have unusual failure rates. Test and maintenance practices and history are also reviewed to determine the frequency and duration of these activities. This information is used to supplement the generic data base. This supplemented generic data base is used in the analysis of accident sequences.

3.6 Accident Sequence Analysis

The event tree and fault tree models and the data base are integrated in the accident sequence analysis task to calculate accident sequence frequencies and to identify the most probable faults contributing to each accident sequence. This is a time-consuming task generally performed with the assistance of a computer. There are many activities performed in this task, principally:

1. Preparing computer input representing the logic of the fault trees.
2. Identifying and correcting errors in the fault trees.
3. Assigning failure probabilities to each basic fault in the fault tree and inputting these to the computer.
4. Merging support system fault trees with the appropriate front-line system fault trees.
5. Developing logic expressions and their complements, if used, for the fault trees.
6. Developing expressions of combinations of component faults (i.e., cut sets) resulting in each accident sequence.
7. Quantifying the frequencies of all important accident sequences, including consideration of operator recovery actions.

The results of this task are computerized, correct models representing the plant systems and both qualitative expressions of fault combinations and quantitative expressions of cut set and accident sequence frequencies for all potentially important accident sequences. These products form the basis for the final task.

3.7 Interpretation and Analysis of Results

The final task in an IREP analysis is the interpretation and analysis of the results produced in the accident sequence analysis task. Of primary interest are insights into plant features contributing significantly to risk. Some of these insights are developed by examining the cut sets which contribute most to the frequency of the most probable sequences (termed "dominant accident sequences"). Those cut sets represent plant faults which contribute significantly to the possibility of core melt.

Further insight may be developed by performing importance calculations of various types. There are standard codes which calculate various measures of importance for individual events or classes of events. Sensitivity analyses on important assumptions or particularly questionable data also assist in developing insight and perspective into the meaning of the study's results.

Finally, limited uncertainty calculations are performed. These primarily involve sampling of data from the distributions associated with each element in the data base and determining the effect on accident sequence frequencies. By repeating this process many times, an estimate of the possible range of results due to data uncertanties may be obtained.

3.8 Information Needs

A considerable amount of detailed plant information must be supplied to the analysis team to ensure the performance of an accurate analysis in a timely manner. A listing of the documentation needed is shown in Table 3.8-1.

Basic plant information is contained in the Final Safety Analysis Report (FSAR). This information is generally not sufficiently detailed to allow complete IREP models to be developed. Rather, it must be supplemented by detailed piping, instrumentation, and control drawings. In addition, the analysis team must have copies of or access to emergency, test, and maintenance procedures to facilitate the analysis of potential human errors. Even with such detailed information, however, a point of contact at the plant and occasional visits to the site are essential sources of information for the study.

The team must, of course, have copies of this document to provide direction to the analysis. Copies of supporting methods documents referred to in later parts of this document are also needed. Copies of previous IREP analyses and any similar analyses performed on the plant under study may prove worthwhile.

Finally, several documents are useful for various types of data. These include:

1. EPRI NP-2230 [3]: this contains data for the frequency of transient initiating events.
2. Plant specific and other licensee event reports: these provide insight into possible problem areas for more investigation and for collecting plant-specific data.
3. WASH-1400 [4]: this provides additional background.
4. NUREG/CR-1278 [5]: this details the procedure for analyzing human reliability and for quantifying human error probabilities.

This information provides the basis for the analysis. It must, undoubtedly, be supplemented by specialized analyses or calculations or other documents pertinent to issues which will arise over the course of the specific plant analysis.

Table 3.8-1. Basic Information Needs for IREP

Final Safety Analysis Report
System Descriptions and Plant Drawings
Other Probabilistic Analyses of the Plant or a Similar Plant
Electrical One-line Drawings
Control and Actuation Circuitry Drawings
Emergency, Test, and Maintenance Procedures
Plant Contact
Plant Visits
Methods Documents
EPRI NP-2230, "ATWS: A Reappraisal-Part III, Frequency of Anticipated Transients" [3]
Plant Specific and Other Licensee Event Reports
WASH-1400, "Reactor Safety Study" [4]
NUREG/CR-1278, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications" [5]

4. Makeup of the Analysis Team and a Representative Schedule

4.1 The Analysis Team

IREP analyses are integrated, full plant analyses requiring a broad range of expertise. Success of the project depends strongly on the ability to assemble this expertise and coordinate their diverse activities. Based on the experience gained in previous IREP analyses, the following team is suggested for future IREP studies:

1 team leader experienced in probabilistic risk assessment (PRA)
3-4 systems analysts
1 analyst familiar with plant operations
1 human reliability analyst, part-time
1 data analyst
2 computation specialists, part-time initially with full participation later in the study

The previous IREP analysis teams consisted of people from a variety of organizations and backgrounds. Experienced PRA analysts headed each team. The teams primarily consisted of experienced systems analysts with varying degrees of PRA experience from national laboratories, contractors, the NRC, and the participating utilities. In some cases, utilities supplied experienced operations personnel to assist in the analysis. Computer, data, and human reliability specialists assisted in portions of the analysis. For most teams, all individuals were in one location. Some had broad utility involvement; others had more limited utility participation. Each team was somewhat different in makeup, affording the opportunity to better understand the characteristics sought for future analysis teams.

4.1.1 Team Leader

The team leader manages and integrates the analysis and should have the requisite authority to do so effectively. He is responsible for the technical content of the analysis and for ensuring consistency with the procedures and among different analysts. He should be someone experienced in probabilistic risk assessment. The team leader provides perspective and direction to the effort. His primary technical role in the study is to integrate the various portions of the analysis. This is a difficult task which requires experience to provide the perspective necessary for this role. In addition, probabilistic risk assessments involve considerable judgment since many issues as yet unresolved in the technical community must be treated in the analysis. The team leader must weigh differing viewpoints and decide how the analysis is to be performed. This is often a matter of judgment, but depends heavily on the objectives of the study and what portions need to be emphasized. In the course of the analysis, questions involving subtleties in modeling arise; guidance is needed as to the level of detail at which to terminate modeling. To make these and other judgments, the team leader must have been involved in a PRA previously. Many of these problems he will have faced before, and his experience will be invaluable in resolving new ones.

4.1.2 Utility Involvement

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

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

4.1.3 Analytical Expertise Required

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

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

An IREP analysis produces logic models which are generally impractical to evaluate without use of a Boolean algebra manipulating code. The team should include personnel familiar with the preparation of input and operation of the chosen code.

4.2 Manpower Estimates and Schedule

Manpower estimates by task are presented in Table 4.2-1; a representative schedule is presented in Figure 4.2-1. These are discussed briefly below. Reporting and quality assurance are included in the table and figure, but are discussed in the next section.

The plant familiarization task precedes all others and forms the basis for construction of the event tree and fault tree models. This task takes about six weeks and involves about nine man-months of effort.

The accident sequence delineation and plant systems analysis tasks proceed in parallel. There is considerable iteration involved in each. A substantial portion of the event tree analysis has been performed in the plant familiarization tasks of identifying the initiating events and responding systems. As a result, this task is estimated to take about three months and three man-months effort. The construction of detailed models for all front-line and support systems requires considerably more time, estimated to take 6 months and require 33 man-months effort.

The human reliability and procedural analysis and the data base development tasks also proceed concurrently with the modeling efforts since both support the modeling. The human reliability analysis occurs over a longer period of time since this tends to be an iterative process. Refinements in both data and human reliability rates are made during the accident sequence analysis when the more important events have been identified. Both tasks are estimated to entail about three man-months work.

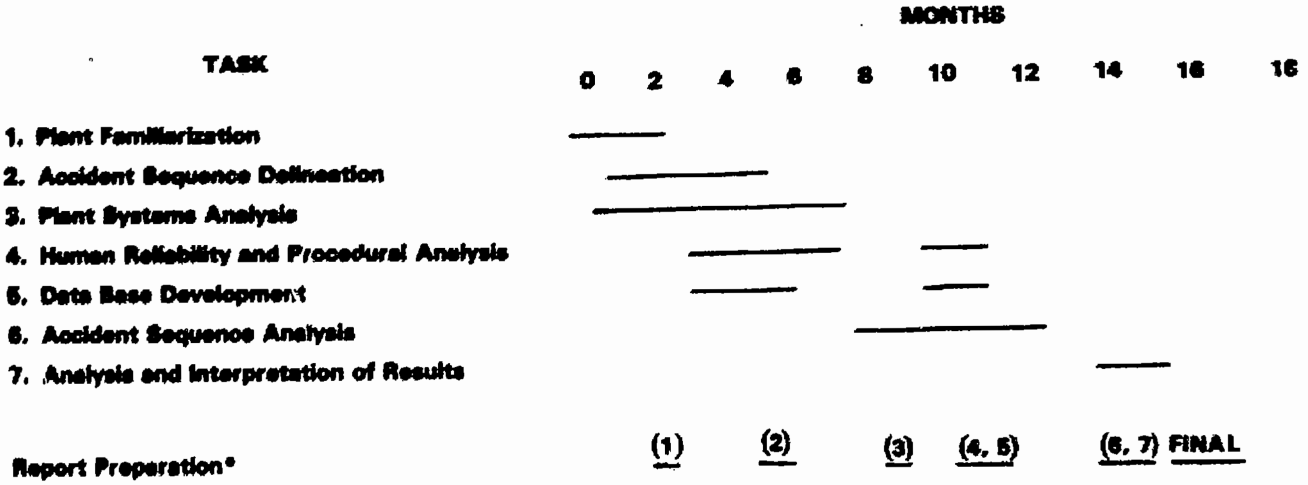
The accident sequence analysis is a time-consuming, iterative process. This task follows the construction of the models. Much of the activity is devoted to ensuring integration of the models, ensuring they are correct and consistent, and then quantifying them. This task takes about 5 months and involves about 20 man-months effort.

The final task, analysis and interpretation of results, follows the accident sequence analysis. The quantitative analysis is done with standard codes and is generally not too time consuming. The qualitative analysis is fairly straightforward given the results of the previous task. This task takes about six weeks and requires about three man-months effort.

Table 4.2-1. Manpower Estimates by Task

Task	Manpower Estimate (Man-months)*
1. Plant Familiarization	9
2. Accident Sequence Delineation	3
3. Plant Systems Analysis	33
4. Human Reliability and Procedural Analysis	3
5. Data Base Development	3
6. Accident Sequence Analysis	20
7. Analysis and Interpretation of Results	3
Report Preparation	14
Quality Assurance and Management	12
Total	100

*This may vary by as much as 10% higher or lower in actual application.



*–(numbers) correspond to tasks

Figure 4.2-1. Representative IREP Schedule

5. Quality Assurance and Reporting

5.1 Quality Assurance

A function important to the efficiency and credibility of the analysis is quality assurance. An ongoing review of the work, rather than at completion of the study, is the most effective approach to quality assurance. Each analyst should keep a notebook of his analysis containing pertinent information such as descriptive material, correspondence, and notations regarding assumptions made and supporting rationale. To maximize the quality of the product, people with various perspectives should review the work. A thorough review by the team leader of all work products provides the most effective means of assuring quality. The team leader should pay particular attention to assumptions made in the analysis and to consistency among different analysts in addition to ensuring the accuracy of the analysis.

Plant personnel should review the analyses to ensure that the modeling is consistent with current plant design and operation. In addition to ensuring accuracy of the analysis, plant personnel should particularly review assumptions involved to ensure their plausibility and to ensure that the analysis is as realistic as possible.

Recent IREP analyses were periodically reviewed by a team of experienced PRA analysts not directly involved in the work. This team was effective in improving consistency among the various analysis teams and in improving the quality of the analyses being performed. Interim status reports were provided at the completion of each major work product. Each was thoroughly reviewed by the independent review team. Comments were provided to the team leaders and corrections to the model and improvements to the analyses were made as the study progressed. This helped to ensure high quality analyses throughout the program and helped eliminate errors before they were propagated in subsequent tasks.

The emphasis of the review depends upon the product undergoing review. Review of the plant familiarization activity should focus on how well plant information has been integrated, the selection and grouping of initiating events, and the identification of and success criteria for front-line systems. In particular, adequate documentation should be available to support the choice of success criteria.

Emphasis in the review of the event trees should be on the appropriateness of event headings and on the proper reflection of system and phenomenological dependencies in the event tree structure. Phenomenological dependencies are often not well known, and assumptions made in this regard should be carefully documented and reviewed.

The top events of the fault trees should correspond to the converse of the success criteria defined in the event tree. The entire tree should, of course, be reviewed. Particular attention, however, should be focused on the top logic of the fault tree. It is in this portion of the tree that major logic errors may arise. System specific assumptions are often reflected near the top of the fault tree. Lower in the tree, similar logic should appear for similar components. Development of the tree should terminate at a level consistent with the data available.

Review of the human reliability task should ensure that test, maintenance, and emergency procedures have been thoroughly reviewed for potential sources of human error. Each component which is placed in an inoperable position during testing or removed from service during maintenance should have human errors in the appropriate fault tree associated with failure to restore the component to an operable state unless the probability of such errors is so low that they are insignificant. Assumptions associated with the human reliability analysis of accident response errors should be reviewed, particularly by plant personnel, to ensure that the scenarios analyzed reflect expected accident conditions in terms of timing, information, and actions to be performed.

The data base review should ensure that plant pecularities reflected in licensee event reports are included in the data. The review should pay particular attention to the applicability of the events reflected in the number of trials involved in demand failure probability calculations.

Review of the accident sequence analysis activity is somewhat more difficult since much of the work is performed by the computer. The general approach taken by the team, however, should be thoroughly discussed. Often, accident sequence expressions are reduced by truncating probabilistically negligble terms from the expression. This aspect of the analysis should be reviewed in particular, with emphasis on truncation values used, when the truncation is performed, and the treatment of complement events. Truncation values should not exceed 10^{-6} and truncation should be performed at the cut set level. Truncated complement equations may be used, if necessary, provided they are consistent with the truncated failure equations and are developed from the truncated system equation. Dominant accident sequences should be reviewed to ensure that:

1. The cut sets actually will cause the sequence to occur (each literal causes some equipment/system to fail; the combination should result in all failures reflected in the sequence).
2. Each event in the dominant cut sets is properly quantified.
3. Recovery factors reflect an understanding of actions to be taken and of their plausability under accident conditions.

The uncertainty and sensitivity analysis should reflect proper ranges of values for the data and should address major assumptions made in the analysis. Insights developed should reflect major findings associated with the dominant accident sequences and any plant peculiarities identified in the study.

Finally, the final report should be reviewed to ensure that:

1. Findings of the study are clearly stated (and supported by the analysis)
2. Assumptions inherent to the analysis in general and related to systems/sequences in particular are clearly stated
3. Information pertinent to the calculation of the frequency of dominant and near dominant sequences is presented in sufficient detail to allow the reader to replicate these calculations.

Quality assurance and management of the project are ongoing throughout the project. They are estimated to entail approximately 12 man-months effort.

5.2 Reporting

Reports are desirable at the completion of each major work product. Preparation of these reports facilitates timely documentation of analysis assumptions and techniques and forms the bases of review for the team leader, plant personnel, and the independent review team.

A recommended list of reports and their timing is presented in Table 5.2-1. An informal report consists of a letter presenting results of the task and explaining their derivation. Interim reports are more formal documents presenting results and explaining their development in detail. The contents of these reports should, to the extent possible, reflect the contents of the appropriate sections of the final report. Although this requires more effort initially, it facilitates the review process and reduces the work necessary to prepare the draft report at the conclusion of the study.

Documentation associated with an IREP analysis is substantial and is a time consuming task. As presented in the previous section, reporting requires greater than a man-year of effort. This, however, is time well spent. A well-prepared documentation of this thorough analysis will serve as a reference for future analyses and decisions to be made by the utility.

Table 5.2-1. Recommended Reports

1. Informal Report: Plant familiarization	2 Months
2. First Interim Report: Plant familiarization, event trees, preliminary front-line system fault trees	6 Months
3. Second Interim Report: Front-line and support system fault trees, preliminary human reliability and data analysis	9 Months
4. Informal Report: Initial accident sequence analysis (techniques, initial results), revised human reliability and data analyses	12 Months
5. Draft Report: Results and their interpretation	15 Months
6. Final Report (ready for publication)	17 Months

Part II. Procedures for an IREP Analysis

Part I of this guide presented an overview of performing and managing an IREP analysis. It is intended primarily for managers who may be considering performing such an analysis. This part of the guide, however, is intended primarily for analysts who will be performing the analysis. The purpose is to provide, in the context of the analysis as a whole, procedures for conducting each major task of the analysis.

To achieve this purpose, this part of the procedures guide discusses each of the seven major tasks:

1. Plant Familiarization
2. Accident Sequence Delineation
3. Plant Systems Analysis
4. Human Reliability and Procedural Analysis
5. Data Base Development
6. Accident Sequence Analysis
7. Interpretation and Analysis of Results

For each task, an overview is presented describing the task purpose, scope, and relationship to other tasks Information needs and assumptions pertinent to the task are also discussed. The overview serves to place the task in perspective relative to the other tasks and to the analysis as a whole.

Given this perspective, step-by-step procedures are provided for performing each major task. These procedures present a logical approach for achieving the task's objectives. An identified product corresponds to each step in the procedure. The procedure contains all of the principal steps involved in performing the task. However, the reader is cautioned not to view this as a "cookbook" exercise. Considerable judgment must be exercised by the analyst throughout the analysis, and unique situations will undoubtedly arise.

Further guidance supplementing the procedures in methodologically difficult areas is presented in Part III of the guide. Again, this discussion cannot be viewed as complete. New problems undoubtedly arise which the analysts will have to solve. Part III of the guide provides guidance for solving some of the problems found in previous analyses.

Concluding the discussion of each major task is a section detailing information to be included in the report of the task. Included are representative products from completed IREP analyses to provide additional insight into the desired products and format.

In many instances limitations are placed on the scope and depth of the analysis. In some cases, these are based on experience which has shown additional detail to be probabilistically unimportant. In other cases, such as the treatment of recovery, analysis is limited to potentially significant sequences. In a few instances the methodology is not sufficiently developed to facilitate analysis of a particular area in a manner consistent with the rest of the analysis.

Although limitations often exist, many of them are not inherent limitations to the application of PRA techniques. If desired, the analyst could investigate these areas in greater depth using similar techniques. This portion of the guide details procedures consistent with the scope and depth of previous IREP analyses.

The procedures reflect the assumptions to be made and the steps to be performed to conduct an analysis of similar scope to past IREP analyses. If analyses of a broader scope are considered—for example, inclusion of external events, expanded treatment of common modes, or expanded treatment of cognitive human errors—the assumptions, guidelines, and procedures should be reexamined.

A summary of the procedural steps and products is contained in Section 8 of this part of the document.

1. Plant Familiarization

1.1 Overview of the Plant Familiarization Task

1.1.1 Purpose

An IREP analysis integrates diverse sources of information and analyses to perform a detailed analysis of reactor systems and accident sequences. To efficiently and effectively conduct the analysis, it is important that the analysts initially gain an overall familiarity with the facility and that a preliminary identification of models to be constructed be made. The purpose of the plant familiarization task is to develop this familiarity and to establish the foundation for subsequent modeling activities by identifying the initiating events to be considered in the analysis, the systems to be modeled, and the dependencies among systems and their support systems.

1.1.2 Products

The products of the plant familiarization task used in subsequent portions of the analysis are as follows:

1. A list of initiating events to be included in the analysis grouped according to common mitigating system requirements.
2. A table showing mitigating system success criteria for each initiating event group.
3. A list of systems needed to respond to one or more initiating events; these are termed "front-line systems" and correspond to the systems defined in the success criteria.
4. A list of systems which support one or more of the front-line systems; these are termed "support systems."
5. A table showing dependencies between front-line and support systems and among support systems.

Examples of these products from previous IREP analyses are contained in Section 1.3 below.

1.1.3 Relationship to Other Tasks

The plant familiarization task is the initial task of the analysis. The products of this task are used in the accident sequence delineation and plant systems analysis tasks.

The list of grouped initiating events corresponds to the initiating events in the event trees constructed in the accident sequence delineation task. One event tree is generally constructed for each initiating event group. The headings of a particular event tree correspond to the front-line systems responding to the initiating event group. This information is contained in the table showing system success criteria for each initiating event group.

The lists of front-line and support systems correspond to all systems to be modeled in the plant systems analysis task. Success criteria contained in the system success criteria table are transformed into the corresponding statement of system failure which is the "top event" of the appropriate front-line system fault tree. Success criteria for the support systems is not a product of the plant familiarization task. These must be developed in the context of the front-line system model. However, fault trees are constructed for all systems in the support systems list, and they are attached to the appropriate front-line and support system/support system systems as shown in the front-line support-system and support system dependency tables.

These interrelationships are summarized in Table 1.1-1. There is no input from other tasks since this is the first task of the analysis. Task products are listed along with the corresponding tasks using each product.

1.1.4 Information Needs

This being the initial task in the analysis, no information from other tasks is used. The infoɪ.ɔation needs for this task are as follows:

1. Final Safety Analysis Report.
2. Licensee Event Reports for the plant under study and for other plants of similar design.

Table 1.1-1. Plant Familiarization Task Relationships

Input From Other Tasks	Products	Other Tasks Using Products
None	1. Initiating events list, grouped by mitigating requirements	Accident Sequence Delineatien—one event tree for each initiating event group
	2. System success criteria	Accident Sequence Delineation—defines headings for each event tree
	3. Front-line systems list	Plant Systems Analysis—defines systems to be modeled
	4. Support systems list	Plant Systems Analysis—defines systems to be modeled
	5. System dependency diagrams	Plant Systems Analysis—defines context for support system modeling

3. EPRI NP-2230, "ATWS: A Reappraisal—Part 3, Frequency of Anticipated Transients [3]".
4. Analyses, if any, pertinent to the selection of success criteria.

Section 1.2 discusses the use of this information to perform this task.

1.1.5 Scope

The investigation of initiating events performed in this task is limited to those events associated with internal plant equipment. The only exception to this is loss of offsite power. Environmental initiating events such as tornados, wind, ice, etc., are generally excluded as are events such as earthquakes, fires, and floods. The resulting list of initiating events should be viewed as preliminary. Additional tasks will yield more insight which could modify the list. Full power operation places the most severe requirements on responding systems. As a result, transients are assumed to occur at full power; events occurring at cold shutdown are generally not included in the analysis.

The system success criteria should be as realistic as possible. One purpose of an IREP analysis is to perform as realistic an analysis of the plant as is practical. As such, excess conservatism should be avoided. Often, specific analysis may be necessary to ascertain the most realistic success criteria. The time necessary to obtain this information may necessitate using information from the FSAR in the tables produced in this task, recognizing that these may be modified later as more documentation becomes available.

Areas requiring closer investigation, such as certain success criteria, should be identified as early as possible in this analysis. Work should begin to resolve these areas as soon as possible. Lacking more specific information, however, a conservative assumption should be made and work should progress.

1.1.6 Assumptions and Guidelines

The investigation of support system faults which could result in a reactor trip and which could affect the reliability of mitigating systems (Step 8, below) is limited to a postulation of single faults. This analysis, while not complete, identifies many of these potentially important faults. Further analysis would be extremely time consuming and many multiple faults are expected to be probabilistically insignificant.

1.2 Plant Familiarization Procedures

The plant familiarization task involves 13 steps. Figure 1.2-1 illustrates the interrelationships among the various steps of this task.

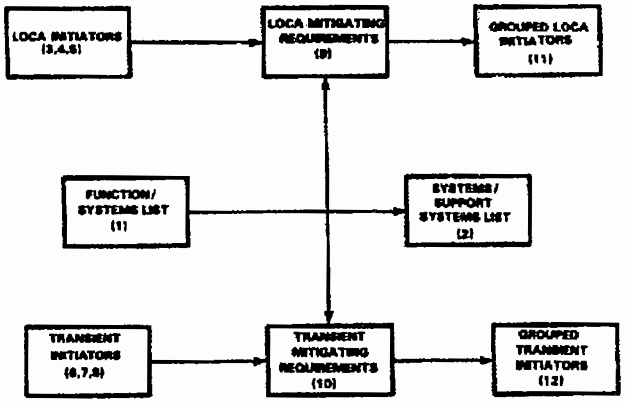

LOCA INITIATORS (3,4,5)
LOCA MITIGATING REQUIREMENTS (9)
GROUPED LOCA INITIATORS (11)
FUNCTION/ SYSTEMS LIST (1)
SYSTEMS/ SUPPORT SYSTEMS LIST (2)
TRANSIENT INITIATORS (6,7,8)
TRANSIENT MITIGATING REQUIREMENTS (10)
GROUPED TRANSIENT INITIATORS (12)

Figure 1.2-1. Step Relationships for Plant Familiarization Task

1.2.1 Description of Each Plant Familiarization Procedural Step

Function/System Relationships

Step 1. Identify the systems performing each function important to preventing or mitigating the consequences of a core melt following a loss-of-coolant accident or transient initiating event.

Description: The functions to be performed following a LOCA or transient in pressurized and boiling water reactors are discussed in Part III. The functions to be performed following a LOCA are summarized as follows [6]:

LOCA FUNCTIONS

PWR	BWR
A. Render reactor subcritical	A. Render reactor subcritical
B. Remove core decay heat 1. During injection phase 2. During recirculation phase	B. Remove core decay heat
C. Protect containment from overpressure due to steam evolution 1. During injection phase 2. During recirculation phase	C. Protect containment from overpressure due to steam evolution 1. Early 2. Late
D. Scrub radioactive material from containment atmosphere 1. During injection phase 2. During recirculation phase	D. Scrub radioactive material from containment atmosphere

The functions to be performed following a transient are summarized as follows [6]:

TRANSIENT FUNCTIONS

PWR	BWR
A. Render reactor subcritical	A. Render reactor subcritical
B. Remove core decay heat 1. Environment heat sink 2. Containment heat sink	B. Remove core decay heat 1. Environment heat sink 2. Containment heat sink
C. Protect reactor coolant system from overpressure failure	C. Protect reactor coolant system from overpressure failure
D. Protect containment from overpressure due to steam evolution	D. Protect containment from overpressure due to steam evolution
E. Scrub radioactive material from containment atmosphere	E. Scrub radioactive material from containment atmosphere

The effort to develop a simple, complete catalogue of accidents involving a reactor core is facilitated by distinguishing between front-line systems and support systems (see step 2). Front-line systems are those which perform the functions listed above. Examples of such systems include the reactor protection system, the core spray and low pressure coolant injection systems, and the containment spray and fan cooler systems.

Using information from the Final Safety Analysis Report supplemented by discussions with plant personnel or systems information from the plant, identify the systems performing each plant function tabulated above.

Product: List of systems performing each function.

Step 2. Identify supporting systems for each system identified above (in Step 1).

Description: For each system identified in the preceding step, identify those support systems required to faciliate operation of the system in response to a LOCA or transient. Such systems generally actuate the front-line system, supply motive and control power, supply component or room cooling, and supply other services. Where system operation requires operator control, consider the operators as a "support system" in the sense that they facilitate system response to the initiating event. Information needed to perform this step is contained in the Final Safety Analysis Report. This may be supplemented by discussions with plant personnel or system information supplied by the plant.

Further, identify any other support systems upon which these support systems depend.

Product: List of support systems for each system performing a LOCA or transient function and systems upon which support systems depend.

Initiating Events

Step 3. Identify ranges of loss-of-coolant accidents.

Description: The primary coolant system contains piping of various sizes. The IREP analysis examines accident sequences initiated by postulated pipe breaks ranging from the smallest LOCA for which emergency systems would be required to respond (those for which the coolant loss rate exceeds the capacity of the normal makeup system) up to and including the largest piping in the primary system. Using information contained in the Final Safety Analysis Report and plant drawings, identify these extremes.

The lower bound on the break area for the class of smallest LOCAs may be significant. Small leaks and very small line breaks are rather common in reactor coolant systems. Thus the assessed frequency of occurrence of the smallest LOCA class is likely to be a sensitive function of the minimum break area. This may prove to be important to the calculated risk. Thus some care should be taken in identifying the smallest LOCA sizes which would lead (realistically) to core melt if emergency core cooling fails.

In addition, subdivide the range of LOCAs into classes for which plant response, in terms of systems and the required subsystem operability, is the same. This information is contained in the Final Safety Analysis Report or may be found in analyses of particular events performed by the vendor or the utility.

Product: List of LOCA break sizes.

Step 4. Identify locations of potential loss-of-coolant accidents in systems which interface with the primary coolant system.

Description: Loss-of-coolant accidents may occur in piping which is normally isolated from the primary system but which, because of failure of isolation, could become part of the primary system. A loss-of-coolant accident in such systems is not likely unless the system is a low pressure system. If, however, low pressure piping is exposed to primary system pressure, rupture of the piping could occur.

Identify all systems which interface with the primary system. For these systems, search for paths through which primary system coolant could enter low pressure piping should isolation valves fail to be or remain closed. The analyst notes in this search flow-limiting orifices which could reduce pressure of the intruding primary coolant flow.

Most interfacing systems contain some low pressure piping. Thus, all are potential LOCA sources. However, generally if more than two independent failures must occur before reaching the low pressure piping or if orifices must fail, the probability of such a LOCA will be negligible and need not be considered in the analysis. List all systems in which such an interfacing system LOCA could occur. Note which of these could occur outside containment, and note which could be isolated.

Product: Interfacing systems LOCA list.

Step 5. Identify LOCA break locations which could disable or partially disable responding systems.

Description: For breaks in certain locations in the primary system, the functionability of emergency coolant injection systems may be impaired due to the injected coolant flowing out the break rather than onto the core. Examples of this could be a cold leg break in which flow from one accumulator or low pressure injection system line may be diverted out the break. Such situations influence the calculation of accident sequence frequencies both in terms of the initiating event frequency and of the probability of successful mitigation.

Two special cases deserve mention. One involves a loss-of-coolant accident whose symptoms do not actuate the Safety Features Actuation System. An example could be a LOCA initiated by rupture of a reactor pump seal. In such a case, manual actuation of the mitigating systems may be required. Another involves a loss-of-coolant accident outside the emergency core cooling design envelope. An example of this would be gross rupture of the reactor vessel. In such a case, it is generally assumed that the emergency coolant injection systems are not adequate to prevent core melt.

An additional possibility could be a break location where, because of entrapment volumes below the break, flow would not reach the sump. In such cases, operability of recirculation systems could be impaired if containment spray systems have failed.

Survey the primary coolant system to identify any such break locations. Note the effect on the systems which supply emergency coolant and note any other peculiar response characteristics.

Product: List of LOCAs which impact mitigating systems.

Step 6. Identify applicable transients from the list of "standard" transients.

Description: The Electric Power Research Institute (EPRI) has classified and estimated generic occurrence rates for transient event initiators at nuclear power plants in EPRI NP-2230 [3]. This work serves as a starting point from which to estimate the types and frequencies of transients to be expected in the subject plant. Tabulate which of the transients in the EPRI list are applicable to the plant and indicate their generic occurrence frequency.

Product: List of "standard" transients for this particular plant.

Step 7. Review plant history to identify additional transient initiating events.

Description: The plant may be susceptible to transients other than those listed in EPRI NP-2230. Review the licensee event reports from the plant and from plants of similar design and discuss the plant's operating history with plant personnel to ascertain whether transients other than those identified in Step 6 have occurred or could occur. Add these to the list of transient initiating events.

Product: List of plant-specific transient initiating events.

Step 8. Identify support system faults which could cause the reactor to trip and which could affect responding systems.

Description: Some transient events may be initiated by component failures in support systems which could not only initiate the incident but also affect the operability of systems needed to respond to the event. These dependencies for such transient initiating events influence the calculation of accident sequence frequencies.

Postulate single faults in each support system identified in Step 2. Ascertain (1) whether the fault would cause the reactor to trip and, if so, (2) whether the reliability of any of the front-line systems responding to the transient would be affected. If both conditions are satisfied, add the fault to the list of transient initiating events to be analyzed.

Such faults must first of all cause the reactor to trip. Otherwise, the plant systems would not be called upon to respond, and the event would not be of interest to this analysis. If the reliability of responding systems is not also affected by the fault, the fault can be grouped with other plant transients requiring the same mitigating systems and need not be given special consideration in the quantification process.

Support system faults are most readily evaluated on a train level, e.g., loss of particular ac or dc buses or loss of a component cooling loop or cooling to a particular room. It is at this level that the effects on mitigating systems is most readily discernible. To calculate the frequency of such events, however, the contributions of individual component failure rates must often be evaluated. These are then combined to give train-level failure rates.

Additional support system initiating events may be discovered in subsequent tasks when developing the system fault trees, examining support system/front-line system interfaces, or reviewing plant procedures. Any such events should be added to the set of initiating events for the analysis.

Product: List of transients initiated by support system faults.

Mitigating System Requirements

Step 9. Identify mitigating system requirements for each LOCA size and location.

Description: Fundamental to the development of plant models in subsequent tasks is the identification of mitigating systems and success criteria for each LOCA and transient initiating event. For each of the LOCAs identified in Steps 3 - 5, identify the combinations of systems called upon to perform each plant function (a subset of the systems from Step 1) and the number of trains of the system needed to successfully perform the function (e.g., one out of two core spray loops). This information may be found in the Final Safety Analysis Report.

The objective of the IREP study is to use realistic analyses of accident phenomenology. Thus it is unnecessary to employ licensing conservatism in the identification of mitigation requirements often found in the FSAR. If more realistic analyses have been performed, the results should be used. However, realistic analyses of emergency core cooling system (ECCS) requirements may not be available. It may be more efficient to proceed with the analysis employing the conservative licensing criteria to define ECCS requirements, but to note instances of suspected conservatisms. If after the initial assessment of accident sequence frequencies the conservatisms are predicted to influence the core melt frequency significantly, more refined ECCS success/failure criteria should be performed.

Product: Table of LOCA mitigating systems and success criteria.

Step 10. Identify mitigating system requirements for each transient initiating event.

Description: This step is analogous to Step 9. For each transient initiating event identified in Steps 6 - 8, identify the combinations of systems called upon to perform each plant function and the associated system success criteria. Success criteria should be as realistic as possible, but the analysis should not be halted while realistic calculations are performed. Rather, conservative assumptions should be made which may be relaxed later, if necessary and appropriate.

Product: Table of transient mitigating systems and success criteria.

Initiating Event Groups

Step 11. Group LOCA initiating events according to common mitigating system requirements.

Description: Using the results of Step 9, group LOCA initiating events according to common mitigating system requirements. That is, group all LOCAs in which the systems responding to the LOCA and the success criteria associated with each system are the same. In pressurized water reactors (PRWs) this can generally be done by effective break size. In boiling water reactors (BWRs) whether the break is a liquid or steam line break is also generally a determining factor. LOCAs involving interfacing systems or in locations affecting the operability of responding systems often cannot be grouped with others and form their own separate groups.

This grouping forms the basis for the development of event trees and the quantification of accident sequence frequencies. One event tree is developed for each LOCA group. Generally a frequency is established for each group, and calculation of the sequence frequency is performed using this frequency.

Product: List of grouped LOCA initiating events.

Step 12. Group transient initiating events according to common mitigating system requirements.

Description: This step is analogous to Step 11. Group all transients in which the systems responding to the transient and the success criteria associated with each system are the same. Transients initiated by support system faults often cannot be grouped with others because of their effects on the reliability of the mitigating systems.

Product: List of grouped transient initiating events.

Task Products

Step 13. Summarize task products for the task report.

Description: The five products of the plant familiarization task are listed below. The first product corresponds to the products of Steps 11 and 12. System success criteria tables summarizing success criteria for each LOCA and transient initiating event group are developed by combining the groupings with the mitigating system requirements specified in Steps 9 and 10.

The list of front-line systems for the analysis corresponds to those systems listed on the tables summarizing the system success criteria. (Note: This list may not correspond to the list developed in Step 1. For example, the standby liquid control system may perform a reactor subcriticality function in BWRs, but it may not shut down the reactor quickly enough to adequately respond to any of the initiating events identified for the analysis.) In some cases the same system may be called upon to perform different functions with different success criteria. If so, multiple success criteria should be noted on the front-line system list. For the purposes of the systems analysis, these are analyzed as separate cases. Each must be analyzed.

The list of support systems corresponds to the support systems from Step 2 for each front-line and support system. Finally, front-line system/support system and support system/support system dependencies are summarized in tabular or diagram form.

Products:

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 front-line systems.
4. List of support systems.
5. Table/diagram relating front-line/support system and support system/support system dependencies.

1.3 Plant Familiarization Documentation and Example Products

The documentation associated with the plant familiarization task should clearly present the logical thought process used in performing the task. This process involves the identification of plant functions and system relationships, the identification of LOCA and transient initiating events, and the grouping of initiating events according to common mitigating system requirements and the system success criteria associated with each initiating event group. In addition, areas for further investigation and refinement in subsequent portions of the study should be documented. This section suggests information to be documented upon completion of this task and includes example products from previous analyses. This report constitutes the informal report on the plant familiarization task to be reviewed approximately two months after beginning the analysis.

1.3.1 Plant Functions and Systems Relationships

The initial effort of this task is the identification of plant functions and relationships between plant systems and functions and among the systems. The functions selected for preventing core melt and for mitigating the consequences should a core melt occur should be documented. A list, such as in Table 1.3-1, relating plant systems to the functions they perform should be provided. Accompanying the list should be a discussion of the sources of information used in its development. A subset of these systems, as identified in Step 13, comprises the set of front-line systems for the analysis. List these as well (see Table 1.3-2). A brief explanation of why certain systems on the function/system list are not front-line systems should be included if there are any such systems.

The dependencies among front-line systems and their support systems should also be documented. For the purposes of this task, a table such as Table 1.3-3 would suffice along with a discussion of how the dependencies were identified. From this table, a listing, such as in Table 1.3-4, of support systems to be analyzed in the plant systems analysis task should be compiled.

Table 1.3-1 Transient Function/System Index

Transient Function	System(s)
Reactor Subcriticality	a. Reactor Protection System b. High Pressure Injection System*
Core Cooling	a. Power Conversion System b. Emergency Feedwater System c. High Pressure Injection System & Pressurizer Safety Relief Valves
Reactor Coolant System (RCS) Overpressure Protection/RCS Integrity	Pressurizer Safety Relief Valves
RCS Inventory Makeup	High Pressure Injection System
Containment Overpressure Protection	a. Reactor Building Spray System b. Reactor Building Cooling System
Radioactivity Removal	Reactor Building Spray System

*The high pressure injection system may only perform reactor subcriticality if the reactor coolant system components survive the overpressure transient following reactor protection system failure.

Adapted from Reference [8].

Table 1.3-2. List of Front-Line Systems

Reactor Protection System

Core Flood System

High Pressure Injection/Recirculation

Low Pressure Injection/Recirculation

Reactor Building Spray Injection/Recirculation

Reactor Building Cooling System

Power Conversion System

Emergency Feedwater System

Pressurizer Safety Relief Valves

Table 1.3-3. Front-Line Systems vs Support Systems Dependencies

Support Systems Front Line Systems	Offsite AC Power	Diesel AC Generators	125V DC Power	Engineered Safeguards Actuation system	Emergency Feedwater Initiation and Control System	Service Water System	Instrument Air system	Integrated Control System	Intermediate Cooling System	AC Switchgear Room Cooling	DC Switchgear Room Cooling	High Pressure Pump Room Cooling	Low Pressure/Spray Pump Room Cooling	Non-Nuclear Instrumentation Power
Reactor Protection System														
Core Flood System														
High Pressure Injection/ Recirculation	✓	✓	✓	✓		✓				✓	✓	✓		
Low Pressure Injection/ Recirculation	✓	✓	✓	✓		✓				✓	✓		✓	
Reactor Building Spray Injection/Recirculation	✓	✓	✓	✓		✓				✓	✓		✓	
Reactor Building Cooling System	✓	✓	✓	✓		✓				✓	✓			
Power Conversion System	✓		✓		✓	✓	✓	✓	✓	✓	✓			✓
Emergency Feedwater System	✓	✓	✓		✓	✓				✓	✓			
Pressurizer Safety Relief Valves														

Note: All requirements for diesel generators assume loss of station power.

Adapted from Reference [8].

Table 1.3-4. List of Support Systems

Offsite ac Power
Diesel ac Generators
125V dc Power
Engineered Safeguards Actuation System
Emergency Feedwater Initiation and Control System
Service Water System
Instrument Air System
Integrated Control System
Intermediate Cooling System
ac Switchgear Room Cooling
dc Switchgear Room Cooling
High Pressure Pump Room Cooling
Low Pressure/Spray Pump Room Cooling
Nonnuclear Instrumentation Power

1.3.2 Initiating Events

The selection of initiating events, both LOCAs and transients, is a major product of this task. These should be clearly identified, and the selection process documented to establish the basis for developing event trees and determining initiating event frequencies in subsequent tasks. This effort may be summarized in a table, such as the one shown in Table 1.3-5, produced in Step 13. This table lists all initiating events to be used in the analysis.

The identification of LOCA initiators involves several different steps. First of all, the range of piping diameter in the primary systems should be documented and, in particular, how the smallest LOCA size was chosen should be discussed. The search for potential interfacing LOCAs should be documented by listing the systems interfacing with the primary system and how they were assessed for inclusion as initiating events. This should provide the reader with a clear understanding of why some were chosen and others were not. For the example in Table 1.3-5, no interfacing LOCAs were selected for further analysis. Finally, any particular break locations which could adversely affect the initiating systems should be noted, and these effects should be discussed.

The selection of transient initiating events may be documented by reproducing the list of initiators found in EPRI NP-2230 and noting which are applicable for the plant. A brief explanation for those not found to be applicable should be provided. Those events added to this list as a result of the review of the plant's operating history should be discussed, and the events should be summarized. Finally, the review of support systems for single faults which could both cause a plant trip and adversely affect the reliability of the mitigating system should be discussed.

Table 1.3-5. Initiating Events to be Used in the Analysis

Designator	Initiating Event Description
B(1.2)	LOCA with a 0.38 to 1.2 in. equivalent diameter break
B(1.66)	LOCA with a 1.2 to 1.66 in. equivalent diameter break
B(4)	LOCA with a 1.66 to 4 in. equivalent diameter break
B(10)	LOCA with a 4 to 10 in. equivalent diameter break
B(13.5)	LOCA with a 10 to 13.5 in. equivalent diameter break
B(>13.5)	LOCA with an equivalent diameter break greater than 13.5 in.
T(LOP)	Loss of offsite power transient
T(PCS)	Transient initiated by a total interruption of main feedwater
T(FIA)	All other transients which do not affect front-line systems significantly
T(A3)	Transient initiated by a failure of ac power bus A3
T(B5)	Transient initiated by a failure of ac power bus B5
T(DO1)	Transient initiated by a failure of dc power bus DO1
T(DO2)	Transient initiated by a failure of dc power bus DO2
T(LOSW)	Transient initiated by failure of Service Water Valve CV-3824

Adapted from Reference [8].

1.3.3 Mitigating Systems, Success Criteria, and Initiating Event Groupings

The final significant product of this task is the grouping of initiating events by mitigating system requirements and the identification of mitigating system success criteria for each initiating event group. How the mitigating systems for each initiating event were identified should be described as well as the process of grouping the initiating events. This process may be summarized by listing the LOCA break size ranges to be considered and by listing the transients in each transient initiating event group. An example is shown in Table 1.3-6 listing the EPRI NP-801[7] transients (the source used in the analysis from which the example was taken) in each of these initiating event groups.

The selection of mitigating system success criteria for each initiating event group should be discussed. This discussion should provide references and support for each success criterion and note which ones are thought to be conservative and those which are to be further investigated. This information may be summarized in a table such as the one shown in Table 1.3-7.

1.3.4 Areas for Further Investigation

This being the initial stage of the analysis, there will undoubtedly be a number of questions which need to be answered and assumptions requiring further substantiation before the analysts feel comfortable with the products of this task. The analysis must proceed, but a listing of items for further investigation should be compiled and the plan for addressing each should be discussed.

Table 1.3-6. Grouped EPRI NP-801 Transient Initiating Events Requiring an Immediate Rapid Reactor Shutdown

Transient Designator	Description	EPRI NP-801 Transients
T(LOP)	Loss of offsite power	35
T(PCS)	Total interruption of the Power Conversion System (main feedwater)	16, 17,* 18, 20, 21, 22, 24, 25, 29, 30
T(FIA)	All other transients which do not affect front-line systems significantly	1, 2, 3, 6, 10, 14, 15, 17,* 33, 34, 37, 38, 39, 23

*One feedwater pump will be lost on a MSIV closure of one steam generator loop. Both feedwater pumps could be lost depending on the position of a trip selector switch in the control room. Therefore, since it is a 50-50 chance of losing both pumps, half of #17's frequency falls in T(PCS) and half of T(FIA).

Adapted from Reference [8].

Table 1.3-7. LOCA Success Criteria

		Injection Phase			Recirculation Phase		
LOCA Size	Reactor Subcriticality	Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Emergency Core Cooling	Containment Overpressure Protection Due to Steam Evolution	Post Accident Radioactivity Removal	Emergency Core Cooling
7.9E-4 – 0.008 ft^2 .38 in.–1.2 in. D Stuck Open ERV = 0.0056 ft^2 Max. recorded RCP seal failure 0.0035 ft^2	≥6 control rod groups inserted into the core by the reactor protection system (RPS)*	1/2 reactor bldg. spray injection (RBSI) OR 1/4 reactor bldg. fan coolers (RBCS)	1/2 RBSI	1/3 high pressure injection (HPIS) and 1/2 safety/relief valves (SRV) OR 1/3 HPIS and 1/2 emergency feedwater (EFS)	1/2 reactor bldg. spray recirc. (RBSR) and sump mixing with 1/3 HPRS and 1/2 LPRS heat exchanger OR 1/4 RBCS	1/2 RBSR	1/3 high pressure recirc. (HPRS) and 1/2 LPRS heat exchanger OR 1/2 EFS (during injection phase) and 1/2 decay heat removal system
0.008 – 0.015 ft^2 1.2 – 1.66 in. D Stuck Open P_z Safety 0.0145 ft^2	↓	↓	↓	2/3 HPIS and 1/2 SRV OR 1/3 HPIS and 1/2 EFS	↓	↓	1/3 HRPS and 1/2 LPRS heat exchanger
0.015 – 0.087 ft^2 1.66 – 4 in. D	↓	↓	↓	1/3 HPIS	↓	↓	↓
0.087 – 0.55 ft^2 4 – 10 in. D	↓	↓	↓	1/3 HPIS and 1/2 low pressure injection (LPIS)	1/2 RBSR and sump mixing with 1/2 LPRS heat exchanger OR 1/4 RBCS	↓	1/2 low pressure recirc. (LPRS)
0.55 – 1.0 ft^2 10 – 13.5 in. D	No system needed	↓	↓	1/2 LPIS and 1/2 core flood tanks (CFS)	↓	↓	↓
>1 ft^2 >13.5 in. D	↓	↓	↓	1/2 LPIS and 2/2 CFS	↓	↓	↓

*The HPIS can perform reactor subcriticality by injecting borated water in the event of RPS failure. However, since operation of the HPIS cannot prevent the pressure transient associated with RPS failure, the HPIS should not be considered a reactor subcriticality front-line system.

Adapted from Reference [8]

2. Accident Sequence Delineation

2.1 Overview of the Accident Sequence Delineation Task

2.1.1 Purpose

An IREP analysis consists of an evaluation of accident sequences—initiating events followed by combinations of successful and/or unsuccessful operations of responding systems—which could lead to core melt. Event tree models are constructed to delineate the appropriate accident sequences to be analyzed. The purpose of this task is to develop both functional and systemic event trees delineating accident sequences to be analyzed.

2.1.2 Products

The products of the accident sequence delineation task are as follows:

1. Functional event trees for plant response to loss-of-coolant accidents.
2. Functional event trees for plant response to transient initiating events.
3. Systemic event trees, one for each initiating event group (defined in the plant familiarization task).
4. Descriptions of each functional accident sequence, each systemic event tree and its events, and interrelationships reflected in the structure of each systemic event tree.

Examples of these products from previous IREP analyses are contained in Section 2.3 below.

2.1.3 Relationship to Other Tasks

The initiating event groups for which event trees are to be constructed are identified in the plant familiarization task. Specifically, the plant familiarization task produced lists of LOCA and transient initiating events grouped according to common mitigating system requirements. These lists define the event trees to be constructed in this task, one for each initiating event group. In addition, the system success criteria tables produced in the plant familiarization task for each initiating event group define the functions and front-line systems which appear as headings of the appropriate functional and systemic event trees. Thus the basic information needed to begin the event trees—the initiating events and responding functions and systems—is identified by the preceding task.

Several of the products of this task are used subsequently in the analysis. The systemic event trees define the accident sequences to be analyzed in the accident sequence analysis task. The frequency of each core-melt accident sequence is quantified by combining initiating events with the appropriate system fault trees as defined by the event tree.

The event descriptions accompanying each systemic event tree specify the conditions under which the plant system models are to be developed in the plant systems analysis task. These must be clearly specified to ensure that the system models are consistent with the event tree structure to facilitate proper accident sequence analysis. They also provide guidance to the accident sequence analyst should he need to consider any special conditions among events.

These interrelationships are summarized in Table 2.1-1 in which the input from other tasks are related to their use in this task and the products are related to other tasks using the products.

2.1.4 Information Needs

The following information, which are products of the plant familiarization task, is needed:

1. List of LOCA initiating events grouped according to mitigating requirements.
2. List of transient initiating events grouped according to mitigating requirements.
3. System success criteria for LOCA initiating event groups.
4. System success criteria for transient initiating event groups.

Other information pertinent to the performance of this task includes the Final Safety Analysis Report, similar analyses of this or a similar plant, analyses relating containment phenomenology to plant system operability during core-melt sequences, emergency operating procedures for the events under question, and supplemental methodological information contained in Part III of this guide.

How this information is used in the steps performed in this task is discussed in Section 2.2.

Table 2.1-1. Accident Sequence Delineation Task Relationships

Inputs From Other Tasks	Use in This Task	Products	Other Tasks Using Products
1. List of LOCA initiating events grouped according to mitigating requirements (plant familiarization task).	Identifies number and type of LOCA systemic event trees to be constructed.	1. LOCA functional event trees.	
2. List of transient initiating events grouped according to mitigating requirements (plant familiarization task).	Identifies number and type of transient systemic event trees to be constructed.	2. Transient functional event trees.	
3. Table summarizing system success criteria for each LOCA initiating event group (plant familiarization task).	Identifies front-line systems to be used as event headings on appropriate LOCA systemic event trees.	3. Systemic event trees for each LOCA and transient initiating event group.	Accident Sequence Analysis—defines initiating even‘ and system combinations to be analyzed.
4. Table summarizing system success criteria for each transient initiating event group (plant familiarization task).	Identifies front-line systems to be used as event headings on appropriate transient systemic event trees.	4. Descriptions accompanying each event tree	Plant Systems Analysis—specifies conditions under which systems to be modeled. Accident Sequence Analysis—specific special conditions to be incorporated into the sequence analysis.

2.1.5 Scope

The event trees constructed in this task should reflect not only systems whose operability influences whether an accident sequence results in core melt, but also systems whose operability influences the consequences of the accident sequence. Some systems, such as those associated with containment overpressure protection and postaccident radioactivity removal, may affect only the timing and magnitude of radioactive material released without affecting the possibility of core melt. Such systems should be included on the event tree even though the emphasis of the IREP analysis is only on core-melt sequences. For further use of the analysis, the incorporation of consequence distinctions in the event tree may prove useful.

In addition to functional and system interrelationships, the event tree structure should reflect possible phenomenological considerations which may influence core conditions, system operability, and/or accident consequences. A detailed investigation of accident phenomenology is beyond the scope of IREP. Rather, Part III of this guide includes a brief compilation of phenomenological relationships which have been included in some previous risk assessments. These provide a starting point for consideration in constructing event trees for a particular plant. The analyst, however, should seek to identify any additional phenomenological relationships which may be unique to the particular plant.

Many of these phenomenological issues are not currently resolved. The analyst must make his best judgment regarding assumptions for the particular analysis. Issues for which assumptions are uncertain and which may influence the results of the analysis should be identified as candidates for the sensitivity analysis discussed as part of the interpretation and analysis of results task.

2.1.6 Assumptions and Guidelines

In general, separate systemic event trees should be constructed for each LOCA and transient initiating event group. Each tree should have a unique structure, reflecting the different mitigating system requirements which were the basis for the groupings of initiating events. Event tree headings consist only of the front-line systems responding to the given initiating event group.

The structure of the event trees may differ for one or more of the following reasons. First, the combinations of front-line systems responding to the initiating events may differ. Second, although the combinations of systems may be the same, the success criteria for certain systems may differ among different initiating events. Finally, the functional and system interrelationships reflected by the tree structure itself may differ among different initiating events.

In some instances, the same event tree structure may apply for different initiating events. The most frequent instances of this are the event trees for loss-of-offsite power and for loss-of-main feedwater transients. If the two trees are identical, then only one event tree need be constructed. In such cases, however, the same accident sequences need to bc evaluated for each initiating event since quantification of the sequences would differ due to differing system power dependencies for the different initiating events.

The following assumptions have generally been made in past analyses and should be made in conducting future analyses of similar scope:

1. Failure of containment overpressure protection systems will cause containment failure which, in turn, will fail core cooling systems drawing water from the sump (sequence S_2C, e.g., in WASH-1400 [4]).
2. Credit has been given for containment fan coolers in a core-melt environment. The possibility of their failing due to aerosols in containment is treated as a sensitivity issue.
3. Credit has been given for recirculating systems (e.g., containment sprays) drawing from the sump in a post-core-melt environment. The possibility of their failing due to debris in the sump is treated as a sensitivity issue.
4. Once the core has melted, possible consequence distinctions associated with pouring water on the core debris using the emergency core cooling systems have not been considered. Operability of containment sprays, however, has been considered.
5. The possibility of successfully terminating accidents involving anticipated transients without scram (ATWS) has been considered in analyses of pressurized water reactors. This generally includes the implicit assumption that the reactor coolant system survives the initial pressure spike. In boiling water reactors, ATWS events have generally been considered to lead to core melt.
6. Vessel failure due to pressurized thermal shock has generally not been included, nor have steam generator tube rupture events.
7. Recovery of systems once initially failed has generally not been considered in the event trees, but rather has been treated as part of the final sequence analyses of potentially dominant accident sequences.
8. In boiling water reactors, long-term operability of containment overpressure protection systems following failure to inject coolant onto the core has generally not been considered. Operability of these systems is not expected to influence consequences of the core-melt accident.

2.2 Accident Sequence Delineation Procedures

The accident sequence delineation task involves 25 steps. Figures 2.2-1 and 2.2-2 illustrate the interrelationships among the various steps of the accident sequence delineation task. Part III, Section 2, of this guide contains further methodological guidance.

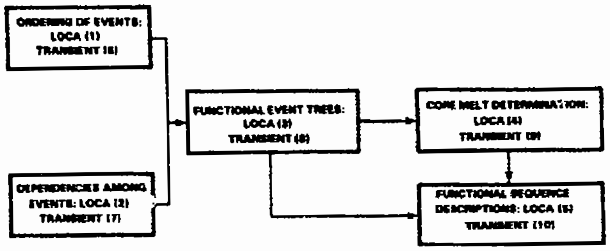


Figure 2.2-1. Step Relationships for Accident Sequence Delineation Task: Functional Event Trees

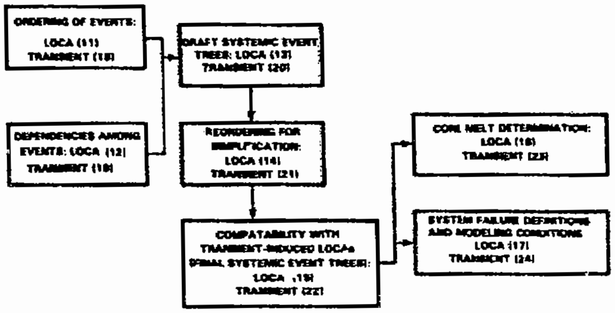


Figure 2.2-2. Step Relationships for Accident Sequence Delineation Task: Systemic Event Tree

2.2.1 Description of Each Accident Sequence Delineation Procedural Step

LOCA Functional Event Trees

Step 1. Place the functions required following a LOCA as identified in the plant familiarization task in the approximate order they will be called upon.

Description: Event trees generally present the functions in the approximate order they will be called upon following the initiating event. Therefore, the initial step in constructing the functional event tree is to identify the order in which the required functions will be performed.

The LOCA functions for both PWRs and BWRs were specified in Step 1 of the plant familiarization task. These are listed in the approximate order they would be called upon following the LOCA during the injection phase of the accident. Note that some functions are performed during injection and recirculation phases of the accident. Recirculation functions generally follow completion of all injection functions.

The LOCA functions should be reviewed in light of the mitigating systems identification performed in the plant familiarization task. It may well be that the functions required change for different sizes of LOCAs. For example, the subcriticality function is ensured by the physical processes associated with some break sizes. In that case, the subcriticality function would not be required and, hence, would not appear on the event tree. Separate functional event trees should be developed for each LOCA category.

Product: Ordered list of functions to be accomplished following a LOCA.

Step 2. Identify dependencies among the set of LOCA functions.

Description: The event tree structure reflects dependencies among the functions performed following the initiating event. To facilitate construction of the tree, these dependencies should be clearly identified. Functional dependencies are of three types:

1. The function succeeds/fails by definition due to success/failure of another function or set of functions.
2. The function fails/succeeds due to the expected physical processes associated with the accident sequence.
3. Success/failure of the function does not affect the potential for core melt or reduce the consequences of a core melt due to the success/failure of other functions in the accident sequence.

An example of the first dependency would be the failure of the "remove core decay heat during recirculation phase" function if it failed during the injection phase, assuming the same equipment is expected to perform each function. A possible example of the second type of dependency would be the failure of the "protect containment from overpressure due to steam evolution" function should some physical process following core melt be known to disable containment systems. (As mentioned in Section 2.1.6, however, credit is generally given for containment system operability.) An example of the third type of dependency would be that the performance of the "scrub radioactive material from containment atmosphere" function does not matter if other functions have been successfully performed and core melt has been averted.

To perform this step, information regarding the systems performing the functions developed in the plant familiarization task should be reviewed. Commonalities among the systems performing the functions alert the analyst to possible dependencies on the function level. This approach is most useful in identifying the first type of dependency.

The other two types of dependencies are most readily identified by thinking through each functional accident sequence in light of possible phenomenological relationships and in terms of whether each function in the sequence affects whether the core melts and/or the consequences of a core melt. This may be done best by first constructing the functional event tree reflecting the first type of dependencies and then by reviewing the tree sequence by sequence (see Step 3).

Product: List of dependencies among LOCA functions.

Step 3. Construct functional event trees, one for each LOCA category in which the functions or dependencies change, incorporating the dependencies identified in Step 2.

Description: The functional event tree reflects the functions to be performed following the initiating event and the dependencies among these functions. One functional event tree is constructed for each category of LOCAs in which the required functions differ or the dependencies among the functions differ.

The functional event tree is constructed by first ordering the events to be considered. This was done in Step 1, above. The first event tree heading is the initiating event. The others correspond to the responding functions ordered as in Step 1. Each event is given a unique alphabetic designator. Conceptually, the initial event tree has success/failure branches for each function. Actual construction of the tree involves the analyst deciding at each branch point whether a success/failure branch is needed, depending upon dependencies among the functions and reflecting this logic in the tree. Functional dependencies were identified in the preceding step. As mentioned in Step 2, it is perhaps easier to initially reflect only dependencies in which functions succeed/fail by definition due to success/failure of other functions. Phenomenological dependencies and inconsequential functions are easiest identified in the context of the functional accident sequences reflected by the event tree being developed. The final functional event tree reflects these aspects by removing the appropriate branches from the tree.

Product: Functional event trees for each unique LOCA category.

Step 4. Assess each LOCA functional accident sequence to ascertain whether it results in core melt.

Description: The only sequences of interest in the analysis are those which result in core melt. Therefore, each functional accident sequence identified in the functional event tree should be assessed to determine whether it results in core melt. Sequences involving failure to remove core decay heat result in core melt. Other sequences may result in core melt if failure of other functions indirectly results in loss of core heat removal as, for example, in the case of containment overprotection failure resulting in loss of core heat removal during recirculation.

Product: Tabulation next to each LOCA functional accident sequence noting whether core melt results or not.

Step 5. Prepare a brief description of each LOCA functional accident sequence.

Description: The event tree is a pictorial representation of accident sequences to be analyzed. As is apparent from the previous steps, development of the event tree involves several thought processes. To communicate the meaning of the event tree, a description of each functional accident sequence is prepared. This description briefly discusses the functions succeeding and failing in the sequence, relationships and dependencies among the functions (often reflected in the tree structure as well), the physical processes associated with the sequence, and whether and why it results in core melt. The discussion should explain each omitted branch point in the sequence. This step summarizes Steps 1-4.

Product: Descriptions to accompany LOCA functional event trees.

Transient Functional Event Trees

The steps for constructing transient functional event trees are analogous to Steps 1-5, above, for constructing LOCA functional event trees. Therefore, descriptions of Steps 6-10 are omitted; the user should refer to the description of Steps 1-5 and apply them to the transient tree. Steps 6-10 are, however, summarized below.

Step 6. Place the functions identified in the plant familiarization task as necessary following a transient in the approximate order they will be called upon.

Product: Ordered list of functions to be accomplished following a transient.

Step 7. Identify dependencies among the set of transient functions.

Product: List of dependencies among transient functions.

Step 8. Construct functional event trees, one for each transient category in which the functions or dependencies change, incorporating the dependencies identified in Step 7.

Product: Functional event trees for each unique transient category.

Step 9. Assess each transient functional accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each transient functional accident sequence noting whether core melt results or not.

Step 10. Prepare a brief description of each transient functional accident sequence.

Product: Descriptions to accompany transient functional event trees.

LOCA Systemic Event Trees

Part III, Section 2.2, discusses in more detail the development of a systemic event tree. The steps involved are briefly discussed as follows:

Step 11. Place the front-line systems identified in the plant familiarization task as responding to each LOCA initiating event group in the approximate order they will be called upon following a LOCA.

Description: Systemic event trees generally present the systems in the approximate order they will be called upon following the initiating event. Therefore, the initial step in constructing the systemic event tree is to identify the order in which the required systems will respond.

The systemic event trees consist of the initiating event and the front-line systems which respond to the event. The front-line systems for each LOCA initiating event group are those systems contained in the table summarizing system success criteria for each LOCA initiating event group (Step 13, plant familiarization task). This is a subset of the list of front-line systems.

The approximate ordering of system response may be ascertained by referring to the order the functions are performed (Step 1, above).

By matching the systems with the functions in order of functions as in Step 1, a first approximation of system order is obtained. For those functions performed by more than one system, the order of the systems is governed by other considerations (see Steps 12, 14). For this step, the analyst need not be concerned with such details.

Product: Ordered list of front-line systems responding to each LOCA initiating event group.

Step 12. Identify dependencies among the set of front-line systems responding to each LOCA initiating event group.

Description: The systemic event tree structure reflects dependencies among the systems responding to the initiating event. To facilitate construction of the tree, these dependencies should be clearly identified. System dependencies are of three types:

1. The system succeeds/fails by definition due to success/failure of another system or set of systems.
2. The system fails due to expected physical processes associated with the accident sequence.
3. Success/failure of the system does not affect the potential for core melt or reduce the consequences of core melt due to the success/failure of other systems in the accident sequence.

An example of the first dependency would be the failure of the containment spray system in the recirculation mode if the low pressure recirculation system has failed, assuming they share the same pumps and suction. An example of the second type of dependency would be failure of the low pressure recirculation system following loss of the containment cooling systems in the injection mode. Loss of containment cooling could cause early containment failure. Sudden depressurization of containment could cause water in the sump to boil, failing pumps drawing water from the sump. Part III, Section 2.1, of this guide contains a brief discussion of some phenomenological dependencies found in past risk assessments. An example of the third type of dependency would be in the functionability of a sodium hydroxide system to remove postaccident radioactivity. This may be ineffective at reducing post-core-melt consequences and does not influence whether the core would melt. Therefore, its operability is inconsequential to the analysis, and it should be removed from the tree.

To perform this step, information regarding the mitigating systems for each initiating event group in the summary success criteria table should be reviewed to identify potential dependencies. In addition, often the same equipment is used as part of different systems. This will become clear when each system is investigated in the following task. The same equipment may also be used in both the injection and recirculation modes with only minor valve realignments or with different success criteria. Such commonalities alert the analyst to possible dependencies. Generally, the analyst must make a probabilistic judgment—if the most probable faults are shared between two systems, both may be assumed to fail when one does. In some cases, such as a shared refueling water storage tank, failure of such common equipment is sufficiently improbable that the dependency may be ignored <u>in the event tree</u>. When in doubt, neglect the dependency when constructing the event tree. This will merely add a few more sequences to the tree, which is better than losing a potentially significant one. Any dependencies will be appropriately treated when the fault trees are combined in the sequence analysis.

The other two types of dependencies are most readily identified by thinking through each systemic accident sequence in light of possible phenomenological relat'onships and in terms of whether each system in the sequence affects whether the core melts and/or the consequences of a core melt. This may be done best by first constructing the systemic event tree reflecting the first type of dependencies and then reviewing the tree sequence by sequence (see Step 13).

Product: List of dependencies among front-line systems for each LOCA initiating event group.

Step 13. Construct systemic event trees, one for each LOCA initiating event group, incorporating the dependencies identified in Step 12.

Description: Construction of the initial systemic event tree is analogous to the development of the functional event tree described in Step 3, only using systems rather than functions. Refer to that discussion inserting "system" for function, "Step 11" for Step 1, and "Step 12" for Step 2.

Product: Systemic event trees for each LOCA initiating event group.

Step 14. Review each LOCA systemic event tree to ascertain whether the structure would simplify, while retaining system dependency information, if the order of events were changed. If so, modify the tree.

Description: The initial ordering of systems was in terms of approximate order of response following the LOCA. Several systems performing the same function were ordered in no particular fashion. As a result, the event tree constructed in the previous step may not be in its most reduced (i.e., fewest sequence) form.

The tree structure should reflect all possible combinations of systems necessary to perform a given function. Once the function has been successfully performed, success/failure choices for other systems performing the functions are generally inconsequential (similar to the third type of dependency above). As a result, there is often a given ordering of systems to minimize the number of potential outcomes. This is particularly true if the same system is involved with differing success criteria in combination with other systems to perform a given function.

The analyst must search for the proper ordering of systems within a given function to reduce the total number of sequences. Unfortunately, this process is more or less by trial and error. Part III contains an example of this step.

There may also be instances in which the reordering of systems on the event tree which perform different functions may result in simplification of the tree. The analyst should review the tree structure and simplify the tree, if possible.

Product: Further simplified LOCA systemic event trees.

Step 15. Identify where transient-induced LOCAs transfer into the LOCA systemic event trees. Review the structure to ensure applicability of the tree for transient-induced LOCAs. If the structure is not applicable, modify the tree.

Description: In many cases, an accident sequence initiated by a transient develops into a LOCA due to a stuck-open relief valve, opening of a relief valve to establish feed-and-bleed cooling, or leaking or rupture of a reactor coolant pump seal. Such sequences are generally modeled by transferring from the transient tree to the appropriate LOCA tree. The LOCA event tree structure should be constructed to be compatible with such a transfer.

Since this has not yet been considered, the existing structure may not be compatible. To be compatible, the tree must be structured such that: (a) no system whose operability has been determined prior to the transfer point on the transient tree appears subsequent to the transfer point on the LOCA tree; and (b) all systems and only those systems required to successfully terminate the transient-induced LOCA or to reduce its consequences appear subsequent to the transfer point on the LOCA tree. The analyst should review the tree structure to ensure these two conditions are met. If not, modify the tree.

Product: LOCA systemic event trees compatible with transient-induced LOCAs.

Step 16. Assess each LOCA systemic accident sequence to ascertain whether it results in core melt.

Description: This step is analogous to the analysis of LOCA functional accident sequences. See the description of Step 4 considering "systemic" rather than functional accident sequences.

In addition, assign a mnemonic designator to each sequence consisting of the initiating event designator and the designators of each failed system in the sequence, and note to which functional accident sequence each system accident sequence corresponds. This may be done by noting the corresponding functional accident sequence number.

Product: Tabulation next to each LOCA systemic accident sequence noting whether core melt results or not, a mnemonic designator, and the corresponding functional accident sequence.

Step 17. Develop system failure definitions and system modeling conditions for each system for each LOCA initiating event group.

Description: System models developed in the next task must be constructed to be compatible with the assumptions and criteria used to develop the systemic event tree. Therefore, the analyst should document this information reflecting his understanding of the context in which the system fault tree will be used in the sequence analysis. Any important timing considerations should also be noted.

In addition, the analyst should document all dependencies reflected in the event tree structure. Each omitted branch point on the tree should be explained.

Product: Descriptions to accompany each LOCA systemic event tree.

Transient Systemic Event Trees

The steps for constructing transient functional event trees, except for the transfer to the LOCA tree for transient-induced LOCAs, are analogous to Steps 11-17, above, for constructing LOCA systemic event trees. Therefore, except for Step 22, descriptions of Steps 18-24 are omitted; the user should refer to the descriptions of Steps 11-17 and apply them to the transient tree. Steps 18-24 are, however, summarized below.

Step 18. Place the front-line systems identified in the plant familiarization task as responding to each initiating event group in the approximate order they will be called upon following the transient.

Product: Ordered list of front-line systems responding to each transient initiating event group.

Step 19. Identify dependencies among the set of front-line systems responding to each transient-initiating event group.

Product: List of dependencies among front-line systems for each transient-initiating event group.

Step 20. Construct systemic event trees, one for each transient-initiating event group, incorporating the dependencies identified in Step 19.

Product: Systemic event trees for each transient-initiating event group.

Step 21. Review each transient systemic event tree to ascertain whether the structure would simplify, while retaining system dependency information, if the order of events were changed. If so, modify the tree.

Product: Further simplified transient systemic event trees.

Step 22. Identify which sequences result in a transient-induced LOCA. For these sequences, transfer to the appropriate LOCA tree at the appropriate branch point in the tree.

Description: Many transients become loss-of-coolant accidents due to a stuck-open relief valve, opening of a relief valve to establish feed-and-bleed cooling, or leaking or rupture of a reactor coolant pump seal. Such sequences are generally modeled by transferring from the transient tree to the appropriate LOCA tree. The transfer is generally made from the transient tree just after the event which results in the LOCA, for instance "safety or relief valve fails to reclose." Compatibility with the LOCA tree should be considered as discussed in Step 15. In most cases, only the LOCA tree requires modification. In some cases, however, it may be necessary to modify the transient tree.

Product: Transient systemic event trees with transfers to the appropriate LOCA tree for transient-induced LOCAs.

Step 23. Assess each transient systemic accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each transient systemic accident sequence noting whether core melt results or not, a mnemonic designator, and the corresponding functional accident sequence.

Step 24. Develop system failure definitions and system modeling conditions for each system for each transient-initiating event group.

Product: Descriptions to accompany each transient systemic event tree.

Task Products

Step 25. Summarize task products for the task report.

Description: The four products of the accident sequence delineation task are listed below. The LOCA functional event tree corresponds to the product of Step 4. The transient functional event tree corresponds to the product of Step 9. The systemic event trees for LOCAs and transients correspond to the products of Steps 16 and 23, respectively. The accompanying descriptions were developed in Steps 5, 10, 17, and 24.

Products:

1. LOCA functional event trees.
2. Transient functional event trees.
3. Systemic event trees for each LOCA and transient-initiating event group.
4. Descriptions accompanying each event tree.

2.3 Accident Sequence Delineation Documentation and Example Products

The documentation of the accident sequence delineation task should present both the functional and systemic event trees and should clearly state the event definitions for use in subsequent tasks. This section suggests information to be documented upon completion of this task and includes example products from previous IREP analyses. This constitutes a major portion of the first interim report on the analysis.

2.3.1 Functional Event Trees

The initial products of this task are LOCA and transient functional event trees. The development of these trees should be discussed, and the final version of the trees should be presented with each sequence numbered and annotated as to whether it results in core melt or not. Each sequence on the trees should be discussed in terms of which functions succeed and fail, the relationships and dependencies among the functions, the physical processes associated with the sequence, and whether and why it results in a core melt.

An example functional event tree is shown in Figure 2.3-1. A description of Sequence 3, adapted from the Arkansas Nuclear One IREP analysis [8] follows.

Sequence 3—In Sequence 3, the emergency coolant recirculation function is unavailable which causes a core melt. The containment overpressure protection during recirculation and radioactivity removal during recirculation functions are available, however, to potentially reduce accident consequences. The containment overpressure protection during recirculation function can delay or prevent a post core melt overpressure failure. The effectiveness of the containment overpressure protection during recirculation and radioactivity removal during recirculation functions in reducing accident consequence therefore depends on how long the systems performing containment overpressure protection can delay overpressure or if overpressure can be prevented.

2.3.2 Systemic Event Trees

The other principal products of this task are the systemic event trees. The development of these trees should be discussed, and the final version of the trees should be presented with each sequence given a mnemonic designator and annotated with whether it results in core melt and the corresponding functional accident sequence. Each event should be briefly described and the appropriate success criterion for the event in the context of the particular systemic event tree should be clearly stated. In addition, each branch point on the tree for which a success/failure choice has been omitted should be noted and the reason for not including a choice stated. A sequence-by-sequence description of the event tree need not be included due to the large number of sequences.

An example systemic event tree, taken from the Arkansas Nuclear One IREP analysis[8], is shown in Figure 2.3-2. The following dependencies are reflected in the tree by omitting success/failure choices at certain branches.

1. The reactor protection system (RPS) does not appear as an event on this tree. For breaks of this size range, it is predicted that operation of the RPS is not required. The core is rendered subcritical by voiding of the core following the LOCA.

2. A decision branch for reactor building spray injection (RBSI) can be eliminated for sequences in which core cooling and the reactor building fan coolers (RBCS) both succeed. For these sequences, the core and containment are successfully protected during the injection phase. Whether or not the RBSI operates would not affect accident consequences and therefore does not matter. The reason for eliminating the RBSI branch rather than the RBCS branch, which also performs the containment overpressure protection function, is that the RBCS would be actuated first following a LOCA at 4 psig while the RBSI starts later at 30 psig.
3. If the core flood system (CFS) fails, a decision branch for the low pressure injection system (LPIS) does not appear since core cooling fails and operation of the LPIS is moot. (In reality, CFS failure may not cause core melt but rather only limited core damage. The Arkansas Nuclear One IREP study assumed core melt will occur because no information was available to ascertain the amount of core damage.)
4. A decision branch for the low pressure recirculation system (LPRS) is not given for sequences involving failure of core cooling during injection (i.e., following CFS or LPIS failure).
5. Since the RBSI and reactor building spray recirculation (RBSR) share most of the same equipment, failure of the RBSI precludes success of RBSR. Therefore, no decision branch is given for RBSR, given Event C. A branch can also be eliminated for sequences in which the RBCS and the high pressure recirculation system (HPRS) both succeed. For these sequences, the core and containment are successfully protected during the recirculation phases. Whether or not the RBSR operates would not affect accident consequences and therefore does not affect accident consequences and therefore does not matter.
6. Decision branches for low pressure recirculation system heat exchangers (LPRSX) are only given if the RBCS fails and the RBSR succeeds. If RBCS fails, containment overpressure protection is already provided and LPRSX is not required. Event G, the alternate method of containment overpressure protection, requires success of both LPRSX and RBSR. If RBSR fails, then, operation of LPRSX is moot.

Definitions of D_4 and D_2 are as follows:

Event D_4 — Core Flood System (CFS) Failure— Following a large LOCA, the CFS operates in conjunction with the LPIS to provide the function of emergency core cooling during the injection phase. The CFS consists of two tank trains which passively inject borated water to the reactor vessel when the vessel pressure drops below 600 psig.

Based on discussions with the vendor, successful CFS operation following a B(13.5) LOCA requires that the contents of one of two tank trains be injected into the vessel.

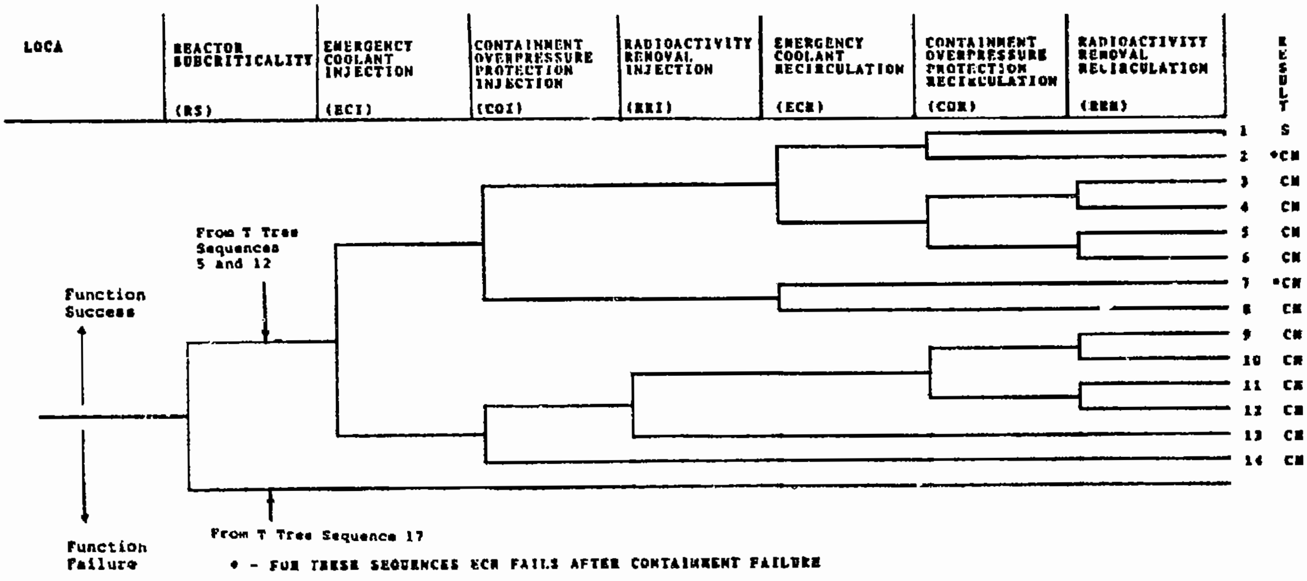

LOCA
REACTOR SUBCRITICALITY (RS)
EMERGENCY COOLANT INJECTION (ECI)
CONTAINMENT OVERPRESSURE PROTECTION INJECTION (COI)
RADIOACTIVITY REMOVAL INJECTION (RRI)
EMERGENCY COOLANT RECIRCULATION (ECR)
CONTAINMENT OVERPRESSURE PROTECTION RECIRCULATION (COR)
RADIOACTIVITY REMOVAL RECIRCULATION (RRR)
RESULT
1 S
2 *CM
3 CM
4 CM
5 CM
6 CM
7 *CM
8 CM
9 CM
10 CM
11 CM
12 CM
13 CM
14 CM
From T Tree Sequences 5 and 12
From T Tree Sequence 17
Function Success
Function Failure
* - FOR THESE SEQUENCES ECR FAILS AFTER CONTAINMENT FAILURE

Figure 2.3-1. Example LOCA Functional Event Tree

Event D_2 — Low Pressure Injection System (LPIS) Failure—As discussed in the previous subsection, the LPIS operates in conjunction with the CFS.

Based on discussions with the vendor, successful LPIS operation requires that the flow of one of two pumps be delivered to the reactor vessel via one of two low pressure injection lines.

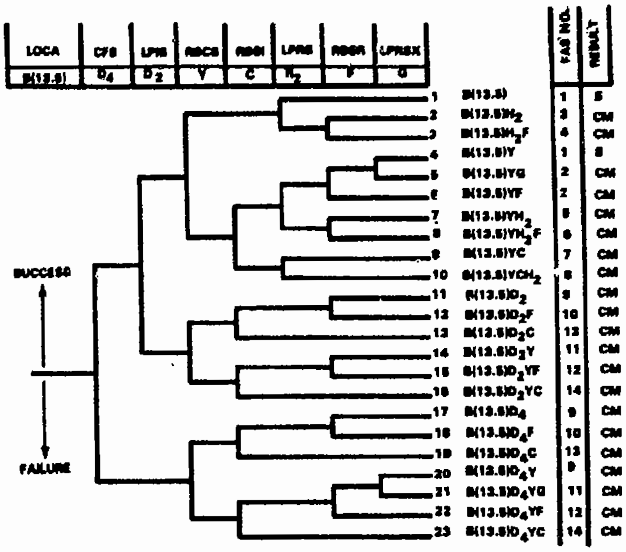


Figure 2.3-2. Example LOCA Systemic Event Tree for Breaks 10 in. <D≤13.5 in.

2.3.3 Issues for Sensitivity Analysis

There may be instances in which success criteria or phenomenological considerations are not well-known and in which assumptions must be made. These may well be candidates for sensitivity analysis later in the analysis. These should be documented for later reference. An example of one such issue is discussed in Part II, Section 7.3.2.1

3. Plant Systems Analysis

3.1 Overview of the Plant Systems Analysis Task

3.1.1 Purpose

A major objective of an IREP analysis is to identify and quantify the principal ways in which core melt accidents may occur. Event trees, as described in the previous section, define the combinations of system failures which, for a given initiating event, could cause core melt. To identify the ways in which each plant system may fail, fault tree models are constructed. These models represent all ways within the scope of the analysis in which a certain undesired event (the "top event," in this case system failure) may occur. The purpose of this task is to develop fault tree models for each front-line system and for each support system in the context of the front-line systems it supports.

3.1.2 Products

The products of the plant systems analysis task are as follows:

1. Fault trees for each front-line system for each of the success criteria specified on the event trees.
2. Fault trees for each support system developed in the context of each front-line system it supports.
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. An identification of further component failure rate data needs, if any.

Examples of these products from previous IREP analyses are contained in Section 3.3 below.

3.1.3 Relationship to Other Tasks

The plant systems analysis task integrates information from several other analysis tasks to produce system models for each plant system in the analysis. As such, it interfaces with several other analysis tasks.

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

Support system fault trees are developed in the context of the front-line systems they support. The system dependency diagrams developed in the plant familiarization task convey the relationships between front-line and support systems and among support systems. Generally, at least one support system fault tree is necessary for each front-line system it supports.

The descriptive material accompanying the systemic event trees produced in the accident sequence delineation task further specifies conditions under which the fault trees are developed. It is important that these conditionalities be clearly defined and incorporated into the fault trees to ensure compatibility between fault trees and event trees in the accident sequence analysis task.

The human reliability and procedural analysis task supports the development of the fault trees by identifying ways in which operator actions may cause systems, or more specifically, system components to fail. These actions generally fall into two categories: those associated with restoration of components to operability following test and maintenance activities and those associated with operator response under accident conditions. The identified human errors are included, as appropriate, in the fault tree development of the system.

Finally, the data base provided by the data base development task provides the plant systems analyst with guidance as to the level of detail to develop the system fault trees. The fault trees should be developed to a level of detail consistent with the existing data base—less detail or more detail will make quantification of the accident sequences difficult. On the other hand, the systems analyst may identify failure modes for components in the system which are not included in the data base. Should this occur, these needs should be discussed with those responsible for the data base development task to ensure that the appropriate data is available for the accident sequence analysis.

The products of the plant systems analysis task are used primarily in the accident sequence analysis task. One of the primary purposes of that task is to develop expressions containing all the ways each core melt accident may occur. This is done by first merging the support system fault trees with the appropriate front-line system fault trees as defined in the appropriate event tree accident sequence. The products of the plant systems analysis task form a key element in the accident sequence analysis. System descriptions produced as part of this task are included in the final report.

These interrelationships are summarized in Table 3.1-1 in which the input from other tasks is related to their use in this task and the products are related to other tasks using the products.

3.1.4 Information Needs

The following information is needed from other IREP analysis tasks:

1. From the plant familiarization task: the front-line systems list, the support systems list, system success criteria, and system dependency diagrams.
2. From the accident sequence delineation task: systemic event trees and accompanying event descriptions.
3. From the human reliability and procedural analysis task: the list of human errors associated with test and maintenance activities and associated with operator response to accidents.
4. From the data base development task: the generic data base.

In addition to these inputs from other tasks, substantial documentation on plant system design and operation is needed. Such documentation includes:

Final Safety Analysis Report
System descriptions (often used in operator training)
As-built system drawings
Electrical one-line drawings
Control and actuation circuitry drawings
Emergency, test, and maintenance procedures.

Furthermore, Part III of this guide and accompanying references provides additional guidance to assist in performing this task. How this information is used in the steps performed in this task is discussed in Section 3.2 below.

3.1.5 Scope

Fault trees should be constructed for each front-line system, one for each set of success criteria. Front-line system fault trees terminate at the component and an identification of support system requirements. Conditions specified in the event trees should be reflected in the fault trees.

Fault trees should be constructed for each support system in the context of the front-line systems each supports. For example, if electric power is needed by a component, an electric power fault tree for supplying power to the component is developed. This tree includes the breaker at the component. Often one bus supplies many components so that portions of the electric system fault tree are common to many components. In such cases, liberal use of transfer symbols eliminates duplic.tion in drawing the trees. Support system fault trees should be developed to reflect each logical variation necessary for each front-line system application.

Table 3.1-1. Plant Systems Analysis Task Relationships

Inputs From Other Tasks	Use in This Task	Products	Other Tasks Using Products
1. Front-line systems list (plant familiarization task).	Defines front-line systems for which fault trees to be constructed.	1. Fault trees for each front-line system for each of the success criteria and consistent with conditions specified in the systemic event trees.	Accident Sequence Analysis—identifies all ways each system may fail to use in deriving ways in which accident sequence may occur.
2. Support systems list (plant familiarizations task).	Defines support systems for which fault trees to be constructed.	2. Fault trees for each support system developed in the context of each front-line system it supports	Accident Sequence Analysis—provides models to merge with front-line system fault trees to identify all ways in which each front-line system may fail including support system faults, to use in deriving ways in which accident sequences may occur.
3. System success criteria (plant familiarization task).	Defines top events for front-line system fault trees.	3. System descriptions.	
4. System dependency diagrams (plant familiarization task).	Defines relationship between front-line and support system fault trees in context of each supported front-line system.	4. Identification of further component failure rate data needs.	Data Base Development—additional data to be collected to supplement the generic data base.
5. Systemic event trees and accompanying event descriptions (accident sequence delineation task).	Specifies conditions for front-line system fault trees.		
6. Identified test and maintenance restoration errors (human reliability and procedural analysis task).	Identifies faults for inclusion in the fault trees.		
7. Identified human errors in response to accidents (human reliability and procedural analysis task).	Identifies faults for inclusion in fault trees.		
8. Existing data base (data base development task).	Specifies level of detail for fault trees.		

The fault trees should reflect the detail contained in the data base and should include component unavailability 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. 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 analysis task.

The following common mode failure aspects should be reflected in the fault trees:

- Initiating event—system response interrelationships
- Common support system faults effecting more than one front-line system or component
- Coupled human errors associated with test and maintenance activities and in response to accident situations
- Shared components among front-line systems.

Environmental common causes, e.g., dust, ice, fire, etc., are not within the scope of the analysis. Other commonalities such as manufacturing deficiencies and installation errors are also considered beyond the scope of the analysis. Finally, β factors describing "other," unspecified causes of system failure are not to be included as part of the analysis.

3.1.6 Assumptions and Guidelines

A variety of approaches may be used to develop system fault trees. This guide has chosen not to specify a particular approach, since all approaches should yield equivalent results. It is, however, important to clearly specify the assumptions and guidelines associated with the fault tree development to ensure consistency.

Although a specific approach is not specified by this guide, it is suggested that all analyses begin by simplifying the system drawings and dividing them into piping segments, for fluid systems, or wiring segments for electrical systems. Guidance for such segmentation is provided in Part III, Section 3.1, of this guide. The top-level logic of the fault tree should then be constructed in terms of these segments. Once the top-level logic is so developed, the fault tree further develops the logic for each segment.

It is not necessary to construct fault trees for all plant systems. Those systems which do not interface with other plant systems and for which sufficient system-wide reliability data exists may not require fault trees. Examples of such systems are the reactor protection system or control rod hydraulic system, power-operated relief and code safety valves, and the power conversion system. In the case of power conversion system faults, data exists for losses of power conversion system. This system does, however, interface with other plant systems. It is important to separate out the interfacing faults in the analysis. A technique for treating the power conversion system is discussed in Part III, Section 3.3, of this guide.

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.

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

1. Include only single passive failures (such as pipe breaks) which can fail the entire system unless they are initiating events as well.
2. Consider flow diversion paths for fluid systems 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.
3. Consider spurious control faults for components after initial operation 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.

The inclusion of potential human errors in the fault trees is also limited by the following assumptions:

1. Do not include misposition faults of valves prior to an accident in those cases where the valve position is indicated in the control room and monitored each shift.
2. Do not include misposition faults prior to an accident if the component receives an automatic signal to return to its operable state under accident conditions.
3. Do not include potential operator recovery actions in the fault tree; "verify" statements in procedures should be treated as recovery actions. Recovery actions are considered as part of the final accident sequence analysis for potentially dominant accident sequences.

Maintenance faults should be included for each applicable component. Often technical specifications do not permit multiple trains of a given system to be out for maintenance. Building this aspect into the fault trees increases modeling complexity substantially. Thus it is recommended to include all maintenance faults in the tree. Should the analyst desire to preclude technical specification violations, this may be done by removing the terms which violate technical specifications from the accident sequence expressions developed in the accident sequence analysis task.

A naming scheme should be developed for identification of fault tree events. This should be done prior to development of the trees and should be used consistently by each analyst. Use of a specified naming scheme helps ensure accurate reduction and quantification of the fault tree.

The analysts should also be aware of introducing logic loops into the fault trees. These often occur when time-dependent interrelationships among auxiliary systems (e.g., electric power, room cooling, service water) have not been adequately considered. This is particularly a problem when different analysts develop the front-line and corresponding support systems. While these loops can be resolved when the front-line and support system fault trees are combined in the Accident Sequence Analysis Task, it is preferable to avoid introducing loops in the logic in the first place. This topic is discussed in some detail in Part III, Section 6.1.

3.2 Plant Systems Analysis Procedures

The plant systems analysis task involves 14 steps. Figure 3.2-1 illustrates the interrelationships among the various steps of the plant systems analysis task. Part III, Section 3, of this guide contains further methodological guidance.

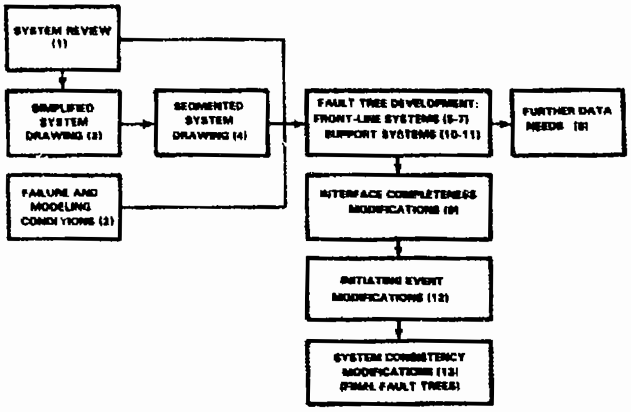

SYSTEM REVIEW (1)
SIMPLIFIED SYSTEM DRAWING (3)
SEGMENTED SYSTEM DRAWING (4)
FAILURE AND MODELING CONDITIONS (2)
FAULT TREE DEVELOPMENT: FRONT-LINE SYSTEMS (5-7) SUPPORT SYSTEMS (10-11)
FURTHER DATA NEEDS (8)
INTERFACE COMPLETENESS MODIFICATIONS (9)
INITIATING EVENT MODIFICATIONS (12)
SYSTEM CONSISTENCY MODIFICATIONS (13) (FINAL FAULT TREES)

Figure 3.2-1. Step Relationships for Plant Systems Analysis Task

3.2.1 Description of Each Plant Systems Analysis Procedural Step

System Review and Fault Tree Definition

Step 1. Review information for each front-line system to ascertain how the system operates, interfaces with other systems, instrumentation and control for the system, and how it is tested and maintained.

Description: Before beginning to develop a system fault tree, it is essential that the analyst thoroughly understand the system to be analyzed. This includes an understanding of system operation in terms of how the system performs its intended function under all conditions specified in the event trees, of which components must operate, of which must change state, and whether such operations are manual or automatic. In addition, the analyst must identify instrumentation associated with system operation and any associated control systems to thoroughly understand manual or automatic operation.

System boundaries, particularly in sites with multiple units and for systems supported by several systems, must be clearly defined. Generally, no credit is given in the initial fault tree for receiving flow from another unit unless this is the normal flow path. This may be treated subsequently when possible recovery actions are evaluated. Front-line systems generally include all principal components in the system and local support for the components (e.g., circuit breaker, control circuits) which do not affect other components or systems. Further support systems are modeled as support systems (see Step 11). Such front-line system-/support system interfaces should be well understood by the systems analyst before modeling activities begin. Much of this information has been developed as part of the plant familiarization task.

Test and maintenance procedures should be reviewed paying particular attention to identifying the components which are removed from their accident-response state to perform test or maintenance. To ascertain the importance of these alignments, the analyst should also investigate whether such components receive a signal to return the operability in event of an accident, whether there is a test override circuit, and the frequency and procedure for checking component positions, both locally and in the control room.

This information may be developed for each front-line system by searching the FSAR, system descriptions often used in operator training, system and support system drawings, and emergency, test, and maintenance procedures.

Product: System descriptions for each front-line system.

Step 2. Using system success criteria from the plant familiarization task and event failure definitions accompanying the systemic event trees, develop clearly stated failure conditions and modeling conditions for each front-line system.

Description: It is also essential that the analyst clearly define the event to be modeled and the associated conditionalities before beginning the fault tree. The "top event" of the fault tree is derived by converting the success criteria specified for the system into a statement of system failure. This is simply the converse of the success criteria. For example, requiring 1 of 4 trains for system success is equivalent to a top event of 4 of 4 trains of the system failing to operate under the specified conditions.

Modeling conditionalities, such as timing of events, were specified in the accident sequence delineation task in the context of each particular event tree sequence. Such conditionalities should be clearly understood; the systems analyst and event tree analyst should work together closely at this stage to ensure compatibility of the models.

More than one fault tree may be required for a front-line system should the system respond to different initiating events with different success criteria or under different conditionalities.

Product: Statement of a top event for each front-line system fault tree.

Step 3. Develop a simplified system drawing depicting the system to be modeled in the fault tree.

Description: Often the as-built system drawings contain considerably more information than is required in the systems analysis. To assist the analyst in clearly specifying his system and to simplify review of the analysis, the analyst should develop a simplified drawing specifying the system as modeled in the analysis. Simplifications include the omission of instrumentation from the drawing, omission of pipe segments which do not have a significant impact on system performance (e.g., piping less than one-third the diameter of the main system piping), and omission of supply lines for which credit is not taken in the initial analysis (e.g., alternate supply from another unit). In addition, lines containing normally closed manual valves which could only improve system performance if opened may be omitted unless procedures specify their opening in response to accidents. Such actions are considered only in the consideration of operator recovery actions.

The simplified drawing, however, should contain all piping segments and components included in the analysis. It should show the state of the components just prior to system actuation and possess labels corresponding to the plant equipment labels for each component. The system description (Step 1) should address components per their label and specify which components change state (and how) upon system actuation.

Product: Simplified system drawing for each front-line system.

Step 4. Decompose the simplified system drawing into piping or wiring segments.

Description: Development and review of the top level logic of the fault tree is facilitated by use of piping or wiring segments. Decomposition of the system into segments is the first step in this process. The decomposition is performed simply by placing a node on the simplified drawing at each point where two or more pipes or wires intersect. Each portion of the system between nodes is a segment. Part III, Section 3.1, of the guide contains an example of this process.

Product: Simplified drawing annotated with segments for each front-line system.

Fault Tree Development

Step 5. Develop system logic for each top event in terms of the pipe or wire segment configuration.

Description: Once the analyst is familiar with his system and modeling conditions, the fault tree modeling may begin. There are several approaches to developing fault trees (see References 9 to 11). All yield equivalent results, so no particular method is suggested here. The top level logic, however, should be constructed in terms of the segments specified in Step 4. This greatly simplifies review of the basic tree structure.

Product: Top-level logic for each front-line system.

Step 6. Develop logic for each segment in terms of segment components.

Description: Given the top-level logic has been developed, the fault tree development proceeds by modeling the logic associated with the components in each segment. This is generally a collection of component failures under an OR gate due to the way in which the segments were defined.

Product: Front-line system fault trees developed to the component level.

Step 7. Develop the logic for each component including hardware faults, test and maintenance unavailability, human errors, and support system faults.

Description: Development of the front-line system fault tree is completed by modeling the causes of the component being unavailable including hardware, human, and support system faults, and test and maintenance unavailability. Human errors include both restoration errors associated with test and maintenance activities and accident response errors as identified in the human reliability and procedural analysis task (see Part III, Section 3.5.) Support system faults should be developed only to the system level at this time. That is, development should terminate with faults such as failure of component cooling or ac power, etc. Support system faults are developed in Step 10 of this task.

Throughout the fault tree development, the analyst should ensure that the event naming scheme has been consistently used.

Product: Complete initial fault tree for each front-line system.

Step 8. Ensure that the data base includes data for each fault in the fault tree. If data for any events are missing, inform the data analyst.

Description: To quantify the frequency of each accident sequence, unavailability data must be provided for each basic event in the fault tree. The data base development task produces a set of data for use in the analysis. This data base should be reviewed by each systems analyst to ensure that data exists for each basic event in the analyst's fault tree. If not, the data analyst should be informed so as to develop the appropriate data for use in the quantification process.

Product: List of further data needs for the data base development task.

Step 9. Review each front-line system to ensure all support system interfaces have been included in the tree. If some are omitted, add them.

Description: As an additional check on the completeness of the fault tree, the analyst should ensure that all front-line/support system dependencies identified in the plant familiarization task have been included at the appropriate component in the front-line system fault tree. Any noted omissions should be added to the tree.

Product: Revised fault tree for each front-line system.

Step 10. Define the top events for each support system in the context of the developed front-line system fault trees.

Description: Fault trees for the support systems are not necessarily developed on the system level. Rather, they are developed to reflect only those portions of the system needed to support a given component. Top events are defined in terms of this front-line system support such as "failure to provide ac power to high pressure pump A." The analyst should also specify any modeling conditionalities, particularly with respect to timing of events. Unrealistic failure modes may be postulated if such conditions are not taken into account.

Product: Statement of top events for each support-system fault tree.

Step 11. Develop fault trees for each support system as in Steps 1-9 and consistent with the conditions specified in Step 10.

Description: The support system fault trees are constructed in a manner analogous with the development of the front-line system fault trees as described in Steps 1-9 above.

Guidance for modeling control circuits and actuation systems is provided in Part III, Section 3.2. Part III, Section 3.4, provides guidance for modeling continuously operating systems common among support systems. These include systems such as the component cooling system and plant electrical system.

Product: Fault trees for each support system.

Step 12. Ensure that all initiating events which could affect system operability are included in each front-line and support system fault tree. If not, include them.

Description: To accommodate the dependencies among initiating events and mitigating systems in the accident sequence analysis, it is important that the initiating events which affect system operability be included in the fault trees. Such events include LOCAs in an injection line or in a location such that flow will be diverted out the break, loss-of-offsite power, and other support-system-initiated transients such as loss-of-service water or particular power buses. The initiating events should be included at the appropriate level in the tree, generally as component failure modes.

Product: Further revised fault tree for each front-line and support system.

Step 13. Review all fault trees to ensure common equipment and common faults among different systems have been given the same event names. If not, modify the trees to ensure consistency.

Description: To ensure proper accounting for common failures in the accident sequence analysis, it is important that common faults each have the same identifier. In most cases, different analysts will have analyzed different systems and may not have ensured that the same component or fault was given the same name. This is particularly true if each front-line system analyst has developed his own support systems. An example of such a commonality would be the sump suction valves frequently shared by the containment spray and low pressure recirculation systems. Failure of these valves should have the same name in both front-line system fault trees. The analysts must review their fault trees together to ensure consistency among the trees.

Product: Final set of fault trees for each front-line and support system for use in the accident sequence analysis task.

Task Products

Step 14. Summarize task products for task report.

Description: The task products are listed below. The fault trees correspond to the final set of fault trees produced in Step 13. The system descriptions correspond to the products of Step 1 and the first part of Step 11. Data needs were identified in Steps 8 and 11.

Products:

1. Fault trees for each front-line system for each of the success criteria and consistent with conditions specified in the systemic event trees.
2. Fault trees for each support system developed in the context of each front-line system it supports.
3. System descriptions for each front-line and support system.
4. List of further data needs.

3.3 Plant Systems Analysis Documentation and Example Products

The documentation of the plant systems analysis task should provide a clear understanding of each plant system as modeled by the analyst and should contain the initial fault tree model of the system. This section suggests information to be documented upon completion of this task and includes an example system description from a previous analysis. This constitutes the major portion of the second interim report.

3.3.1 System Description

The system descriptions developed in this task for each front-line and support system should be documented. The description should begin with a brief description of the system's purpose; that is, what are the principal functions the system helps perform and to what accident initiators is it expected to respond. A description of the piping/wiring configuration should follow, accompanied by a simplified schematic of the system. Piping/wiring segments should be noted on the schematic. This discussion should clarify system boundaries used in the modeling effort. If certain flow paths have been ignored, these should be noted and rationale provided.

The systems supporting the front-line or support system should be delineated, and the effect of failure of the support system should be discusssed. This should be done by using tables such as those generated in a failure modes and effects analysis. Other auxiliaries such as instrumentation and control systems and their relation to system operation should also be discussed.

Testing and maintenance associated with the system should be discussed. This discussion should include a discussion of testing and maintenance frequencies and associated equipment manipulations to facilitate a clear understanding of which equipment is taken out of service and which may be candidates for errors of restoration following the activity. This information may be summarized in tables such as those in the example (see Section 3.3.3). Any pertinent technical specifications should also be mentioned.

Operation of the system in response to various initiating events should also be discussed. This discussion should specify equipment which changes state to initiate the system, what signals cause the system to actuate, and any required operator actions. If the operator is to perform any backup actions (such as initiating flow from an alternate water source should the primary source fail), these should be discussed along with the control room or local indications that the operator would have to perform the action.

3.3.2 System Fault Tree

The systems analysis effort culminates in the development of the fault tree model for each front-line and support system. At this stage of the analysis, the initial fault trees are complete. These should be included in the task documentation. Accompanying the fault tree of each system should be a clear statement of the failure criterion under each set of accident conditions. Assumptions made in the development of the fault tree should be delineated, and rationale for the assumption should be provided.

The entire fault tree for each system should be included. This includes the top logic in terms of piping/wiring segments and the logic for each segment. Accompanying the fault tree should be a fault summary sheet. At this stage of the analysis, the sheet contains only the fault identifier and a brief description of the event. Data entries are added in a subsequent task.

Finally, a list of data not found in the data base should be included for use by the data base analyst.

3.3.3 Example System Description

An example system write-up for the emergency feedwater system taken from the Arkansas Nuclear One Unit 1 (ANO-1) IREP analysis [8] follows.

3.3.3.1. System Description of the Emergency Feedwater System

The Emergency Feedwater System (EFS) described and analyzed in the ANO-1 report differs from the current system installed at ANO-1. Changes proposed to the current system have been approved by NRC and are scheduled for implementation in early 1982. Because they will result in significant improvements in the availability of EFS functions under certain postulated plant conditions, it was deemed appropriate to analyze the system as it will be configured following these changes.

The major revisions to the EFS will be the change from "normally closed" to "normally open" of some EFS block valves, the change from ac power to battery-backed dc power for certain valve functions, and the installation of a new safety-grade control system for emergency feedwater system pumps and valves. Because some engineering and administrative details of the revised system have not yet been completed, it was necessary to make assumptions regarding some aspects of the system for purposes of analysis. These assumptions will be indicated in the following discussion where appropriate.

3.3.3.2 Purpose

The purpose of the ANO-1 EFS is to backup the Main Feedwater System (MFS) in removing post-shutdown decay heat from the reactor coolant system via the steam generators. During normal shutdowns the MFS is throttled down to a level capable of removing decay heat, and the EFS is not utilized. However, if the plant shutdown is caused by a loss of the MFS or the reactor coolant pumps, or if the MFS is lost subsequent to the plant shutdown, then the EFS is put into operation. It is important to note that at some other PWRs the MFS is not throttled down during normal shutdowns. Instead, the MFS is tripped and the backup feedwater system at these plants, the "auxilliary" feedwater system, is put into operation during all shutdowns. This note is made to explain why the backup feedwater system at ANO-1 is labeled emergency rather than auxiliary.

3.3.3.3. Description

The EFS consists of two interconnected trains, capable of supplying emergency feedwater to either or both SGs from either of two water sources under automatic or manual initiation and control. A simplified piping diagram is included as Figure 3.3-1.

The system pumps take suction from either the condensate storage tank or from the service water system and discharge to the SGs. In the flow path between the emergency feedwater pumps and the SGs there are EFS isolation valves, check valves, control valves, flow instrumentation, and pressure instrumentation to control the flow of emergency feedwater to the SGs. The EFS is designed tc provide a minimum of 500 gal/min of emergency feedwater to the SGs at 1050 psig within 50 seconds of a system initiation signal.

The primary water source for both EFS trains is the condensate storage tank, T-41. This tank is required by technical specifications to contain a reserve of 107,000 gallons for EFS use. Water is supplied from this tank to a common suction header via a single eight-inch line containing a locked-open valve, CS19.

Calçulations based on an approximate cumulative deca·· heat curve indicate that the condensate storage tank reserve is sufficient for over ten hours of EFS operation. This period of EFS operation would not normally occur since the decay heat removal system would be brought into operation after about four hours. There are other connections to this suction supply line. These are supply connections to the condensate transfer pumps and an interconnection with the unit 2 condensate storage tanks, 2T-41A and 2T-41B. The unit 2 condensate storage tanks will usually be available as an alternate water supply for the unit 1 EFS. (They are not shown on Figure 3.3-1, because, this source of potential emergency feedwater was not analyzed.)

An alternate suction source is available from the nuclear service water system, loops one and two. Suction may be manually transferred from the condensate storage tank to the nuclear service water system by means of ac motor-operated valve pairs CV2806/CV2802 and CV2803/CV2800. A common control switch for each pair causes the valves to assume opposite positions; that is, if one valve (e.g., CV2806) is open, the other valve (CV2802) is closed and vice versa. A second operator action, the opening of ac motor-operated valves CV3850 and CV3851, is also required. Operators are alerted to perform this suction transfer by a low condensate storage tank alarm and by a low suction pressure alarm on the common suction header.

The EFS train B uses a turbine-driven pump (P7A) rated at 720 gal/min at 1070 psig. The train A pump (P7B) is motor-driven and is rated at 780 gal/min at 1070 psig. These flows include a normal recirculation flow of 15 gal/min and, under low system flow conditions, recirculation flow paths open to allow 78 gal/min flow.

The pumps are interconnected downstream from a check valve at their discharge by two separate cross-ties, one containing dc-powered valves and the other ac-powered valves. In addition, there is another cross-tie containing two normally closed ac-powered valves. Thus each pump can supply either or both steam generators.

The flow of emergency feedwater to each SG is controlled by redundant motor-operated control valves in parallel paths. These control valves are designed to fail "as is." Initiation and control instrumentation for these valves are described in Section 3.3.3.5.

Each SG can be isolated from emergency feedwater flow by normally closed motor-operated valves (CV2620, CV2670, CV2626, and CV2627). These valves are located in the parallel lines downstream of the normally open emergency feedwater control valves (CVX-1, CVX-2, CVX-3, and CVX-4). Initiation and control instrumentation for these valves is described in Section 3.3.3.5.

Steam supply for emergency feedwater pump P7A turbine is obtained from both steam generators via valves CV2666, CV2667, and CV2617. Downstream of these valves, the pipes join to form a common supply to the pump turbine. A check valve is installed in each line downstream of valves CV2617 and CV2667 (see Figure 3.3-1) to preclude blowing down a good steam generator in the event of a steam line or feed line break at the other steam generator. Upstream of the turbine are redundant dc motor-operated normally closed valves (CVY-1 and CVY-2). These valves are opened automatically on EFS initiation. They may also be manually opened. A description of the controls for these valves is contained in Section 3.3.3.5.

Steam from valves CVY-1 and CVY-2 passes through a redundant pressure-reducing station and on to the turbine governor and overspeed trip valve. Turbine trip is alarmed in the control room. The valve must be reset locally. Two overpressure relief valves (PSV 6601 and PSV 6602) are connected to the steam supply line upstream of the turbine governor. These valves will protect the piping and turbine downstream of the pressure-reducing valves in the event of PRV failure to limit pressure surges.

Turbine exhaust is vented directly to the atmosphere.

All ac- and dc-powered valves fail "as is" on the loss of electric power. All such valves, shown on Figure 3.3-1, are controllable locally (manually) and from the control room, and their position is indicated in the control room. Power for the indication and control of these valves is derived from the power source for the respective valve motors.

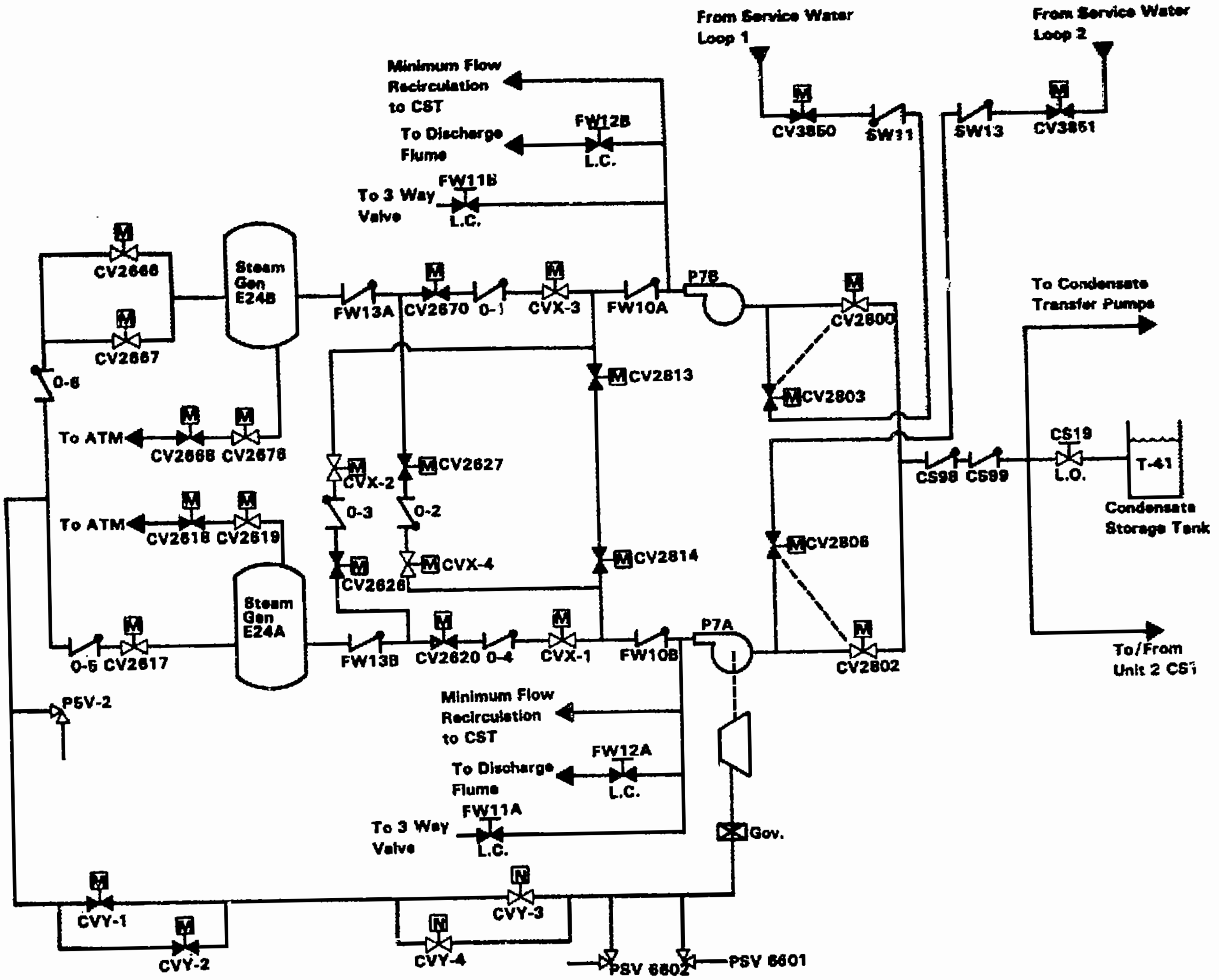


Figure 3.3-1. Arkansas Nuclear One, Unit 1 Emergency Feedwater System

3.3.3.4 System Interfaces/Support System FMEA

Except for electric power, the emergency feedwater pumps, pump motor and turbine are self-contained entities without dependencies on secondary support systems. The bearings on the turbine and both pumps are lubricated by slinging oil from reservoirs near the bearings. Cooling is accomplished by water flow through the pumps and by heat transfer to the surroundings. System interactions which could affect availability are detailed in Table 3.3-1. (Only some of the interactions are detailed in this example system description.) A system not listed is the Emergency Feedwater Initiation and Control (EFIC) system, which is actually a subsytem to the EFS. EFIC is discussed in detail in a separate system description and in general in Section 3.3.3.5 of this description.

The two EFS trains are powered from diverse power sources. The motor-driven pump (P7B) is powered by ac. Power for ac-driven components needed to obtain emergency feedwater flow is derived from diesel generator-backed 4160 Vac busses. In addition to pump P7B, the following valves are ac powered: CV2800, CV2803, CV281ˉ, CV2814, CV2626, CV2667, CV3850, CV2666, CV3851, CV2670, CV2617, CVX-2, and CVX-3.

To ensure emergency feedwater flow in the event of a loss of all ac power, the turbine-driven pump train (train B) derives its steam from the SGs and electric power from a battery-backed dc buss for its steam feed valves. Valves requiring battery-backed dc power are as follows: CV2815, CV2816, CVY-1, CVY-2, CVX-1, CV2802, CV2806, CVX-4, CV2620, and CV2627.

Table 3.3-1. ANO-1 Emergency Feedwater System Interaction—FMEA

Support (Sub)System	Component Affected	Failure Mode	Detection/ Recovery Potential	Component Failure Effect on System Operation (Assume no Recovery)	Effect of Support Subsystem Failure on Overall System Function (assume no recovery)
4160V Bus A-3	Motor-driven pump p7B	Loss of function	1. Multiple Low voltage alarms	Loss of one-out-of-two EFS pumps	Loss of Train A upstream from crossover. Loss of alternative water supply from service water system to Train A.
	Valve CV2800	Fail open	2. Autostart of diesel generator #1. Autoclosure of output breaker ≤15 s.	None	
	Valve CV2626	Fail closed		None	
	Valve CV2667	Fail closed		None	
	Valve CV2670	Fail closed		None	
	Valve CV3850	Fail closed		Loss of alternate water supply from service water system Loop 1	
	Valve CV2803	Fail closed		Loss of alternate water supply from service water system Loop 1	
	Valve CV2813	Fail closed		Loss of alternate crossover path between Train A and Train B	
4160V Bus A-4	Valve CVX-2	Fail open	1. Multiple low voltage alarms	None	Loss of alternative water supply from service water system to Train B
	Valve CVX-3	Fail open		None	
	Valve CV2617	Fail open	2. Autostart of diesel generator #2. Autoclosure of output breaker ≤15 s	None	
	Valve CV2666	Fail closed		None	
	Valve CV2814	Fail closed		Loss of alternate crossover path between Train A and Train B	
	Valve CV3851	Fail closed		Loss of alternate water supply from service water system Loop 2	
Service water Loop 1	Pump P78	Loss of service water suction	1. Multiple alarms	Loss of alternate water supply from service water system to EFS Train A	Loss of EFS Train A upstream from crossover after depletion of condensate storage tank
			2. Start service water pump and/or realign service water system		

3.3.3.5 Instrumentation and Control

The EFIC is an instrumentation system designed to provide the following:

1. Initiation of the EFS.
2. Control of emergency feedwater to maintain appropriate steam generator level set points (approximately 2 and 20 feet).
3. Level rate control when required to minimize RCS overcooling.
4. Termination of main feedwater to a steam generator during approach to an overfill condition.
5. Directing emergency feedwater to the appropriate steam generator(s) under conditions of steam line break or main feedwater or emergency feedwater line break downstream of the check valve.
6. Termination of emergency feedwater to a steam generator on approach to overfill conditions.
7. Control of set points for the atmospheric dump valves.

EFIC is a safety-grade system which operates on battery-backed dc power. The logic is contained in relay racks and individual component controllers. Automatic initiation will occur whenever one of four conditions exist:

- Loss of both main feedwater pumps
- Loss of all four reactor coolant pumps
- Low water level in either steam generator
- Low pressure in either steam generator.

The automatic initiation will open valves CVY-1 and CVY-2 to start the turbine-driven pump. The initiation signal also closes the circuit breaker to start the motor-driven pump. Once a pump is started, emergency feedwater flow will occur, since the flowpaths, including the discharge cross-ties, are either normally open or automatically opened by the EFIC system.

Bypass controls are provided to prevent undesired initiation of the EFS due to low steam generator pressure during startup and shutdown or during maintenance activities. The bypass is administratively controlled and does not preclude EFS initiation due to loss of reactor coolant pumps, main feedwater pumps, or low steam generator level.

Normal control of emergency feedwater flow is achieved with flow control valves CVX-1, CVX-2, CVX-3, and CVX-4. If the EFIC system senses a loss of main feedwater pumps, loss of reactor coolant pumps, or low level or pressure in the steam generators, it starts both emergency feedwater pumps and closes the main feedwater valves CV2624, CV2625, CV2674, and CV2675. Emergency feedwater flow is directed through CV2620, CV2626, CV2627, and CV2670 to the upper nozzles in the steam generators.

CVX-1 through CVX-4 are normally controlled by the EFIC system. The EFIC system adjusts these valves to attain and maintain one of two steam generator level set points, depending on reactor coolant pump (RCP) status. If the RCPs are running, the low level is maintained. If the RCPs are off, the high set point is maintained in order to promote natural circulation in the reactor coolant system. A loss of the EFIC signal will result in the valve failing in the "as is" position which, depending on SG conditions at the time of failure, could be the closed position. All valve and pump controllers are designed so that signals from the EFIC system will override any other control signals.

Instrumentation provided in the control room and its availability given three (i.e., power source dependency) plant conditions are:

Indication	Loss of MFW	Loss of MFW Due to Loss of Offsite Power	Loss of All ac Power
CST-1 level	No	No	No
CST-1 level alarms	Yes	Yes	Yes
Emergency feedwater flow	Yes	Yes	Yes
Valve positions	Yes	Yes	No*
OTSG level	Yes	Yes	Yes
OTSG level alarms	Yes	Yes	Yes

*For all except dc-powered valves CVX-1, CV2802, CV2806, CVX-4, CVY-1, CVY-2, CV2815, CV2816, CV2620, and CV2627.

3.3.3.6 Operator Actions

For a loss of MFW, no operator action is required to establish emergency feedwater flow. The operator will verify proper flow control and adjust the flow control valves as required. Certain failures (e.g., mispositioned valves, pumps fail to auto start, etc.) have the potential of being corrected from the control room.

In the event of total loss of ac power, the turbine-driven pump would start automatially and all the dc powered valves would be aligned to permit flow to the steam generators. In addition, during the course of such a transient, the operator could control these valves from the control room.

3.3.3.7 Surveillance

NOTE: Test procedures have not yet been prepared for the proposed EFS configuration covered in this analysis. It is assumed here that testing frequencies and procedures will be equivalent tc those for the current system, as described below.

The procedures for periodic testing are summarized in Table 3.3-2. These procedures verify capability for manual (but not automatic) start and control of the EFS. (The automatic start capability is currently "tested" when the EFS is required, i.e., upon loss of MFW during operation.) Emergency feedwater flow ratc to the steam generators at expected steam generator temperatures and pressures is not verified due to concern for deleterious effects on the system (e.g., thermal shock to feedwater nozzles and potential for rapid cooldown events). Tests that have impacts on system availability which were addressed in the analysis are shown in Table 3.3-3.

3.3.3.8 Maintenance

Maintenance acts, which are analyzed here, are those which require isolation of the component. The EFS has 20 active components (MOVs, pumps) capable of being isolated. Isolation is achieved by closing the appropriate upstream and downsteam valves from the component under maintenance (see Table 3.3-4). (Only a partial list is included in this example system description.)

Table 3.3-2. Summary of Emergency Feedwater System Testing and Periodic Maintenance

Supplement I (Monthly)	Start electric pump manually—measure suction and discharge pressures, bearing vibration.
Supplement II (Monthly)	Start turbine pump—measure suction and discharge pressures, bearing vibrations and turbine steam valve stroke times.
Supplement III (Quarterly)	Operate all system control valves and record stroke times and interlock functions.
Supplement IV (18 Months)	Start electric pump and feed steam generators, record flow to steam generators (~225 psi head).
Supplement V (Refueling)	Disconnect turbine from pump. Measure turbine speed at which overspeed trips occur and calibrate as necessary.
Supplement VI (Refueling)	Flush lines between Service Water System Loops 1 and 2 and pump suction.

Table 3.3-3. Emergency Feedwater System Component Test Summary Sheet

Component Undergoing Test	Type of Test	Test Procedure Number	Components Which Must Be Aligned Away From Emergency Position With With No Auto Return	Expected Frequency of Test	Expected Outage Time for Test
Pump P7A	Flow	1106.06 Supplement 2	CVX-1 CVX-4	Monthly	1 Hour
Pump P7B	Flow	1106.06 Supplement 1	CVX-2 CVX-3	Monthly	1 Hour

Table 3.3-4. Emergency Feedwater System Component Test Summary Sheet

Component Undergoing Test	Type of Maintenance	Maint. Procedure Number	Components Which Must Be Aligned Away From Emergency Position With With No Auto Return	Expected Frequency of Maintenance	Expected Outage Time for Maintenance
Pump P7B	Maintenance Requiring Disassembly; Motor Maintenance	A-EFW-1	Close CV2800 Disable Breaker 5333 Close CVX-3* Close CVX-2 Disable Breaker A311	3.1E-5/h	7 h
Pump P7A	Maintenance Requiring Disassembly	A-EFW-3	Disable Breaker 6181 Close CV2802 Close CVX-1 Close CVX-4 Disable Breaker Y-1** Disable Breaker Y-2** Disable Breaker 5533	3.1E-5/h	7 h
CV2803	Maintenance Requiring Assembly; Valve Motor Maintenance	A-EFW-4	Disable Breaker 5193 Close CV2800 Close CVX-3 Cloxe CVX-2 Disable Breaker A311 Disable Breaker 5194	1.8E-6/h	4 h
CV2806	Maintenance Requiring Disassembly; Valve Motor Maintenance	A-EFW-6	Disable Breaker 6181 Close Valve CV2802 Close CVX-1 Close CVX-4 Close CVY-1 Close CVY-2 Disable Breaker 6185	1.8E-6/h	4 h
CVX-3	Maintenance Requiring Disassembly; Valve Motor Maintenance	A-EFW-8	Disable Breaker X-3 Disable Breaker A311 Disable Breaker 5193 Close CV2800 Close CVX-2 Close CV2670 Disable Breaker 5533	1.8E-6/h	4 h
CV2670	Maintenance Requiring Disassembly	A-EFW-10	Disable Breaker 5332 Close CVX-3 Close CVX-4	1.8E-6/h	4 h

3.3.3.9 Technical Specification Limitations

The limiting condition for operation for the EFS requires two independent emergency feedwater pumps and associated flow paths be operable with:

1. One emergency feedwater pump capable of being powered from an operable emergency bus.
2. One emergency feedwater pump capable of being powered from an operable steam supply system.

If one emergency feedwater train becomes inoperable for 24 hours, the plant must be placed in hot shutdown within the next 12 hours. If not restored to operable status within the next 36 hours, the unit shall be brought to a cold shutdown condition within the next 12 hours.

Technical specifications also require the availability of 107,000 'gallons of water in the condensate storage tank (T-41) for EFS use.

3.3.3.10 Operation

A simplified schematic of the EFS is given in Figure 3.3-1. From the figure it can be seen that the EFS is a two-train system—a steam-driven turbine pump train and an electric pump train. The pump trains draw from either the preferred condensate storage tank or from the service water system and deliver to the steam generators. Due to interties at the pumps' discharge, either pump can feed either steam generator. Steam required to operate the turbine pump is extracted from either steam generator upstream of the two main steam isolation stop valves.

Both pumps are started automatically under any of the conditions listed in 3.3.3.5, or by operator action. Pump P7B is started by application of power to the electric motor. Pump P7A is started by opening of valves CVY-1 and CVY-2 to admit steam from the steam generators to the pump turbine. Upon initiation, emergency feedwater will flow from pump P7B to steam generator A through valves FW10A, CVX-3, Q-1, CV2670, and FW13A. Pump P7B will also feed steam generator B via valves FW10A, CVX-2, Q-3, CV2626, and FW13B. Similar discharge paths are provided for pump P7A. Flow to steam generator B is through valves FW10B, CVX-1, Q-4, CV2620, and FW13B. Flow to steam generator A is via valves FW10B, CVX-4, Q-2, CV2627, and FW13A.

Under normal operation all four of the flow paths described are open. If it is necessary to isolate one steam generator (see Section 3.3.3.5), the motor-operated valves in the appropriate paths will be closed. For example, steam generator A would be isolated by closing valves CVX-3, CV2670, CVX-4, and CV2627. Regulation of feedwater flow is normally accomplished by controlling the position of valves CVX-1, CVX-2, CVX-3, and CVX-4. Additional flexibility in directing feedwater flow can be achieved by operator control of valves CV2813 and CV2814. However, this has not been reflected in the analysis. Steam supply for the turbine-driven feedwater pump flows to a common header from steam generator A (via valves CV2666, CV2667, and 0-6) and steam generator B (through valves CV2617 and 0-5). From this point, flow is through parallel control valves, CVY-1 and CVY-2, and parallel regulating valves CVY-3 and CVY-4, which control steam flow and pressure. Pressure safety valves PSV6601 and PSV6602, downstream of CVY-3 and CVY-4, open if necessary to protect against pressure surges. A governor valve and an overspeed trip mechanism are included in the turbine housing.

Suction water supply to the feedwater pumps is normally provided from the condensate storage tank to a common suction header through valves CS19, CS98, and CS99. From this point, flow to pump P7B is through valve CV2800 and to pump P7A is through valve CV2802. An alternate suction source is provided for each pump. Water from Service Water Loop 1 can be provided to pump P7B through valves CV3850, SW11, and CV2803. Water can be supplied to pump P7A from Service Water Loop 2 through valves CV3851, SW13, and CV2806. Note that valve CV2800 is interlocked with CV2803 and that valve CV2802 is interlocked with CV2806 so that the service water system and the condensate storage tank cannot be directly connected to each other. The condensate transfer pumps and the unit 2 condensate storage tanks are also connected to the unit 1 CST through valve CV19. (No credit was given in the analysis for the use of the unit 2 condensate storage tank as an alternate water supply.)

A recirculation flow path of 15 gal/min is provided for pump P7B (through valve FW1056) and for pump P7A (through valve FW1055) to allow for pump cooling. In addition, a 78 gal/min recirculation flow path is provided through valves CV2815 and CV2816. These valves are interlocked with pump discharge valves CV2620, CV2626, CV2627, and CV2670 so that the 78 gal/min recirculation path is open whenever normal pump discharge flow is blocked.

4. Human Reliability and Procedural Analysis

4.1 Overview of the Human Reliability and Procedural Analysis Task

4.1.1 Purpose

An important aspect of any probabilistic risk assessment is the treatment of human action. Given the high degree of hardware reliability and redundant design associated with nuclear power plant systems, human interfaces with the system are often significant contributors to system unavailability. This may manifest itself in errors in the restoration of equipment to operability following test and maintenance activities or in errors in manipulating equipment in response to accident situations. On the other hand, operators may take actions to correct misalignments of equipment or to overcome failures under accident conditions. The purpose of this task is to identify potential human errors during or following test and maintenance activities, to identify potential human errors in response to accidents, and to quantify the most significant of these. In addition, analysis performed in this task serves to help identify and evaluate operator recovery actions under accident conditions.

4.1.2 Products

The products of the human reliability and procedural analysis task are as follows:

1. A list of potential test and maintenance restoration errors for each front-line and support system.
2. A list of potential significant human errors in response to each important accident sequence.
3. Upper bound failure probabilities for each identified human error.
4. Human reliability analysts' best estimate failure probabilities for all significant human errors.
5. Estimated probabilities for postulated operator recovery actions for the most frequent core melt accident sequences.

Examples of these products from previous IREP analyses are contained in Section 4.3.

4.1.3 Relationship to Other Tasks

The human reliability and procedural analysis task relies upon input from other tasks to specify the nature of the analysis. The analysts performing this work must work closely with those constructing the event tree and fault tree models and with those performing the accident sequence analysis.

The systems to be reviewed for potential human errors associated with test and maintenance activities are specified in the front-line and support system lists produced in the plant familiarization task. The test and maintenance procedures for each system are reviewed to give the analyst a thorough understanding of these activities and to identify potential human errors which could result in equipment being inoperable when called upon. The product of this review is a list of potential test and maintenance restoration errors for each system to be included in the fault trees produced in the plant systems analysis task.

The accident sequence delineation task identifies accident sequences to be analyzed. An important aspect of this analysis is a review of operator actions to be performed in response to each accident situation. The analysts performing the human reliability and procedural analysis must work closely with those performing the event tree analysis and receive from them the set of situations to be reviewed. For each, the emergency operating procedures are reviewed to identify potential human errors. These are then conveyed to the appropriate plant system analyst for incorporation into the appropriate fault trees.

Human actions quantified in this task are input to the accident sequence analysis task. There are three sets of products produced. First, upper bound failure probabilities are developed for each test and maintenance and accident response error. These values are used in the initial accident sequence evaluation to determine potentially significant accident sequences. Once the potential probabilistically significant accident sequences are identified, the accident sequence analyst provides the human reliability analyst with a list of sequences for closer scrutiny. The second set of products are best estimate probabilities for the human errors contained in these sequences for use in the final accident sequence analysis. In addition, potential operator recovery actions are examined for the potentially significant accident sequences. The human reliability analyst works with the sequence analysts to help identify potential recovery actions as part of the accident sequence analysis task. The list of potential recovery actions is evaluated to produce the third set of values used in the accident sequence analysis, the set of estimated probabilities of recovery actions. These relationships are summarized in Table 4.1-1 in which the input from other tasks is related to their use in this task, and the products are related to other tasks using the products.

Table 4.1-1. Human Reliability and Procedural Analysis Task Relationships

Inputs From Other Tasks	Use in This Task	Products	Other Tasks Using Products
1. Lists of front-line and support systems (plant familiarization task)	Identifies systems for which test and maintenance procedures should be reviewed	1. List of potential test and maintenance restoration errors for each front-line support system	Plant Systems Analysis–errors to be incorporated into front-line and support system fault trees
2. List of accident sequences to be reviewed (accident sequence delineation task)	Identifies sequences for which emergency procedures should be reviewed	2. List of potential significant human errors in response to each important accident sequence	Plant Systems Analysis–errors to be incorporated into appropriate front-line and support system fault trees
3. List of potentially important accident sequences following initial screening (accident sequence analysis task)	Identifies human errors requiring accurate probability estimates	3. Upper bound failure probabilities for each identified human error	Accident Sequence Analysis–data to be used in initial screening calculations
4. List of potential recovery actions for selected accident sequences (accident sequence analysis task)	Identifies recovery actions for which probability estimates are needed	4. Human reliability analysts' best estimate failure probabilities for all significant human errors	Accident Sequence Analysis–data to be used in final sequence calculations
		5. Estimate probabilities for recovery actions	Accident Sequence Analysis–data to be used in consideration of recovery for selected sequences

4.1.4 Information Needs

The human reliability and procedural analysts work closely with the other analysts of the program and receive information for several other tasks:

1. From the plant familiarization task, the list of front-line and support systems.
2. From the accident sequence delineation task, a list of sequences to be analyzed for human errors.
3. From the accident sequence analysis task, a list of accident sequences for which accurate human error probabilities are needed and a list of operator recovery actions to be quantified.

In addition to input from other tasks, considerable information is required pertinent to plant operation. These needs include test and maintenance procedures for each front-line and support system, a complete set of emergency operating procedures, and plant administrative procedures. In addition, familiarity with control room layout and, in some instances, quite specific information relating to control panel layout is needed. Documentation provides some of the needed information, but a visit to the control room and discussions with plant personnel are needed. Finally, accompanying methods documentation contained in Part III, Section 4, of this guide and in NUREG/CR-1278 [5] provide further guidance for the conduct of this task. How this information is used in the steps performed in this task is discussed in Section 4.2.

4.1.5 Scope

For the fault tree models, it is desirable to have as complete an identification of human errors as possible within certain constraints. For test and maintenance, each system should be thoroughly reviewed. For operators' errors in response to accidents, however, the postulation of errors should be limited to improperly performing actions called for in the emergency operating procedures. The analysis generally does not include accident diagnosis errors nor does it include postulating random errors of commission. Should a review of the operators' training, the plant's limits and precautions, or the control room layout lead the analyst to expect diagnostic errors or errors of commission, these should be included. It is expected, however, that few such errors will be included in the analysis.

The quantification of human errors is often a time-consuming task, and the number of available experienced human reliability analysts is limited. Therefore, it is desirable to initially develop only upper bounds for the human errors. The initial screening calculations done in the accident sequence analysis task will substantially reduce the number of accident sequences which require further scrutiny. Only for human errors contained in these sequences do improved estimates need to be obtained.

4.1.6 Assumptions and Guidelines

The review of emergency procedures for identification of human errors associated with accidents may appear to be a formidable task. However, such a review is greatly simplified by the fact that many accident sequences appear similar and that only a few steps involve actions which must be analyzed. One procedure frequently applies to many sequences.

The estimation of human error probabilities should follow the guidelines of NUREG/CR-1278 [5]. Test and maintenance restoration error probabilities can often be developed from a single model which reflects the plant's administrative practices associated with these activities. The estimation of human error probabilities associated with accident response, however, is sequence specific. Care must be taken to develop a model applicable for the particular situation in question.

4.2. Human Reliability and Procedural Analysis Procedures

The human reliability and procedural analysis task involves 17 steps. Figure 4.2-1 illustrates the interrelationships among the various steps of the human reliability and procedural analysis task. Note that some steps are independent of others in the task. Part III, Section 4, of this guide contains further methodological guidance.

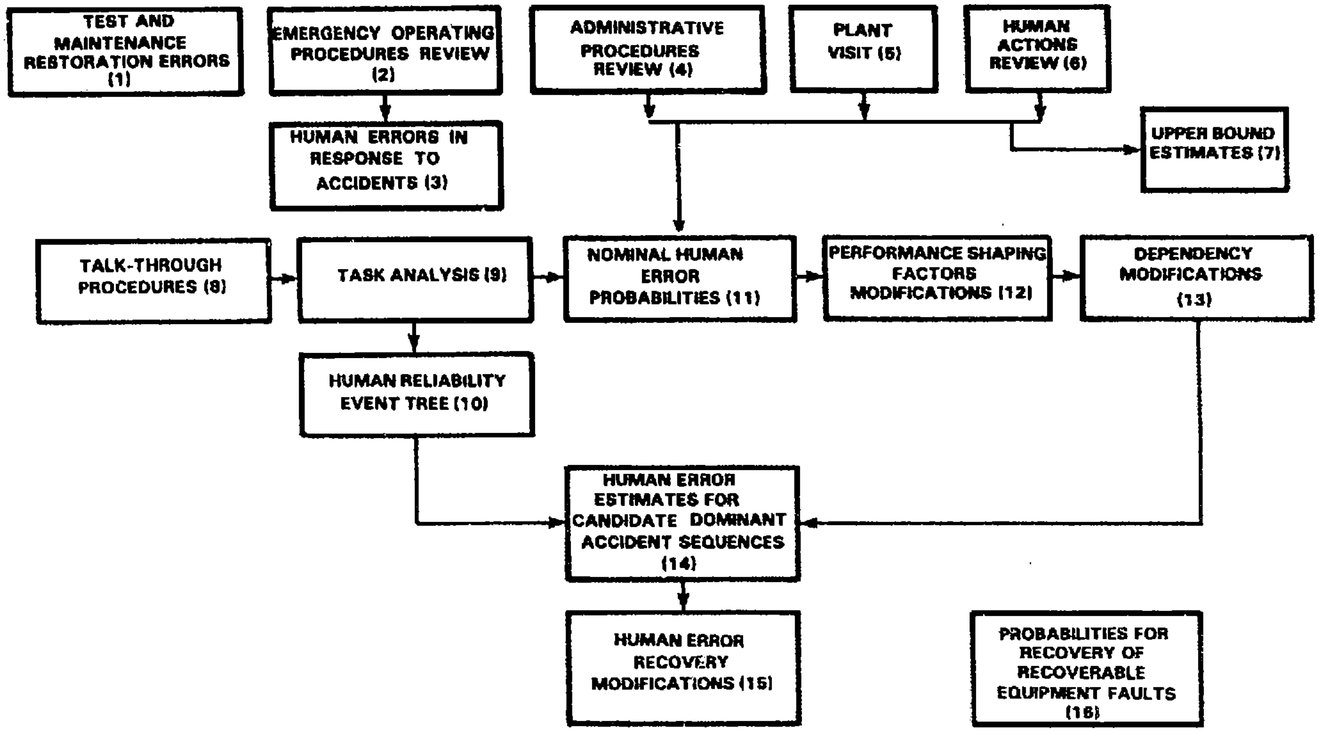

TEST AND MAINTENANCE RESTORATION ERRORS (1)
EMERGENCY OPERATING PROCEDURES REVIEW (2)
ADMINISTRATIVE PROCEDURES REVIEW (4)
PLANT VISIT (5)
HUMAN ACTIONS REVIEW (6)
HUMAN ERRORS IN RESPONSE TO ACCIDENTS (3)
UPPER BOUND ESTIMATES (7)
TALK-THROUGH PROCEDURES (8)
TASK ANALYSIS (9)
NOMINAL HUMAN ERROR PROBABILITIES (11)
PERFORMANCE SHAPING FACTORS MODIFICATIONS (12)
DEPENDENCY MODIFICATIONS (13)
HUMAN RELIABILITY EVENT TREE (10)
HUMAN ERROR ESTIMATES FOR CANDIDATE DOMINANT ACCIDENT SEQUENCES (14)
HUMAN ERROR RECOVERY MODIFICATIONS (15)
PROBABILITIES FOR RECOVERY OF RECOVERABLE EQUIPMENT FAULTS (16)

Figure 4.2-1. Step Relationships for the Human Reliability and Procedural Analysis Task

4.2.1 Description of Each Human Reliability and Procedural Analysis Procedural Step

This section contains a brief summary of the procedural steps for the human reliability and procedural analysis task. A more detailed discussion of selected steps is contained in Part III, Section 4. Substantial portions of this section and the section in Part III were taken directly from NUREG/CR-2254, SAND81-1655, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants" by B. J. Bell and A. D. Swain [12].

Identification of Potential Human Errors

Step 1. Review test and maintenance procedures for each front-line and support system. Identify all components moved from their accident response states or taken out of service. Postulate restoration errors for these components.

Description: Equipment is occasionally moved from its accident response position for testing and often removed from service for maintenance. If the equipment is not restored to its operable position following these activities, it could be unavailable to respond to accident situations. Such faults are included in the front-line and support system fault trees.

To identify these potential errors, the test and maintenance procedures should be reviewed to identify components removed from their accident response states. Particular attention should be given to identifying components closed to facilitate maintenance of another component, for example, the closing of manual valves on either side of a pump to perform pump maintenance. This information should be documented as part of the system description, Step 1 of the preceding task. Postulate restoration errors for each case and include them in the fault trees developed in the previous task.

Product: List of potential restoration errors following test and maintenance activities.

Step 2. Review the emergency operating procedures applicable to each accident sequence. List all human actions to be performed in response to the accident.

Description: The plant operators are often called upon to perform valve realignments or to actuate equipment in response to accident situations. Such actions are specified in the emergency operating procedures. The procedures associated with each accident sequence delineated in the event trees should be reviewed, and a list should be compiled of the operator actions to be performed for each sequence.

The investigation, at this point, is limited to those actions specified in the procedure. While it is recognized that the operator may perform other actions which could assist in recovery from the accident, these are not of interest at this time but will be treated subsequently. Similarly, the operator may perform unspecified incorrect actions which could degrade plant response to the accident. These are not considered other than postulating that actions specified in the procedure are incorrectly performed.

Product: List of accident response actions as defined in the procedures.

Step 3. Ascertain which human actions identified in Step 2 could degrade the availability of front-line and support system components if improperly performed. Postulate human errors for these actions.

Description: All actions in response to an accident may not necessarily adversely affect safe shutdown of the plant if improperly performed. For example, the procedures may call for radiological protective actions which, if not performed properly, may not influence whether or not the core melts. On the other hand, actions associated with the front-line systems called upon to mitigate the accident could well influence the ability to safely shut down the plant if improperly performed.

The analyst should review each action identified in the previous step to ascertain which ones are important in this regard. For these, human errors are postulated, and the faults are incorporated into the appropriate fault trees.

Product: List of potential significant human errors in response to accidents.

Information Acquisition and Upper Bound Probability Estimation

Step 4. Review administrative procedures to understand the plant's administrative control system.

Description: An important element in the estimation of human error probabilities is the administrative practices of the plant, particularly the tag out procedure for removing equipment from service and returning it to operability. The human reliability analyst should develop a general understanding of these practices. A more thorough understanding will be gained in subsequent steps.

Product: Basic understanding of plant's administrative controls.

Step 5. Visit the plant to gain familiarity with the control room, with the implementation of administrative controls, and to clarify questions raised in the procedural review.

Description: At least one plant visit specifically including a detailed survey of the control room should be made at the onset of a human reliability analysis.

In the initial visit to the plant, the human reliability analyst should make notes on relevant performance shaping factors, especially those dealing with the control room operations and the paperwork associated with change and restoration activities. General information about the plant's operating characteristics and a "feel" for the effectiveness of the plant's administrative control system are to be derived from this visit.

In surveying the control room, note specifics relating to the layout of controls and displays. Take copious notes on the characteristics of critical controls and displays, noting any factors that would influence their use—anything that would aid or hinder the operators in either locating, manipulating, or interpreting them. Deviations from good human factors engineering practices should be noted. Record any specifics relative to the operation of critical subsystems that have been pinpointed for observation by the systems analysts. If they have already identified any plant procedure that will be examined, use the time at this point to perform a talk-through of that procedure (see Step 8).

Product: Basic understanding of control room environment and improved understanding of plant's administrative controls.

Step 6. Review the context of performance of human actions identified in Step 3 to ensure factors important to evaluation of these actions learned from the plant visit are so noted.

Description: For a given scenario or sequence of events, the systems analysts pinpoint human actions that directly affect the system-critical components they have previously identified (see Step 3). In the light of the information obtained from the plant visit, the human reliability analyst must review these actions in the context of their actual performance to determine whether any factors exist that influence behavior on these system-critical actions that may have been overlooked by the systems analysts. For example, if performance of a different task affects performance of a system-critical action, this effect must be considered in the human reliability analysis even though the first task in itself is not important to the reliabilty of the system as defined by the systems analysts.

Product: Notes on insights gained from the plant visit pertinent to postulated human errors.

Step 7. Develop upper bound estimates of human errors identified in Steps 1 and 3 for use in initial screening calculations of accident sequence frequencies.

Description: The initial accident sequence analysis involves performing screening calculations to identify accident sequences for closer scrutiny. Upper bound estimates of human error probabilities suffice for these screening calculations. For those sequences surviving the screening process, termed "candidate dominant accident sequences," a better estimate is needed (see Steps 8-15).

Upper bound estimates are developed by reviewing the general human error probabilities contained in NUREG/CR-1278 [5] and modifying those, roughly, in light of the information gained from the previous steps. Precision is not important at this stage of the analysis. The human reliability analyst, however, should be certain that his estimates are truly upper bound estimates.

Product: Set of upper bound probability estimates for each identified human error.

Development of Best Estimate Human Error Probabilities

Step 8. Talk through the procedures associated with each action contributing to the candidate dominant accident sequences identified in the accident sequence analysis task with plant operating personnel to gain a full understanding of the performance of each task.

Description: For those human errors contributing to sequences which survive the initial screening calculations, it is important to develop best estimate human error probabilities. The first step in this process is to tal': through the procedures associated with each significant human action. In a talk-through of a set of procedu.:es for which safety-critical events have been identified, the human reliability analyst questions someone familiar with the performance of that procedure on specific points of the procedure until the analyst is so familiar with the tasks that he could perform them himself or at least be able to understand fully the performance of an operator. During the talk-through, the human reliability analyst must determine the performance shaping factors that influence behavior, such as the location and the physical and operating characteristics of specific controls, the type and location of alarms and annunciated indicators, control room manning and task allocation, and time requirements and limits for alarm indications and responses. The analyst must also determine the meaning of the specific instruction resulting from each command that is given in the set of procedures. The analyst must specify in language he can understand the exact interpretation the operators will make from the sometimes vague wording of plant procedures. At times, these interpretations are based on the operator's knowledge of system operation rather than on a standardized plant definition of the term in question. When this is the case, the human reliability analyst must ascertain whether all the operators define that term in the same way.

Product: Understanding necessary to analyze more closely the potentially significant human errors associated with the plant.

Step 9. Perform a task analysis of each task contributing to the candidate dominant accident sequences. This forms the basis for the development of human reliability event tree models.

Description: At this point, a formal breakdown of the procedure into tasks or smaller units of behavior should be done; that is, for each step in the procedure that was identified for analysis by the systems analysts, individual units of operator performance must be identified, along with other information germane to these performances. These individual units of performance constitute elements of behavior for which potential errors can be identified. In other words, a large task made up of a set of steps should be broken down in order that errors associated with each step might be identified.

Once the breakdown of task steps has been done, errors likely to be made must be identified for each step. The steps should be listed chronologically. Based on the characteristics of the actual performance situation, the human reliability analyst must determine which types of errors the operator is likely to make and which he is not.

Once the errors likely to be made on each unit of performance have been identified, the analyst must examine the situation for other factors that may influence performance. The entire performance scenario must be considered in this examination. The analyst is looking for elements taking place usually outside the scope of the procedures the operator is following that could influence his performance. For example, if something is to be done at the discretion of the shift supervisor, whether the supervisor remembers to order the task will have a definite effect on whether the operator performs the task. These factors extraneous to the procedure itself that affect the probability of human error often involve some sort of failure of the plant's administrative control system. The quality and the potential (during a particular performance sequence) for disruption of the plant's personnel communication system will also have to be examined in these cases.

Events other than human actions that, on occurring, affect subsequent performance must also be taken into account. If an operator's cue to initiate a task involves some signal from the equipment or an order from a supervisor, the probability of that signal being generated or that order being given must be considered.

Part III, Section 4.1, contains more guidance for conducting the task analysis.

Product: A listing of activities associated with each task pertinent to the candidate dominant accident sequences.

Step 10. Develop human reliability event trees for each task associated with the candidate dominant accident sequences.

Description: In making a probabilistic statement as to the likelihood of occurrence of human error events, each error defined as likely in the task analysis is entered as the right limb in a binary branch of a human reliability analysis (HRA) event tree. Chronologically, in the order of their potential occurrence, these binary branches form the limbs of the HRA event tree.

Development of the HRA event tree is the most critical part of the process for quantifying the probabilities of human errors. If the task analysis has listed the possible human error events in the order of their potential occurrence, the transference of this information onto the HRA event tree is made much easier. Each potential error and success are represented as binary branches on the tree, with subsequent errors and successes following directly from immediately preceding ones. Take care not to omit the incorporation of errors not found in the task analysis table that were determined to have a potential effect on the human error probabilities listed in the table. For example, errors of administrative control that affect a task's not being performed but that may not appear in the task analysis table must be included in the HRA event tree.

Part III, Section 4.2, contains more guidance for developing human reliability event trees.

Product: Event tree models for each potentially significant human error associated with the analysis.

Step 11. Assign nominal human error probabilities to each event on each human reliability event tree.

Description: Now that the errors have been identified, defined, and diagrammed, estimates of the probability of occurrence for each of them must be assigned. Chapter 20 of NUREG/CR-1278 [5] provides guidance for this activity, including data on basic human error rates. The source for the human error probabilities for each event should be recorded along with the assumptions made in their derivations.

Part III, Section 4.3, contains more guidance for assigning nominal human error probabilities.

Product: Initial estimates for each event on the human reliability event trees.

Step 12. Estimate the relative effects of performance shaping factors on the human error probabilities and modify them accordingly.

Description: A primary consideration in conducting a human reliability analysis is the variability of human performance. This variability occurs within any given individual in the performance of tasks across time (from day to day, from week to week, etc.). Variability is caused by performance shaping factors acting within the individual or on the environment in which the task is performed. Because of this variability, the reliability of human performance usually is not predicted solely as a point estimate but is determined to lie within a range of uncertainty. A point value human error probability for the analysis can be estimated by considering the effects of relevant performance shaping factors for the task in question. Estimates discussed so far in this document apply to nonstressful, normal working conditions. Modifications of these nominal estimates can be made on the basis of guidelines provided in NUREG/CR-1278 [5].

The nominal human error probabilities are to be used when the scenario outlined in the Handbook [5] (NUREG/CR-1278) reflects the situation being analyzed. If the plant situation is worse in terms of the performance shaping factors or the response requirements than the one described in the Handbook, the human error probability for that task should be higher than the nominal value. That is, if the analyst judges the situation under study to more likely result in error than the one outlined in the Handbook, a human error probability closer to the upper bound than the nominal value should be used. Likewise, if a plant's situation is judged to be less likely to result in a human error than the one outlined in the Handbook, a human error probability closer to the lower bound than the nominal should be used.

Product: Revised human error probabilities including performance-shaping factor effects.

Step 13. Assess the level of dependence among different tasks and incorporate this into the human error probability estimates.

Description: Dependence can occur between two performances with respect to errors of omission, errors of commission, or both. If dependence is assessed due to the fact that two actions are called for in the same procedural step, dependence is likely to affect human error probabilities for errors of omission. If components are to be manipulated at different times in a given procedure, the dependence is likely to affect the human error probabilities for errors of commission, especially for selection errors. In effect, the performance shaping factors referred to in the previous step may not only result in a general raising or lowering of estimated human error probability, they may also change the dependence among tasks. Part III, Section 4.4, discusses this subject in detail.

Product: Revised human error probabilities including dependence among tasks.

Step 14. Estimate the probability of each human error contributing to the candidate dominant accident sequences using the human reliability analysis event trees from Step 10 and event probability estimates from Step 13.

Description: Once the human error events have been identified and quantified individually, their contribution to the probabilities of system success and failure must be determined. All paths in an HRA event tree should be defined as contributing to system success or failure in terms of their possible system consequences, not in terms of the specific human errors leading to these consequences.

At this point in the human reliability analysis, the systems analysts should examine the HRA event tree for discrepancies between their understanding of the system and the human reliability analyst's representation of it.

Product: Human error probabilities for each event contributing to the candidate dominant accident sequences.

Recovery Considerations

The accident sequence analysis task uses the above-developed best estimate human error probabilities and other improved data to derive improved accident sequence frequency estimates. Potential recovery actions are assessed for all sequences which contribute significantly to the frequency of core melt.

Step 15. For human errors expected to contribute significantly to the core melt frequency, determine the effects of possible recovery actions and modify the human error probabilities appropriately.

Description: The incorporation of recovery factors should be done in stages, the purpose of this being to decrease the amount of time required for each human reliability analysis. If there are five recovery factors operating for a given scenario, the human reliability analyst may for example choose to model only two of them at first. If the inclusion of these factors sufficiently reduces the frequency of the given sequence such that it is no longer a significant contributor to the frequency of core melt, no more work needs to be done at this time. If this scenario still shows up as one of the potentially dominant sequences, the other three recovery factors should be analyzed.

Some recovery factors are highly situation-specific, while others can be applied generically. Alerting cues for recovery actions for any given transient will always depend on the specifics of the response requirements for that transient. However, when analyzing recovery factors operating after maintenance activities, it will sometimes be possible to generate generic HRA event trees that can be applied without modification to every such case for that plant. This is possible because in many plants a single procedure dictates the steps to be followed in restoring components following maintenance. In either case, the recovery factor can take the form of a point value (a human error probability) or of a separate HRA event tree. The point value or the total success probability of the recovery HRA event tree should be inserted on the associated error limb of the main HRA event tree. The probability of error for that limb is then multiplied by the failure probability for the recovery factor to obtain the probability of an unrecovered error.

Product: Revised human error probabilities for significant human errors.

Step 16. For recovery actions associated with recoverable nonhuman-error related events (component failures, etc.) identified in the accident sequence analysis task, estimate the probability of properly performing each action.

Description: Many faults which are not related to human errors may, in fact, be recoverable. The most significant of these are determined in Steps 15 and 16 of the accident sequence analysis task. Estimation of recovery probabilities is, at this time, not an advanced art. The model used in past IREP studies first determined whether faults were recoverable or not, then how much time was available to perform recovery actions. For those faults deemed recoverable, the action required and the location of the action were ascertained. The model which was used assigned a probability of recovery for all recoverable actions based on the time available and whether the actions could be performed in the control room or locally.

This model should be reviewed for the plant under question. Improvements in the art should be taken advantage of as well. In particular, consideration should be given to the length of time needed to diagnose the situation, to perform local actions, and the effect these factors have on the probability of recovery. These estimates are then used in the final sequence frequency quantification.

Product: Estimates of recovery probability for recoverable faults associated with the candidate dominant accident sequence.

Task Products

Step 17. Summarize task products for the task report.

Description: The products of the human reliability and procedural analysis task are listed below. Test and maintenance errors were identified in Step 1. Significant accident response errors were identified in Step 3. Upper bound and best estimate human error probabilities were developed in Steps 7 and 14, respectively. Recovery estimates were developed in Steps 15 and 16.

Products:

1. List of potential test and maintenance restoration errors for each front-line and support system.
2. List of potential significant human errors in response to each accident sequence.
3. Upper bound failure probabilities for each identified human error.
4. Human reliability analysts' best estimate failure probabilities for each human error contributing to the candidate dominant accident sequence.
5. Revised human error probabilities, including recovery actions.
6. Estimated probabilities for recovery of all recoverable faults.

4.3 Human Reliability and Procedural Analysis Documentation and Example Products

The human reliability and procedural analysis task identifies potential human errors to be included in the analysis, provides probability estimates for these errors, and assists in the inclusion of operator recovery actions in the analysis. This task supports the plant systems analysis and accident sequence analysis tasks. This section suggests documentation of this task. This information comprises parts of the second interim and the second informal reports.

4.3.1 Review of Procedures and Initial Probability Estimates

The initial steps of this task involve review of the test and maintenance procedures to identify potential restoration errors and review of the emergency procedures to identify potential accident response errors. The results of the test and maintenance procedure review may be documented in the test and maintenance summary sheets of each system description (see Part II, Section 3.3). These sheets summarize components removed from their operable state for test and maintenance activities. Each has a possible restoration error.

The review of emergency procedures should be described. This should discuss the relation of particular procedures to particular accident sequences, and it should summarize those steps of the procedure which, if improperly performed, would degrade plant response to the accident. The components affected should be specified as well as the actions to be performed. An example summary discussion from the Arkansas Nuclear One IREP [8] may be found in the following section.

Initial screening calculations generally use upper bound estimates for human error probabilities. The values chosen for each class of human error—those associated with test and maintenance restoration and those associated with accident responses—should be specified, and supporting rationale should be provided.

4.3.1.1 Example Summary of a Review of Emergency Procedures

If a break in the reactor coolant system occurs, various alarms and indications in the control room will notify the operator that a LOCA is occurring. In response to a large LOCA, the operator is expected to follow the LOCA emergency procedures to bring the plant to a safe shutdown condition. These procedures outline the appropriate operator actions which must be performed during the accident (e.g., monitor ECCS pump flow rates, change the position of certain valves, etc.). If certain critical procedural steps are either omitted or not performed correctly (i.e., errors of omission and commission), the reliability of the front-line and support systems responding to the LOCA may be degraded. It is important, then, to identify these critical procedural steps so that potential operator errors associated with performing them can be assessed and included in the fault tree models for the systems responding to the LOCA.

In response to a LOCA which is $\gtrsim 0.01$ ft^2, the main procedures the operator would follow are:

1202.06 Section 1..Loss of Coolant/RC Pressure–Rupture Greater Than HPI Capacity

1202.06 Section 2..Loss of Coolant/RC Pressure–Rupture Within HPI Capacity

Referring to the LOCA emergency core cooling success criteria (Table 1.3-7), it can be deduced that Section 1 is implemented following LOCAs greater than 10 inches in diameter, Section 2 is implemented following LOCAs less than 4 inches in diameter, and both sections are implemented following LOCAs of between 4 inches and 10 inches in diameter.

In response to a LOCA which is ≤ 0.01 ft^2, the main procedures the operator would follow are:

1202.06	Section 2..Loss of Coolant/RC Pressure-Rupture Within HPI Capacity
1102.10	Plant Shutdown and Cooldown
1104.04	Section 6..Decay Heat Removal Cooldown
1103.11	Draining and N_2 Blanketing of the Reactor Coolant System

Procedure 1202.06, Section 2, would be implemented during all accident sequences represented on the B(1.2) event tree corresponding to LOCAs of diameter less than 1.2 in. Procedures 1102.10, 1104.04, and 1103.11 would only be implemented during B(1.2) accident sequences involving operation of the DHRS.

The LOCA procedures were reviewed by thc event tree analysis team and plant personnel in order to identify critical procedure steps. For a step to be identified as critical, it must have the potential for degrading the reliability of the front-line and support systems responding to the LOCA if the step is omitted or incorrectly performed.

Those steps identified to be potentially critical are summarized in Table 4.3-1 It can be noted that certain potentially critical operator actions are not described by a step in the LOCA procedures. These operator actions were discovered through discussion with plant personnel. Operator errors of omission and commission, which are appropriate to the performance of these steps, were assessed and incorporated into systemic fault tree models.

4.3.2 Human Reliability Models

Following initial screening calculations, certain sequences are selected for closer scrutiny. For human error events in these sequences, best estimate probability estimates are derived. Each human error event chosen for closer scrutiny should be discussed. For each, describe the action to be performed in the context of the applicable accident sequence. This discussion should not only describe the event, but it should also detail the information available to the operator, the appropriate performance shaping factors, level of dependence, and other information pertinent to the model. The discussion should culminate in the development of the human reliability event tree and its quantification.

Some events will contribute to dominant accident sequences and recovery considerations will be a part of the analysis. For these events, include a discussion of recovery and its influence on the estimation of the event probability.

4.3.3 Recovery of Component Failures

Selected component failures in the dominant accident sequences may be recovered by judicious operator action. The human reliability analyst and systems analysts develop a recovery model for these events as part of this task. This model should be documented and discussed in terms of the criteria for recoverability, the estimation of the time to perform the act, and the estimated recovery probability.

5. Data Base Development

5.1. Overview of the Data Base Development Task

5.1.1 Purpose

To quantify the frequency of each accident sequence, failure rate data is required for each basic event in the fault trees. Some of these events are human errors; the quantification of these was described in the previous task. The vast majority of events, however, consists of failures of components and unavailabilities due to testing and maintenance outages. Each component, in turn, may fail in several ways. The purpose of the data base development task is to develop generic data and, where appropriate, plant specific data for each mode of failure and for the testing and maintenance unavailabilities for all components in the front-line and support system fault trees.

5.1.2 Products

The products of the data base development task are as follows:

1. A table of generic component failure rate data for each event in the fault trees.
2. A table of plant specific test and maintenance unavailabilities for each system/component.
3. A list of initiating event frequencies for each initiating event group.
4. Plant specific component failure rate data for selected components.

Examples of these products from previous IREP analyses are contained in Section 5.3.

5.1.3 Relationship to Other Tasks

The generic data base for use in IREP analyses is provided in Part III, Section 5, of this guide. However, the data base should be reviewed to ascertain whether

Table 4.3-1. LOCA Emergency Procedures "Critical Steps"

Procedure	Applicable LOCA Size*	Potentially Critical Step (s)	System Affected Which Must Respond to LOCA	How System Could Be Affected

1202.06 Rev. 8
Section 1
"Leakage greater than HPI capacity"
	B(>13.5)
	B(13.5)
	B(13.5)
	B(10)
		3.1	LPIS	Flow must be throttled to prevent pump cavitation.

			RBSI	Flow must be throttled to prevent pump cavitation.
		3.3	LPRS	Suction switchover from BWST to sump to prevent pump burnout.
			RBSR	Suction switchover from BWST to sump to prevent pump burnout

1202.6 Rev. 8
Section 2
"Rupture within HPI Capacity
	B(10)
	B(4)
	B(1.66)
		3.2
		or
		3.4
			HPIS	Pumps could be shut off if margin to saturation criteria is not properly followed.

1202.6 Rev. 8 Section 2 "Rupture within HPI capacity"	B(1.2)	2.5-Start standby HPI pump and realign operating HPI pump from MU tank to BWST	HPIS	For these size LOCAs makeup tank would most likely empty before HPIS receives an ES auto start signal. Failure to realign from makeup tank to BWST would to cause pump failure. Operator must also manually start the standby HPI pump since an ES signal may not be received.
1202.6 Rev. 8 Section 2 "Rupture within HPI capacity"	B(1.66)	3.3.1 or 3.3.2	EFS/PCS	Loss of RCP cooling. RCPs would fail causing loss of forced circulation to steam generators.
		3.3.3	EFS/PCS	Loss of service water cooling of ICW could cause loss of instrument air (fails PCS) and/or loss of RCP cooling.

1202.06 Rev. 8
Section 2
"Rupture within HPI capacity"
	B(1.66)
	B(4)
		3.7	HPRS/LPRS	Suction switchover from BWST to LPRS discharge to prevent pump burnout. Open pump crosstie valves to enhance HPRS supply line redundancy.

1202.06 Rev. 8
Section 2
"Rupture within HPI capacity"
	B(1.66)
	B(4)
		3.9	HPRS/LPRS	Low pressure pumps suction switchover from BWST to sump to prevent pump burnout.

			RBSR	Spray pumps suction switchover from BWST to sump to prevent pump burnout.
	B(1.66)	5.6.1.2	EFS/PCS	Upon ES signal RCPs are tripped (see step 2.4). To establish forced circulation, operator must bump pumps.
None	All breaks	Discussions with shift supervisor indicate that reactor building sprays would be turned off and on (after initial auto start) to control building pressure as required	RBSI/RBSR	Operator could fail to manually actuate spray pumps when required

*The notation indicates maximum diameter size. For example, B(13.5) corresponds to LOCAs of 10-13.5 inches in diameter. Refer to Table 1.3-7 for corresponding break size ranges.

Adapted from Reference [8]

all of the needed data is contained in the list. In addition, the fault tree analysts may provide the data base developer with a list of further data needs.

The generic data base, however, must be supplemented by plant specific data in some instances. Test and maintenance frequencies generally differ from plant to plant. This information is needed for each of the systems/components contained in the front-line and support systems lists provided by the plant familiarization task.

In addition to component failure rate data and test and maintenance frequencies, the data analyst provides an estimate of initiating event frequencies. A frequency is needed for each initiating event group identified in the plant familiarization task.

The generic data base supplemented by plant specific test and maintenance frequencies and by the few peculiar data needs missing from the original list provide guidance to the fault tree analyst regarding the appropriate level of detail. This data base and the list of initiating event frequencies form the basis for the quantification of accident sequence frequencies.

Once the initial sequence calculations are performed, a set of potentially significant accident sequences is identified by the accident sequence analysis task. Data associated with these sequences should be checked more carefully to ensure it applies to the particular plant. It may be that some data for the events in these sequences differs substantially from the generic data. If so, it is important to replace the generic data with plant specific data to obtain a more realistic estimate of accident sequence frequencies for the final sequence quantification.

These relationships are summarized in Table 5.1-1. Input from other tasks is listed along with the corresponding use of this information in this task. Task products are also listed along with the corresponding tasks using each product.

Table 5.1-1. Data Base Development Task Relationships

Inputs from Other Tasks	Uses in This Task	Products	Other Tasks Using Products
1. List of front-line and support systems (plant familiarization task)	Identifies systems and components for which test and maintenance frequencies are needed	1. Generic failure rate data for all component failures	Accident Sequence Analysis–used in initial sequence quantification Plant Systems Analysis-provides guidance as to appropriate level of detail
2. List of initiating events grouped according to common mitigating requirements (plant familiarization task)	Identifies initiating events and groups for which frequencies are needed	2. Plant specific test and maintanance unavailabilities for each system/component	Accident Sequence Analysis–used to quantify accident sequence frequencies
3. List of component failure rate data needs, if any, not contained in generic data base (plant systems analysis task)	Identifies further data needs for the particular plant analysis	3. Initiating event frequencies for each initiating event group	Accident Sequence Analysis–used to quantify accident sequence frequencies
4. List of potential dominant sequences (accident sequence analysis task)	Identifies component data requiring closer scrutiny	4. Plant-specific component failure rates for selected components	Accident Sequence Analysis–used in quantification of frequency of dominant accident sequences

5.1.4 Information Needs

The data base developer requires some input from other tasks:

1. From the plant familiarization task, the lists of front-line and support systems and the list of initiating events grouped according to common mitigating requirements.
2. From the plant systems analysis task, an identification of any deficiencies in the generic data base.
3. From the accident sequence analysis task, a list of potentially significant accident sequences providing a set of data for closer scrutiny.

This input must be supplemented by a substantial amount of information. The generic data base is provided in this guide (see Part III, Section 5). Generic and, in some cases, plant specific initiating event data is contained in EPRI NP-2230 [2]. To supplement this data and to ascertain plant-specific anomalies, the data base developer should obtain all licensee event reports for the facility. To the extent practicable, plant maintenance and control room logs should be reviewed to reveal any components with particular high outages. Test intervals may be obtained from a review of the plant's technical specifications. Plant logs are needed to ascertain maintenance frequencies and durations. How this information is used in the steps performed in this task is discussed in Section 5.2.

5.1.5. Scope

The collection of plant-specific data is a time-consuming task. This should be limited to obtaining test and maintenance frequencies and durations, and to a brief review of logs or discussions with plant personnel to ascertain abnormally failure-prone or unusually reliable components. A more detailed search should be limited to those components contributing to potentially dominant accident sequences.

5.1.6 Assumptions and Guidelines

The data base developed should contain mean values, medians, and error factors. Generally a lognormal failure rate is assumed. Mean values should be provided for use in point estimate accident sequence frequency calculations. Median values and error factors are required for propagation of uncertainties.

5.2 Data Base Development Procedures

The data base development task involves 13 steps. Figure 5.2-1 illustrates the interrelationships among the various steps of the data base development task. Note that some steps are independent of others in this task. Part III, Section 5, of this guide contains further guidance.

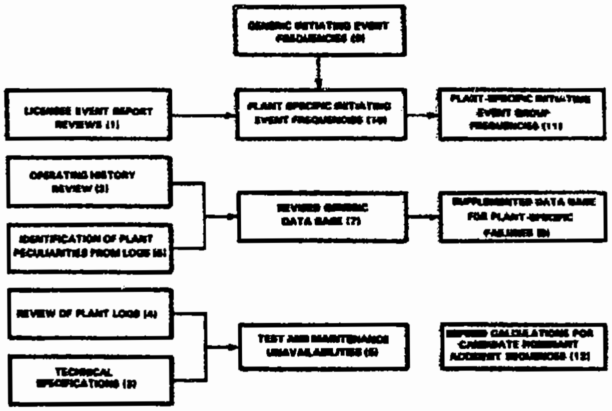

GENERIC INITIATING EVENT FREQUENCIES (9)
LICENSEE EVENT REPORT REVIEWS (1)
PLANT SPECIFIC INITIATING EVENT FREQUENCIES (10)
PLANT-SPECIFIC INITIATING EVENT GROUP FREQUENCIES (11)
OPERATING HISTORY REVIEW (2)
IDENTIFICATION OF PLANT PECULIARITIES FROM LOGS (5)
REVISED GENERIC DATA BASE (7)
SUPPLEMENTED DATA BASE FOR PLANT-SPECIFIC FAILURES (8)
REVIEW OF PLANT LOGS (4)
TECHNICAL SPECIFICATIONS (3)
TEST AND MAINTENANCE UNAVAILABILITIES (6)
REFINED CALCULATIONS FOR CANDIDATE DOMINANT ACCIDENT SEQUENCES (12)

Figure 5.2-1. Step Relationships for the Data Base Development Task

5.2.1 Description of Each Data Base Development Procedural Step

<u>Operating History</u>

Step 1. Review licensee event reports for the facility and note any peculiar problems associated with plant operation.

<u>Description:</u> A generic data base for use in IREP analyses is presented in Part III, Section 5, of this guide. Each plant is different, however, and it is important to identify areas where the plant's operating history is at variance with the generic data base. The first source of information which should be reviewed in this regard are the licensee event reports.

Product: List of plant-specific occurrences which may raise questions regarding the applicability of generic data.

Step 2. Discuss plant operating history with knowledgeable plant personnel to ascertain peculiar operational problems.

Description: A further source of information regarding plant peculiarities is the experience of the plant operators. Often they can point the analyst to particularly troublesome equipment or can supplement data in licensee event reports based on their responses to the incidents.

Product: Further list of plant-specific occurrences which may raise questions regarding the applicability of generic data.

Test and Maintenance Data

Step 3. Review plant technical specifications for each front-line and support system to ascertain test intervals for each system.

Description: Calculations of system unavailability due to outage for testing requires knowledge of the frequency of testing. This, of course, is the reciprocal of the test interval. Testing intervals are specified in the plant's technical specifications. These should be reviewed to determine the test interval for each front-line and support system identified in the plant familiarization task.

Product: Test frequencies for each front-line and support system.

Step 4. Review plant logs and conduct discussions with plant personnel to determine test durations, maintenance frequencies, and maintenance durations for each front-line and support system/component.

Description: The calculation of test and maintenance unavailabilities also requires knowledge of the test duration and maintenance frequencies and durations. The data will vary from system to system and component to component. Plant logs contain much of this information. This should be supplemented by information gained from discussions with plant personnel. Often, data on individual components is grouped to obtain data on component types due to the scarcity of data for a particular component. This is done, for example, for pumps and valves of given type. Such a procedure is certainly acceptable.

Product: Test durations, maintenance frequencies, and durations for each front-line and support system/component.

Step 5. Calculate test and maintenance unavailabilities for each system/component and estimate the error factors associated with each.

Description: Using test and maintenance frequencies and durations, calculate the unavailability of each front-line and support system/component using the formulas contained in Part III, Section 5.3, of this guide.

Product: Plant specific test and maintenance unavailability data.

Generic Data Base Modifications

Step 6. From the review of plant logs performed in Step 4, add to the list of plant pecularities from Step 2 any components for which the maintenance frequency is abnormally high.

Description: Components which have high maintenance frequencies not only suffer large maintenance unavailabilities, but also have high failure rates. Add these components to the list of components for which generic failure rates may not be appropriate.

Product: More complete list of plant peculiarities.

Step 7. For the components for which the generic data base does not seem appropriate, calculate new failure rates and modify the generic data base.

Description: Using data collected from the review of licensee event reports, plant logs, and discussions with plant personnel, calculate failure rates for each component listed in Steps 1, 2, and 6. Guidance and formulas for performing these calculations are contained in Part III, Section 5.2, of this guide. Modify the generic data base with these plant-specific failure rates.

Product: Modified generic data base.

Step 8. For those component failure rates not included in the generic data base, as identified by the plant systems analysts, develop estimates for their failure probability and associated error factors.

Description: The plant systems analysts may identify components or failure modes for which failure rate data is not contained in the generic data base. A list of such data needs is a product of the plant systems

analysis task. In the same manner as other failure rates are obtained, calculate failure rates for these components or component failure modes. For questionable failure rates, use conservative values.

Product: Supplements to the data base to make it complete for this analysis.

Initiating Event Frequencies

Step 9. For each initiating event identified in the plant familiarization task as applicable to the plant, list the generic frequency given in EPRI NP-2230 [3].

Description: Accident sequence frequency estimates require frequencies of the initiating event in addition to system unavailabilities. The plant familiarization task has identified the initiating events applicable to this analysis and has grouped them according to common mitigating system response. The first step in developing initiating event frequencies is to simply compile the generic frequencies for each applicable initiating event given in EPRI NP-2230 [3].

In some cases, such as for support systems related initiating events, the generic initiating event data base may not contain the event. For these cases data may be contained in the generic hardware data or the analyst may need to develop plant-specific data from plant information.

Product: List of initiating events applicable to the plant and the associated generic frequency.

Step 10. From EPRI NP-2230, licensee event reports, or other data sources, note where plant-specific initiating event frequencies differ substantially from those in Step 9. Modify the initiating event frequencies accordingly.

Description: Initiating event frequencies vary from plant to plant. For those which differ substantially from the generic frequencies, plant-specific frequencies should be used. EPRI NP-2230 contains this information for some plants. For others, this must be obtained directly from the operating history by counting the incidence of the initiating event and dividing by the number of years the plant has operated.

Product: List of initiating event frequencies consistent with plant experience.

Step 11. From the data prepared in Step 10, calculate the frequency of each initiating event group identified in the plant familiarization task and estimate the associated error factors.

Description: Event trees are constructed for each initiating event group. Thus accident sequence calculations begin with the frequency of each group rather than individual initiating events. The frequency of the initiating event group is simply the sum of the frequencies of the events in the group. Information regarding error factors for initiating events may be found in Reference [13].

Product: Plant-specific data for the frequency of each initiating event group.

Data Refinement

Step 12. For each event in the set of candidate dominant accident sequences identified in the accident sequence analysis task, reexamine the data used to ensure it is consistent with data developed in the previous steps. For selected components, develop plant-specific data consistent with plant operating experience.

Description: Initial calculations of accident sequence frequencies performed in the accident sequence analysis task result in a selection of sequences for closer scrutiny. These are termed "candidate dominant accident sequences." Data for all events appearing in the candidate sequences should be reviewed to ensure it reflects the analyst's best estimate failure probability based on his review of the plant's history and data developed in the previous steps. Any component failure contributing greatly to core melt should be given particular attention. Modifications to the data used in initial screening calculations should be given to the sequence analyst for use in the final sequence frequency calculations.

Product: Refined data, as needed, for use in final sequence quantification.

Task Products

Step 13. Summarize task products for the task report.

Description: The products of this task are listed below. Generic failure rate data is given in Part III, Section 5. Plant-specific test and maintenance unavailabilities were derived in Step 5. Initiating event group frequencies were produced in Step 11. A modified generic data base reflecting plant-specific variations and additional failure modes synthesizes the products of Steps 7, 8, and 12.

Products:

1. Generic failure rate data for all component failures.
2. Plant-specific test and maintenance unavailabilities for each system/component.
3. Initiating event frequencies for each initiating event group.
4. Supplemented and modified generic data base and plant-specific component failure rates for selected components.

5.3 Data Base Development Documentation and Example Products

The data base development task produces component failure rate and initiating event frequency data in support of the plant systems analysis and accident sequence analysis tasks. This section suggests documentation of this task. This information constitutes part of the second interim report and the second informal report.

5.3.1 Component Failure Rate Data

The final set of data compiled for the accident sequence analysis task should be presented. This set should include component failure rates and test and maintenance unavailabilities for each front-line and support system component. The table should include means, medians, and error factors. Deviations from the generic data base should be noted and discussed in the accompanying text. The text should also summarize any pertinent events which have occurred at the plant. The table should be similar in form to the generic data base found in Part III, Section 5.

This information also appears in other task reports. Test and maintenance frequencies are included in the test a d maintenance summaries for each system description (see Section 3.3). Component failure rates are also entered on the fault summary sheets accompanying each fault tree (see Section 6.3).

5.3.2 Initiating Event Frequencies

Another product of this task used in the quantification of accident sequence frequencies is the set of the initiating event frequencies. The compiled frequencies of each initiating event group should be presented. Means, medians, and error factors for each event should be included. Each entry developed from information other than that of EPRI NP-2230 should be so noted and discussed in the accompanying text. The text should also discuss any pertinent initiating events from the plant's history. The table of initiating events from the Arkansas Nuclear One IREP [8] is shown in Table 5.3-1. This table presents median values only and does not include means and error factors.

Table 5.3-1. Initiating Events Used in the ANO-1 Analysis

Designator	Initiating Event Description	Frequency Per Reactor Year
B(1.2)	LOCA with a 0.38 to 1.2 in. equivalent diameter break	$2.0x10^{-2}$
B(1.66)	LOCA with a 1.2 to 1.66 in. equivalent diameter break	$3.1x10^{-4}$
B(4)	LOCA with a 1.66to 4 in. equivalent diameter break	$3.8x10^{-4}$
B(10)	LOCA with a 4 to 10 in. equivalent diameter break	$1.6x10^{-4}$
B(13.5)	LOCA with a 10 to 13.5 in. equivalent diameter break	$1.2x10^{-5}$
B(>13.5)	LOCA with an equivalent diameter break >13.5 in.	$7.5x10^{-6}$
T(LOP)	Loss of offsite power transient	$3.2x10^{-1}$
T(PCS)	Transient initiated by a total interruption of main feedwater	1.0
T(FIA)	All other transients which do not affect front-line systems significantly	7.1
T(A3)	Transient initiated by a failure of ac power bus A3	$3.5x10^{-2}$
T(B5)	Transient initiated by a failure of ac power bus B5	$3.5x10^{-2}$
T(D01)	Transient initiated by a failure of dc power bus D01	$1.8x10^{-2}$
T(D02)	Transient initiated by a failure of dc power bus D02	$1.8x10^{-2}$
T(LOSW)	Transient initiated by failure of Service Water Valve CV-3824	$2.6x10^{-3}$

6. Accident Sequence Analysis

6.1 Overview of the Accident Sequence Analysis Task

6.1.1 Purpose

The previous tasks have involved the development of models representing plant systems and accident sequences which lead to core melt. To quantify these models, data was developed for each fault tree event. The accident sequence analysis task integrates these portions of the analysis to calculate the frequency of each core melt accident sequence. The purpose of this task is to identify the dominant accident sequences for the plant, that is, those core melt sequences expected to have the highest frequency. This is done by analyzing the accident sequences defined by the event trees using the fault trees for each front-line and support system and the human reliability, test and maintenance, and component failure rate data.

6.1.2 Products

The products of the accident sequence analysis task are as follows:

1. Fault tree models for each front-line system including all support system faults.
2. Estimated frequencies for each core melt accident sequence.
3. A list of accident sequences for closer scrutiny and consideration of operator recovery actions (these are termed "candidate dominant accident sequences").
4. A qualitative expression, including recovery, containing the most significant contributors to each potentially dominant accident sequence.
5. A table of dominant accident sequences and their frequencies.

Examples of these products from previous IREP analyses are contained in Section 6.3.

6.1.3 Relationship to Other Tasks

The accident sequence analysis task consists of integrating the information developed in the preceding tasks to calculate core melt accident sequence frequencies and qualitative expressions of the failures contributing most significantly to each sequence. The event trees developed in the accident sequence delineation task define the combinations of initiating events and success/failure states of responding systems to be analyzed. The front-line and support system models developed in the plant systems analysis task, when merged, constitute the system models to be used in the sequence analysis. Given these two inputs, qualitative expressions of the combinations of component failures, human errors, test and maintenance unavailabilities, and restoration errors which result in each core melt accident sequence are developed.

The quantification of accident sequence frequencies generally takes place in at least two stages. In order to calculate initial sequence frequencies, the first stage, termed the initial screening calculation, uses:

1. Upper bound failure probabilities from the human reliability and procedural analysis task.
2. Initiating event frequencies, generic component failure rates, and plant-specific test and maintenance frequencies and durations from the data base development task.

This list of sequences and sequence frequencies is used in the subsequent task—interpretation and analysis of results—for sensitivity analyses.

Following initial calculations of sequence frequencies, a group of the most frequent accident sequences is chosen for closer scrutiny and consideration of operator recovery actions. This list of sequences and their qualitative expressions of failure are used by the human reliability analysts to determine those human errors for which best estimate failure probabilities are to be calculated and by the data base analyst to identify component failures which should be checked for accuracy in light of plant-specific information. This set of sequences is also used in the next task for performing sensitivity calculations.

A final calculation of accident sequence frequencies is performed for the candidate dominant accident sequences using the improved human error estimates and recovery probabilities provided by the human reliability and procedural analysis task and including any changes made in the data base. The most frequent sequences are termed "dominant accident sequences." The expressions of failure combinations and the estimated sequence frequencies form the basis for the interpretation and analysis of results task in which engineering insights regarding the most significant plant features are developed and in which uncertainty, sensitivity, and importance calculations are performed.

Table 6.1-1 summarizes the relationship of the accident sequence analysis task to the others in terms of the relation of input from other tasks to this task and the relation of products of this task to other tasks.

Table 6.1-1. Accident Sequence Analysis Task Relationships

Inputs From Other Tasks	Uses in This Task	Products	Other Tasks Using Products
1. Systemic event trees for each LOCA and transient initiating event group (accident sequence delineation task)	Defines accident sequences–initiating event and system success/failure combinations—to be analyzed	1. Fault tree model for each front-line system including all support system faults	
2. Fault trees for each front-line and support system (plant systems analysis task)	Provides fault trees to be merged; merged models used in sequence analysis, combined according to event tree structure	2. Estimated frequencies for each core melt accident sequence	Analysis and Interpretation of Results–used in sensitivity analysis
3. Upper bound failure probabilities for each identified human error (human reliability and procedural analysis task)	Used in initial screening calculations of accident sequence frequencies	3. List of candidate dominant accident sequences for closer scrutiny and recovery considerations; qualitative expression of significant contributions for each sequence	Data Base Development–identifies component failure rate data requiring closer scrutiny Human Reliability and Procedure Analysis–identifies human errors for which best estimate failure probabilities are to be calculated and recovery actions for which probability estimates are needed Analysis and Interpretation of Results–used in sensitivity analysis
4. Generic failure rate data for each component failure in merged fault trees (data base development task)	Used in initial screening calculations of accident sequence frequencies		
5. Plant-specific test and maintenance frequencies and durations for each system/component (data base development task)	Used in calculation test and maintenance contributors to accidents sequence frequencies	4. Table of dominant accident sequences and their frequencies; qualitative expressions of significant contributors to each	Analysis and Interpretation Results–basis for development of engineering insights, uncertainty, sensitivity, and importance calculations
6. Initiating event frequencies for each initiating event group (data base development task)	Used in quantification of accident sequence frequencies		
7. Best estimate failure probabilities for human errors in candidate dominant accident sequences (human reliability and procedural analysis task)	Used in final quantification of accident sequences frequencies		
8. Plant-specific component failure rates for selected components (data base development task)	Used in final quantification of accident sequence frequencies		
9. Estimated probabilities for recovery actions (human reliability and procedural analysis task)	Used in recovery considerations for final quantification of accident sequence frequencies		

6.1.4 Information Needs

The accident sequence analysts require the systemic event trees from the accident sequence delineation task and the fault trees for each front-line and support system from the plant systems analysis task. A variety of data pertaining to human error rates, recovery probabilities, initiating event frequencies, component failure rates, and test and maintenance restoration error probabilities are provided by the human reliability and procedural analysis and data base development tasks. These are listed on Table 6.1-1.

Part III, Section 6, of this guide provides substantial guidance for dealing with the complexities of this task. A computer code for dealing with large Boolean equations is essential. If thorough familiarity with the code is not already possessed by someone on the analysis team, code documentation would be necessary. In considering possible recovery actions, detailed information regarding information available to the operator and possible actions which can be taken from the control room are needed. Analyses of the time to irreparable damage to components, to dryout of the steam generators, and to the onset of core uncovery are also needed for selected accident sequences. How this information is used in the steps performed in this task is discussed in Section 6.2 below.

6.1.5 Scope

Core melt accident sequence frequencies should initially be calculated for all sequences using the generic data base and upper bound human error estimates. From this list of sequences and their frequencies, a set of candidate dominant accident sequences should be selected for further analysis. No further analysis need be performed on sequences excluded from the candidate set.

The qualitative expressions developed for each fault tree and each accident sequence tend to include many, many terms. These expressions may be judiciously truncated based on probability. However, the analyst must be careful to truncate at the proper time in the analysis and at appropriately small values to preclude losing potentially significant terms. Guidance in this regard is given below and in the accompanying methods documentation.

The development of qualitative accident sequence expressions should include not only initiating events and system failures, but also system successes as well, as defined by the event tree. Inclusion of system successes may eliminate some terms from the failure equation which are logically precluded by success of another system. Failure to account for system successes may result in erroneous sequence equations and overestimated accident sequence frequencies. The over-estimation can be quite large.

Possible operator recovery actions should be investigated only for the candidate dominant accident sequences and, for these sequences, only for the most significant cut sets. Recovery actions and probabilities differ for each combination of failures; hence, it is desirable to limit these investigations to only the most important cut sets of the most important sequences. Point estimate values should be used for all sequence calculations. Whenever possible, mean values should be used. The associated statistical distributions are used only in the limited uncertainty analysis described in the next task.

6.1.6 Assumptions and Guidelines

The initial task of the accident sequence analysis is to merge the support system trees with the appropriate front-line system trees to obtain a set of fault trees consistent with the event trees including support system faults. The resultant merged trees should be carefully checked for accuracy including consistency of event names and descriptions with the system and conditions modeled, removal of any logic loops (discussed in Part III, Section 6.1), without loss of any cut sets, and resolution of any gates "dangling," that is without appropriate output. A plot of these trees is a useful tool as is a check of the cut sets obtained by solving the trees. It is very important that errors in the fault trees be removed *before* proceeding to the sequence quantification. Otherwise, much time and money will be wasted!

In the development of expressions for each system (to be used in the sequence analysis), faults in the fault trees are often coalesced into "superevents" or "independent subtrees." Such a practice is acceptable, in fact desirable, provided that the events coalesced are independent of *all* other events in the analysis. Coalescing faults independent only within the given system can lead to failure to properly treat commonalities among system in the sequence calculation and a possible underestimation of sequence frequencies.

Standard assumptions made in system and sequence quantification are that events with different names are independent and that the rare event approximation is acceptable. As mentioned above, system and sequence expressions may be truncated on probabilistic grounds to improve efficiency in the calculation. However, the expression for each system should use *upper bound* estimates for questionable event probabilities (e.g., human errors). The probability of any event which may also be an initiating event (i.e., loss of offsite power and support system initiating events) should be set to 1.0 in all truncation operations. Failure to follow these guidelines could result in some terms being dropped from the expression that should not be. Truncation should also be performed based on the probability of a cut set, not the number of terms or on the value of a given event. Cut sets, not events, should be deleted from the expression.

Truncation values of 10^{-9} or less are acceptable for cut sets in either systems or sequences. Truncation values greater than 10^{-6} are unacceptable unless absolutely necessary. Between these two values, the analyst must make a judgment. For systems responding only to loss-of-coolant accidents, truncation values of 10^{-6} are acceptable. When combined with the initiating event frequency, this corresponds to keeping all terms of at least 10^{-8} Since transient frequencies can exceed 1 per reactor year, it is desirable to truncate systems responding to transient events as close to 10^{-9} as possible. However, this value may result in too many cut sets for the available computing capabilities even after coalescing independent faults in the fault trees. In such cases, truncation should be made as low as existing capabilities permit.

The inclusion of success events in the sequence expressions may be performed in several ways depending upon the capabilities of the given team. Should a complement equation for each system be developed, however, it should either be the complete complement or the complement formed from the truncated system equation. Truncation of the complement equation may lead to erroneous results.

Finally, consideration of recovery actions should generally be limited to simple actions which may be performed from the control room. The first consideration for recovery is whether the fault is recoverable or not. Damaged or failed equipment is considered nonrecoverable, i.e., no credit is given for equipment repair. Misposition or actuation faults are often recoverable, as are human errors made in response to the accident. The second consideration involves the time available to perform the act and where the action may be accomplished. Faults which are recoverable from the control room are generally included in the analysis if there is sufficient information available to diagnose the problem and time to perform the action. Faults which require local recovery actions are generally excluded from the analysis. Exceptions to this guideline may be reasonable if substantial time exists for performing the action. However, for actions outside the control room, consideration must be given to the location and its characteristics (temperature, radiation environment, security, etc.) in considering whether the fault is in fact recoverable and in considering the time to perform the act.

6.2 Accident Sequence Analysis Procedures

The accident sequence analysis task involves 19 steps. Figure 6.2-1 illustrates the interrelationships among the various steps of the accident sequence analysis task. Part III, Section 6, of this guide contains further methodological guidance.

6.2.1 Description of Each Accident Sequence Analysis Procedural Step

Fault Tree Preparation

Step 1. Form complete fault trees for each front-line system by merging the support system fault trees, as appropriate, with the front-line system fault trees.

Description: Fault trees were produced in the plant systems analysis task for each front-line and each support system. In this task, an expression for the ways in which each accident sequence may occur is desired, including both front-line and support system faults. The first step in this process is to form fault trees for each front-line system including support system faults. This is done by attaching the appropriate support system fault trees to the front-line system trees. This merging process results in having a set of fault trees, one for each event tree heading.

Product: Front-line system fault trees complete with support system faults.

Step 2. Plot each merged front-line system fault tree.

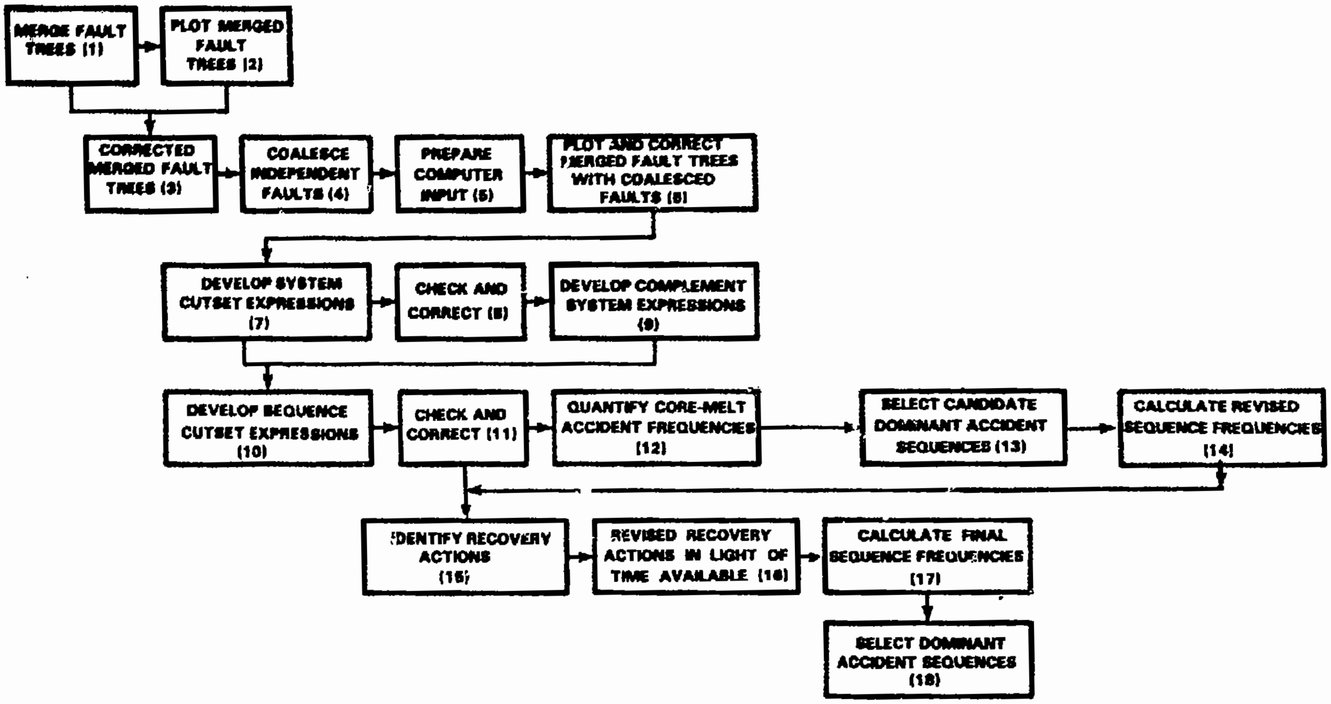

MERGE FAULT TREES (1)
PLOT MERGED FAULT TREES (2)
CORRECTED MERGED FAULT TREES (3)
COALESCE INDEPENDENT FAULTS (4)
PREPARE COMPUTER INPUT (5)
PLOT AND CORRECT MERGED FAULT TREES WITH COALESCED FAULTS (6)
DEVELOP SYSTEM CUTSET EXPRESSIONS (7)
CHECK AND CORRECT (8)
DEVELOP COMPLEMENT SYSTEM EXPRESSIONS (9)
DEVELOP SEQUENCE CUTSET EXPRESSIONS (10)
CHECK AND CORRECT (11)
QUANTIFY CORE-MELT ACCIDENT FREQUENCIES (12)
SELECT CANDIDATE DOMINANT ACCIDENT SEQUENCES (13)
CALCULATE REVISED SEQUENCE FREQUENCIES (14)
IDENTIFY RECOVERY ACTIONS (15)
REVISED RECOVERY ACTIONS IN LIGHT OF TIME AVAILABLE (16)
CALCULATE FINAL SEQUENCE FREQUENCIES (17)
SELECT DOMINANT ACCIDENT SEQUENCES (18)

Figure 6.2-1. Step Relationships for the Accident Sequence Analysis Task

Description: A plot of each fault tree is highly desirable as a mechanism for checking the tree for consistency and for the analyst to review against the system. The merged fault trees can be quite large and use of a computerized plotting routine facilitates this step.

Product: Set of plots for front-line systems.

Step 3. Using the plots developed in Step 2, check the fault trees to ensure consistency of event names with system drawings, compatibility with failure definitions for the events on the event trees, absence of logic loops, and absence of dangling gates. Correct any errors found.

Description: The fault trees may contain any of several errors. The analyst should search these out, referring to the plot, to ensure that the fault trees are correct before proceeding.

The first check involves simply checking the plot against the system drawing and the analyst's knowledge of the system to ensure that it logically represents the system and that the fault tree event names are consistent with those on the system drawing. Care should be taken, once again, to ensure that common faults among different systems have been given the same name.

The systems analyst and event tree analyst should also review the tree together to ensure compatibility with the system failure definitions specified by the event tree. In particular, conditionalities specified by the event tree should be reflected in the fault tree.

Logic loops may become apparent after merging the support systems with the front-line systems. An example of such a loop would be a diesel generator relying on service water (to keep the diesel cool) and the service water depending on the diesel generator for power if offsite power is lost. Any such loops found should be removed as the code will not be able to solve trees with loops. This should be done carefully so as to ensure that no cut sets are lost in the process. Often, such loops are not real; that is, some conditionality has been lost. For example, a motor-operated valve may depend on the diesel to change the valve's state at the start of the accident. The diesel, in turn, relies on service water, as above. However, failure of service water results in long-term failure of the diesel and, hence, is not a failure mode of the valve which changes state early in the sequence. Such unrealistic loops should be removed. In fact, the analyst should check all such components to ensure that nonreal fault modes are removed. Some logic loops, such as in the first example above, are real. The logic must then be "cut" and, often, the structure of the tree must be slightly rearranged. The topic of logic loops is discussed in more detail in Part III, Section 6.1.

A final problem which will be apparent from the plot is the problem of dangling gates. Each gate should have inputs and outputs. Often, however, due to a keypunching error or misnaming, gates will appear which lack an input or an output. Such problems are readily apparent and easily solved.

Product: Corrected, merged front-line system fault trees.

Step 4. Coalesce fault tree events which are independent of all other systems into "superevents," as appropriate, in each merged front-line system fault tree.

Description: As mentioned above, the fault trees may be quite large. To more efficiently solve for the expression for each accident sequence, faults which do not appear elsewhere in any other fault tree may be coalesced into single events to replace portions of the appropriate front-line system fault tree. This must be done with care, however, to ensure that all events in the super-event are truly independent lest potential common events be lost in the process. Computer codes are available which perform this operation; alternatively, the knowledgable analyst can do this by hand, using the plots produced in Step 2. This is generally done only up to the pipe segment level. That is, independent faults in different pipe segments are not coalesced. Part III, Section 6.2, of the guide contains a further discussion of this process.

Product: Merged front-line system fault trees with coalesced independent faults.

Step 5. Prepare input to the fault tree analysis code for each merged front-line system fault tree with coalesced independent faults.

Description: The trees developed in Step 4 are those which will be used in the accident sequence analysis. Prepare the input to the code for these trees following the appropriate input format.

Product: Computerized fault trees for each merged front-line system fault tree with coalesced independent faults.

Step 6. Plot each merged front-line system fault tree with coalesced independent events and perform the same checks as in Step 3. Correct any errors found.

Description: The analyst should ensure that the trees produced in Step 4 and input in Step 5 are correct before proceeding with the sequence analysis. The description of Step 3 provides guidance in this regard.

Product: Corrected, merged front-line system fault trees with coalesced independent faults.

Front-Line System Expressions

Step 7. Develop qualitative expressions for the combinations of events—cut sets—which could result in failure of each front-line system. Truncate each expression by eliminating cut sets having a probability of 10^{-9} or less (unless a higher truncation value is necessary).

Description: Before proceeding to the development of cut set expressions for each accident sequence, expressions should be developed for each front-line system. This is generally done with a Boolean algebra code. The expressions can be quite large. This is somewhat alleviated by truncating from the expression all cut sets having a value of 10^{-9} or less. Experience has shown that cut sets having a value this small do not contribute significantly to the accident sequence frequency, even if they are common failures among several systems. Should the expression still be too large, a higher truncation value may be chosen, but it is not recommended. The higher the truncation value, the greater the chance that significant contributors may be lost. Part III, Section 6.3, of this guide further discusses the development of system minimal cut sets and truncation.

Product: Truncated, qualitative cut set expressions for each front-line system fault tree.

Step 8. Check the most probable and fewest term cut sets for each front-line system failure to ensure these combinations of events actually do cause the top event. If not, correct the fault tree.

Description: It is important that these qualitative expressions be correct and represent the actual ways in which the system may fail before proceeding to the development of accident sequence expressions. It is impractical to check all of the cut sets. However, the systems analyst should check those contributing most to the probability of system failure and those having the fewest terms. Ensure each combination causes the system to fail. If not, the fault tree must be corrected. Check to ensure that the corrections do not contradict the coalescing of independent events. If so return to Step 4. Otherwise, return to Step 6.

Product: Verified, and corrected if necessary, cut set expressions for each front-line system.

Step 9. If complement equations are to be used to account for system success states in the accident sequence analysis, form the complement of each truncated front-line system expression.

Description: Accident sequences include system successes as well as system failures. It is important that the accident sequence cut set expressions contain only combinations of events which do not contradict the system successes included in the sequence. System successes may be accounted for in several ways (see Part III, Section 6.4). However, if complement equations are formed, they should be formed from the truncated front-line system expressions developed in Step 8.

Product: Complement expressions for each front-line system fault tree.

Screening Calculations for Sequence Frequencies

Step 10. Form qualitative expressions for each core melt accident sequence by appropriately combining initiating events and front-line system success and failure expressions (from Steps 8 and 9). Truncate these expressions, if necessary, by eliminating sequence cut sets having a frequency of 10^{-9} or less (unless a higher truncation value is necessary).

Description: Qualitative expressions of the combinations of events leading to each core melt sequence are developed by combining the system success and failure expressions with the initiating event in the combinations specified in the event trees This is done essentially by combining under an AND gate the appropriate expressions and solving using the laws of Boolean algebra (see Part III, Section 6.4).

These expressions can be quite large. They may be judiciously truncated by dropping all cut sets of value 10^{-9} or less. A higher truncation value may be chosen, if necessary, but it is not recommended. There may hundreds of cut sets of order 10^{-8}; truncation at 10^{-8} would result in miscalculating the frequency of a 10^{-6} sequence which, experience has shown, may be significant. The truncation value should be consistent with or higher than that used in Step 7 multiplied by the frequency of the initiating event. Choice of a lower value would result in an incomplete expression, to that order, since some terms would have been lost in Step 7.

Product: Qualitative, truncated cut set expressions for each accident sequence.

Step 11. Check the most frequent and fewest term sequence cut sets to ensure these combinations of events actually do cause the accident sequence to occur. If not, correct the appropriate model.

Description: The qualitative expression for each sequence should be checked to ensure that each combination of events results in the sequence occurring. It is impractical to check all the cut sets. However, the analyst should check those contributing most to the frequency of the sequence and those having the fewest terms. To correct errors, generally changes must be made to the fault trees. Depending on the nature of the error, return to Step 4 or Step 7.

Product: Verified, and corrected if necessary, cut set expressions for each core melt accident sequence.

Step 12. Quantify the frequency of each core melt accident sequence using the generic data base and upper bound estimates, where necessary.

Description: The frequency of each core melt accident sequence should be estimated using the generic data base and plant-specific test and maintenance unavailabilities from the data base development task and upper bound human error estimates from the human reliability and procedural analysis task. More accurate data is not used at this step. The purpose here is to estimate the sequence frequencies for the purpose of selecting a subset for more accurate quantification. If truncation was performed in Step 10, an estimate of the sequence frequency may already have been obtained. This process is discussed more fully in Part III, Section 6.5.

Product: **Estimated frequencies for each core melt accident sequence.**

Step 13. Select a set of accident sequences for closer scrutiny, refined data estimates, and recovery considerations. These are termed "candidate dominant accident sequences."

Description: Development of plant-specific data, best estimate human error probabilities and recovery data can be a time-consuming task. It is advantageous to limit these activities to those sequences which could contribute most to the frequency of core melt. Thus in this step, a subset of sequences termed "candidate dominant accident sequences" are chosen for more precise frequency estimations.

The selection of sequences is generally a matter of analyst judgment. Often, a natural break point in the spectrum of sequence frequencies will be apparent; for instance, there may be a few sequences with frequencies around 10^{-4} to 10^{-5}, several with frequencies of 10^{-6}, and many with frequencies of 10^{-7} or less. The analyst may choose to examine only those having frequencies 10^{-6}. The choice of sequences, however, is not too critical. If all chosen sequences have their frequencies reduced below the chosen cutoff frequency as a result of improved calculations and inclusion of operator recovery actions, the analyst need only examine more sequences.

Product: Set of candidate dominant accident sequences.

Final Sequence Frequency Calculations

Step 14. Using the human reliability analysts' best estimate human error probabilities and revised component failure rate data (where appropriate), calculate the frequency of each candidate dominant accident sequence.

Description: An improved frequency estimate of each candidate dominant accident sequence is obtained by repeating Step 12 using best estimate human error probabilities from the human reliability and procedural analysis task and improved component failure rate data from the data base development task. These calculations represent the best estimate accident sequence frequencies, excluding recovery considerations. This step is discussed further in Part III, Section 6.6.

Product: Revised sequence frequency estimates for the candidate dominant accident sequences.

Step 15. Identify the cut sets which contribute significantly to the revised candidate dominant accident sequence frequency estimates. For each, determine which faults are recoverable, the action which must be taken, the location from which the action is to be taken, and time required to perform the action. Tabulate this information.

Description: Each sequence cut set represents one way the accident sequence may occur. The information available to the operator and the recovery action to be taken varies depending on the particular cut set. Thus potential operator recovery actions cannot be considered on a sequence level, but rather they must be considered on a sequence cut set level. This investigation is limited to those cut sets which contribute significantly to the frequency of each candidate dominant accident sequence.

To evaluate the potential for operator recovery, certain information must be compiled. First, determine if the faults in the sequence are recoverable. If not, recovery for the cut set need not be further considered. Generally, only simple faults such as misalignment or actuation faults are considered recoverable. No credit is given for repairing components or heroic actions.

Given that a fault is recoverable, the recovery action to be taken, where it is to be taken, and the time required to perform the action complete the basic information regarding recovery actions for the recovery model. This information should be collected in a table.

Product: Table of faults for which recovery will be considered and data pertinent to their quantification.

Step 16. Estimate the time available for performing each recovery action. If this time is less than that required to perform the act, remove the fault from the list of recoverable faults. Add this information to the recovery table from Step 15.

Description: In addition to the data collected in the previous step, one must consider how much time is available to perform the recovery action. This time, referred to in Part III, Section 6.7, as the "critical time," depends on the accident sequence and may, in some cases, depend upon the cut set. This time is related to the phenomena associated with the sequence such as the time to boil dry the steam generators, the time to the onset of core uncovery, or the length of time a component may operate without cooling. The critical time for the sequence should be compared with the time it takes to perform the recovery action (see Step 15). For those cases in which the critical time is less than the time to recover, the fault should be removed from the set of recoverable faults. Otherwise, add the critical time to the recovery table.

Product: Modified recovery table to be used in quantification of recovery actions.

Step 17. Using estimates of the probability of recovery from the human reliability analyst, recalculate the frequency of each candidate dominant accident sequence including recovery.

Description: The final sequence frequent calculation is performed by multiplying each sequence cut set by the probability of nonrecovery (1-P(recovery)). This step is described in more detail in Part III, Section 6 7, of this guide.

After performing the calculation, check the set of cut sets for each sequence to ensure that the largest cut set for which recovery was not considered (recall in Step 15 that recovery was considered for only the significant cut sets) is still not significant compared to the values after including recovery of those previously deemed significant. If any cut sets appear to be significant and recovery has not been considered, repeat Steps 15-17 including these additional cut sets.

Product: Final estimate of the frequency of each candidate dominant accident sequence.

Step 18. Select a set of the most frequent accident sequences to be termed "dominant accident sequences."

Description: Using the results of Step 17, a subset of candidate dominant accident sequences is chosen as the dominant accident sequences. The choice is again a matter of analyst judgment, but often all sequences greater than a given frequency, say 10^{-6}, are chosen or the sequences contributing greater than a certain percent, say 90%, of the core melt frequency are chosen.

Product: Set of dominant accident sequences for the plant.

Task Products

Step 19. Summarize task products for the task report.

Description: The products of the accident sequence analysis task are listed below. The fault tree models correspond to those produced in Step 6. Estimated frequencies for each core melt accident sequence were calculated in Step 12. Frequencies and qualitative expressions for the candidate dominant and dominant accident sequences were developed in Steps 11, 17, and 18.

Products:

1. Fault tree models for each front-line system including support system faults.
2. Estimated frequencies for each core melt accident sequence.
3. Set of candidate dominant accident sequences, their frequencies, and qualitative expressions of significant contributors to each.
4. Set of dominant accident sequences, their frequencies, and qualitative expressions of significant contributors to each.

6.3 Accident Sequence Analysis Documentation and Example Products

The documentation of the accident sequence analysis task should provide the final set of merged fault trees for each front-line system, a clear description of the analysis process, and information pertinent to the selection and quantification of candidate and dominant accident sequences. This section suggests information to be documented upon completion of this task and includes examples from previous analyses. These constitute the products of the second informal report and the results for the draft final report.

6.3.1 Merged Fault Trees

A principal product of this task is the set of merged, front-line system fault trees. The initial set of fault trees was documented as part of the plant systems analysis task. The final set of fault trees, which is the set of front-line system fault trees merged with their support systems, should be documented upon their completion. These should be plotted in terms of their independent subtrees, if used. Accompanying these plots should be completed fault summary sheets showing the faults in each independent subtree, briefly describing each event, and showing the pertinent failure rate data.

Examples of these products are shown in Figure 6.3-1 and Table 6.3-1. These illustrate portions of the emergency feedwater system fault tree and fault summary sheets from the ANO-1 IREP analysis.

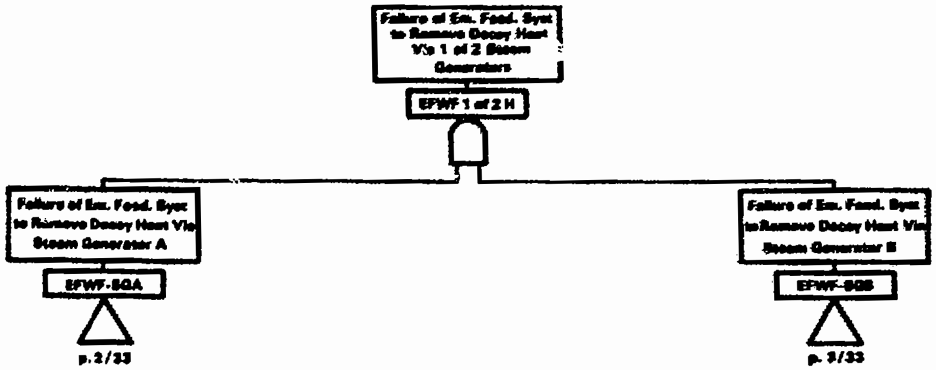

Failure of Em. Feed. Syst to Remove Decay Heat Via 1 of 2 Steam Generators
EFWF 1 of 2 H
Failure of Em. Feed. Syst to Remove Decay Heat Via Steam Generator A
EFWF-SGA
p. 2/33
Failure of Em. Feed. Syst to Remove Decay Heat Via Steam Generator B
EFWF-SGB
p. 3/33

Figure 6.3-1. Fault Tree for the Emergency Feedwater System

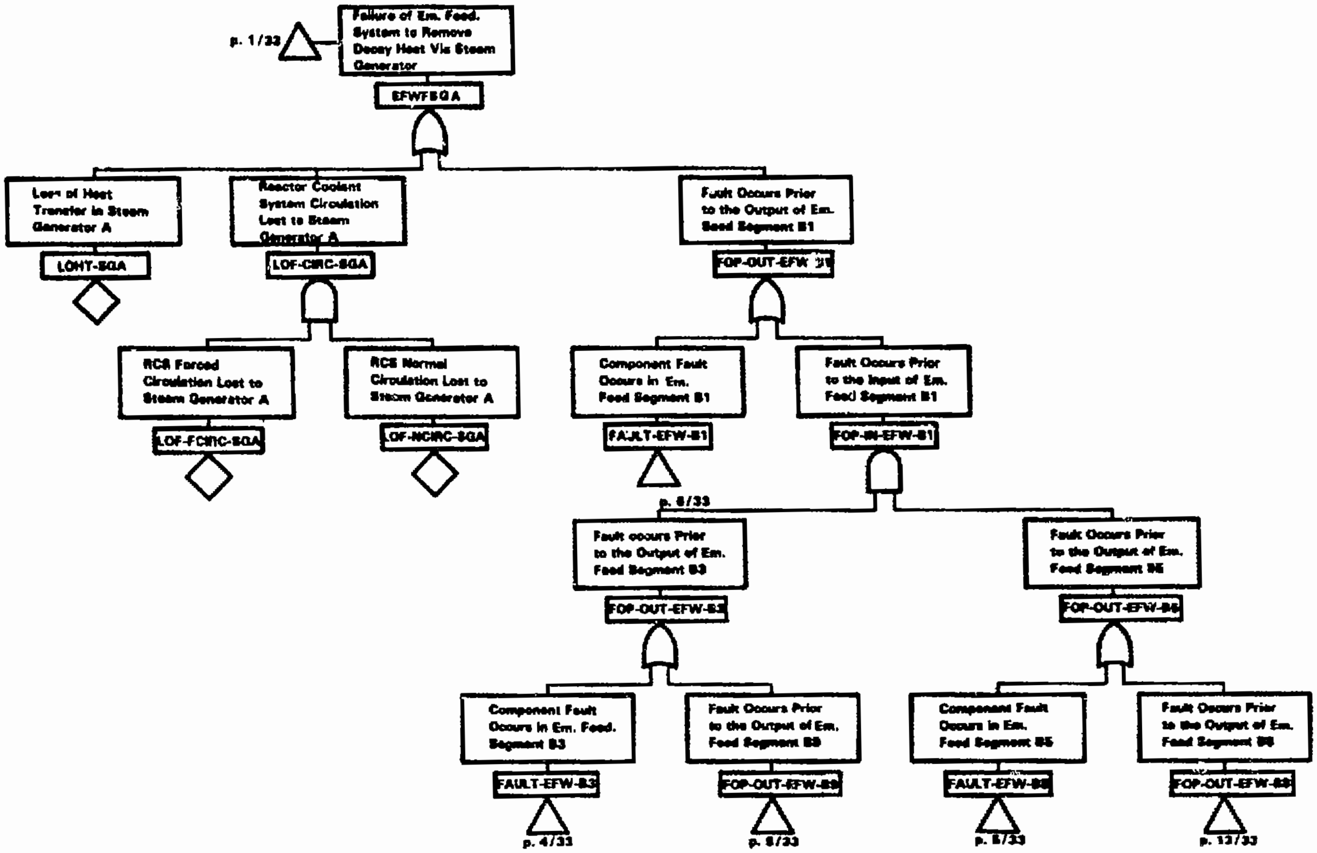

p. 1/33
Failure of Em. Feed. System to Remove Decay Heat Via Steam Generator
EFWFSGA
Loss of Heat Transfer in Steam Generator A
LOHT-SGA
Reactor Coolant System Circulation Lost to Steam Generator A
LOF-CIRC-SGA
Fault Occurs Prior to the Output of Em. Feed Segment B1
FOP-OUT-EFW-B1
RCS Forced Circulation Lost to Steam Generator A
LOF-FCIRC-SGA
RCS Normal Circulation Lost to Steam Generator A
LOF-NCIRC-SGA
Component Fault Occurs in Em. Feed Segment B1
FAULT-EFW-B1
p. 6/33
Fault Occurs Prior to the Input of Em. Feed Segment B1
FOP-IN-EFW-B1
Fault occurs Prior to the Output of Em. Feed Segment B3
FOP-OUT-EFW-B3
Fault Occurs Prior to the Output of Em. Feed Segment B6
FOP-OUT-EFW-B6
Component Fault Occurs in Em. Feed. Segment B3
FAULT-EFW-B3
p. 4/33
Fault Occurs Prior to the Output of Em. Feed Segment B9
FOP-OUT-EFW-B9
p. 8/33
Component Fault Occurs in Em. Feed Segment B6
FAULT-EFW-B6
p. 5/33
Fault Occurs Prior to the Output of Em. Feed Segment B8
FOP-OUT-EFW-B8
p. 13/33

Figure 6.3-1. (cont)

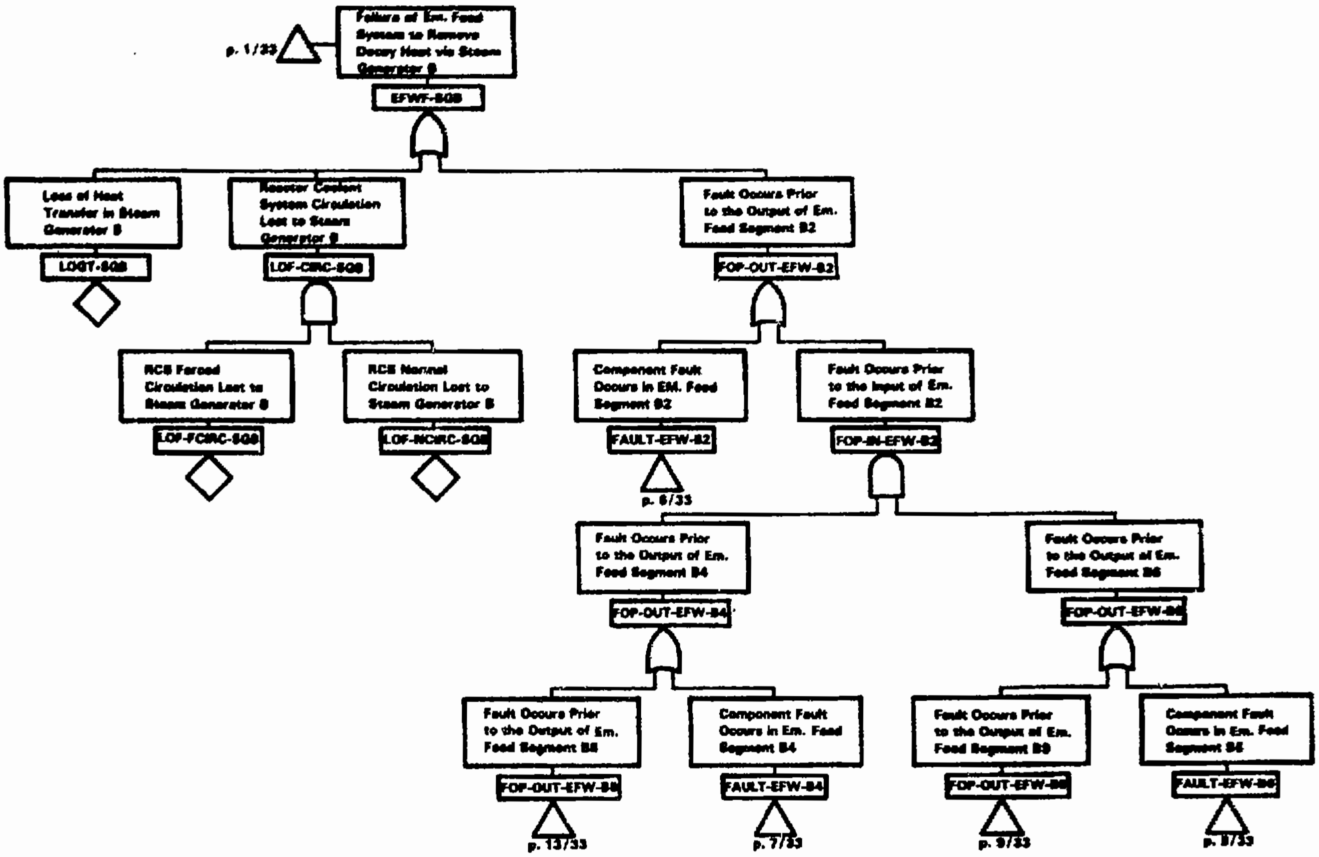

p. 1/33
Failure of Em. Feed System to Remove Decay Heat via Steam Generator B
EFWF-SGB
Loss of Heat Transfer in Steam Generator B
LOGT-SGB
Reactor Coolant System Circulation Lost to Steam Generator B
LOF-CIRC-SGB
Fault Occurs Prior to the Output of Em. Feed Segment B2
FOP-OUT-EFW-B2
RCS Forced Circulation Lost to Steam Generator B
LOF-FCIRC-SGB
RCS Normal Circulation Lost to Steam Generator B
LOF-NCIRC-SGB
Component Fault Occurs in EM. Feed Segment B2
FAULT-EFW-B2
p. 6/33
Fault Occurs Prior to the Input of Em. Feed Segment B2
FOP-IN-EFW-B2
Fault Occurs Prior to the Output of Em. Feed Segment B4
FOP-OUT-EFW-B4
Fault Occurs Prior to the Output of Em. Feed Segment B6
FOP-OUT-EFW-B6
Fault Occurs Prior to the Output of Em. Feed Segment B8
FOP-OUT-EFW-B8
p. 13/33
Component Fault Occurs in Em. Feed Segment B4
FAULT-EFW-B4
p. 7/33
Fault Occurs Prior to the Output of Em. Feed Segment B9
FOP-OUT-EFW-B9
p. 9/33
Component Fault Occurs in Em. Feed Segment B6
FAULT-EFW-B6
p. 8/33

Figure 6.3-1. (cont)

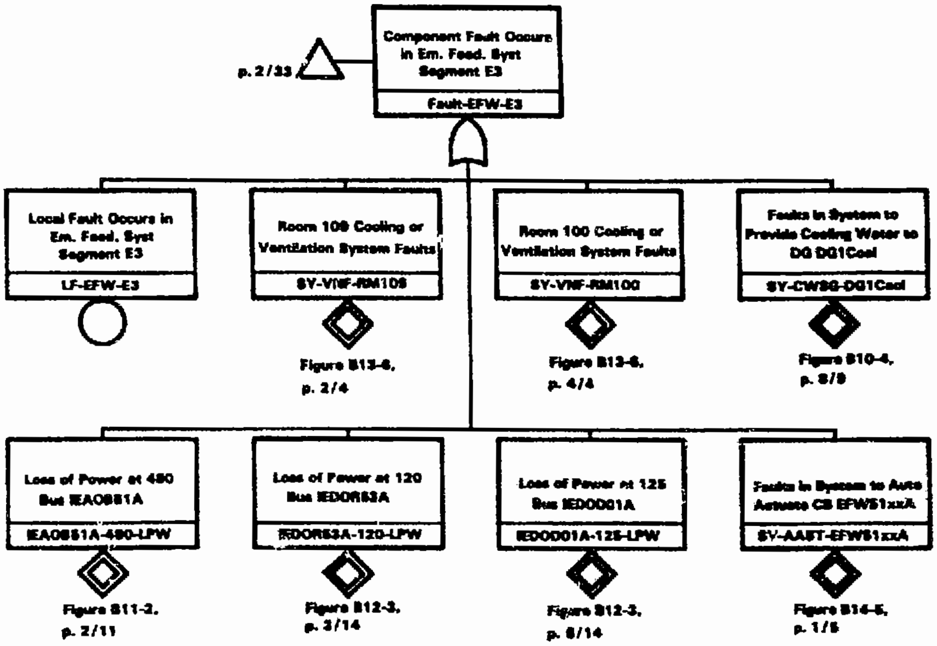

p. 2/33
Component Fault Occurs in Em. Feed. Syst Segment E3
Fault-EFW-E3
Local Fault Occurs in Em. Feed. Syst Segment E3
LF-EFW-E3
Room 108 Cooling or Ventilation System Faults
SY-VNF-RM108
Figure B13-6, p. 2/4
Room 100 Cooling or Ventilation System Faults
SY-VNF-RM100
Figure B13-6, p. 4/4
Faults in System to Provide Cooling Water to DG DG1Cool
SY-CWSG-DG1Cool
Figure B10-4, p. 8/9
Loss of Power at 480 Bus IEAOSS1A
IEAOSS1A-480-LPW
Figure B11-2, p. 2/11
Loss of Power at 120 Bus IEDORS3A
IEDORS3A-120-LPW
Figure B12-3, p. 3/14
Loss of Power at 125 Bus IEDOD01A
IEDOD01A-125-LPW
Figure B12-3, p. 6/14
Faults in System to Auto Actuate CB EFWS1xxA
SY-AAST-EFWS1xxA
Figure B14-5, p. 1/5

Figure 6.3-1. (concluded)

Table 6.3-1. Fault Summaries for Emergency Feedwater System

Event Name	Subevent Name	Component Type	Subevent Description	Failure Rate/h	Fault Exposure Time (h)	Fault Duration Time (h)	Subevent Unavailability	Event Unavailability
LF-EFW-E3	EFWOOQ1X-CCC-LF	Check Valve-CC	Failure to open				1E-4	
	EFWOOX3A-VOC-LF	Motor-Operated Valve-OC	Failure to remain open				1E-4	
	EFW2670A-VCC-LF	Motor-Operated Valve-CC	Failure to open				4E-3	
			Failure to remain open				1E-4	
	EFW51XXA-CBL-LF	Cable	Open circuit	3E-6	360		1.1E-3	
	EFW51XXA-B00-LF	Circuit Breaker-OO	Failure to transfer				1E-3	
	EFW51XXA-BOO-CC	Circuit Breaker	Faults in control circuit				2E-3	
	A-EFW-8	CVX-3	Maintenance	1.8E-6		4	7.2E-6	
	A-EFW-10	CVZ670	Maintenance	1.8E-6		4	7.2E-6	8.4E-3
LF-EFW-E4	EFWOOQ4X-CCC-LF	Check Valve-CC	Failure to open				1E-4	
	EFWOOX1A-VOC-LF	Motor-Operated Valve-OC	Failure to remain open				1E-4	
	EFW2620B-VOC-LF	Motor-Operated Valve-CC	Failure to open				4E-3	
			Failure to remain open				1E-4	
	EFWODO2B-CBL-LF	Cable	Open circuit	3E-6	360		1.1E-3	
	EFWODO2B-BOO-LF	Circuit Breaker-OO	Failure to transfer				1E-3	
	EFWODO2B-BOO-CC	Circuit Breaker	Faults in control circuit				2E-3	
	A-EFW-11	CVX-1	Maintenance	1.8E-6		4	7.2E-6	
	A-EFW-12	CV2620	Maintenance	1.8E-6		4	7.2E-6	8.4E-3
LF-EFW-ES	EFWOOQZX-CCC-LF	Check Valve-CC	Failure to open				1E-4	
	EFWOOX4B-VOC-LF	Motor-Operated Valve-OC	Failure to remain open				1E-4	

6.3.2 Sequence Analysis

The principal activity of this task is the development of qualitative cut set expressions for each accident sequence and the quantification of accident sequence frequencies. To facilitate an understanding of the evaluation process, the technique used should be briefly described. This discussion should discuss the integration of the event trees, fault trees, and data base as the input to the accident sequence analysis and clearly describe each step in the analysis. This includes the process of identifying independent subtrees (if they were used), the development of system cut set expressions and the development of sequence cut set expressions (including success events). Truncation values used in various stages of the analysis should be stated, and rationale for their selection should be provided.

The selection of candidate dominant accident sequences should be discussed, including the criterion for candidacy. The recovery model used in the analysis should be discussed as well. Modifications made to the data following initial screening calculations should also be documented including the tables documenting recovery actions.

To clarify the analysis process, an example calculation illustrating each step of the process should be provided. An example recovery table is presented in Table 6.3-2. To this table should be added more explicit identification of the action to be taken and time required for the action.

Table 6.3-2. Example Recovery Table*

Pipe (or Wire) Segment Local Fault: LF-SWS-S2 System: Service Water
Sequence Considered: All LOSP Critical Time: 30 minutes
Unavailability w/o Recovery: 5E-3 Unavailability w/Recovery: 4.6E-4
Probability of Non-Recovery: 0.09

Sub-Event Name	Is It Recoverable?	Location of Recovery Action	q,w/o Rec.	P(NR)	q,w/Rec.	Comments
SWSOO1BX-COC-LF	—	—	ε	—	ε	
SWSOO2BX-COC-LF	—	—	ε	—	ε	
A-SWS-3	N	—	2.2E-4	1	2.2E-4	
SWSOP4BA-PMD-LF	Y	Control Room	1.7E-3	0.05	8.5E-5	Start standby pump is recovery action
0303-CBL-LF	Y	Control Room	1E-4	0.05	5E-6	
SWSO303A-BOO-LF	Y	Control Room	1E-3	0.05	5E-5	
SWSO303A-BOO-CC	Y	Control Room	2E-3	0.05	1E-4	

*Taken from Reference 8.

6.3.3 Accident Sequence Documentation

The information provided for each accident sequence should provide the user with sufficient information to verify the fault contributors to the sequence and to approximate the calculation of sequence frequency. Documentation could become voluminous; the suggested documentation provides a minimum necessary to achieve the above objectives.

Each candidate dominant accident sequence should be documented as follows. Provide a table containing the initiating event and its frequency and the initial sequence frequency (following initial screening) and the final sequence frequency. In addition, include the dominant minimal cut sets and their initial and final probability. The fault summary sheets provide the definition of minimal cut set identifiers.

An example of this is shown in Table 6.3-3. In thisexample, sequence and cut set unavailabilities are provided. These do not reflect the frequency of the initiating event. The sequence frequency, obtained by multiplying the sequence unavailability by the initiating event frequency, is also provided.

The dominant accident sequences should also be listed. Each should be briefly discussed in terms of the systems which succeed and fail and the associated accident sequence timing and phenomenology. The accident sequence frequency should be stated and the dominant fault contributors discussed. In addition, the dominant cut sets, their description, and their frequency should be listed. An example dominant accident sequence discussion taken from the Arkansas Nuclear One IREP analysis is found in the following section.

Table 6.3-3 LOCA Accident Sequence Cut Sets*

Initiating Event: B(1.2)   Initiating Event Frequency: 0.02/yr

Sequence Identifier: B(1.2)D_1
(Sequence 24 on B(1.2) Event Tree)

Total Sequence: B(1.2) $\overline{K}D_1\overline{Y}\,\overline{C}\,\overline{F}$

	Unavailability	Frequency
Sequence (without recovery)	1.1E-3	2.2E-5/yr
Sequence (with recovery)	1.4E-4	2.8E-6

Dominant Minimal Cut Sets	Unavailability w/o Recovery	Probability Non-Recovery	Unavailability w/Recovery
LF-HPI-H14*LF-SWS-VCH4B	3.2E-4	0.01	3.2E-6
LF-HPI-H14*LF-SWS-S14	1.4E-4	0.01	1.4E-6
LF-HPI-H14*LF-SWS-S5	1.4E-4	0.01	1.4E-6
LPI1407A-VCC-LF*LF-HPI-H14	1.1E-4	0.23	2.6E-5
HPI-PUMP-CM	1E-4	1.0	1E-4
LF-HPI-H14*LF-SWS-S2	7E-5	0.05	3.5E-6
LF-HPI-H14*LF-ECS-ROOM100	7E-5	0.01	7E-7
LF-HPI-H14*LF-AC-B5	6.2E-6	0.05	3.1E-7
LF-HPI-H14*LF-AC-A3	3.4E-6	0.23	7.7E-7

*Adapted from Reference [8]

6.3.4 Example Dominant Accident Sequence Discussion

Sequence $B(1.2)D_1$ α, γ, β, ϵ: This sequence is initiated by a reactor coolant pump seal rupture or a rupture in the reactor coolant system (RCS) piping in the range 0.38 in. $< D \leq 1.2$ in. (B(1.2)), followed by failure of the high pressure injection system (D_1). Containment failure is predicted by one of the following: vessel steam explosion (α), containment overpressure due to hydrogen burning (γ), penetration leakage (β), or base mat melt-through (ϵ).

This sequence assumes a small LOCA occurs followed by failure of the high pressure injection system. Containment systems would operate as designed to control containment pressure and to remove radioactivity from the atmosphere, but failure of the core cooling system would lead to boiloff of the water covering the core resulting in core melt.

The dominant failure mode of the high pressure injection system is predicted to be failure of the operator to initiate the system. Information received from the vendor indicates an engineered safeguards high pressure injection system actuation signal due to low RCS pressure may not be generated following some LOCAs <1.2 inches in diameter. This sequence assumes an engineered safeguards signal will not be generated prior to core uncovery and that the operator must initiate the system.

The frequency of this sequence is estimated as:

$B(1.2)D_1 = 2.8 \times 10^{-6}$.

The dominant contributors, or cut sets, to this frequency are listed and discussed below.

Cut Set	Cut Set Frequency[1]
B(1.2)*HPI-PUMP-CM	2×10^{-6} (1)[2]
B(1.2)*LF-HPI-H14*LPI1407A-VCC-LF	5.3×10^{-7} (.23)
B(1.2)*LF-HPI-H14*LF-SWS-S2	7×10^{-8} (.05)
B(1.2)*LF-HPI-H14*LF-SWS-VCH4B	6.4×10^{-8} (.01)
B(1.2)*LF-HPI-H14*LF-SWS-S5	2.8×10^{-8} (.01)
B(1.2)*LF-HPI-H14*LF-SWS-S14	2.8×10^{-8} (.01)

<u>Term Descriptions</u>

B(1.2) — reactor coolant pump s failure; F (B(1.2)) = 2×10^{-2}/Ryr.

HPI-PUMP-CM — failure of operator to initiate HPIS; p(HPI-PUMP-CM) = 1×10^{-4}.

LF-HPI-H14 — local faults in HPIS pipe segment H14 (fails C pump); p(LF-HPI-H14) = 0.014.

LPI1407A-VCC-LF — local faults of valve CV1407 (fails A and B pump suction); p(LPI1407A-VCC-LF) = 8.2×10^{-3}.

LF-SWS-S2 — local faults in SWS pipe segment S2 (fails A and B pump cooling); p(LF-SWS-S2) = 5×10^{-3}.

LF-SWS-VCH4B — local faults of ac and dc switchgear room cooler VCH4B (fails A and B pump ac/dc power cooling); p(LF-SWS-VCH4B) = 0.023.

LF-SWS-S5 — local faults in SWS pipe segment S5 (fails A and B pump cooling); p(LF-SWS-S5) = 0.01.

LF-SWS-S14 — local faults in SWS pipe segment S14 (fails A and B pump cooling); p(LF-SWS-S14) = 0.01.

The containment failure mode probabilities and release category placements are:

$P(\alpha)$	=	0.0001;	category 1
$P(\gamma)$	=	0.5;	category 2
$P(\beta)$	=	0.007;	category 5
$P(\epsilon)$	=	0.5;	category 7

Multiplying the sequence frequency with the containment failure mode probabilities results in the final sequence values.

An important insight realized from the analysis of this sequence is that a possibility exists for failing one of the three high pressure injection system pumps given a LOCA <1.2 inches in diameter prior to generation of an engineered safeguards signal. During normal operation, one of the pumps is operating and takes suction from the makeup tank to perform the function of makeup and purification of the RCS. (This same pump is realigned to take suction from the borated water storage tank upon an engineered safeguards signal to perform the function of emergency core cooling.)

Upon a small LOCA the pressurizer level and pressure would begin to decrease and automatic control actions will cause the makeup flow control valve

[1] The number in parentheses represents the probability of nonrecovery which was factored into the cut set frequency. To obtain the cut set frequency without recovery, divide the frequency listed by the number in parentheses.

[2] In general, operator errors are given a nonrecovery factor of 1. This is because the human factor models of these faults have explicitly considered recovery.

to go fully open and the pressurizer heaters to turn on, respectively. An auxiliary calculation indicates that the pressurizer heaters will remain covered for an extended period and thus maintain RCS pressure well above the engineered safeguards actuation set point. The calculation also indicates that the makeup tank would empty prior to uncovering the pressurizer heaters. The makeup tank is estimated to empty within ~14 mins after LOCA initiation or about 10 mins after the low makeup tank level alarm. Upon dry out of the makeup tank it is assessed that the operating high pressure injection pump will fail in a short time.

It should be noted that failure of the operator to initiate the high pressure injection system prior to makeup tank dryout is part of the analyzed failure of the operator to initiate the system prior to core uncovery.

7. Interpretation and Analysis of Results

7.1 Overview of the Interpretation and Analysis of Results Task

7.1.1 Purpose

The previous task quantified the frequency of each core melt accident sequence, identified the dominant accident sequences, and developed expressions for the combinations of failures contributing most to the frequency of each dominant accident sequence. There remains the most important task of the analysis: that of interpreting and analyzing these results. The purpose of this task is to develop engineering insight into those plant features contributing most to the frequency of core melt and to estimate the uncertainties and sensitive assumptions associated with the results.

7.1.2 Products

The products of the interpretation and analysis of results task are as follows:

1. An identification and discussion of the plant features contributing most to the frequency of core melt
2. An estimate of the range of uncertainty associated with each dominant accident sequence and with the overall core melt frequency
3. An identification of assumptions which, if changed, could change the results, an estimation of the size of the changes, and a discussion of their significance
4. Calculations of importance measures and elucidation of any additional engineering insights arising from the calculations.

Examples of these products from previous IREP analyses are contained in Section 7.3.

7.1.3 Relationship to Other Tasks

The interpretation and analysis of results task relies upon information provided by the accident sequence analysis task. The qualitative expressions for the dominant and candidate dominant accident sequences form the basis for the development of insight into those plant features contributing significantly to the core melt frequency. These expressions are also the basis for the uncertainty, sensitivity, and importance calculations performed to give additional insight into the importance of various plant features, the uncertainty of the results, and the sensitivity of results to various analysis assumptions.

Uncertainty calculations are performed primarily to estimate the range of results arising from uncertainties in the input data. To do these calculations, information regarding the distribution and error factors associated with each event in the expressions for the dominant accident sequences is needed. This is primarily provided by the data base development task. Should any human errors contribute, however, this information must come from the human reliability analysts.

Sensitivity analysis is performed to better understand the effects of modeling uncertainties and analysis assumptions. The sensitivity analysis may entail considerations which effect more than just the dominant or candidate dominant accident sequences. If so, the estimated frequencies of each core melt accident sequence may be needed from the accident sequence analysis task.

This being the final task of the analysis, the products of this task are not used in other tasks. Rather, they form the basis for developing conclusions for the final report.

The task relationships for the interpretation and analysis of results task are summarized in Table 7.1-1.

Table 7.1-1. Interpretation and Analysis of Results Task Relationships

Inputs From Other Tasks	Uses in This Task	Products
1. Table of dominant accident sequences and their frequencies; qualitative expressions of significant contributors to each (accident sequence analysis task)	Basis for identifying plant features contributing most to core melt frequency; used for uncertainty, importance, and sensitivity analyses	1. Identification and discussion of the plant features contributing most to the frequency of core melt
2. Table of candidate dominant accident sequences and their frequencies; qualitative expressions of significant contributors to each (accident sequence analysis task)	Used for identifying additional insights into important plant features; used in sensitivity analyses	2. Estimated range of uncertainty associated with each dominant accident sequence and with the overall core melt frequency
3. Estimated frequencies of each core-melt accident sequence (accident sequence analysis task)	Used in sensitivity analyses if assumptions effect more than candidate dominant accident sequences	3. Sensitivity analysis of assumptions which could change the results
4. Distribution and error factors associated with data base (data base development and human reliability and procedural analysis tasks)	Used in uncertainty calculations	4. Importance calculations and discussion of engineering insights derived therefrom

7.1.4 Information Needs

The information required for this task is primarily provided by the accident sequence analysis task. This includes the dominant and candidate dominant accident sequences, their frequencies and cut set expressions, and the estimated frequencies of each core melt sequence. From the data base development and human reliability and procedural analysis tasks are the distributions and error factors associated with dominant accident sequence contributors obtained.

Part III, Section 7, of this guide contains methodological guidance for performing the analyses of this task. The uncertainty and importance calculations are facilitated by having a computer code available. If familiarity with the codes is not already possessed by someone on the analysis team, code documentation would prove useful.

7.1.5 Scope

A primary purpose of an IREP analysis is to develop engineering insights into plant features significant to core melt. This information is contained in the cut set expressions for the most important core melt sequences. Uncertainty, sensitivity, and importance calculations may provide additional insight. However, the primary objective of these analyses is to develop further insight into important plant features and into the analysis, rather than to develop statistical evidence to accompany the quantitative analysis. Hence, these analyses are fairly restrictive in scope.

Uncertainty analysis is performed on only the dominant accident sequences. As stated above, the purpose is to develop an estimate of the possible range of uncertainty of the results, not to develop statistical confidence intervals. Similarly, the importance calculations are performed only on the variables and classes of events associated with the dominant accident sequences.

While the sensitivity analyses may well involve an examination of a broader class of accident sequences, the analyses should be limited only to those assumptions for which there are great uncertainties and assumptions which the analyst believes could affect the analysis results, if changed.

Importance calculations are performed on the basis of the importance of events to the frequency of core melt. If properly normalized, the results of individual event importance calculations can be added together to obtain importance estimates for classes of events.

7.1.6 Assumptions and Guidelines

Standard assumptions regarding component failure rate data are that they exhibit lognormal distributions. Human error data are sparse and uncertainties are generally large. In performing sensitivity analyses, parameters are generally varied one at a time. Importance measures are generally restricted to the Birnbaum and Fussell-Vesely measures.

7.2 Interpretation and Analysis of Results Procedures

The interpretation and analysis of results task involves 14 steps. Figure 7.2-1 illustrates the relationships among the various steps of the interpretation and analysis of results task. Part III, Section 7, of this guide contains further methodological guidance. Note that some steps are independent of others within this task.

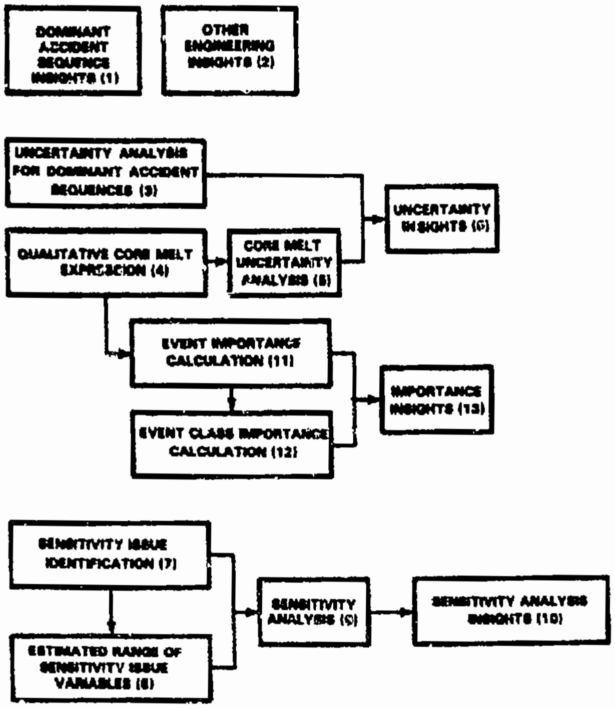

DOMINANT ACCIDENT SEQUENCE INSIGHTS (1)
OTHER ENGINEERING INSIGHTS (2)
UNCERTAINTY ANALYSIS FOR DOMINANT ACCIDENT SEQUENCES (3)
QUALITATIVE CORE MELT EXPRESSION (4)
CORE MELT UNCERTAINTY ANALYSIS (5)
UNCERTAINTY INSIGHTS (6)
EVENT IMPORTANCE CALCULATION (11)
EVENT CLASS IMPORTANCE CALCULATION (12)
IMPORTANCE INSIGHTS (13)
SENSITIVITY ISSUE IDENTIFICATION (7)
ESTIMATED RANGE OF SENSITIVITY ISSUE VARIABLES (8)
SENSITIVITY ANALYSIS (9)
SENSITIVITY ANALYSIS INSIGHTS (10)

Figure 7.2-1 Step Relationships for the Interpretation and Analysis of Results Task

7.2.1 Description of Each Interpretation and Analysis of Results Procedural Step

Engineering Insights

Step 1. Analyze the qualitative expressions of failure combinations contributing most to the frequency of the dominant accident sequences identified in the previous task to identify those particular aspects of plant design contributing significantly to the likelihood of core melt.

Description: Insight into the plant features contributing most to core melt can be gained directly from the qualitative cut set expressions developed in the previous task for each dominant accident sequence. The analyst should identify which components and which component failure modes contribute significantly to each dominant accident sequence.

In addition to the specific-plant equipment contributing significantly, patterns or classes of failures may be evident. The analyst should examine the relative contributions of human errors, test and maintenance, and hardware faults. Analyzing the results from the perspective of which initiating events contribute most significantly yields additional insight. These results are substantiated by importance calculations (see Steps 11-13).

Product: Set of engineering insights associated with the dominant accident sequences.

Step 2. Assemble insights developed in the course of performing the tasks of the analysis which, although they may not contribute significantly to the frequency of core melt, are interesting observations about the plant design and operation.

Description: Insights are often gained over the course of the analysis which do not contribute to the dominant accident sequences. Examples of such insights may be single failures in certain systems or equipment which is not adequately tested by following the test procedures. These constitute a valuable product of the analysis and should be illuminated.

System level insights may be gained from the analysts' review of the systems and their operation or from the system failure expressions developed in the previous task. Additional sequence insights may be gained from the sequence expressions of the nondominant accident sequences. Any such insights should be documented as results of the analysis.

Product: Additional engineering insights regarding plant design and operation.

Uncertainty Analysis

Step 3. Using the medians and error factors associated with each event, statistically estimate the median frequency and associated error factors for each dominant accident sequence.

Description: The accident sequence frequencies calculated in the previous task were point estimates based on using mean values for each failure probability. Additional information is contained in the frequency distribution associated with each dominant accident sequence. The investigation of uncertainties is limited to the distributions associated with each dominant accident sequence.

The technique generally used, described in Part III, Section 7.2, of this guide, consists of a Monte Carlo sampling from the distributions associated with each variable in the accident sequence expression. From many samples, a distribution of frequencies for the accident sequence is developed. Care must be taken to ensure that values selected for correlated variables are selected from the same distribution in each simulation. From the distributions, median and mean frequencies and associated error factors can be estimated for each dominant accident sequence.

Product: Uncertainty estimates for each dominant accident sequence.

Step 4. Form a qualitative expression of the combinations of failures leading to core melt from the dominant accident sequence expressions.

Description: To estimate the frequency and associated uncertainty of core melt and to perform importance calculations with respect to core melt, an expression of the ways of having core melt occur is needed. The entire core melt expression would be enormous. An approximate expression containing the most significant contributors is formed by taking the Boolean sum of the dominant accident sequence expressions. (See Part III, Section 7.1).

Product: Cut set expression for core melt.

Step 5. Using the medians and error factors associated with each event, statistically estimate the median frequency and associated error factors for core melt.

Description: Using the expression developed in Step 4, calculate the median and mean core melt frequency and associated error factors in a manner analogous to that described in Step 3.

Product: Core melt frequency and uncertainty estimate.

Step 6. Identify the principal sources of uncertainty associated with each dominant accident sequence and with core melt.

Description: Analyze the results of Steps 3 and 5 to ascertain which variables and which sequences contribute most to the uncertainty associated with the dominant accident sequences and with the frequency of core melt. Document these findings as additional insights into the analysis.

Product: Insight into aspects of the analysis contributing significantly to the uncertainty of the analysis results.

Sensitivity Analysis

Step 7. Identify assumptions/data which could vary due to lack of knowledge or uncertainty and which could, if changed, alter the set of dominant accident sequences.

Description: Additional insight into the analysis may be gained by performing limited sensitivity analysis. Many assumptions were made in the analysis and, sometimes, data are sparse suggesting possible wide variations. Examples include whether or not to give credit for feed and bleed cooling, whether pump cooling or pump room cooling is required, and the probability of internal disk rupture for a motor-operated valve. Compile a list of assumptions or data which could have an impact on the analysis results.

Product: Set of topics to be analyzed in the sensitivity analysis.

Step 8. Identify the range of variation possible for each sensitivity issue.

Description: For each topic identified in Step 7, identify the range of variation to be used in the sensitivity analysis. For assumptions, this is often merely a choice of making the assumption or not. For data, upper and lower bounds are identified.

Product: Range of variation for each sensitivity issue.

Step 9. Assess the effect on the dominant accident sequences and their frequencies resulting from varying each sensitivity issue over its possible range of values.

Description: Recalculate the frequencies of each dominant accident sequence by varying each sensitivity issue *one at a time* over its range identified in Step 8. If the analyst believes there is a strong correlation among the issues, sensitivity calculations should include multiple variations of assumptions at the same time.

Product: Sensitivity analysis for each selected issue.

Step 10. Identify the assumptions/data which, if varied, result in significant changes in the analysis results.

Description: Compare the results of the previous step with the original dominant accident sequence frequencies. Observe which change the analysis results significantly and which do not. Document these insights.

Product: Insight into issues which, if varied, result in significant changes in the analysis results.

Importance Calculations

Step 11. Using the expression for core melt developed in Step 4, calculate the importance of each event to core melt.

Description: Standard measures, termed "importance measures," have been developed to express the relative importance of events in a cut set expression. These measures generally reflect the sensitivity of the total probability to the change in event probability. Part III, Section 7.3, of this guide discusses some of these measures.

Of particular interest is the sensitivity of core melt frequency to changes in event probabilities. In the case of an event contributing to only one term in the core melt expression, the sensitivity is fairly obvious. If the event contributes to several terms, however, a bit more computation is required. Calculate the importance of each event in the core melt expression.

Product: Event importance with respect to core melt.

Step 12. Calculate the importance with respect to core melt of each desired class of events.

Description: The relative importance of classes of events is also of interest. Some such classes include: human errors, test and maintenance unavailabilities, initiating events, and classes of hardware faults such as power, room cooling, and component cooling faults. The importance of such classes of events may be calculated from the results of Step 11 as described in Part III, Section 7.3, of this guide.

Product: Event class importance with respect to core melt.

Step 13. Identify the most important events and event classes in terms of core melt.

Description: Assess the results of Steps 11 and 12 and note which events and event classes are most important to core melt. That is, to which event and event class probabilities is the frequency of core melt most sensitive. Compare with the insights developed in Step 1. Those insights from Step 1 should be confirmed. Additional insights may have been gained as well.

Product: Insight into the most important events/event classes to core melt.

Task Products

Step 14. Summarize task products for the task report.

Description: The products of the interpretation and analysis of results task are listed below. Plant features contributing to core melt are identified and discussed in Step 1. Uncertainty estimates for the dominant accident sequences and core melt are developed in Steps 3 and 5. Sensitive assumptions are identified in Step 10. Importance insights are derived in Step 13.

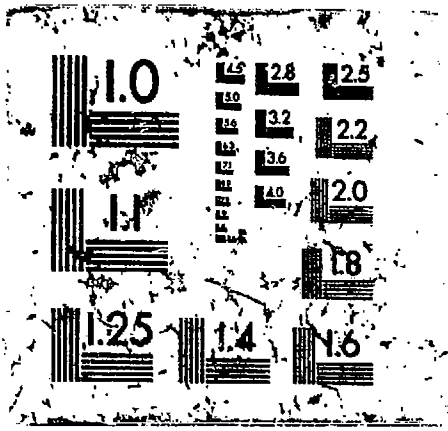
Products:

1. Identification and discussion of the plant features contributing most to the frequency of core melt
2. Identification of the principal sources of uncertainty and an estimate of the range of uncertainty associated with the frequency of each

2 OF 2

NUREG

CR-2728



dominant accident sequence and with the frequency of core melt

3. Identification of assumptions which, if varied, could significantly change the results and an estimate of the possible range of results
4. Identification of the most important events and classes of events to the core melt frequency.

7.3 Interpretation and Analysis of Results Documentation and Example Products

This task concludes the IREP analysis and pulls together the engineering insights sought from the analysis. As such, this is one of the most important tasks and should be clearly documented. This section suggests documentation for this task. This information is included in the draft final report.

7.3.1 Engineering Insights

The insight into the plant features contributing significantly to core melt constitute the most important study results. The dominant cut sets of each dominant accident sequence should be discussed in the documentation of each sequence (see Section 6.3). Additional system level insights may be found in the system descriptions. These insights should be assembled and summarized. Insights from the uncertainty, sensitivity, and importance calculations should be included as well.

The Arkansas Nuclear One IREP summarized the insights in bullet form. An example follows.

7.3.1.1 Example Engineering Insights

During the course of the Arkansas Nuclear One IREP analysis, several engineering insights were realized concerning the operational safety of the plant. Some of the plant Design Engineering Insights are listed below.

- The list of the dominant sequences and those identified to be near dominant indicates that the following general classes of accident sequences contribute most to the ANO-1 core melt frequency.

  -LOCAs initiated by reactor coolant pump seal ruptures contribute ~20%.
  -Station blackout sequences contribute ~20%.
  -Sequences initiated by ANO ac and dc power bus failures contribute ~35%.
  -Other transients and small LOCAs contribute ~20%.
  -Large LOCA sequences contribute <5%.

- The total frequency of core melt for ANO-1 is estimated at 5x10^{-5}/yr. This estimate is similar to estimates made for several other light water reactors in other probabilistic risk assessments, e.g., Surry [4], Peach Bottom [4], Oconee [14], and Grand Gulf. [15].

- Several single failures were identified in front-line and support systems. Operator recovery of some of these single failures is possible, however. The single failures identified were:

  -The high pressure recirculation system pump room cooling has several single failures due to loss of electric power and service water events. The operator may recover from this event by starting an alternate room cooler, but plant procedures and/or control room indication may not be adequate to perform recovery actions before high pressure pump failure occurs.

  -A single valve failure can obstruct the common service water discharge line. This would cause a reactor trip and several transient mitigating systems would be unavailable. The operator may recover from this event by performing actions away from the control room and utilizing an alternate discharge line.

  -Both emergency feedwater pumps take suction from the condensate storage tank through a common header containing three valves. Failure of any of these valves could cause failure of both pumps before the operator recognizes the problem and aligns the suction of the pumps to an alternate water supply.

  -All pumps located within the high pressure, low pressure, and spray system take suction from the borated water storage tank via a common header containing a manual valve. Failure of this valve in the closed position would cause failure of all three systems. No recovery action was identified since the dominant valve failure mode would require disassembly of the valve to correct it.

- The list of dominant accident sequences indicate that support system faults are important to the risk of the plant. The most important support systems were ac/dc power and a service water. Of lesser importance were room cooling systems and automatic actuation systems. The former were most important because faults within these systems can cause a reactor initiating event with concomitant failure of several safety system components. Service water and ac/dc faults also had lower recovery potential than other support systems. Room cooling and auto actuation system faults were of less importance because significant initiating events were not identified and recovery potential was generally high.

7.3.2 Uncertainty, Sensitivity, and Importance Calculations

Uncertainty, sensitivity, and importance calculations are performed to add further perspective on the results. The techniques used in the uncertainty analysis should be discussed and the results summarized in a table such as Table 7.3-1.

The discussion of each sensitivity issue should state why the issue was chosen for sensitivity analysis and the results of the analysis. Any additional insights gained from the analysis should be noted. An example sensitivity discussion, taken from the ANO-1 IREP analysis [8], is found in the following section.

Finally, the techniques used in the importance calculations should be discussed. The importance measures chosen should be identified and briefly discussed, and the results should be presented in tabular form. Any additional insights gained from the analysis should be noted.

Table 7.3-1. Data Uncertainty Analysis Results*

Sequence	Point Estimate	Median	Mean	Error Factor
$B(1.2)D_1$	2.8E–6	5.2E–6	6.5E–6	3
$B(1.2)D_1C$	4.4E–6	5.5E–6	7.0E–6	3
$T(LOP)LD_1YC$	9.9E–6	1.7E–5	6.4E–5	11.4
$B(4)YH_1$	1.4E–6	1.7E–6	2.0E–6	2.4
$T(D01)LD_1YC$	3.1E–6	3.6E–6	4.2E–6	3.8
$T(D02)LD_1YC$	2.5E–6[1]	2.2E–6	3.4E–6	4.4
$B(1.66)H_1$	1.2E–6	1.5E–6	1.8E–6	2.2
$T(D01)LQ\text{–}D_3$	4.0E–6	4.8E–6	1.6E–5	11.6
$T(A3)LQ\text{–}D_3$	3.3E–6	4.7E–6	1.6E–6	13
$T(FIA)KD_1$	2.8E–6	2.8E–6	2.0E–5	37
$T(D01)LD_1$	2.2E–6	3.2E–6	4.3E–6	3.2
$T(A3)LD_1$	9.5E–7	1.4E–6	1.8E–6	3.4
$T(D01)LD_1C$	1.8E–6	2.2E–6	3.0E–6	3.3
$T(A3)LD_1C$	1.4E–6	1.9E–6	2.5E–6	3.0
Total Core Melt	4.2E–5[2]	6.0E–5	9.2E–5	4.3

NOTES:

1. Point estimate is larger than median due to cut set truncation which was required to perform the Monte Carlo simulation.
2. This is the total core melt frequency of these 14 sequences only.

*Taken from Reference [8]

7.3.2.1 Sensitivity Analysis of Reactor Coolant Pump (RCP) Seal Rupture Initiating Event Frequency

The frequency of B(1.2) LOCAs (0.02/Ryr) was dominated by reactor coolant pump seal ruptures. This frequency estimate was based upon generic industry data [9]. On May 10, 1980, ANO-1 experienced one of the most severe RCP seal rupture events that have occurred in the nuclear industry. The peak flow rate was estimated at 350 gal/min and the high pressure injection was actuated by the operators in accordance with the ANO LOCA emergency procedure. Before termination of the event, 60,000 gallons of RCS water accumulated in the containment. This section will recalculate the frequency of core melt accidents initiated by B(1.2) LOCAs using ANO specific, rather than generic, RCP rupture date.

Before presenting the results of the recalculation, it should be noted that generic RCP seal rupture data was used because a statistical significance test indicated that generic and ANO specific data were not inconsistent. The recalculation presented below is, therefore, only meaningful if for some reason ANO should in the future become atypical via an occurrence of another RCP rupture event.

ANO-1 has operated for ~7 years with the occurrence of one major (i.e., >50 gal/min) LOCA due to a RCP seal rupture. The B(1.2) LOCA frequency based on this data is 0.14/Ryr. The frequency estimates of sequences B(1.2) D_1, and B(1.2) D_1C are increased to $2x10^{-5}$ and $3.5x10^{-5}$, respectively, via use of this datum. In addition, some sequences which were previously nondominant would now become important. These are listed below:

B(1.2)D_1YC = $5.1x10^{-6}$/Ryr.

B(1.2)LH_1 = $6x10^{-6}$/Ryr.

Increasing the frequency of these four sequences in turn raises the ANO core melt frequency from $5x10^{-5}$ to $9.7x10^{-5}$/Ryr.

8. Summary of IREP Procedures

Part II of this guide has presented the procedures for conducting an IREP analysis including an overview of each task, procedures and descriptions for each task, and documentation suggestions and example products. For the convenience of the user desiring a more compact set of procedures, this section summarizes the procedures developed in the previous sections.

8.1 Summary of Plant Familiarization Procedures

Function/System Relationships

Step 1. Identify the systems performing each function important to preventing or mitigating the consequences of a core melt following a LOCA or transient initiating event.

Product: List of systems performing each function.

Step 2. Identify supporting systems for each system identified above (in Step 1).

Product: List of support systems for each system performing a LOCA or transient function and systems upon which support systems depend.

Initiating Events

Step 3. Identify ranges of LOCAs.

Product: List of LOCA break sizes.

Step 4. Identify locations of potential LOCAs in systems which interface with the primary coolant system.

Product: Interfacing systems LOCA list.

Step 5. Identify LOCA break locations which could disable or partially disable responding systems.

Product: List of LOCAs which impact mitigating systems.

Step 6. Identify applicable transients from list of "standard" transients.

Products: List of "standard" transients for this particular plant.

Step 7. Review plant history to identify additional transient initiating events.

Product: List of plant-specific transient initiating events.

Step 8. Identify support system faults which could cause the reactor to trip and which could affect responding systems.

Product: List of transients initiated by support system faults.

Mitigating System Requirements

Step 9. Identify mitigating system requirements for each LOCA size and location.

Product: Table of LOCA mitigating systems and success criteria.

Step 10. Identify mitigating system requirements for each transient initiating event.

Product: Table of transient mitigating systems and success criteria.

Initiating Event Groups

Step 11. Group LOCA initiating events according to common mitigating system requirements.

Product: List of grouped LOCA initiating events.

Step 12. Group transient initiating events according to common mitigating system requirements.

Product: List of grouped transient initiating events.

Task Products

Step 13. Summarize task products for task report.

Products:

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 front-line systems.
4. List of support systems.
5. Table/diagram relating front-line support and systems and support system/support system dependencies.

8.2 Summary of Accident Sequence Delineation Procedures

LOCA Functional Event Trees

Step 1. Place the functions required following a LOCA as identified in the plant familiarization task in the approximate order they will be called upon.

Product: Ordered list of functions to be accomplished following a LOCA.

Step 2. Identify dependencies among the set of LOCA functions.

Product: List of dependencies among LOCA functions.

Step 3. Construct functional event trees, one for each LOCA category in which the functions or dependencies change, incorporating the dependencies identified in Step 2.

Product: Functional event trees for each unique LOCA category.

Step 4. Assess each LOCA functional accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each LOCA functional accident sequence noting whether core melt results or not and a mnemonic designator for each.

Step 5. Prepare a brief description of each LOCA functional accident sequence.

Product: Descriptions to accompany LOCA functional event trees.

Transient Functional Event Trees

Step 6. Place the functions identified in the plant familiarization task as necessary following a transient in the approximate order they will be called upon.

Product: Ordered list of functions to be accomplished following a transient.

Step 7. Identify dependencies among the set of transient functions.

Product: List of dependencies among transient functions.

Step 8. Construct functional event trees, one for each transient category in which the functions or dependencies change, incorporating the dependencies identified in Step 7.

Product: Functional event trees for each unique transient category.

Step 9. Assess each transient functional accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each transient functional accident sequence noting whether core melt results or not.

Step 10. Prepare a brief description of each transient functional accident sequence.

Product: Descriptions to accompany transient functional event trees.

LOCA Systemic Event Trees

Step 11. Place the front-line systems identified in the plant familiarization task as responding to each LOCA initiating event group in the approximate order they will be called upon following the LOCA.

Product: Ordered list of front-line systems responding to each LOCA initiating event group.

Step 12. Identify dependencies among the set of front-line systems responding to each LOCA initiating event group.

Product: List of dependencies among front-line systems for each LOCA initiating event group.

Step 13. Construct systemic event trees, one for each LOCA initiating event group, incorporating the dependencies identified in Step 12.

Product: Systemic event trees for each LOCA initiating event group.

Step 1/. Review each LOCA systemic event tree to ascertain whether the structure would simplify, while retaining system dependency information, if the order of events were changed. If so, modify the tree.

Product: Further simplified LOCA systemic event trees.

Step 15. Identify where transient-induced LOCAs transfer into the LOCA systemic event trees. Review the structure to ensure applicability of the tree for transient-induced LOCAs. If the structure is not applicable, modify the tree.

Product: LOCA systemic event trees compatible with transient-induced LOCAs.

Step 16. Assess each LOCA systemic accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each LOCA systemic accident sequence noting whether core melt results or not, a mnemonic designator, and the corresponding functional accident sequence.

Step 17. Develop system failure definitions and system modeling conditions for each system for each LOCA initiating event group.

Product: Descriptions to accompany each LOCA systemic event tree.

Transient Systemic Event Trees

Step 18. Place the front-line systems identified in the plant familiarization task as responding to each initiating event group in the approximate order they will be called upon following the transient.

Product: Ordered list of front-line systems responding to each transient initiating event group.

Step 19. Identify dependencies among the set of front-line systems responding to each transient initiating event group.

Product: List of dependencies among front-line systems for each transient initiating event group.

Step 20. Construct systemic event trees, one for each transient initiating event group, incorporating the dependencies identified in Step 19.

Product: Systemic event trees for each transient initiating event group.

Step 21. Review each transient systemic event tree to ascertain whether the structure would simplify, while retaining system dependency information, if the order of events were changed. If so, modify the tree.

Product: Further simplified transient systemic event trees.

develop clearly stated failure conditions and modeling conditions for each front-line system.

Product: Statement of top events for each front-line system fault tree.

Step 3. Develop a simplified system drawing depicting the system to be modeled in the fault tree.

Product: Simplified system drawing for each front-line system.

Step 4. Decompose the simplified system drawing into piping or wiring segments.

Product: Simplified drawing annotated with segments for each front-line system.

Fault Tree Development

Step 5. Develop system logic for each top event in terms of the pipe or wire segment configuration.

Product: Top-level logic for each front-line system.

Step 6. Develop logic for each segment in terms of segment components.

Product: Front-line system fault trees developed to the component level.

Step 7. Develop the logic for each component including hardware faults, test and maintenance unavailability, human errors, and support system faults.

Product: Complete initial fault tree for each front-line system.

Step 8. Ensure that the data base includes data for each fault in the fault tree. If data for any events are missing, inform the data analyst.

Product: List of further data needs for the data base development task.

Step 9. Review each front-line system to ensure all support system interfaces have been included in the tree. If some are omitted, add them.

Product: Revised fault tree for each front-line system.

Step 22. Identify which sequences result in a transient-induced LOCA. For these sequences, transfer to the appropriate LOCA tree at the appropriate branch point in the tree.

Product: Transient systemic event trees with transfers to the appropriate LOCA tree for transient-induced LOCAs.

Step 23. Assess each transient systemic accident sequence to ascertain whether it results in core melt.

Product: Tabulation next to each transient systemic accident sequence noting whether core melt results or not, a mnemonic designator, and the corresponding functional accident sequence.

Step 24. Develop system failure definitions and system modeling conditions for each system for each transient initiating event group.

Product: Descriptions to accompany each transient systemic event tree.

Task Products

Step 25. Summarize task products for task report.

Products:

1. LOCA functional event trees.
2. Transient functional event trees.
3. Systemic event trees for each LOCA and transient initiating event group.
4. Descriptions accompanying each event tree.

8.3 Summary of Plant Systems Analysis Procedures

System Review and Fault Tree Definition

Step 1. Review information for each front-line system to ascertain how the system operates, interfaces with other systems, instrumentation and control for the system, and how it is tested and maintained.

Product: System descriptions for each front-line system.

Step 2. Using system success criteria from the plant familiarization task and event failure definitions accompanying the systemic event trees, Step 10. Define the top events for each support system in the context of the developed front-line system fault trees.

Product: Statement of top events for each support-system fault tree.

Step 11. Develop fault trees for each support system as in Steps 1-9 and consistent with the conditions specified in Step 10.

Product: Fault trees for each support system.

Step 12. Ensure all initiating events which could affect system operability are included in each front-line and support system fault tree. If not, include them.

Product: Further revised fault tree for each front-line and support system.

Step 13. Review all fault trees to ensure common equipment and common faults among different systems have been given the same event names. If not, modify the trees to ensure consistency.

Product: Final set of fault trees for each front-line and support system for use in the accident sequence analysis task.

Task Products

Step 14. Summarize task products for task report.

Products:

1. Fault trees for each front-line system for each of the success criteria and consistent with conditions specified in the systemic event trees.
2. Fault trees for each support system developed in the context of each front-line system it supports.
3. System descriptions for each front-line and support system.
4. List of further data needs.

8.4 Summary of Human Reliability and Procedural Analysis Procedures

Identification of Potential Human Errors

Step 1. Review test and maintenance procedures for each front-line and support system. Identify all components moved from their accident response states or taken out of service. Postulate restoration errors for these components.

Product: List of potential restoration errors following test and maintenance activities.

Step 2. Review the emergency operating procedures applicable to each accident sequence. List all human actions to be performed in response to the accident.

Product: List of accident response actions as defined in the procedures.

Step 3. Ascertain which human actions identified in Step 2 could degrade the reliability of front-line and support system components if improperly performed. Postulate human errors for these actions.

Product: List of potential significant human errors in response to accidents.

Information Acquisition and Upper Bound Probability Estimation

Step 4. Review administrative procedures to understand the plant's administrative control system.

Product: Basic understanding of plant's administrative controls.

Step 5. Visit the plant to gain familiarity with the control room, with the implementation of administrative controls, and to clarify questions raised in the procedural review.

Product: Basic understanding of control room environment and improved understanding of plant's administrative controls.

Step 6. Review the context of performance of human actions identified in Step 3. Ensure that factors learned from the plant visit important to evaluation of these actions are so noted.

Product: Notes on insights gained from the plant visit pertinent to postulated human errors.

Step 7. Develop upper bound estimates of human errors identified in Steps 1 and 3 for use in initial screening calculations of accident sequence frequencies.

Product: Set of upper bound probability estimates for each identified human error.

Development of Best Estimate Human Error Probabilities

Step 8. Talk through the procedures associated with each action contributing to the candidate dominant accident sequences identified in the accident sequence analysis task with plant operating personnel to gain a full understanding of the performance of eac) ‘ask.

Product: Understanding necessary to analyze more closely the potentially significant human errors associated with the plant.

Step 9. Perform a task analysis of each task contributing to the candidate dominant accident sequences. This forms the basis for the development of human reliability event tree models.

Product: A listing of activities associated with each task pertinent to the candidate dominant accident sequences.

Step 10. Develop human reliability event trees for each task associated with the candidate dominant accident sequences.

Product: Event tree models for each potentially significant human error associated with the analysis.

Step 11. Assign nominal human error probabilities to each event on each human reliability event tree.

Product: Initial estimates for each event on the human reliability event trees.

Step 12. Estimate the relative effects of performance-shaping factors on the human error probabilities and modify them accordingly.

Product: Revised human error probabilities including performance-shaping factor effects.

Step 13. Assess the level of dependence among different tasks and incorporate this into the human error probability estimates.

Product: Revised human error probabilities including dependence among tasks.

Step 14. Estimate the probability of each human error contributing to the candidate dominant accident sequences using the human reliability analysis event trees from Step 10 and event probability estimates from Step 13.

Product: Human error probabilities for each event contributing to the candidate dominant accident sequences.

Recovery Considerations

Step 15. For human errors expected to contribute significantly to the core melt frequency, determine the effects of possible recovery actions, and modify the human error probabilities appropriately.

Product: Revised human error probabilities for significant human errors.

Step 16. For recovery actions associated with recoverable nonhuman-error related events (component failures, etc.) identified in the accident sequence analysis task, estimate the probability of properly performing each action.

Product: Estimates of recovery probability for recoverable faults associated with the candidate dominant accident sequence.

Task Products

Step 17. Summarize task products for the task report.

Products:

1. List of potential test and maintenance restoration errors for each front-line and support system.
2. List of potential significant human errors in response to each accident sequence.
3. Upper bound failure probabilities for each identified human error.
4. Human reliability analysts' best estimate failure probabilities for each human error contributing to the candidate dominant accident sequence.
5. Revised human error probabilities, including recovery actions.
6. Estimated probabilities for recovery of all recoverable faults.

8.5 Summary of Data Base Development Procedures

Operating History

Step 1. Review licensee event reports for the facility and note any peculiar problems associated with plant operation.

Product: List of plant-specific occurrences which may raise questions regarding the applicability of generic data.

Step 2. Discuss plant operating history with knowledgeable plant personnel to ascertain peculiar operational problems.

Product: Further list of plant-specific occurrences which may raise questions regarding the applicability of generic data.

Test and Maintenance Data

Step 3. Review plant technical specifications for each front-line and support system to ascertain test intervals for each system.

Product: Test frequencies for each front-line and support system.

Step 4. Review plant logs and conduct discussions with plant personnel to determine test durations, maintenance frequencies, and maintenance durations for each front-line and support system/component.

Product: Test durations, maintenance frequencies, and durations for each front-line and support system/component.

Step 5. Calculate test and maintenance unavailabilities for each system/component and estimate the error factors associated with each.

Product: Plant-specific test and maintenance unavailability data.

Generic Data Base Modifications

Step 6. From the review of plant logs performed in Step 4, add to the list of plant peculiarities from Step 2 any components for which the maintenance frequency is abnormally high.

Product: More complete list of plant peculiarities.

Step 7. For the components for which the generic data base does not seem to be appropriate, calculate new failure rates and modify the generic data base.

Product: Modified generic data base.

Step 8. For those component failure rates not included in the generic data base, as identified by the plant systems analysts, develop estimates for their failure probability and associated error factors.

Product: Supplements to the data base to make it complete for this analysis.

Initiating Event Frequencies

Step 9. For each initiating event identified in the plant familarization task as applicable to the plant, list the generic frequency given in EPRI NP-2230.

Product: List of initiating events applicable to the plant and the associated generic frequency.

Step 10. From EPRI NP-2230, licensee event reports, or other data sources, note where plant-specific initiating event frequencies differ substantially from those in Step 9. Modify the initiating event frequencies accordingly.

Product: List of initiating event frequencies consistent with plant experience.

Step 11. From the data prepared in Step 10, calculate the frequency of each initiating event group identified in the plant familiarization task and estimate the associated error factors.

Product: Plant-specific data for the frequency of each initiating event group.

Data Refinement

Step 12. For each event in the set of candidate dominant accident sequences identified in the accident sequence analysis task, reexamine the data used to ensure it is consistent with the data developed in the previous steps. For selected components, develop plant-specific data consistent with plant operating experience.

Product: Refined data, as needed, for use in final sequence quantification.

Task Products

Step 13. Summarize task products for the task report.

Product:

1. Generic failure rate data for all component failures.
2. Plant-specific test and maintenance unavailabilities for each system/component.
3. Initiating event frequencies for each initiating event group.
4. Supplemented and modified generic data base and plant-specific component failure rates for selected components.

8.6 Summary of Accident Sequence Analysis Procedures

Fault Tree Preparation

Step 1. Form complete fault trees for each front-line system by merging the support systems fault trees, as appropriate, with the front-line system fault trees.

Product: Front-line system fault trees complete with support system faults.

Step 2. Plot each merged front-line system fault tree.

Product: Set of plots for front-line systems.

Step 3. Using the plots developed in Step 2, check the fault trees to ensure consistency of event names with system drawings, compatibility with failure definitions for the events on the event trees, absence of logic loops, and absence of dangling gates. Correct any errors found.

Product: Corrected, merged front-line system fault trees.

Step 4. Coalesce fault tree events which are independent of all other systems into "superevents," as appropriate, in each merged front-line system fault tree.

Product: Merged front-line system fault trees with coalesced independent faults.

Step 5. Prepare input to the fault tree analysis code for each merged front-line system fault tree with coalesced independent faults.

Product: Computerized fault trees for each merged front-line system fault tree with coalesced independent faults.

Step 6. Plot each merged front-line system fault tree with coalesced independent events and perform the same checks as in Step 3. Correct any errors found.

Product: Corrected, merged front-line system fault trees with coalesced independent faults.

Front-Line System Expressions

Step 7. Develop qualitative expressions for the combinations of events—cut sets—which could result in failure of each front-line system. Truncate each expression by eliminating cut sets having a probability of 10^{-8} or less (unless a higher truncation value is necessary).

Product: Truncated, qualitative cut set expressions for each front-line system fault tree.

Step 8. Check the most probable and fewest term cut sets for each front-line system failure to ensure these combinations of events actually do cause the top event. If not, correct the fault tree.

Product: Verified, and corrected if necessary, cut set expressions for each front-line system.

Step 9. If complement equations are to be used to account for system success states in the accident sequence analysis, form the complement of each truncated front-line system expression.

Product: Complement expressions for each front-line system fault tree.

Screening Calculations for Sequence Frequencies

Step 10. Form qualitative expressions for each core melt accident sequence by appropriately combining initiating events and front-line system success and failure expressions (from Steps 8 and 9). Truncate these expressions, if necessary, by eliminating sequence cut sets having a frequency of 10^{-9} or less (unless a higher truncation value is necessary).

Product: Qualitative, truncated cut set expressions for each accident sequence.

Step 11. Check the most frequent and fewest term sequence cut sets to ensure these combinations of events actually do cause the accident sequence to occur. If not, correct the appropriate model.

Product: Verified, and corrected if necessary, cut set expressions for each core melt accident sequence.

Step 12. Quantify the frequency of each core melt accident sequence using the generic data base and upper bound estimates, where necessary.

Product: Estimated frequencies for each core melt accident sequence.

Step 13. Select a set of accident sequences for closer scrutiny, refined data estimates, and recovery considerations. These are termed "candidate dominant accident sequences."

Product: Set of candidate dominant accident sequences.

Final Sequence Frequency Calculations

Step 14. Using best estimate human error probabilities and revised component failure rate data (where appropriate), calculate the frequency of each candidate dominant accident sequence.

Product: Revised sequence frequency estimates for the candidate dominant accident sequences.

Step 15. Identify the cut sets which contribute significantly to the revised candidate dominant accident sequence frequency estimates. For each, determine which faults are recoverable, the action which must be taken, the location from which the action is to be taken, and the time required to perform the action. Tabulate this information.

Product: Table of faults for which recovery will be considered and data pertinent to their quantification.

Step 16. Estimate the time available for performing each recoverable action. If this time is less than that required to perform the act, remove the fault from the list of recoverable faults. Add this information to the recovery table from Step 15.

Product: Modified recovery table to be used in quantification of recovery actions.

Step 17. Using estimates of the probability of recovery from the human reliability analyst, recalculate the frequency of each candidate dominant accident sequence including recovery.

Product: Final estimate of the frequency of each candidate dominant accident sequence.

Step 18. Select a set of the most frequent accident sequences to be termed "dominant accident sequences."

Product: Set of dominant accident sequences for the plant.

Task Products

Step 19. S'immarize task products for the task report.

Products:

1. Fault tree models for each front-line system including all support system faults.
2. Estimated frequencies for each core melt accident sequence.
3. Set of candidate dominant accident sequences, their frequency, and a qualitative expression of significant contributors to each.
4. Set of dominant accident sequences, their frequency, and a qualitative expression of significant contributors to each.

8.7 Summary of Interpretation and Analysis of Results Procedures

Engineering Insights

Step 1. Analyze the qualitative expressions of failure combinations contributing most to the frequency of the dominant accident sequences identified in the previous task to identify those particular aspects of plant design contributing significantly to the likelihood of core melt.

Product: Set of engineering insights associated with the dominant accident sequences.

Step 2. Assemble insights developed in the course of performing the tasks of the analysis which, although they may not contribute significantly to the frequency of core melt, are interesting observations about the plant design and operation.

Product: Additional engineering insights regarding plant design and operation.

Uncertainty Analysis

Step 3. Using the medians and error factors associated with each event, statistically estimate the median frequency and associated error factors for each dominant accident sequence.

Product: Uncertainty estimates for each dominant accident sequence.

Step 4. Form a qualitative expression of the combinations of failures leading to core melt from the dominant accident sequence expressions.

Product: Cut set expression for core melt.

Step 5. Using the medians and error factors associated with each event, statistically estimate the median frequency and associated error factors for core melt.

Product: Core melt frequency and uncertainty estimate.

Step 6. Identify the principal sources of uncertainty associated with each dominant accident sequence and with core melt.

Product: Insight into aspects of the analysis contributing significantly to the uncertainty of the analysis results.

Sensitivity Analysis

Step 7. Identify assumptions/data which could vary due to lack of knowledge or uncertainty and which could, if changed, alter the set of dominant accident sequences.

Product: Set of topics to be analyzed in the sensitivity analysis.

Step 8. Identify the range of variation possible for each sensitivity issue.

Product: Range of variation for each sensitivity issue.

Step 9. Assess the effect on the dominant accident sequences and their frequencies resulting from varying each sensitivity issue over its possible range of values.

Product: Sensitivity analysis for each selected issue.

Step 10. Identify the assumptions/data which, if varied, significantly change the analysis results.

Product: Insight into issues which, if varied, result in significant changes in the analysis results.

Importance Calculations

Step 11. Using the expression for core melt developed in Step 4, calculate the importance of each event to core melt.

Product: Event importance with respect to core melt.

Step 12. Calculate the importance with respect to core melt of each desired class of events.

Product: Event class importance with respect to core melt.

Step 13. Identify the most important events and event classes in terms of core melt.

Product: Insight into the most important events/event classes to core melt.

Task Products

Step 14. Summarize task products for the task report.

Products:

1. Identification and discussion of the plant features contributing most to the frequency of core melt.
2. Identification of the principal sources of uncertainty and an estimate of the range of uncertainty associated with the frequency of each dominant accident sequence and with the frequency of core melt.
3. Identification of assumptions which, if varied, could significantly change the results and an estimate of the possible range of results.
4. Identification of the most important events and classes of events to the core melt frequency.

Part III. Methods for an IREP Analysis

Part I of this guide contained information pertaining to organizing and managing an IREP analysis. Procedures for conducting the analysis are contained in Part II of this guide. This part of the document supplements the procedures by providing guidance to assist in performing particular tasks and, in some cases, providing examples. There is one section for each of the seven majo̦r IREP tasks.

1. Plant Familiarization Methods

1.1 LOCA and Transient Functions

One of the initial steps in the plant familiarization task is to determine the functions which must be performed to either successfully mitigate a LOCA or a transient or to lessen the consequences of a core melt should mitigation of the LOCA or transient fail. This section develops a set of accident response functions generic to pressurized and boiling water reactors. Much of this material is taken from Reference 6.

In response to a LOCA, reactor systems perform the following basic functions:

1. Render the reactor subcritical.
2. Remove core decay heat (i.e., provide emergency core cooling).
3. Protect the containment building from overpressure due to steam evolution.
4. Scrub radioactive material from containment atmosphere.

Except for reactor subcriticality, which must be performed immediately after the LOCA, the other functions must be continuously performed for an extended period of time.

As a general rule, systems in a pressurized water reactor (PWR) perform the latter three functions in two distinct phases known as injection and recirculation. During the injection phase, the medium which performs these functions, water, is drawn from a tank outside the containment. After the tank empties, the systems enter the recirculation phase by realigning their suction to the containment sump. Since a PWR core meltdown accident can be initiated by system failures which occur during the injection or recirculation phases, and since the consequences of these two types of accidents may differ, it is necessary to split these functions into subfunctions corresponding to these two phases.

In a boiling water reactor (BWR), the "remove core decay heat" and "scrub radioactive material from the containment atmosphere" functions are not usually split into phases. Systems which perform these functions do not in general require realignment during a LOCA. BWR systems which perform the "protect the containment building from overpressure due to steam evolution" function, however, usually operate during two time frames.

During the early time frame, steam generated by the LOCA is condensed by a passive containment heat sink, the suppression pool. The suppression pool temperature then starts increasing and in several hours it is necessary to reject heat from it. The late time frame is characterized by the activation of systems so that suppression pool cooling can be achieved. Since a BWR core meltdown accident can be initiated by system failures which occur during the early or late containment overpressure protection time frame, and since the consequences of these two types of accidents may differ, it becomes necessary to split this function into subfunctions corresponding to these two time frames.

Note that these time frames represent relative rather than absolute time frames. Depending on the LOCA size, the injection phase may range from approximately 30 minutes to several hours. Furthermore, it is generally assumed that if a function succeeds at the start of a time frame, it will continue to be successful throughout the time frame. This is equivalent to saying that the failure probabilities of the systems which comprise the functions are dominated by their unavailability (e.g., failure to start or change state) rather than the unreliability (e.g., failure to continue successful operation).

In summary, the LOCA functions reactor systems perform are:

Preceding page blank

LOCA Functions

PWR	BWR
1. Render reactor subcritical	1. Render reactor subcritical
2. Remove core decay heat a. During injection phase b. During recirculation phase	2. Remove core decay heat
3. Protect containment from overpressure due to steam evolution a. During injection phase b. During recirculation phase	3. Protect containment from overpressure due to steam evolution a. Early b. Late
4. Scrub radioactive material from containment atmosphere a. During injection phase b. During recirculation phase	4. Scrub radioactive material from containment atmosphere

In response to a requirement for a rapid reactor shutdown caused by transients rather than a LOCA, reactor systems initially perform the following functions:

1. Render the reactor subcritical.
2. Remove core decay heat.
3. Protect the reactor coolant system (RCS) from overpressure failure.

Reactor subcriticality must be achieved immediately following the transient. RCS overpressure protection is necessary if, for a given transient, the plant design requires it or if a delay is experienced in removing core decay heat.

These functions are those required to bring the plant to a safe shutdown condition if the heat sink utilized in core decay heat removal is the environment (e.g., condenser circulating water or steam generator atmospheric dump valves). If the environmental heat sink is not available, core decay heat is dumped to the containment. Since the containment is a closed system, it will heat up and additional systems are required to operate in order to:

4. Protect the containment building from overpressure due to steam evolution.

The PWR systems which perform this function are identical to the systems which perform the same function in a LOCA. The BWR systems which perform this transient function are identical to the systems which perform the same function during the late time frame following a LOCA.

If successful mitigation of the transient cannot be achieved and a core melt ensues, the following plant functions can aid in lessening the consequences of the accident:

4. Protect the containment building from overpressure due to steam evolution.
5. Scrub radioactive material from the containment atmosphere.

It should be noted that one additional function, RCS inventory control, could be included in the above list as being required if an RCS safety or relief valve failed to reclose after performing its RCS overpressure protection function. However, an accident sequence with a stuck open safety or relief valve constitutes a small LOCA and can be treated as such.

In summary, the transient functions reactor systems perform are:

Transient Functions

PWR	BWR
1. Render reactor subcritical	1. Render reactor subcritical
2. Remove core decay heat a. Environment heat sink b. Containment heat sink	2. Remove core decay heat a. Environment heat sink b. Containment heat sink
3. Protect RCS from overpressure failure	3. Protect RCS from overpressure failure
4. Protect containment from overpressure due to steam evolution	4. Protect containment from overpressure due to steam evolution
5. Scrub radioactive material from containment atmosphere	5. Scrub radioactive material from containment atmosphere

2. Accident Sequence Delineation Methods

2.1 Phenomenological Dependencies from Previous Risk Assessments

At the event tree level, system phenomenological interactions have been and should be treated in IREP analysis. In past probabilistic risk assessments, some interactions between containment and core cooling responses to accidents, in particular, have been treated.

For the PWR, early loss of containment systems followed by subsequent containment failure and its effects on core cooling systems is an interaction of potential importance. If, for example, containment failure is sudden and catastrophic, essential injection piping could break or missiles could be generated which could prevent further operation of emergency coolant injection. Failure of containment or containment systems could also affect the recirculation phase of core cooling in a number of ways. Past analyses have, for example, treated:

1. Sump water flashing to steam upon containment failure, thus eliminating the recirculation water supply (as discussed in the S_2C sequence for Surry in WASH-1400).
2. Raising recirculation water temperature such that emergency coolant recirculation pump operation is degraded or even fails.

Other such interactions may also exist which have not generally been considered in past analyses such as those involving the effects of structural failure. Examples of such failures would include:

1. Containment and/or piping debris falling into the sump possibly "choking-off" pump suction or causing pump damage.
2. Damage to piping, valves, or control equipment due to containment debris or other containment failure related phenomena such as hydrogen burning.

These and other possible interactions between the containment and core cooling systems should be reviewed for applicability and importance in the IREP analysis.

For the BWR, similar containment — core cooling system interactions have commonly been assumed. Several analyses have found late containment failure due to loss of containment heat removal to be a dominant accident sequence for BWR designs. This containment failure by eventual overpressure has usually been assumed to cause vigorous suppression pool boiling and/or loss of net positive suction head. Emergency core cooling recirculation pumps drawing from the suppression pool have been assumed to fail given one of these conditions.

In addition, the rise in temperature of suppression pool water for sequences without containment heat removal has been examined as a source of failure of the recirculation core cooling systems. For accident sequences in which the suppression pool water temperature exceeded the design temperature of the recirculation core cooling pumps drawing from the pool, pump failure has been assumed to occur.

As mentioned for the PWR case, the phenomenological interactions between the containment and core cooling systems in BWRs can also be important considerations in calculating the risk from nuclear power plant accidents. The PRA team should assure that such potential interactions are examined and either included in the IREP analysis or eliminated using appropriate justification for the particular plant of interest.

2.2 Development of a Systemic Event Tree

Procedural Steps 11-16 and 18-23 of Part II, Section 2.2, address the construction of LOCA and transient systemic event trees, respectively. This section discusses the construction of a LOCA systemic event tree which appeared in the Arkansas Nuclear One Unit One IREP analysis [8]. The LOCA event tree chosen applied to breaks in the range of 1.2 to 1.6 inches equivalent diameter.

Before construction of the event tree commenced, the system success criteria were determined. In response to a LOCA in the range 1.2 in. < D ≤ 1.66 in., at ANO One, the combinations of front-line systems, grouped according to functions, depicted in Table 2.2-1 must operate.

With these success criteria in mind, the LOCA systemic event was constructed by following Steps 11-16. These steps are given below with a discussion of how they were implemented.

Step 11. Place the front-line systems in the approximate order they will be called upon following the LOCA.

Discussion: Following the LOCA, the front-line systems will respond in the following approximate order. (System acronyms are defined in Table 2.2-1.)

1. The RPS will scram the reactor at an RCS pressure of 1800 psi.
2. 2/3 HPIS pumps will actuate at an RCS pressure of 1500 psi.
3. If one of the HPIS pumps fails, 1/3 HPIS pumps will actuate at 1500 psi.
4. The EFS will actuate upon isolation of the main feedwater system following a 4-psi containment preessure signal.
5. The pressurizer SRVs will be demanded open at 2500 psi due to system repressurization if the EFS fails.
6. The RBCS will actuate at a 4-psi containment pressure signal.
7. The RBSI will actuate at a 30-psi pressure signal.
8. The HPRS will be initiated by the operator upon depletion of the refueling water storage tank.
9. The RBSR will be initiated by the operator upon depletion of the refueling water storage tank.

Table 2.2-1. ANO One Success Criteria for LOCAs 1.2 in.<D≤1.66 in.

		Injection Phase			Recirculation Phase		
Function	Reactor Subcriticality	Emergency Core Cooling	Containment Overpressure Protection	Radioactivity Removal	Emergency Core Cooling	Containment Overpressure Protection	Radioactivity Removal
Front-line system success criteria	Reactor Protection system (RPS) inserts ≥6 control rod groups into the core	2/3 High pressure injection system (HPIS) and 1/2 pressurizer safety relief valves open (SRVO) OR 1/3 HPIS and 1/2 emergency feedwater system (EFWS)	1/2 Reactor bldg. spray injection (RBSI) OR 1/4 reactor bldg. fan coolers (RBCS)	1/2 RBSI	1/3 High pressure recirculation (HPRS)	1/2 Reactor bldg. spray recirculation (RBSR) and sump mixing with low pressure heat exchanger OR 1/4 RBCS	1/2 RBSR

Note: 2/3 High Pressure Injection System means 2 out of 3 HPIS trains are required for success.

Adapted from Reference [8]

Note that the order of the systems corresponds to the order in which the functions are performed.

Step 12. Identify dependencies among the set of front-line systems responding to the LOCA initiating event.

Discussion: There are three types of system dependencies. These dependencies are grouped according to type below.

Type 1. The system succeeds/fails by definition due to success/failure of another system or set of systems.

- The RBSR fails by definition due to failure of RBSI since both systems share most of the same equipment.
- Success of two of three HPIS pumps implies success of one of three HPIS pumps.
- The HPRS fails by definition due to failure of 1/3 HPIS since both systems share most of the same equipment.

Type 2. The system fails due to expected physical processes associated with the accident sequence.

- The HPRS is conservatively predicted to fail following failure of the RBCS and RBSI(R). Failure of RBCS and RBSI(R) leads to containment overpressure failure. Sudden depressurization of containment is assumed to cause the water in the sump to boil vigorously. Since the pumps located in the HPRS are not designed to pump two-phase flow, they are assumed to fail and cause a core melt.

Type 3. Success/failure of the system does not affect the potential for core melt or reduce the consequences expected due to the success/failure of other systems in the accident sequence.

- Given success of the HPIS (HPRS) and the RBCS, the core and containment are successfully protected during the injection (recirculation) phase. Operation of the RBSI (RBSR) does not matter, given success of these systems, since it does not significantly affect the consequences or the potential for core melt.

- Given failure of the SRVO *or* 2/3 HPIS and the EFS, a core melt is predicted to occur. Operation of 1/3 HPIS or the HPRS does not matter, given failure of these systems, since it is not expected to significantly affect the consequences.

- Given success of the EFS and 1/3 HPIS, the pressurizer SRVs will not be demanded and therefore will not affect the outcome of the accident.

- Given failure of 1/3 HPIS *or* the EFS and 2/3 HPIS, a core melt is predicted to occur. Operation of the pressurizer SRVs does not matter, given failure of these systems, since they are not expected to significantly affect the consequences.

- Given success of the EFS, 1/3 rather than 2/3 HPIS pumps are required. Operation of the extra pump will not affect the outcome of the accident.

Step 13. Construct a systemic event tree, incorporating the dependencies identified in Step 12.

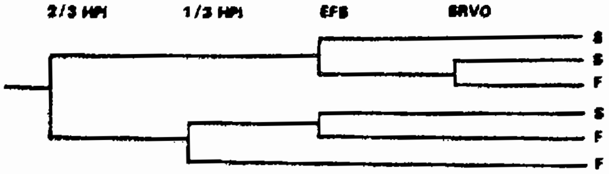
Discussion: The event tree was constructed in the following manner. First, the nine front-line system events were designated as event tree headings and placed in the order depicted in Step 11. Second, the dependencies delineated in Step 12 were incorporated into the event tree structure by removing success/failure decision branches. And finally, a simplification of the event tree structure was identified by reordering the event tree headings. The tree was redrawn (refer to discussion in Step 14), thus producing the final event tree.

The final event tree appears in Figure 2.2-1. At points in the tree in which a decision branch is missing, a number appears which indicates the type of dependency which allowed the branch to be eliminated (refer to Step 12). Each sequence has an assigned mnemonic designator; the first letter in the designator represents the initiating event and the subsequent letters represent the failed systems in the sequence. This nomenclature resembles that utilized in the Reactor Safety Study in order to promote communication in the probabilistic risk assessment community.

Step 14. Review the LOCA systemic event tree to ascertain whether the structure would simplify, while retaining system dependency information, if the order of events were changed.

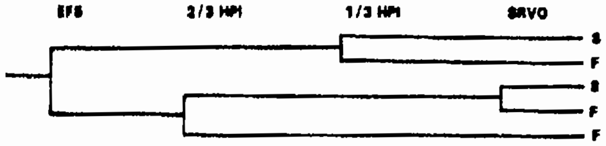
Discussion: As mentioned in Step 13, the order of the event tree headings was modified in order to simplify the event tree structure. The event tree was first drawn with the events in the order listed in Step 11.

This ordering produced the event tree structure, relating to emergency core cooling during the injection phase, depicted below:



This ordering produced six output paths. Each path represents a different way of succeeding (S) or failing (F) emergency core cooling during injection.

It was observed that by reordering these events, five output paths could be produced which contained the same information as the six paths above.



The simplification stems from the observation that if the EFS is successful, 1/3 HPI rather than 2/3 HPI pump is all that is required to ensure successful core cooling during injection. This revised structure reduced the original 45 sequences to the 36 depicted in Figure 2.2-1.

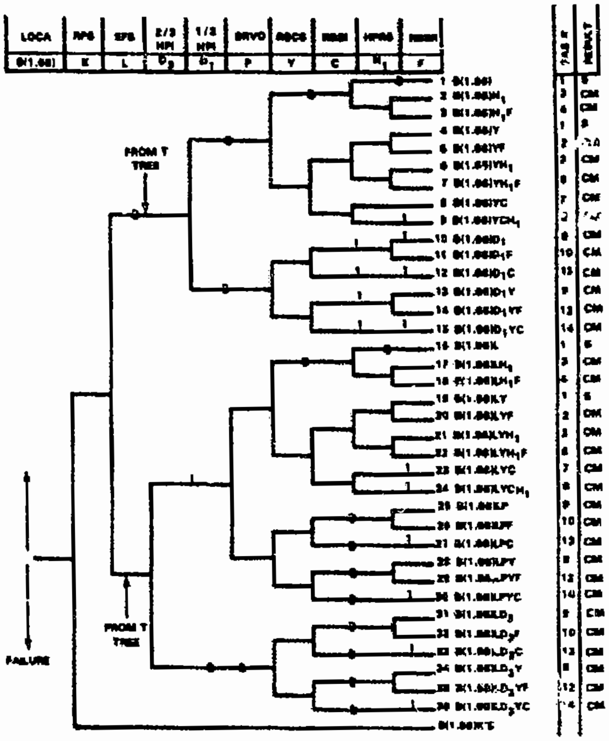
As a final simplification, decision branches following RPS failures were eliminated. At ANO One, a core melt sequence involving a LOCA and failure of RPS is probabilistically insignificant (e.g.,$<10^{-7}$/Ryr). Including these sequences would complicate the event tree by roughly doubling the number of sequences.

Step 15. Identify where transient-induced LOCAs transfer into the LOCA systemic event tree. Review the structure to ensure applicability of the tree for transient-induced LOCAs. If the structure is not applicable, modify the tree.

Discussion: The ANO transient event trees identified possible sequences involving a stuck open pressurizer safety valve. These sequences would be classified as a LOCA since they fall in the range 1.2 in. < D ≤ 1.66 in. The transfer from the transient event trees occurs at the two points indicated in Figure 2.2-1. The LOCA tree was then reviewed to ensure applicability of the tree to this transient-induced LOCA. This revealed that sequences 25-30 do not apply since they involve failure of the pressurizer safety valves to open. When analyzing this event tree in the context of transient-induced LOCAs, it must be remembered that SRVO succeeds with a probability equal to 1.0. (T! is approach was taken rather than reordering the event tree events to avoid increasing the number of event tree sequences.)

Step 16. Assess each LOCA systemic accident sequence to ascertain whether it results in core melt.

Discussion: The results of this step are depicted in the "results" column in Figure 2.2-1. Also listed in the figure is the appropriate functional accident sequence number which applies to the systemic accident sequence. As can be noted, one functional accident sequence may be represented by several systemic accident sequences. Designating the appropriate functional accident sequence serves two purposes. It serves as a check to ensure that the systemic event tree represents all possible functional accident sequences. Also, knowing the functions which have succeeded and failed in a sequence aids in determining the expected core meltdown phenomenology associated with the accident. This is discussed further in Reference [2].



Notes: 1. For transient induced LOCAs, sequences 25 through 30 do not apply.
2. In sequences 5, 8, 20, 23, core melt occurs after containment failure. This represents dependency type 2.

Adapted from Reference 8

Figure 2.2-1. ANO-1 LOCA Systemic Event Tree for Breakers 1.2 in. < D ≤ 1.66 in.

3. Plant Systems Analysis Methods

Fault tree models are constructed for each front-line system and each support system in order to identify the ways the systems may fail. In this section the procedures are described for analysis of the types of systems commonly encountered in a reactor risk assessment. In addition, several topics that affect the development and analysis of the models are presented.

3.1 System Segment Decomposition

3.1.1 Overview

As discussed in Part II, Section 3.2 of this guide, the fault tree development process involves the decomposition of a system into system segments and the development of system fault logic in terms of faults in the segments. This basic approach is followed in fault tree development for all front-line and support systems. In this section the procedures for decomposition of fluid and electrical systems are illustrated.

3.1.2 Fluid System Analysis

Analysis of any system begins by clearly defining the boundaries of the system and becoming familiar with the normal configuration and alternate flowpaths of the system. The first step in the fluid system fault tree development is to develop a simplified system diagram of the system of interest from the system's piping and instrumentation diagram. This is done by eliminating from consideration those pipe segments which do not have a significant impact on the system's performance. As a rule of thumb, piping which interfaces with the main system piping and is less than one-third the diameter of the main system piping should not have a significant impact on the system performance, and thus can be omitted from the simplified system diagram. Likewise, pipe segments containing normally closed manual valves which could only improve the system performance if opened, can be omitted from the simplified system diagram because credit is generally not taken for manual valve manipulation by operators in response to accidents unless it is specified by procedures.

Next, the simplified system diagram is broken down into pipe segments by placing nodes on the diagram at points where two or more pipes intersect. Each length of pipe between adjacent nodes is a pipe segment. Figure 3.1-1 shows a simplified system piping and instrumentation diagram broken down into pipe segments.

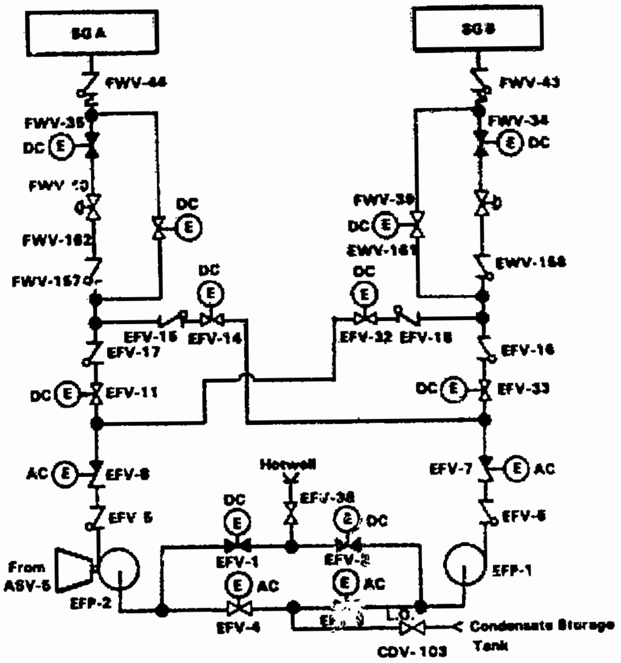


Figure 3.1-1. Example Auxiliary Feedwater System Simplified Diagram

3.1.3 Electrical System Analysis

The electrical system decomposition is based on a bus-to-bus development. This approach provides a sound logical basis for the fault tree development and allows for easy interfacing with the electrical requirements of power plant components.

The electrical system bus-to-bus development starts at the outermost bus, i.e., the bus which is farthest removed from the electrical power sources. The fault tree is then developed by going backward through the electrical system and defining the failure of each bus in terms of local faults, failure in cabling or components between the bus of interest and the immediately preceding bus, or failure of the immediately preceding bus. This development is carried out until the electrical power sources (i.e., offsite power, diesel generators, or station batteries) are reached. The system is decomposed into segments by placing a node at each point where two or more buses intersect.

As an example, consider the electrical diagram shown in Figure 3.1-2. Here, one portion of the system analysis would begin with bus B71 which is an outermost bus. The first step in the development is back to bus B7 which is the bus immediately preceding bus B71. This development continues until the power sources are reached. When bus B72 is developed, it is only necessary to do the development back to bus B7. From that point on, the development done on bus B7 for bus B71 is applicable.

When electrical power faults to power plant components are being modeled, they are described in terms of faults in cabling or electrical components between the component of interest and the first electrical bus or faults in the first electrical bus. Faults in the first bus encountered are described in the development of the electrical system.

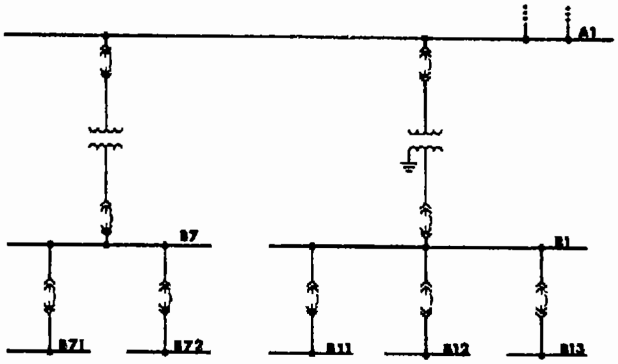


Figure 3.1-2. Example Electrical System Drawing

3.2 Treatment of Actuation Systems and Control Circuits

3.2.1 Overview

Actuation systems continuously monitor plant and equipment status and automatically initiate protective actions based on the detection of abnormal plant conditions. There are two basic types of logic used in actuation systems: "hindrance" logic and "transmission" logic.

In an actuation system using hindrance logic, the output signal is normally "high" (e.g., +12 Vdc) and a trip or actuation command is initiated when the logic output signal goes "low" (e.g., 0 Vdc). Thus a trip signal will automatically be initiated when a signal wire fails open or shorted to ground, when an electronic module is removed from service, or when control power is lost. The failsafe mode of hindrance logic is therefore to generate a trip signal. The reactor protection system (RPS) uses hindrance logic.

In an actuation system using transmission logic, the output signal is normally "low" (e.g., 0 Vdc) and a trip or actuation command is initiated when the logic signal goes "high" (e.g., + 12 Vdc). With transmission logic, no trip or actuation command is initiated on loss of control power or removal of an electronic module from service. The failsafe mode of transmission logic is therefore to *not* generate a trip signal. Actuation systems for some engineered safety feature (ESF) fluid systems use transmission logic.

Both hindrance and transmission logic systems generate on output based on a comparison of two or more input channels in a specific manner (e.g., 2-out-of-3, 1-out-of-2 twice, etc.). The output device of an actuation system is usually a relay coil or load driver which interfaces with contact pairs in the control circuits for specific components. Figure 3.2-1 illustrates the basic function elements of an actuation system. In this particular example, there are four independent input channels and two output channels.

A control circuit implements commands for component actuation. It includes devices (e.g., control switches, contact pairs) necessary to interface with the operator and the actuation system. It also includes protective circuitry, interlocks, and other circuitry which are not considered part of the actuation logic, but which are necessary for component protection, to restrict component operation or to otherwise control component operations. A control circuit is typically associated with a single component. This is in contrast to an actuation system which may provide an actuation input to the control circuits of many components.

Failure of a control circuit may cause (1) an inability to change the operating state of a component, or (2) an unintended change in the operating state of a component. Components that interface *directly* with a control circuit typically include circuit breakers (e.g., medium-voltage switchgear 480 Vac magnetic motor starters), some valves (e.g., solenoid-operated valves and pneumatic/hydraulic valves) and some dampers (e.g., pneumatic/hydraulic dampers). These will be referred to as "directly actuated components." Other components such as pumps, fans, and motor-operated valves or dampers do not have a direct interface with a control circuit and will be referred to as "ultimately actuated components." Their operation is controlled by an intermediate component that has a direct interface with a control circuit. An example of a control circuit is shown in Figure 3.2-2. This particular control circuit directly actuates a circuit breaker, and a medium-voltage motor (e.g., for a large pump) is the ultimately actuated component. The AUTO STOP and AUTO START contact pairs form the interface with the actuation system.

The relationship among ultimately and directly actuated components and the associated control circuit and actuation system is shown in Figure 3.2-3. Also shown in this figure are the potential interface contributors to control circuit and actuation system failure.

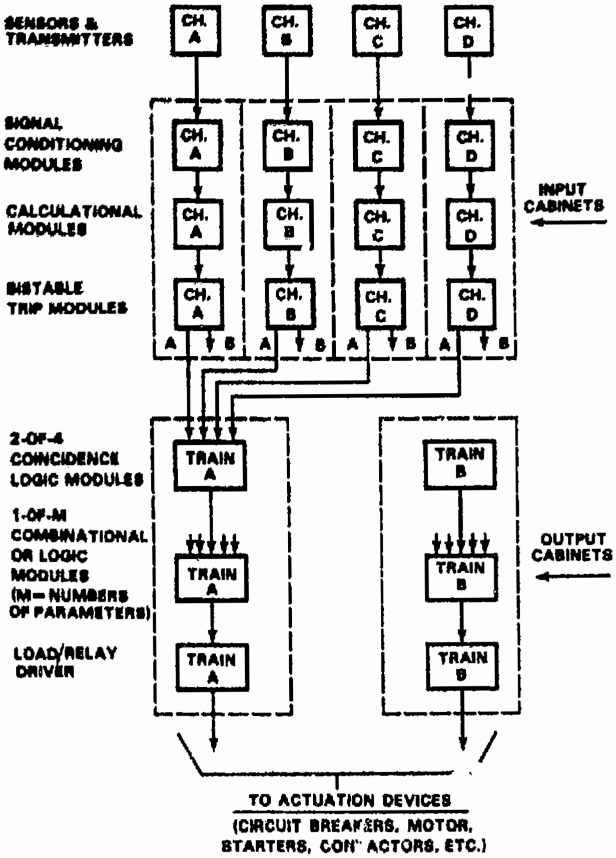

SENSORS & TRANSMITTERS
CH. A
CH. B
CH. C
CH. D
SIGNAL CONDITIONING MODULES
CALCULATIONAL MODULES
BISTABLE TRIP MODULES
INPUT CABINETS
A
B
2-OF-4 COINCIDENCE LOGIC MODULES
1-OF-M COMBINATIONAL OR LOGIC MODULES (M= NUMBERS OF PARAMETERS)
LOAD/RELAY DRIVER
TRAIN A
TRAIN B
OUTPUT CABINETS
TO ACTUATION DEVICES
(CIRCUIT BREAKERS, MOTOR, STARTERS, CON' ACTORS, ETC.)

Figure 3.2-1. Example Actuation System Functional Block Diagram

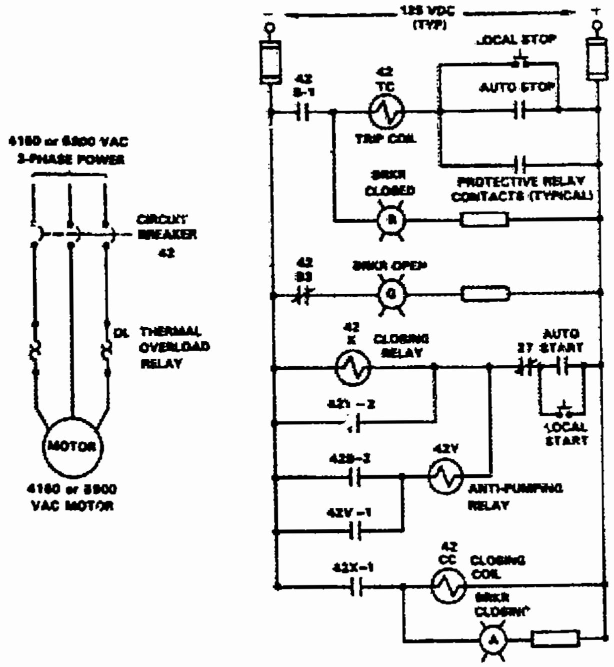


Figure 3.2-2. Example of a Control Circuit for a Medium-Voltage Circuit Breaker

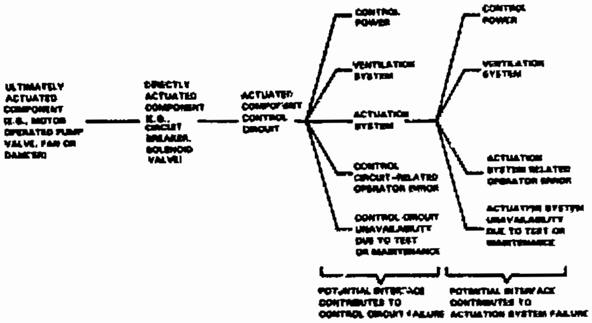

ULTIMATELY ACTUATED COMPONENT (E.G., MOTOR OPERATED PUMP VALVE, FAN OR DAMPER)
DIRECTLY ACTUATED COMPONENT (E.G., CIRCUIT BREAKER, SOLENOID VALVE)
ACTUATED COMPONENT CONTROL CIRCUIT
CONTROL POWER
VENTILATION SYSTEM
ACTUATION SYSTEM
CONTROL CIRCUIT-RELATED OPERATOR ERROR
CONTROL CIRCUIT UNAVAILABILITY DUE TO TEST OR MAINTENANCE
CONTROL POWER
VENTILATION SYSTEM
ACTUATION SYSTEM RELATED OPERATOR ERROR
ACTUATION SYSTEM UNAVAILABILITY DUE TO TEST OR MAINTENANCE
POTENTIAL INTERFACE CONTRIBUTES TO CONTROL CIRCUIT FAILURE
POTENTIAL INTERFACE CONTRIBUTES TO ACTUATION SYSTEM FAILURE

Figure 3.2-3. Interfaces Among Actuated Components, Control Circuits, Actuation Systems, Support Systems, and Operating Personnel

3.2.2 Modeling Control Circuits

A basic approach for modeling control circuits is to decompose the circuit into "networks" and "signal paths." (Figure 3.2-4 illustrates the use of these terms.) A fault tree which describes the logical combination of signal path failures that can cause the network and subsequently the control circuit to fail is then developed. The result is a fault tree which describes control circuit failure in terms of signal path failures. This section describes some of the major considerations in modeling control circuits.

3.2.2.1 Identifying the Control Circuit and Control Power Failures That Can Contribute to the Failure Mode of the Directly Actuated Component Being Modeled

The first step in modeling a control circuit is to identify the portion(s) or network(s) of the circuit containing the physical or electrical interface(s) with the directly actuated component.

The directly actuated component may be a circuit breaker, solenoid valve, or a pneumatic/hydraulic valve or damper which may be in one of two positions: open or closed. Generally, it is a simple matter to determine the control circuit failure that may contribute to a specific failure mode of the directly actuated component. For example, consider the 480 Vac magnetic motor starter in Figure 3.2-5 that has an energize-to-close control circuit and normally open main contacts (the main contacts are considered to be a "circuit breaker"). Faults that prevent completing the control circuit and energizing the magnetic starter are of interest when modeling failure of the main contacts in the open position. Such faults may include open circuits, shorts to ground, and loss-of-control power. If the main contacts were assumed to fail closed, faults that cause the magnetic starter to be energized are of interest and control power faults, i.e., loss of control power, would *not* be modeled because control power is required to maintain the magnetic starter energized. Likewise, control power success would not be modeled because it is a high probability event and could also introduce incoherence into the fault tree.

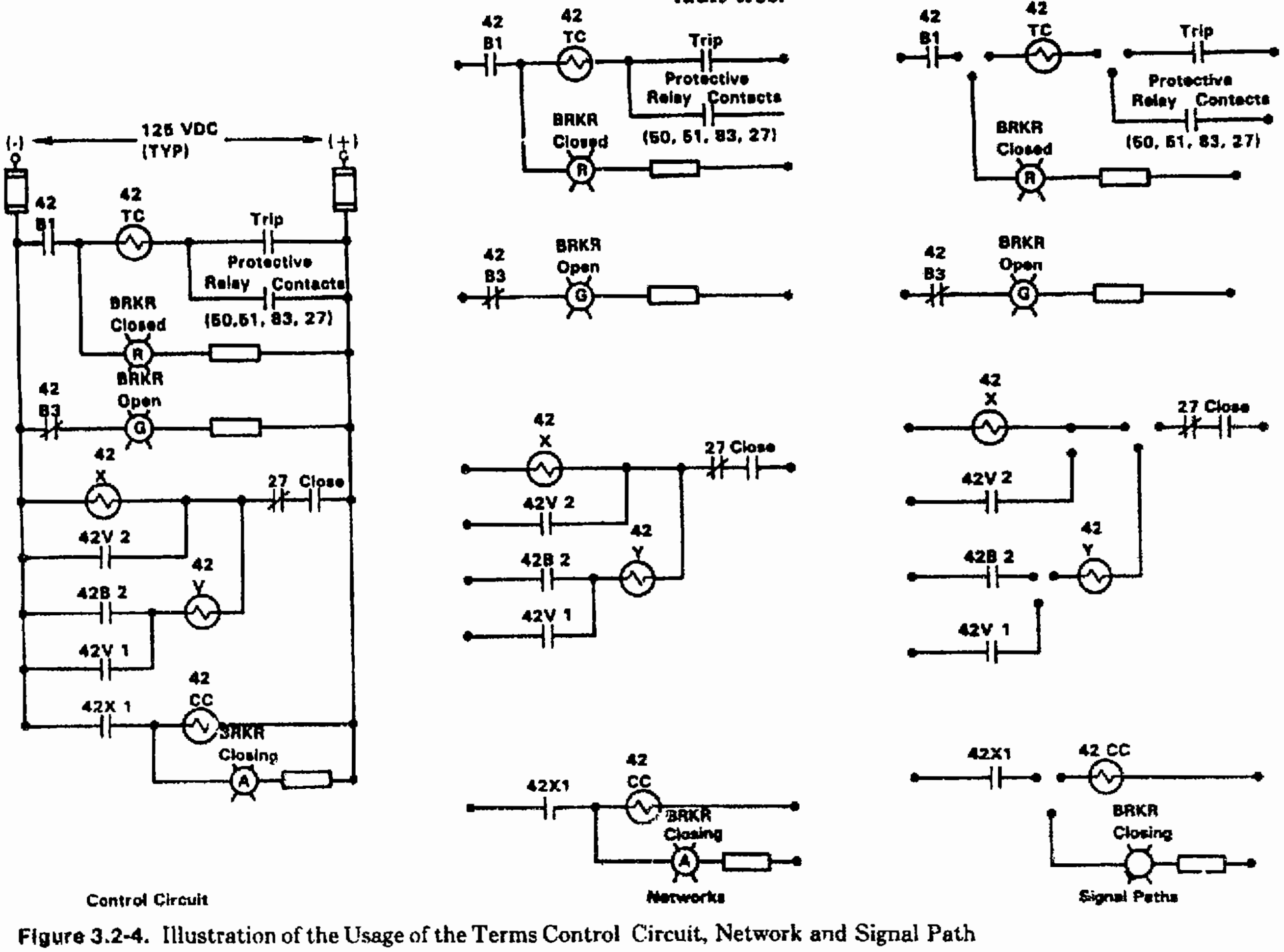


Figure 3.2-4. Illustration of the Usage of the Terms Control Circuit, Network and Signal Path

A more complex case occurs when a control circuit has different networks to perform opening and closing functions and the directly actuated component failure mode being modeled is normally opened/fail opened or normally closed/fail closed. In these cases, it may be necessary to model both portions of the control circuit. Referring to the control circuit in Figure 3.2-2, it can be seen that a normally open circuit breaker can be maintained open if it is never commanded to close (e.g., the network containing the closing coil fails as an open circuit) or if an inadvertent trip command is sent (e.g., the network containing the trip coil fails as a complete circuit).

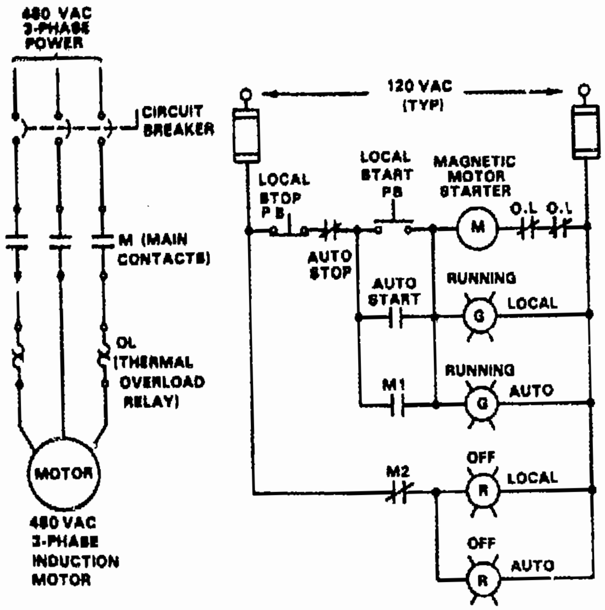


Figure 3.2-5. Example of an Energize-to-Close Control Circuit for a 480 Vac Circuit Breaker (Motor Starter)

3.2.2.2 Identifying the Control Circuit Components to be Modeled

An open circuit condition may be caused by any component in a signal path; therefore, all open circuit component faults in a signal path should be combined under an OR gate. A complete electrical circuit is created when all two-position components in a signal path fail in the closed position; therefore, these component faults should be combined under an AND gate. A few components (e.g., cables, relay coils, magnetic starters) have a success mode associated with forming a complete circuit. These components need not be included in the fault tree when failure as a complete circuit is being modeled because their success is a high probability event and, as mentioned earlier, including success events in a fault tree can introduce incoherence.

3.2.2.3 Identifying the Actuation System Failure Mode To Be Modeled

As described previously, an actuation system usually controls the operation of one or more pairs of contacts in a control circuit. As the fault tree model of the control circuit is developed, the failure mode of individual contact pairs (e.g., fail opened or fail closed) will be defined. Knowing the failure mode of the interfacing contact pair and the type of actuation system logic, the corresponding actuation system failure mode can be determined from Table 3.2-1.

Table 3.2-1. Actuation System Failure Mode To Be Modeled

		STATUS OF INPUT SIGNAL TO CONTACT PAIR				
		1	1	0	0	NORMAL
		1	0	1	0	FAILED
CONTACT PAIR FAILURE MODE BEING MODELED	Fail by Changing Position (OC or CO)	▨	Loss of Output Signal	Spurious Output Signal Generated	▨	
	Fail as-is (OO or CC)	Output Signal Maintained	▨	▨	No Output Signal Generated	
		Hinderance Logic		Transmission Logic		

3.2.3 Modeling Actuation Systems

An actuation system should be modeled as one of the potential contributors to individual control circuit failure (see Figure 3.2-3). This section describes some of the major considerations in developing the actuation system fault model.

3.2.3.1 Determining the Level of Detail To Be Included in the Actuation System Fault Tree

A relatively simple approach for modeling an actuation system is to base the model on the level of detail available in a functional block diagram of the system (see Figure 3.2-1). The system is then decomposed into a series of "signal paths" and "nodes" which are traced from the output devices (e.g., load drivers or relay coils) back to the input sensors. This level of detail allows the major elements of the actuation system to be modeled without having to develop the details of solid-state or relay-type logic. In addition, important interfaces with control power, emergency ventilation systems, and plant personnel can be readily developed. If greater modeling detail is desired, the method described previously for modeling control circuits can also be applied to relay-type actuation systems.

3.2.3.2 Identifying the Type of Actuation System and Failure Mode To Be Modeled

As described previously, there are two basic types of actuation system logic: hindrance and transmission. The ᴾctuation system failure mode to be modeled can be determined from Table 3.2-1 based on the effects on ιhe associated control circuits.

3.2.3.3 Modeling Actuation System Control Power Faults

Unlike control circuits which usually have only a single control power source, actuation systems usually have a separate and independent control power source for each instrument channel. Considering the example actuation system in Figure 3.2-1, input channels A, B, C, and D would likely be powered respectively from divisions A, B, C, and D of the 125 Vdc electric power system. Output trains A and B would likely be powered from 125 Vdc divisions A and B, respectively. In this example, loss of dc division A may cause the failure of input channel A and output train A. In contrast, loss of dc division D may only cause the failure of input channel D.

The separation and independence of control power sources must be carefully modeled in the actuation system fault tree. When modeling the system at the functional block diagram level of detail, control power requirements should be defined for each signal path between system nodes.

3.2.4 Impact of Ventilation System Failure on Control Circuits and Actuation Systems

Failure of an equipment room ventilation system will usually cause the room in question to heat up. Elevated temperature conditions may cause control circuit and/or actuation system fa'lure. The specific failure(s) must be determined on an individual case basis.

The time of control circuit or actuation system failure following ventilation system failure must be considered before deciding to develop ventilation system faults. These faults need not be modeled if the time frame being analyzed is short in comparison to the time it may take for a ventilation system failure to cause control circuit or actuation system failure.

3.3 Power Conversion System Fault Trees

Normally, fluid systems are modeled using the pipe decomposition technique described in Section 3.1.2. However, the power conversion system (PCS) in a PWR can be treated in a different manner. There is sufficient industry data available to determine PCS unavailability due to independent causes. Thus, in keeping with the rule of thumb of developing a fault tree to a level commensurate with the available data, it is appropriate to handle PCS failure due to independent failure as a basic event. It is necessary, however, to develop PCS failure which is caused by a PCS support system in order to properly account for common cause failures with other front-line systems in the accident sequence under consideration. Figure 3.4-1 shows how the PCS is modeled.

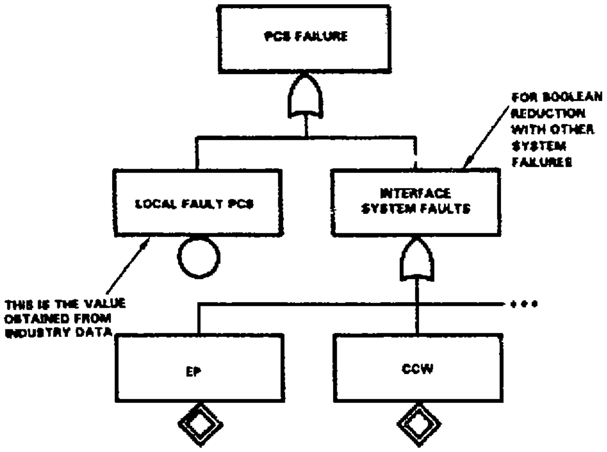

PCS FAILURE
FOR BOOLEAN REDUCTION WITH OTHER SYSTEM FAILURES
LOCAL FAULT PCS
INTERFACE SYSTEM FAULTS
THIS IS THE VALUE OBTAINED FROM INDUSTRY DATA
EP
CCW

Figure 3.3-1. Example of Power Conversion System Modeling

3.4 Modeling Continuously Operating Systems

Frequently, systems which are required for emergency response in nuclear power plants are also used during power operation of the plant. Thus, following most initiating events, these systems are already in operation. It is necessary to take account of this aspect of operation of these systems in order to properly model the normally operating system and remove unnecessary conservatism from the analysis. The following discussion addresses this topic and provides guidance on how to proceed in model development.

It is relatively easy to identify those systems in the plant which perform both safety functions and functions related to power operation. Some examples include the Chemical and Volume Control System, the Component Cooling Water System, many portions of the electrical system, etc. Once these systems have been identified, it is necessary to define any slight changes in equipment alignment or operating mode necessary to go from normal power operation to emergency operation. Often, these changes affect only a few valves and some standby pumps.

The models for these systems do not need to consider valves which are already properly aligned except for a spurious actuation of the valve to an incorrect position. Pumps which are already operating need only be evaluated for failure to run and not for failure to start. Electric power to pumps, ventilation systems, etc., already exist and should continue unless the initiating event is a loss of offsite power or a bus failure related to the equipment. The actual model of the system is not much different than if the system were in standby. The major differences come up in the auxiliaries for the components and the failure modes of the components. All equipment must be considered in both models except manual valves (unless these valves are assumed to be able to change position if failure occurs).

To summarize the concerns, power-operated valves in the proper alignment do not get evaluated for actuation system faults except those dealing with improper, spurious signals to valves. These faults are generally improbable unless a signal is expected to be sent to the component. Operating pumps need not be evaluated for failure to start except when the initiating event removed power to the pump (such as loss of offsite power). Manual valves already in proper alignment do not actually change valve position. Valving which must be operated and pumps which are idle are modeled as usual. Electric power systems need only consider spurious circuit breaker openings or shorts since they are aligned as needed at the start of the initiating event, unless the event includes a power loss.

The above model considerations should impact the systems reliability more than they impact the actual system failure model. This is not different from what might be expected since a standby system model includes a startup phase and a running phase, whereas an operating system model has only a small startup phase, if any, and a running phase. Thus the models may not be that different since most components have failure mechanisms in both the startup and running phases, but the reliability may be different due to a reduction in failures attributable to the startup phase in the operating system model. If startup failures do not dominate the system failure probability, then the system models would give similar results; however, startup failure probabilities are often dominant.

3.5 Modeling of Human Errors in the Fault Tree

An important aspect of any system analysis is the analysis of the human interactions with the system. It is not uncommon for human action (or inaction) to dominate system failure. The two types of human interaction which are of importance in modeling system failure are test and maintenance restoration errors and operator error in response to accident sequences.

The analysis of component unavailability due to test and maintenance is carried out as follows. First, using the system piping and instrumentation diagram and the test and maintenance procedures , the system alignment for each test and maintenance act which may be performed is determined. Then, it is determined whether each test and maintenance alignment requires that component to be put in a nonsafety position. For each component put into a nonsafety position, both the unavailability during test or maintenance and potential restoration errors are modeled. The restoration of a component may or may not be dependent upon the restoration of other components, depending on the procedures used for restoring the components. This determination must be made by the analyst. Figure 3.5-1 shows a typical fault tree development for test and maintenance. Similar development is included for each test and maintenance act. It is informative to label events according to the procedure being used. In Figure 3.5-1 "TP-A-4" stands for Test Procedure A, Step 4, and MP-A-7 stands for Maintenance Procedure A, Step 7.

The contribution of operator error to system failure in response to a given accident is treated with basic events at the component level. That is, under each component which must be manually operated during a particular accident sequence is a basic event which models component failure due to operator error. If two or more operator actions during an accident sequence are dependent, e.g., if the actions are performed in the same step of an operating procedure, the basic events for operator error for these actions are given the same label. Spurious errors which may be instigated by an operator, e.g., the inadvertent actuation of a component, are generally not included in the analysis. Figure 3.5-2 shows a typical fault tree development for operator error. Similar development is included for each operator action. (NOTE: EOP-4-2 stands for Emergency Operating Procedure 4, Step 2.)

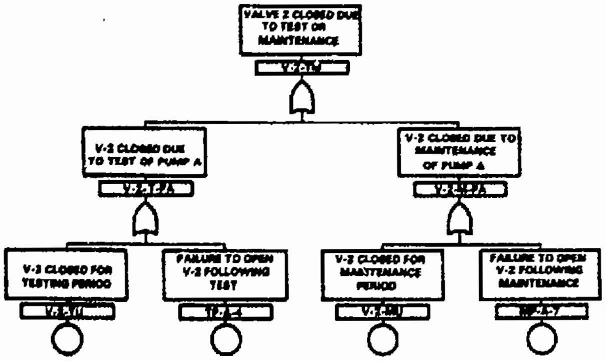

VALVE 2 CLOSED DUE TO TEST OR MAINTENANCE
V-2 CLOSED DUE TO TEST OF PUMP A
V-2 CLOSED DUE TO MAINTENANCE OF PUMP A
V-2 CLOSED FOR TESTING PERIOD
FAILURE TO OPEN V-2 FOLLOWING TEST
V-2 CLOSED FOR MAINTENANCE PERIOD
FAILURE TO OPEN V-2 FOLLOWING MAINTENANCE

Figure 3.5-1. Typical Fault Tree Development for Test and Maintenance

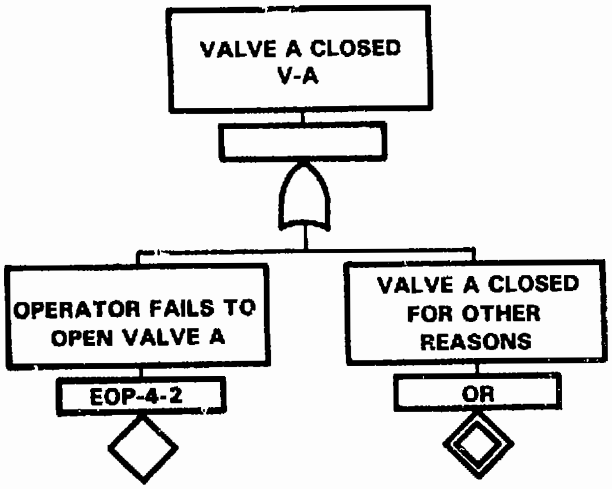

VALVE A CLOSED
V-A
OPERATOR FAILS TO OPEN VALVE A
EOP-4-2
VALVE A CLOSED FOR OTHER REASONS
OR

Figure 3.5-2. Typical Fault Tree Development for Operator Error

4. Human Reliability and Procedural Analysis Methods

Considerable work has been done by Swain, Bell, and Guttmann to develop techniques and procedures for conducting a human reliability analysis. These are documented, along with examples, in NUREG/CR-2254, SAND81-1655, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants." [12] Basic techniques of human reliability analysis are documented in NUREG/CR-1278, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications." [5] The user is referred to these documents for detailed methodological guidance.

Brief summaries of selected tasks of the human reliability analysis follow.

4.1 Task Analysis

A task analysis of each task contributing to the candidate dominant accident sequences is performed. This forms the basis for the development of human reliability event tree models.

A formal breakdown of the procedure into tasks or smaller units of behavior is done; that is, for each step in the procedure that was identified for analysis by the system analysts, individual units of operator performance must be identified, along with other information germane to these performances. These individual units of performance constitute elements of behavior for which potential errors can be identified. In other words, a large task made up of a set of steps should be broken down in order that errors associated with each step might be identified.

All of this information must then be entered into a task analysis table. The format of this table is not specified other than that it contain all the information pertinent to later parts of the analysis. In most cases, the necessary information will consist of such items as the piece of equipment on which an action is performed, the action required of the operator, the limits of his performance, the locations of the controls and displays, and explanatory notes. If different tasks are to be performed by different operators, the allocation of tasks to personnel can be indicated in the task analysis table, or separate task analysis tables can be made for each operator. The detail in the task analysis and the amount of information recorded should facilitate recapitulation at a later date of the rationale for the HEP estimates that were used in the analysis.

Once the breakdown of task steps has been done, errors likely to be made must be identified for each step. The steps should be listed chronologically. Based on the characteristics of the actual performance situation, the human reliability analyst must determine which types of errors the operator is likely to make and which he is not. For example, if an operator is directed by a set of written procedures to manipulate a valve and that valve is fairly well isolated on the panel, is of a different shape than other valves on the same panel, and has been very well labelled, the human reliability analyst may determine that errors of selection are not to be considered in this case. He should also have determined that an error of omission made in following the written procedures might be made. Extreme care should be exercised in deciding which errors, if any, are to be completely discounted for an analysis. Rather than failing to consider a "questionable" error, one the human reliability analyst thinks may be unlikely, the analysis should be completed including it.

4.2 Development of a Human Reliability Event Tree

Human reliability event trees are developed for each task associated with the candidate dominant accident sequences. These are developed as follows.

Each error defined as likely in the task analysis is entered as the right limb in a binary branch of the human reliability analysis (HRA) event tree. Chronologically, in the order of their potential occurrence, these binary branches from the limbs of the HRA event tree, with the first potential error starting from the highest point on the tree at the top of the page. An example of an HRA event tree is shown in Figure 4.2-1.

Any given task appears as a two-limb branch, with each left limb representing the probability of success and each right limb representing the probability of failure. Once a task is diagrammed as having been completed successfully (or unsuccessfully), another task is considered; the binary branch describing the probability of the success (or failure) of the second event extends from the left (or right) limb of the first branch. Thus every limb following the initial branching depicts a conditional probability.

In an IREP analysis, we are usually interested in determining the probability of error on a single task or in the probability that for a set of tasks, none or all will be performed incorrectly. For the first case, no HRA event tree need be developed unless performance on that single task is affected by other factors the probabilities of which should be diagrammed. A description of the task and knowledge of the performance shaping factors are sufficient for entering Chapter 20 of NUREG/CR-1278 [5] to determine a single human error probability. For the second case, in which we want to know the probability of all tasks' being performed without error, a complete-success path through the HRA event tree is followed. Once an error has been made on any task, a criterion for system failure has been met. Given such a failure, no further analysis along that limb is necessary at this point. In effect, probabilities of event success that follow a failure and that still end in a system success probability constitute recovery factors and should be analyzed later in the analysis, if at all. Thus we have HRA event trees that are developed along the complete-success path only. This does not indicate that we think that this is the only combination of events possible; it indicates only that in the initial analysis we go no further once system failure has been met.

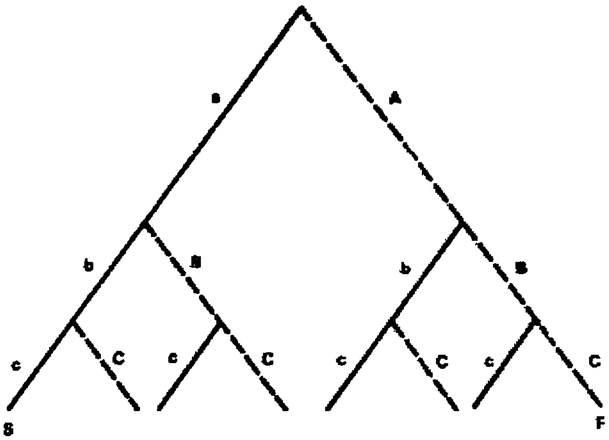


Figure 4.2-1. An Example of HRA Event Tree Diagramming. (Solid lines represent success; dashed lines, error.)

4.3 Assigning Nominal Human Error Probabilities

The first step in quantifying the human reliability analysis event tree is to assign nominal human error probabilities to each event on the tree. Briefly, this is done as follows.

First, the task itself must be categorized. The analyst determines whether he is dealing with an operator manipulating valves, performing a check of another's work, using a written procedure, or attempting some other type of task. A description of each error identified for every task in the task analysis should be looked up in Chapter 20 of the Handbook (NUREG/CR-1278 [5]). That is, the description that most closely approximates the situation under consideration should be identified. In some cases, the description in Chapter 20 will detail a scenario that differs slightly from the one in the analysis. If the differences in specifics are not large, the analyst may judge that they are so minor as not to affect materially the use of the human error probability as is. In other cases, the actual situation and the one described in Chapter 20 may reflect tasks that are basically the same but that are performed under different circumstances. The human error probability must then be modified to reflect the conditions of actual task performance. Usually, this is done during the assessment of the performance shaping factors acting on the task.

Expecially for cases in which an estimated HEP other than one found in the Handbook is used, the source for the human error probability entered on the HRA event trees should be recorded, along with the assumptions made in their derivations. For easy reference, this information can be added to the task analysis tables. New columns in the table for the human error probability and its source can be made. This documentation is necessary for many reasons. Other analysts may want to check the similarity of their solutions to those of other problems. Given that the estimates of many of the human error probabilities in the Handbook are numerically identical, these other analysts must have some method for tracing the original analysis. The assumptions should be recorded to prevent the analyst's having to reinvestigate a situation should there be need to refer to an analysis again. Also, in the course of performing a series of analyses on a single facility, some sections of an analysis may be used several times. The analyst must, however, be able to demonstrate that the situations are indeed identical before reproducing part of one analysis to be used without modification in another.

4.4 Assessing the Level of Dependence Among Different Tasks

Dependence may exist among different tasks performed in operating the plant. The analyst must decide the level of dependence among these tasks to properly assign human error probabilities. NUREG/CR-1278 [5] presents a model for considering dependence.

A decision as to whether complete dependence or complete independence applies to a given case can be made relatively easily. That is, it should be obvious if one action is the causal factor for another or if two actions are totally unrelated. Distinctions among intermediate levels of dependence are more difficult to make. First, decide whether dependence exists at all—whether the actions are completely independent. If dependence exists, decide whether complete dependence is appropriate and, if so, to what circumstances it applies. If a judgment is made that the dependence that exists is greater than zero but less than complete, an intermediate level must be assigned. This judgment can be made based on the relation of the actual situation to zero and complete dependence. If a decision is made that the dependence demonstrated by the situation is much closer to zero than to complete dependence, assign a low level of dependence. If, on the other hand, a decision is made that the situation exhibits a degree of dependence that is very close to but not equal to complete dependence, assign a high level of dependence. If a definitive statement cannot be made to the effect that either of the above is true, assign a moderate level of dependence.

The dependence model in NUREG/CR-1278 [5] deals only with the effects and the quantification of positive dependence. If negative dependence is judged to be appropriate to a situation, its effects will have to be determined directly rather than using the dependence model. Also, keep in mind that dependence is not necessarily symmetrical. The same level of dependence may not exist for the success and the failure paths of an HRA event tree.

The model presents some point estimates that may be used in lieu of equations to determine the conditional probabilities of dependent events. These point estimates should only be used when the nominal human error probability is less than or equal to 0.01. In other cases, the equations should be used.

5. Data Base Development Methods

5.1 IREP Generic Data Base

Table 5.1-1 shows the generic reliability data base to be used for the IREP analyses. This has been adapted from information contained in EGG-EA-5887 [13]. In that document, "nominal values" of component failure rates and error factors, assumed to be 10% and 90% bounds, were given. Nominal values have been assumed to be medium values for this report. The associated means were calculated from the medians and error factors assuming a lognormal distribution. This data base is to be used for preliminary point estimate screening calculations where the purpose is to rank-order the importance of accident sequences by relative likelihood of occurrence and for propagating uncertainty in failure rate parameters to bound estimates of risk. However, a generic data base cannot provide the resolution that can be obtained from using plant specific data. Therefore, where better resolution is desired (e.g., to evaluate dominant accident sequences), plant specific data should be used wherever possible and practical to augment the generic data base. It should not be considered an unusual circumstance for the estimate of the relative importance of accident sequences to change, depending on whether they are evaluated with the data from the generic data base or with plant-specific data.

The IREP generic data base contains failure rates and demand probabilities for classes of equipment commonly found in nuclear power plant safety systems. Four types of numbers are found in this data base:

- Component standby failure rates, which represent the reciprocal of the mean time to failure of components that are normally in standby.
- Component operating failure rates, which represent the reciprocal of the mean time to failure of components that are normally operating.
- Demand failure probabilities for selected standby component types such as pumps and valves.
- Error factors for each failure rate or demand failure probability representing upper and lower bounds on the value of the reliability parameters (failure rate or demand probability). (These bounds are heuristic rather than statistical; they represent a range of values for each parameter that the parameter can reasonably be expected to assume.)

The failure rates are in units of failures per hour. The demand failure probabilities represent failures per demand of the component. The median and error factor for a component failure mode define a lognormal distribution that describes the uncertainty in the reliability parameter for that failure mode, *if* the error factor is interpreted as representing a 90 percentile region for the parameter. Thus a data base containing only a median and error factor can be assumed to imply that the errors are lognormally distributed. This is the suggested interpretation for conduct of the IREP analyses.

The failure rate and demand probability values listed in Table 5.1-1 represent both mean and median values, all given to one significant figure. Mean values are required for point estimates. The mean value is related to both the median and error factor. Table 5.1-2 shows (for error factors of 3, 10, 30, and 100), multipliers to the median to compute the mean. For instance, referring to Table 5.1-1, the median demand failure probability for motor-operated valves failing to open is 1E-3/demand, with error factor 10. Using the multiplier from Table 5.1-2 for error factor 10 results in an estimate of 2.66 E-3 for the mean demand failure probability (rounded to 3E-3). The general expression to compute the multiplier from the error factor is:

$$M = \mathrm{EXP}\left[\left(\frac{1}{1.645}\ln[\mathrm{E.F.}]\right)^2/2\right],$$

where M is the multiplier and E.F. is the error factor associated with a *90%* confidence interval (if a different percentile confidence interval is used, the constant 1.645 must be adjusted accordingly).

Another caution in using the failure data of Table 5.1-1 involves the meaning of the demand failure probabilities contained therein. Although these data are listed as demand failure probabilities, in reality they were originally generated simply as a matter of computational convenience, by multipling a failure rate by one half the number of hours in an (assumed) one month test period, i.e., using the expression

$$\bar{q} = \tfrac{1}{2}\,\lambda\,T,$$

where $\bar{q}$ is the demand failure probability, λ is the originally derived failure rate, and T is the number of hours in one month. These values should not be construed to represent true demand failure probabilities, which would depend only on the number of times that the component was cycled from standby to operating and which would be *independent* of the time between tests of operability of the component. For components whose test period is not substantially different from one month (i.e., up to five or six months) the demand failure probability is considered adequate and should be used as stated in the data base. For components whose test period is on the order of a refueling cycle, however, it is suggested that the upper bound on the demand failure probability be used as the computational *median*. The rationale for this is that the demand probability and error factor were generated from a number of different data sources, containing examples of components that were tested at a variety of periods, including (presumably) test periods as long as a refueling cycle. Standby component failure probabilities for most components are probably better modeled as the sum of two contributions — one time dependent and one demand related, as:

$$q_c = q_d + 1/2\,\lambda_s T\ .$$

Assuming that failure mechanisms include both demand related and standby time related failure mechanisms, the upper bound is assumed to represent those components that were tested at the longer test periods. Data are not available to either substantiate or refute this assumption. In the absence of such data, the assumption appears to be reasonable.

Table 5.1-1. Generic Data Base*

Component and Failures Modes	Mean	Median	Error Factor	Remarks
1. Pumps				
1.1 Motor-driven				Pump and motor; excludes control circuits.
1.1.1 Failure to start	3E-3/d	1E-3/d	10	
1.1.2 Failure to run, given start				
1.1.2.1 Normal Environment	3E-5/h	1E-5/h	10	
1.1.2.2 Extreme Environment	3E-3/d	1E-3/h	10	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)	3E-2/d	1E-2/d	10	
1.2.2 Failure to run, given start	1E-5/h	1E-5/h	3	
1.3 Diesel-driven				Pump, diesel, lube oil system, fuel oil, suction and exhaust air, and starting system.
1.3.1 Failure to start	1E-3/d	1E-3/d	3	
1.3.2 Failure to run, given start	8E-4/h	1E-4/h	30	
2. Valves				Catastrophic leakage or "rupture" valves 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	3E-3/d	1E-3/d	10	
2.1.2 Failure to remain open	1E-7/h	1E-7/h	3	
2.1.3 Failure to close	3E-3/d	1E-3/d	10	
2.1.4 Internal leakage (catastrophic)	5E-7/h	1E-8/h	100	
2.2 Solenoid-operated				
2.2.1 Failure to operate	1E-3/d	1E-3/d	3	
2.3 Air/Fluid-operted				
2.3.1 Failure to operate	3E-3/d	1E-3/d	10	
2.4 Check valves				
2.4.1 Failure to open	1E-4/d	1E-4/d	3	
	3E-7/h	1E-7/h	10	Hourly rate is based on one actuation per month.
2.4.2 Failure to close	1E-3/d	1E-3/d	3	
	3E-6/h	1E-6/h	10	Hourly rate is based on one actuation per month.
2.4.3 Internal Leakage				
2.4.3.1 Minor	3E-5/h	1E-6/h	10	
2.4.3.2 Catastrophic	5E-7/h	1E-8/h	100	Valve initially closed, then failed.
2.5 Vacuum breakers				Applies only to BWRs.
2.5.1 Failure to open	1E-5/d	1E-5/d	3	
2.5.2 Failure to close	1E-5/d	1E-5/d	3	
2.6 Manual valves				Failure to operate is dominated by human error; hourly rate is based on one actuation per month.
2.6.1 Failure to operate	1E-4/d	1E-4/d	3	
	3E-7/h	1E-7/h	10	

*Adapted from EGG-EA-5887. [13]

Table 5.1-1. (continued)

Component and Failures Modes	Mean	Median	Error Factor	Remarks
2.7 Code safety valves				Applies only to PWRs; premature opening treated as an initiating event.
2.7.1 Failure to open	1E-5/d	1E-5/d	3	
2.7.2 Failure to close, given open	1E-2/d	1E-2/d	3	
2.8 Primary safety valves				Applies only to BWRs.
2.8.1 Failure to open	1E-5/d	1E-5/d	3	
2.8.2 Failure to close, given open	3E-2/d	1E-2/d	10	
2.9 Relief valves				
2.9.1 Failure to open	3E-4/d	1E-4/d	10	
2.9.2 Failure to close,given open	2E-2/d	2E-2/d	3	
2.10 Stop check valves				
2.10.1 Failure to open	1E-4/d	1E-4/d	3	
3. Switches				Where torque/limit switches are used as part of pumps/valves, switch failure rate is included in pump/valve failure rate.
3.1 Torque				
3.1.1 Failure to Operate	1E-4/d	1E-4/d	3	
3.2 Limit				
3.2.1 Failure to operate	1E-4/d	1E-4/d	3	
3.3 Pressure				
3.3.1 Failure to operate	1E-4/d	1E-4/d	3	
3.4 Manual				
3.4.1 Failure to transfer	3E-5/d	1E-5/d	10	
4. Other				
4.1 Circuit breaker				For sizes 4 kV and smaller.
4.1.1 Failure to transfer	3E-3/d	1E-3/d	10	
4.1.2 Spurious trip	3E-5/d	1E-5/d	10	
4.2 Fuses				
4.2.1 Premature open	3E-6/d	1E-6/h	10	
4.3 Buses				
4.3.1 All modes	1E-8/h	1E-8/h	3	
4.4 Orifices				WASH-1400 data; no alternate data available.
4.4.1 Failure to remain open (plug)	3E-4/d	3E-4/d	3	
4.4.2 Rupture	3E-8/h	1E-8/h	10	
4.5 Transformers				
4.5.1 All modes	1E-6/h	1E-6/h	3	

*Adapted from EGG-EA-5887. [13]

Table 5.1-1. (continued)

Component and Failures Modes	Mean	Median	Error Factor	Remarks
4.6 Emergency diesel (complete plant)				Engine frame and associated moving parts, generator coupling, governor, output breaker, static exciter, lube oil system, fuel oil, intake and exhaust air, starting system; excludes starting air compressor and accumulator, fueling storage and transfer, load sequencers, and synchronizers. Failure to start is failure to start, accept load, and run for 1/2 hour; failure to run is failure to run for more than 1/2 hour, given start.
4.6.1 Failure to start	3E-2/d	3E-2/d	3	
4.6.2 Failure to run, given start (emergency conditions)	2E-3/h	1E-3/h	10	
4.7 Relays				
4.7.1 Contacts fail to transfer (open or close)	3E-4/d	1E-4/d	10	
4.7.2 Coil failure (open or short)	3E-6/h	1E-6/h	10	
4.8 Time Delay Relays				
4.8.1 Premature transfer	3E-4/d	1E-4/d	10	
4.8.2 Fails to transfer				
4.8.2.1 Bimetallic	5E-6/h	5E-6/h	3	Non-consensus source. Data source is MIL-HDBK-217B [17]. Fail-to-transfer rates are not currently available for non-bimetallic time delay relays.
4.9 Battery power system (wet cell)				Assumes out-of-spec cell replacement.
4.9.1 Fails to provide proper output	1E-6/h	1E-6/h	3	
4.10 Battery charger				
4.10.1 Failure to operate	1E-6/h	1E-6/h	3	
4.11 DC motor-generators				
4.11.1 Failure to operate	3E-6/h	1E-6/h	10	
4.12 Inverters				
4.12.1 Failure to operate	1E-4/h	1E-4/h	3	
4.13 Wires (per circuit)				Consistent with IEEE-500 data for 1000 circuit feet
4.13.1 Open circuit	3E-6/h	1E-6/h	10	
4.13.2 Short to ground	3E-7/h	1E-7/h	10	
4.13.3 Short to powered	3E-8/h	1E-8/h	10	
4.14 Solid state devices				For more detailed information, see MIL-HDBK-217C [18].
4.14.1 High power applications	3E-6/h	1E-6/h	10	
4.14.2 Low power applications	3E-6/h	1E-6/h	10	
4.14.3 Bistables	3E-7/d	1E-7/d	10	

*Adapted from EGG-EA-5887. [13]

Table 5.1-1. (concluded)

Component and Failures Modes	Mean	Median	Error Factor	Remarks
4.15 Terminal Boards				Values given are per terminal.
4.15.1 Open circuit	3E-7/h	1E-7/h	10	
4.15.2 Short to adjacent circuit	3E-7/h	1E-7/h	10	
4.16 Dampers				
4.16.1 Failure to operate	3E-3/d	1E-3/d	10	
4.17 Air coolers				
4.17.1 Failure to operate	1E-5/h	1E-5/h	3	Not consensus data. Plant-specific from ANO-1 IREP study.
4.18 Heat exchangers				
4.18.1 Tube leak (per tube)	3E-9/h	1E-9/h	10	
4.18.2 Shell leak	3E-6/h	1E-6/h	10	
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	3E-5/h	1E-5/h	10	
4.20 Scram systems				
4.20.1 Failure to scram	3E-5/d	3E-5/d	3	
4.21 Instrumentation (general)				
4.21.1 Failure to operate	3E-6/h	1E-6/h	10	

*Adapted from EGG-EA-5887. [13]

Table 5.1-2. Multipliers to Compute Mean From Median

Error Factor	Multiplier
3	1.25
10	2.66
30	8.48
100	50.33

5.2 Generation of Plant-Specific Data

Requirements for plant-specific data include the following:

- Estimation of failure rates or demand failure probabilities for selected components such as diesel generators, batteries, or components in dominant cut sets of dominant accident sequences.
- Standby safety system test information, including the set of components tested by a specified test, the failure modes tested for and not tested for, and the test period for each component.
- Component outage data, including test periods and test time distributions, scheduled maintenance frequencies and maintenance time distributions, and unscheduled repair frequencies and repair time distributions.

These data items can, in principle, all be estimated from raw plant data. The quality of the estimate may vary from plant to plant depending on the types of, and availability of, records kept by the plant.

Raw data sources from which to estimate the above-defined plant specific risk model parameters include:

- Plant technical specifications, including Limiting Conditions for Operation and surveillance requirements.
- Licensing Event Reports
- Plant Operating Procedures
- Plant Maintenance Records
- Communication with plant operating personnel and other plant records.

The plant technical specifications define the maximum test period and allow outage time for each safety system. In addition, they may prohibit certain safety system configurations, e.g., removing both parallel trains of a two-train system simultaneously. The Licensing Event Reports contain summary component failure information that may be useful for estimating component failure rates. The plant-operating procedures contain information on the components tested by a specific test, the component failure modes tested for and those not tested for by the test procedure, information on test periods, and whether or not testing is staggered or sequential. The plant maintenance records contain information on scheduled and unscheduled outage frequencies and times. Communications with plant- operating personnel is a valuable source of information not contained in one or more of the aforementioned sources. Table 5.2-1 summarized the sources of plant-specific raw data, the requirements for these data, and the types of data that are obtained from the sources.

Standard statistical techniques will be used to estimate the plant-specific risk model parameters from the data types. In those cases where operating personnel are queried for quantitative estimates, it is desirable to obtain upper and lower bound estimates as well as an "expected" estimate. (Here, the term "expected" is used in a nonstatistical sense and has a meaning that is closer to "most likely" than to the expected value estimator.)

The risk model parameters to be estimated are of four basic types:

- Frequency of occurrence (failure rates, frequency of repair).
- Demand probability.
- Mean outage duration (test time, maintenance outage time).
- Error factor.

Example estimators for the *mean* values of the first three items above are given in the following subsections. Other estimation schemes (e.g., Baysian) are acceptable if appropriately applied.

Error factor estimates can be obtained either approximately from visual scrutiny of the data or by using an accepted statistical technique. Medians can be estimated either directly from the data or by using the mean and error factor.

Several cautions should be observed when estimating model parameters from plant specific data:

- For in-plant data the explicit definition of a component is critical. For instance, does the definition of an MOV include the valve driver and associated logic? Does the definition of a motor-driven pump include the motor as well as the pump? Plant specific component failure rates consistent with generic failure rates can only be estimated if the number of failures are accurately counted — and they can only be accurately counted if the boundaries of the component are explicitly defined. The generic IREP data base defines pumps to include both the pump and associated motor, but not the associated actuation logic necessary to start the pump automatically. Valves are defined in this data base to include the valve driver but not the associated logic.
- Information in the operating procedures should be used preferentially over information in the

Technical Specifications, and information communicated from plant personnel should be used preferentially over information from the operating procedures. Plants may have operating procedures that require more frequent tests than the requirements specified in the Technical Specifications. Plants may also operate in a way that exceeds the requirements of the operating procedures by testing more frequently than the operating procedures specify.

- If an unscheduled repair frequency is estimated from plant data for a component, it should be checked against the component failure rate. The unscheduled repair frequency should be larger than the failure rate since it contains instances where repair was performed on component degradation and insipient failure as well as catastrophic failure. The component failure rate is developed (theoretically) only from catastrophic failures.

Regarding the last point above, let λ_R = unscheduled repair frequency and λ_c = component failure rate. Then if $\lambda_R \geq \lambda_c$:

- Use λ_R to estimate the unscheduled repair outage contribution of the component.
- Use λ_c to estimate the component hardware contribution.

If $\lambda_R < \lambda_c$, then:

- Use λ_c for both the unscheduled repair outage contribution and the component hardware contribution.

or

- Show that there is a statistically significant reason to believe that $\lambda_R < \lambda_c$, and use λ_R for both contributions.

It is pointed out that the true value of λ_R can never be less than the true value of λ_c .

However, the above rule will assure conservative estimates in those cases where the data are too sparse to show statistically significant deviations from the normal.

Table 5.2-1. Summary of Plant-Specific Data Requirements, Data Sources, and Type of Data

Data Requirement	Plant Specific Data Source	Data Type
Component Failure Rate or Demand Failure Probability	• Licensing Event Reports • Operating Procedures • Test Records; Discussions/Operating Personnel	• Times between failures • No. of occurrences of the specified failure mode within a defined operating period (from LERs) • No. of trials that could result in specified failure mode during the operating period
System Test Information	• Operating Procedures • Surveillance Requirements • Discussions/Operating Personnel	• Components tested by a specified test • Failure modes tested for/not tested for • Time between tests (test period)
Component Outage Information	• Operating Procedures • Technical Specifications • Maintenance/Outage Records • Discussions/Operating Personnel	• Test periods and test time distribution information • Scheduled maintenance frequencies and outage time distributions • Unscheduled maintenance frequencies and outage time distributions

5.2.1 Mean Frequency of Occurrence

- The data type is a list of times between occurrences
- Sum the times between occurrences, T_i, and divide by the number of occurrences, N, to obtain the mean time between occurrences

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

- An acceptable estimate of the mean occurrence frequency, λ, is the reciprocal of $\overline{T}$

$$\lambda = 1/\overline{T}$$

5.2.2 Demand Failure Probability

- The data types are number of failures within an operating period, and number of trials within that period.
- Divide the number of failures (N_f) by the number of trials (N_t)

$$q_d = N_f/N_t$$

- q_d is the demand failure probability estimate.

5.2.3 Mean Outage Duration

- The data type is a list of outage duration times.
- The estimator is the same as for $\overline{T}$ above.

5.3 Component Reliability Calculations

This section discusses component point estimate unavailability and unreliability calculation expressions. Two basic component reliability measures are commonly calculated to obtain point estimates for fault trees and event trees:

- Component average unavailability, defined as the average probability that a component will not be available to mitigate an accident
- Component reliability, defined as the probability that a component fails before completing the mission for which it is intended.

Although the component average unavailability is the most commonly used reliability measure, it is occassionally necessary to compute the component *pointwise* unavailability to estimate the unreliability of standby components that are never tested. The component pointwise unavailability is defined with respect to some specified time t, and is the probability that the component is not available at t. The average and pointwise unavailability are related; the average unavailability, q, is:

$$q = \frac{1}{T}\int_0^T q(t)dt,$$

where T is some time interval, q(t) is the pointwise unavailability, and q is the average unavailability over the time interval T.

Two types of contributions to component average unavailability are assessed:

- Component failures
- Component outages

The *component failure* contribution arises because the component may fail. The component *outage* contribution arises when the component is removed from service for test, maintenance, or repair.

5.3.1 Component Failure Contribution

Several considerations are important when evaluating the component failure contribution in terms of unavailability or unreliability. The component may normally be in standby, or it may normally be operating. If the component is part of a *standby* safety system, the component average unavailability is estimated using either a time-based failure rate or a demand failure probability for the component failure mode being assessed. A time-based failure rate is appropriate when the failure mechanism is related to the time that the component is in service between checks of its operability (i.e., component tests). The test period, or time between tests, is an important part of the unavailability calculation for such component failure modes. A demand failure probability is appropriate for component failure modes that do not depend on the test period length, but rather are related to the number of times that the component is "demanded," that is, asked to operate. For a component failure mode that is truly demand dependent, the length of the test period is irrelevant.

For *operating* components, one of two risk measures may be required:

- The unavailability of an operating component.
- The mission failure probability of an operating component.

Operating components or subsystems may appear in standby systems, e.g., electric power buses. The average unavailability of such components must be estimated. For components contained in systems required to operate for a specified period of time to mitigate an accident, for instance during the recirculation phase of an accident, the mission failure probability is estimated.

Point estimate reliability computations for standby and operating components are shown in the following subsections.

5.3.1.1 Standby Components

Two models for estimating standby component average unavailability are (1) use a time-based failure rate and (2) use a demand failure probability. The component average unavailability using a time-based failure rate is approximately estimated as:

$$q_c = 1/2\lambda_s T \ ,$$

where q_c is component average unavailability, λ_s is the *standby* failure rate for the component failure mode being evaluated, and T is the test period length. If, for instance, monthly testing is performed, and if λ_s is the reciprocal of the mean time between failures in hours, then T is the number of hours in a month. The approximation formula is adequate if $\lambda_s T \leq 0.1$.

The demand failure probability for failure modes where it is appropriate to use this measure is given directly in the data base. Therefore,

$$q_c = q_d,$$

where q_c is again the component average unavailability and q_d is the demand failure probability.

The unavailability of components in standby is probably more correctly modeled by assuming that such components have both time dependent and demand failure contributions. Thus the component unavailability model is:

$$q_c = q_d + 1/2\,\lambda_s T \ ,$$

where q_c, q_d, λ_s, and T are as previously defined. However, data are not available to estimate both the time dependent and demand related portions of component unavailabilities. The IREP data base does not contain separate time dependent and demand contributions, so the correct model cannot be used. Rather, the correct model is approximated by either the time based or demand models. These approximations are reasonable for most cases, where the component test period is relatively small (e.g., on the order of 3 or 4 months, or less).

5.3.1.2 Components in Operating Systems

To compute the unavailability of an operating component, assuming that the component is repairable (and that the failure is detected), the approximation expression:

$$q = \lambda_o \tau$$

is used, where q_c is the average component unavailability, λ_o is the *operating* failure rate for the failure mode being evaluated, and τ is the outage time for the failed component. The outage time is the (average) total time that the component is out of service after it has failed. Again, if λ_o is the reciprocal of the mean time to failure in hours, then τ is expressed in hours.

To compute the mission failure probability (or unreliability) of a component, the approximation expression

$$q_c = \lambda_o T_M$$

is used, where q_c and λ_o are as previously defined, and T_M is the total mission time. This formulation assumes that the component is nonrepairable during the mission time T_M. The approximation expression is adequate for $\lambda_o T_M \leq 0.1$.

5.3.1.3 Standby Components That Are Never Tested

Occasionally a situation is discovered where a standby component is never tested during the plant lifetime. Two cases are identified, depending on whether or not it is evident that the situation will be corrected in the near-term by devising a means of testing the component.

Case 1: The Situation Will Be Corrected in the Near Term

In this case it is recommended that the *pointwise* unavailability of the component that corresponds to the current lifetime of the plant be computed. That is, if the plant has been in operation for 10 years at the time that the analysis is being performed, compute the pointwise unavailability of the component at 10 years. The expression is:

$$q_c = 1 - e^{-\lambda_s T_p} \ ,$$

where q_c is the pointwise unavailability evaluated at T_p (e.g., 10 years), and λ_s is the standby failure rate.

Case 2. The Situation Will Not Be Corrected in the Foreseeable Future

In this case it is recommended that the average unavailability of the component over the remainder of plant life be computed. This is the average probability that the component will be in a failed state for the remainder of plant life. The expression is:

$$q_c \approx 2 - e^{\lambda_s T_p} \frac{1}{-\lambda_s (T_{tot} - T_p}) \left(e^{-\lambda_s T_p} - e^{-\lambda_s T_{tot}}\right) ,$$

where q_c, λ_s, and T_p are as previously defined, and T_{tot} is the total plant lifetime.

5.3.1.4 Component Outage Contribution

Component outages occur when components are removed from service for test, maintenance, or repair. The impact of component outages on system reliability is identical to the impact o. failures, with the exception that the repairability of outages may be different than the repairability of failures. Component outages result in the component being unavailable.

Two *classes* of component outages, encompassing three *types* of outages must be considered:

- Scheduled outages, including periodic tests and scheduled maintenance.
- Unscheduled outages, including unscheduled component repair.

Components in standby systems are tested periodically to ensure their operability. If the test results in that component or other components being removed from service for a portion of the test, then a component test outage occurs. If a single test removes more than one component from service, only a single test outage contribution is calculated.

Scheduled maintenance is sometimes conducted on major components during normal reactor operation. When scheduled maintenance removes a component from service, a maintenance contribution to unavailability occurs. Scheduled maintenance is usually conducted at a frequency that is different than the test frequency. Since the test period is the baseline period used to calculate component failure contributions, the frequency of scheduled maintenance (with respect to the test period) must be accounted for when calculating the maintenance outage contribution. Not all plants conduct scheduled maintenance of the type that removes a safety system component from service while the reactor is at power.

Unscheduled repair occurs when a component is found to require repair. For standby components, this often occurs during a periodic test when a component is discovered to be in the failed state. However, it could occur at other times also. Often repair ensues when the component is found to be degraded but operable, or when insipient failures such as leaky seals occur as well as when a catastrophic failure occurs. Thus the *frequency* with which unscheduled repair occurs is expected to be at least as large as the component failure rate, which includes only catastrophic failures.

Point estimate unavailability computations for component outages are presented in the following subsections.

5.3.1.5 Test Outage Contribution

The test outage contribution to component unavailability for point value computations is calculated as:

$$q_t = \tau/T,$$

where q_t is the average unavailability from the test outage, τ is the average duration of the test (in hours), and T is the interval between tests (test period) in hours.

5.3.1.6 Scheduled Maintenance Outage Contributions

The scheduled maintainance outage contribution to component unavailability for point value computations is calculated as:

$$q_M = f_M \cdot (\tau_M/T) ,$$

where q_M is the component unavailability due to maintainance, f_M is the frequency (per test period) of scheduled maintainance, τ_M is the mean component outage time for scheduled maintainance, and T is the time between tests. Since q_M is a probability, the units of all parameters on the right-hand side of the above equation must be compatible and cancel so that q_M is dimensionless. For instance, for monthly testing, if the test period is expressed as hours per month, τ_M is hours, and f_M is the reciprocal of the number of months between maintenance acts, then q_M is dimensionless.

5.3.1.7 Unscheduled Repair Outage Contribution

The unscheduled repair outage contribution to component unavailability for point value computations is calculated as:

$$q_R = f_R \cdot (\tau_R/T),$$

where q_R is the component unavailability due to repair, f_R is the frequency (per test period) with which repair is expected to occur, τ_R is the mean component repair time, and T is the test period (time between tests). Again, the units must cancel because q_R is a probability.

5.3.1.8 Summary of Computational Expressions

Table 5.3-1 summarizes both the component failure and component outage computational expressions for use in obtaining point estimte component reliability values.

6. Accident Sequence Analysis Methods

The accident sequence analysis identifies the accident sequences expected to have the highest frequency and the most important minimal cut sets for these sequences. This is accomplished by analyzing the accident sequences defined by the event trees using the fault trees for each front-line system and the human reliability, test and maintenance, and component failure rate data.

The first quantification of the accident sequences is a screening calculation, designed to eliminate those sequences which have a negligible estimated frequency. This quantification uses estimated upper bounds for the failure probabilities from the human reliability and procedural analysis task and initiating event frequencies, generic component failure rates, and plant-specific test and maintenance frequencies and durations from the data base development task to estimate initial accident sequence frequencies.

The sequences which are not eliminated by the screening quantification are selected for closer scrutiny and consideration of operator recovery actions. These sequences, and their minimal cut sets, are used by the human reliability analysts to determine those human errors for which estimated failure probabilities are calculated. Important component failures represented in these sequences are requantified, if necessary, using plant-specific information. The second calculation of accident sequence frequencies uses the improved human error estimates and recovery probabilities and includes changes in the data based on plant-specific data. The sequences with the highest frequencies are termed "dominant accident sequences." The qualitative expressions for the minimal cut sets of the dominant accident sequences provide the qualitative information needed for the subsequent

Table 5.3-1. Component Reliability Calculational Expressions

Unreliability Contribution	Type of Measure	Calculational formula (Approximate)	Parameter Definition
Hardware Failure (standby component)	Unavailability (average)	$q_c=1/2\lambda_s T$ or $q_c=\lambda_d$	λ_s = standby failure rate T = component test period λ_d = demand failure probability
Hardware Failure (operating component)	Unavailability (average)	$q_c=\lambda_o\tau$	λ_o = operating failure rate τ = component outage time
Hardware Failure (operating component)	Unreliability (mission failure)	$q_c=\lambda_o T_M$	λ_o = operating failure rate T_M = mission time
Hardware Failure (untested standby component)	Unavailability (pointwise)	$q_c=1-e^{-\lambda_s T_P}$	λ_s = standby failure rate T_P = plant operating time, to date
Test Outage (standby component)	Unavailability (average)	$q_t=\tau/T$	τ = test outage time (average) T = test period
Maintanance Outage (standby component)	Unavailability (average)	$q_M=f_M\cdot(\tau_M/T)$	f_M = scheduled maintenance τ_M = maintenance outage time T = test period
Repair Outage (standby component)	Unavailability (average)	$q_R=f_R\cdot(\tau_R/T)$	f_R = unscheduled repair frequency τ_R = repair outage time (average) T = test period

uncertainty and importance calculations. Additional discussion of the accident sequence analysis process may be found in Reference 19.

6.1 Identification and Resolution of Logical Loops

6.1.1 Overview

Logical loops are instances of circular logic which may occur in a multisystem fault tree or in control circuits and which must be resolved before a solution to the fault tree can be obtained. Logical loops frequently occur when time-dependent interrelationships among auxiliary systems (e.g., electric power, room cooling, service water) have not been adequately considered. The basic problem here arises when System A requires System B for startup and/or for initial operation, and System B requires System A, but in some longer-term time frame. Logical loops occur in control circuits in the form of feedback loops.

The type of time dependency occurring in multisystem fault trees can be illustrated by the Class 1E ac and dc electric power systems. The dc power system must supply control power to start the standby ac diesel generator and operate some ac distribution system switchgear. At some later time, determined by battery capacity, the ac power system must supply dc loads via the battery charger to maintain operation of the dc system. The ac power system fault tree will show the dc power system as a required auxiliary system. The dc power system fault tree will show the ac power system as source of dc power, via a battery charger. Each system fault tree by itself is logically correct, but when combined, a logical loop occurs (e.g., ac requires dc which requires ac, etc.).

Some of the logical loops that should be anticipated are shown in simplified form in Figure 6.1-1 and are associated with the following auxiliary systems:

- Control power
- Diesel service water
- Equipment room heating, ventilating, and air-conditioning (HVAC) systems

These loops *do not* appear in the fault tree for a single system. Therefore, a coordinated effort must be made among persons preparing system fault trees if potential logical loops are to be identified and eliminated early in the fault tree development. This section describes the origin of logical loops in detail and presents recommendations for their elimination.

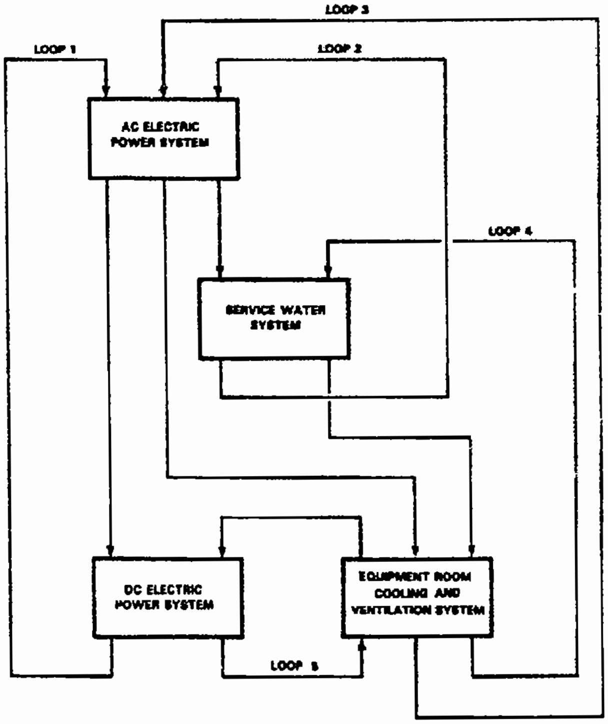


Figure 6.1-1. Overview of Potential Logical Loops

6.1.2 Logical Loops Associated With External Control Power

There are numerous logical loops potentially associated with external control power. These loops are illustrated in Figure 6.1-2. These logical loops *do not* exist for circuit breakers that (1) are manually actuated, or (2) have control circuits with internal control power sources.

Loops A, B, and C in Figure 6.1-2 arise when the dc control power fault tree development continues back through the battery charger and into the ac power distribution system. The logical quandry created by this modeling is that the ac system and diesel generators require dc control power which may be derived from the ac power distribution system via a battery charger. In the short term, the ac supply to the dc power system is not required. Diesel generators are designed so that they can be started and loaded when the battery alone is available as a control power source. Design battery capacity provides for a minimum of one to two hours of operation of the dc system before the battery chargers are required. This time dependency could be reflected in the fault tree for the electrical power systems by providing separate short- and long-term dc power and diesel generator subtrees.

For the short term solution, loops A, B, and C in Figure 6.1-2 are broken by not modeling the dc power supply via the battery charger (path P2). For the long-term solution, path P2 is modeled, but the development of the ac power supply to the dc system is stopped at the first 480 Vac bus. This procedure allows the key interface between the ac and dc power systems to be modeled while breaking loops A, B, and C.

Loop D in Figure 6.1-2 arises when the ac control power fault tree development continues back through an inverter, battery charger and into the ac power distribution system. This loop is broken by the same procedures described previously to handle loops A, B, and C. Loop E in Figure 6.1-2 is also associated with ac control power. Path P8 may be a primary or an alternate power path to a 120 Vac vital bus. In either case, power via this path is not available if offsite power has been lost, and the diesel generator is not in operation. For a short-term solution, Loop E is broken by not modeling path P8. For the long-term solution, path P8 is modeled, but the ac power supply development is stopped at the first 480 Vac bus. This procedure can be implemented by developing short- and long-term electrical power system fault trees as discussed previously. This approach allows the key interface between an ac instrumentation and control power system and the remainder of the ac power distribution system to be modeled while breaking Loop E.

Loop F in Figure 6.1-2 arises when dc control power faults for the battery circuit breaker (if it is power operated) are developed. This loop is broken by developing the control power fault tree only back to the first dc bus (e.g., the battery bus in Figure 6.1-2).

6.1.3 Logical Loops Associated With Diesel Service Water

The logical loop associated with the diesel service water system is illustrated in Figure 6.1-3. This logical loop arises when the diesel generator is supplying ac power, and the development of the fault tree for the diesel service water system continues back into the ac power system to model motive power faults affecting service water pumps and valves. The logical quandry created by this modeling is that the service water system requires ac power, but the ac power system requires the service water system for diesel cooling.

Diesel engines generally have a closed-loop cooling water system that serves as an intermediate heat transfer loop between the engine and an opened-loop service water system. The closed-loop cooling water system usually includes a gear-driven and a dc-powered water pump; therefore, operation of this system is independent of ac power. This system serves as a heat sink for the diesel until the generator is loaded, the service water system is placed in operation, and the heat transfer path to the ultimate heat sink is completed. Only a few minutes may be available to complete the heat transfer path to the ultimate heat sink, but the key point is that the diesel generator can be started and placed in operation without the service water system.

The closed-loop cooling water system in some diesel installations rejects heat directly to the atmosphere by means of water-to-air mechanical draft heat exchangers. Modeling the ac power requirements for the fans associated with this system will introduce the same type of logical loop as the service water system described above.

The logical loop in Figure 6.1-3 can be broken by providing separate short- and long-term diesel generator subtrees. The short-term diesel subtree models diesel generator startup and initial operating requirements, and the logical loop is broken by not modeling the service water system (or the fans, if appropriate). The diesel closed cooling water system is an adequate heat sink for the diesel during this initial operating period. The long-term diesel subtree includes the service water system, but the ac power supply development is stopped at the first 4160 (or 6900) Vac or 480 Vac bus. This approach allows the key interface between the service water system and the ac power system to be modeled while breaking the logical loop in Figure 6.1-3.

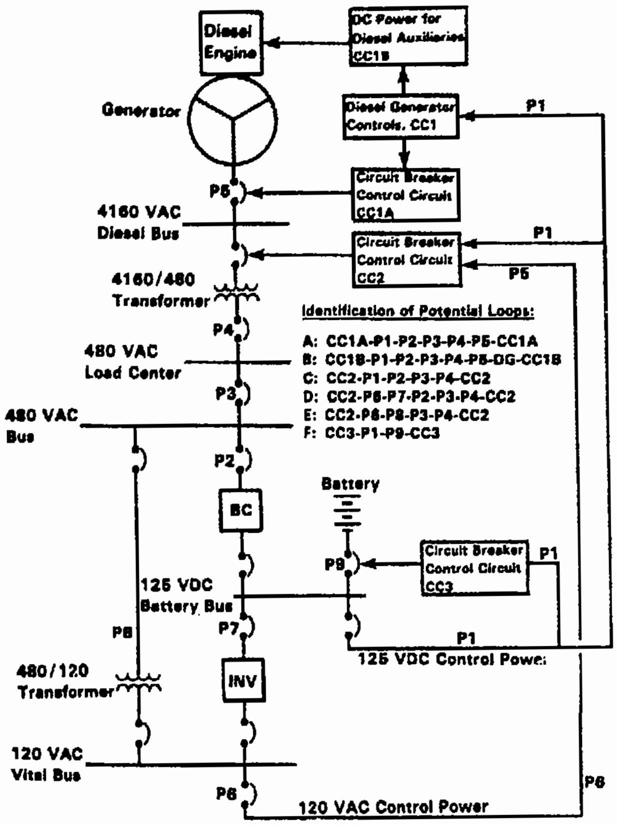

Diesel Engine
DC Power for Diesel Auxiliaries CC1B
Generator
Diesel Generator Controls, CC1
P1
P5
Circuit Breaker Control Circuit CC1A
4160 VAC Diesel Bus
Circuit Breaker Control Circuit CC2
P1
P5
4160/480 Transformer
Identification of Potential Loops:
P4
A: CC1A-P1-P2-P3-P4-P5-CC1A
480 VAC Load Center
B: CC1B-P1-P2-P3-P4-P5-DG-CC1B
C: CC2-P1-P2-P3-P4-CC2
P3
D: CC2-P6-P7-P2-P3-P4-CC2
480 VAC Bus
E: CC2-P6-P8-P3-P4-CC2
F: CC3-P1-P9-CC3
P2
Battery
BC
Circuit Breaker Control Circuit CC3
P1
P9
125 VDC Battery Bus
P8
P7
P1
125 VDC Control Power
480/120 Transformer
INV
120 VAC Vital Bus
P6
P6
120 VAC Control Power

Figure 6.1-2. Potential Logical Loops Associated With External Control Power Systems

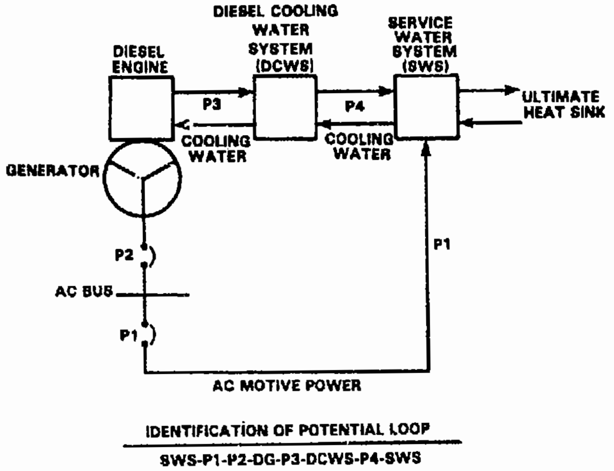

DIESEL COOLING WATER SYSTEM (DCWS)
SERVICE WATER SYSTEM (SWS)
DIESEL ENGINE
P3
P4
ULTIMATE HEAT SINK
COOLING WATER
COOLING WATER
GENERATOR
P1
P2
AC BUS
P1
AC MOTIVE POWER
IDENTIFICATION OF POTENTIAL LOOP
SWS-P1-P2-DG-P3-DCWS-P4-SWS

Figure 6.1-3. Potential Logical Loop Associated With *Diesel Service Water System*

6.1.4 Logical Loops Associated With HVAC Systems

It can usually be assumed that satisfactory ambient conditions exist throughout a plant at the start of an accident (e.g., at time t = 0). Continued operation of equipment without support from room or area HVAC systems may lead to a significant increase in ambient temperature. If severe ambient conditions could cause equipment failure, HVAC system faults should be included in the appropriate fault tree. The time-dependencies associated with HVAC system operation should, however, be determined on an individual case basis.

There are many logical loops potentially associated with HVAC systems that are required for maintaining suitable ambient conditions for continued operation of plant equipment. These loops are illustrated in Figure 6.1-4, and include all equipment and systems in the continuous heat transfer path from an equipment room or area to the ultimate heat sink. These loops arise when HVAC requirements are modeled for the following:

- Control circuits for HVAC equipment.
- ac electric power supply for HVAC equipment.
- dc electric power supply (control power) for HVAC equipment.
- Fluid sytems in the heat transfer path between the room coolers and the ultimate heat sink.

The logical loops in Figure 3.7-4 can all be broken by simply not including HVAC faults in HVAC-related equipment fault trees. This approach yields an accurate model of the faults that may prevent the HVAC equipment from starting (e.g., at time t = 0) and operating for some potentially short-term time period. Equipment HVAC requirements are not usually of concern during this period. If it is determined that equipment room cooling is ultimately required for continued operation of HVAC-related equipment, long-term versions of the fault trees should also be developed for the affected equipment. This version would include the potential contribution of equipment-room cooling system faults; however, the heat transfer path to the ultimate heat sink would not be developed beyond the equipment or area cooler unit (e.g., interfaces of this unit with chilled water, component cooling water, or service water system are not developed). An exception is the following: the fault tree for a control circuit or an ac power supply of an equipment-room cooler unit should not include HVAC faults when the control circuit or supplying ac bus is in the room or area served by the room cooler unit. This approach allows the key interfaces between HVAC-related equipment and their own HVAC support systems to be modeled while breaking the logical loops in Figure 6.1-4.

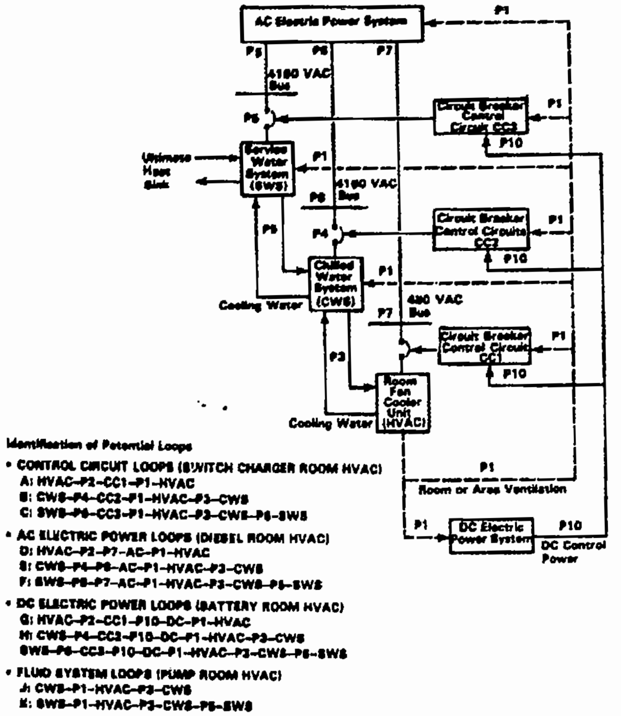

AC Electric Power System
P1
P5
P6
P7
4160 VAC Bus
P6
Circuit Breaker Control Circuit CC3
P1
P10
Ultimate Heat Sink
Service Water System (SWS)
P1
4160 VAC Bus
P6
Circuit Breaker Control Circuits CC2
P1
P5
P4
P10
Chilled Water System (CWS)
P1
Cooling Water
480 VAC Bus
P7
Circuit Breaker Control Circuit CC1
P1
P3
P10
Room Fan Cooler Unit (HVAC)
Cooling Water
Identification of Potential Loops
• CONTROL CIRCUIT LOOPS (SWITCH CHARGER ROOM HVAC)
A: HVAC–P2–CC1–P1–HVAC
B: CWS–P4–CC2–P1–HVAC–P3–CWS
C: SWS–P6–CC3–P1–HVAC–P3–CWS–P5–SWS
• AC ELECTRIC POWER LOOPS (DIESEL ROOM HVAC)
D: HVAC–P2–P7–AC–P1–HVAC
E: CWS–P4–P6–AC–P1–HVAC–P3–CWS
F: SWS–P6–P7–AC–P1–HVAC–P3–CWS–P5–SWS
• DC ELECTRIC POWER LOOPS (BATTERY ROOM HVAC)
G: HVAC–P2–CC1–P10–DC–P1–HVAC
H: CWS–P4–CC2–P10–DC–P1–HVAC–P3–CWS
SWS–P6–CC3–P10–DC–P1–HVAC–P3–CWS–P5–SWS
• FLUID SYSTEM LOOPS (PUMP ROOM HVAC)
J: CWS–P1–HVAC–P3–CWS
K: SWS–P1–HVAC–P3–CWS–P5–SWS
P1
Room or Area Ventilation
P1
DC Electric Power System
P10
DC Control Power

Figure 6.1-4 Potential Logical Loop Associated With HVAC Systems

6.1.5 Feedback Loops in Control Circuits

Feedback loops can occur in control circuits as an inherent part of circuit design. Generally speaking, circuit breakers and relays are the components that indicate feedback loops may appear. For example, if two loops of a control circuit are interconnected by circuit breakers and/or relays, the flow of current in one loop of the circuit will depend on the flow of current in the other loop and vice versa. Thus a situation arises in which there is feedback, either positive or negative, between the two loops. When such a circuit is modeled by a fault tree, the feedback loop appears as circular logic, i.e., in the development of an event, the event reappears as a potential contributor to its own failure.

The circular logic created by feedback loops associated with nonmodulating components, e.g., most pumps and valves can be handled in a relatively simple manner, but depends on whether the feedback is positive or negative. In the case of positive feedback, the fault tree is developed down to the point where the circular logic is encountered. At this point, the development is stopped by the use of a "house" event. The value of the house event depends on the initial conditions in the circuit.

As an example, consider the control circuit shown in Figure 6.1-5. The fault tree development for this circuit where "Motor Runs When It Should Be Off" is the TOP event is shown in Figure 6.1-6. The minimal cut sets for this fault tree are 1, 2-3, 2-4, and 2-FB. In the case where the motor is initially running, i.e., there is current in loop 3, FB is 1, and the minimal cut sets become 1 and 2. In the case where the motor is initially off, FB is 0, and the minimal cut sets become 1, 2-3, and 2-4.

In the case of negative feedback, the fault tree development is stopped at the point where circular logic is encountered by the use of a house event also. However, in this case the house event is always given a value of 1, i.e., it is always "on".

The circular logic created by feedback loops associated with modulating components, i.e., components which operate over a range of speeds or positions, cannot be explicitly handled with the current methodology. Thus it is necessary to handle these control circuits in a simplistic manner, i.e., control circuit failure is handled as a basic event which can cause component failure. The problem then lies in determining an appropriate failure probability for the circuit from operation data, manufactuer's specifications, or some other source.

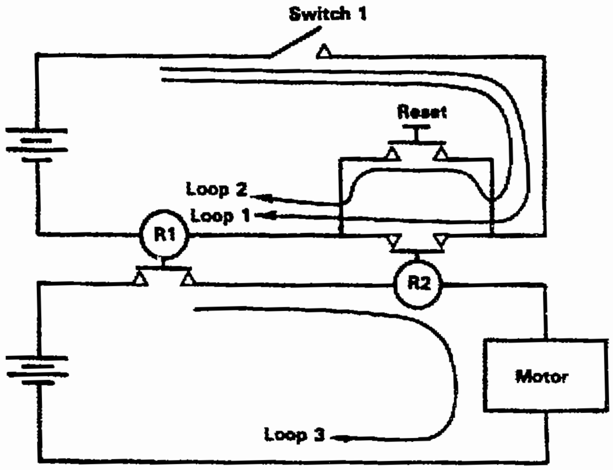


Figure 6.1-5. Control Circuit With Positive Feedback

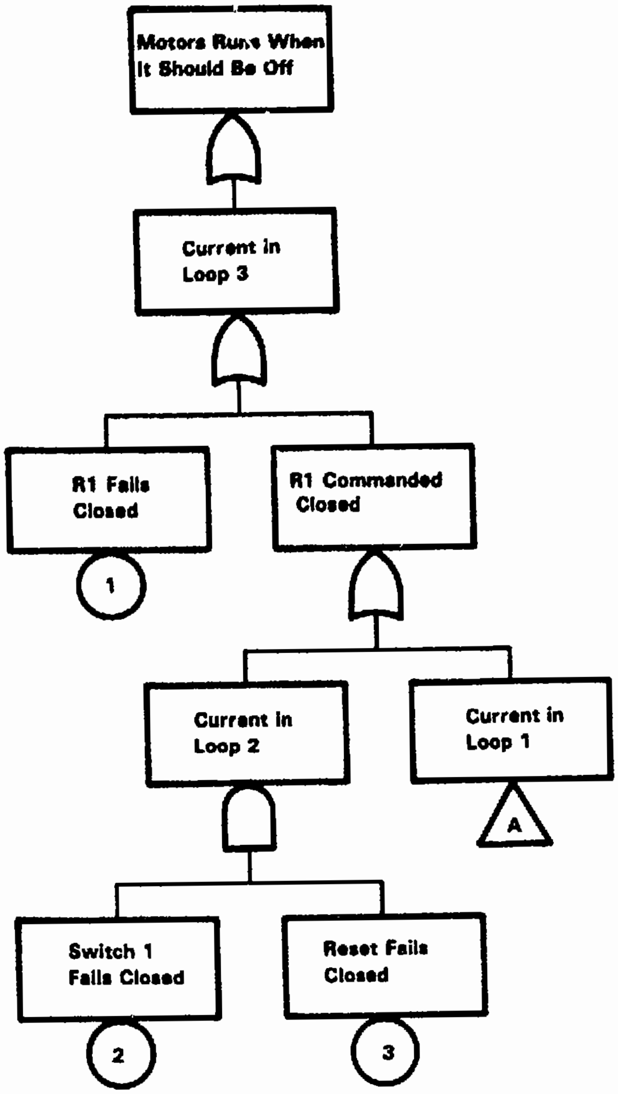


Figure 6.1-6. Fault Tree Development for the Control Circuit in Figure 6.1-5

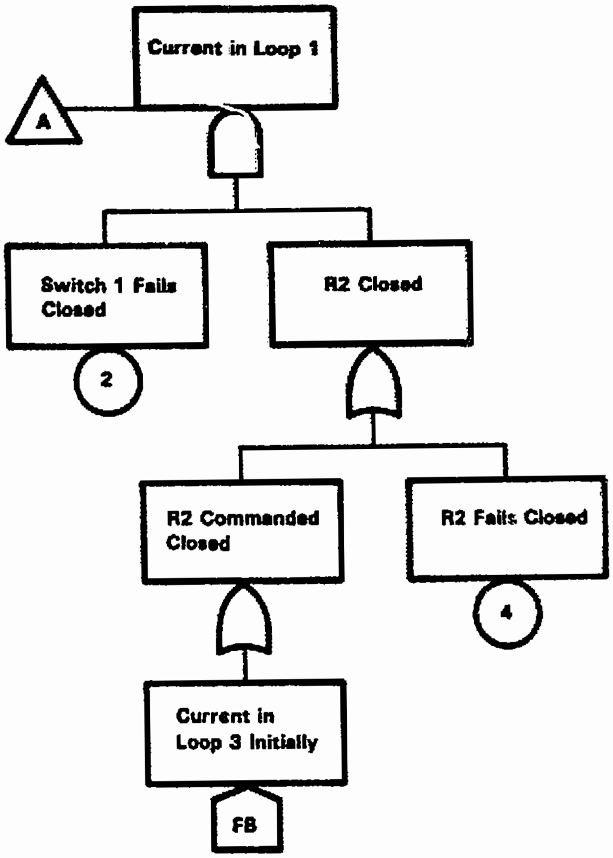


Figure 6.1-6. (Concluded)

6.2 Development of Independent Subtrees

The front-line system failures depicted in the accident sequences are modeled by system fault trees. A minimal cut set of a fault tree is a smallest set of primary events that causes the occurrence of the top event. Since the top event of the system fault tree is the failure of the system, the minimal cut sets of the system fault tree represent all of the fundamental ways the system can fail.

The system fault trees in an IREP analysis are large and complex, representing interactions of many support systems and primary events. Even with the use of a computer code, it may not be possible to identify all of the minimal cut sets of a system fault tree. One technique that reduces the size of the fault tree and the number of minimal cut sets is the identification and solution of the largest independent subtrees.

An independent subtree (or module) of a fault tree is a subtree for which none of its primary events appear elsewhere in the fault tree. An independent subtree behaves as a "super component" in that it is sufficient to know the state of the top event of the independent subtree as opposed to knowing the states of all of the primary events in the subtree. The independent subtrees can be quantified and evaluated individually and replaced by developed events in the system fault trees.

The concept of independent subtrees is relative to the top event of the fault tree being evaluated. This is an important point for accident sequence analysis, since each accident sequence usually combines several system failures. Subtrees that are independent in one system fault tree may contain events that appear in other system fault trees, so treating them as independent in a sequence which combines these system failures is nc: cerrect. The independent subtrees can be identified on a sequence-by-sequence basis, but this is a time-consuming task and produces minimal cut sets that are in terms of different subtrees for different sequences, which can be confusing. It is more efficient and manageable to identify the independent subtrees relative to all of the front-line system fault trees. Then the subtrees identified as independent will be independent in any accident sequence. Some of the advantages of this approach are:

- The independent subtrees are independent relative to any accident sequence.
- Evaluation and quantification of the independent subtrees are done only once and apply to all accident sequences.
- The analyst must become familiar with only one set of independent subtrees to evaluate system fault tree and accident sequence minimal cut sets.

To facilitate the identification of subtrees which are independent in any accident sequence, a global fault tree is formed. The top gate of the global fault tree is an AND gate and the inputs to the top gate are the top gates of all of the front-line system fault trees. Subtrees which are identified as independent subtrees of the global fault tree will be independent in any accident sequence.

After the existing independent subtrees are identified, additional independent subtrees are created. An AND or OR gate, G, can be redefined to create an independent subtree if at least two of the inputs to G are nonreplicated primary events or nonreplicated intermediate events which are tops of independent subtrees. All of the nonreplicated primary events and nonreplicated top events of independent subtrees that are inputs to G, are replaced by a single input from a new gate, G'. The created gate G' has a single output to the gate G and it has as its inputs all of the nonreplicated primary events and nonreplicated top events of independent subtrees that were inputs to G. The created gate G' is the same kind of gate as G, and it is the top event of a new independent subtree. If some of the inputs to G' are tops of existing independent subtrees, then G' is the top of the largest independent subtree which contains these existing independent subtrees.

A pair of consecutive OR gates or a pai- of consecutive AND gates can often be coalesced into a single gate. Any OR gate, G, which has an input from a nonreplicated OR gate, G', can be equivalently represented by replacing the input to G from G' with all of the inputs to G', and deleting the gate G'. Similarly, an AND gate, G, which has an input from a nonreplicated AND gate, G', can be coalesced into a single equivalent AND gate. Coalescing does not create an independent subtree, but by coalescing consecutive gates of the same kind wherever possible, including gates which are the result of previous coalescing, it is often possible to collect, as inputs to the same gate, at least two inputs which are nonreplicated primary events or nonreplicated top events of independent subtrees. Such a gate can then be redefined to create an independent subtree.

6.3 System Fault Tree Minimal Cut Sets and Truncation

The first step in developing minimal cut sets for the front-line system fault trees is to determine the minimal cut sets of the independent subtrees in each system. The probability of each minimal cut set is estimated by computing the product of the point value probability estimates for the primary events in the minimal cut set. The sum of the probabilities of the minimal cut sets of an independent subtree provides an approximation to the probability of the independent subtree. This approximation (called the rare event approximation) is adequate if all of the primary events are small probability events. The top event of the independent subtree is replaced by a primary (developed) event and the probability approximation for this event is added to the data base. For the remainder of the analysis, this event is treated like any other primary event until it is necessary to reintroduce the independent subtree minimal cut sets for the uncertainty analysis and importance calculations.

Even with the use of independent subtrees, a system fault tree may have millions or even billions of minimal cut sets. Since the minimal cut sets of several system fault trees will be combined in some of the accident sequences, the number of minimal cut sets of an accident sequence is generally much greater than the number of minimal cut sets of the system fault trees. With these considerations in mind, a truncation value is selected in order to minimize the number of minimal cut sets which must be determined at this stage of the analysis. In general, the truncation value should be as small as possible, but still limit the number of minimal cut sets to a manageable number. The use of independent subtrees usually permits the use of a smaller truncation value. The actual choice of the truncation value, therefore, is dependent upon the methodology and computer code being used to facilitate the analysis. The same truncation value should be used for all of the system fault trees. If not, it is possible to discard a potentially significant accident sequence minimal cut set which appears in more than one of the system fault trees.

When truncation is used, only minimal cut sets with an estimated probability greater than the truncation value are determined. The minimal cut set probability is estimated by computing the product of the probabilities of the primary events which comprise the minimal cut set. This is the true probability of the minimal cut set if the primary events are statistically independent. A branch and bound algorithm is typically used to take advantage of the fact that including more events in a minimal cut set can only decrease its probability. This makes it possible to discard a large number of minimal cut sets which are less than the truncation value without actually determining the minimal cut sets. However, it also makes it difficult and often impossible to compute the error introduced by truncation. This must be kept in mind when the accident sequence frequencies are generated at a later stage of the analysis. If it becomes necessary to increase the probability point estimate for any of the primary events after the truncation process has been completed, the truncation process should be repeated with the new point estimates. Thus it is important to use upper bound estimates for primary events which have little data (e.g., human error rates) in the initial screening quantification.

There are a few primary events of the system fault trees which correspond to the initiating events of the accident sequences. Loss of offsite power, for example, is one such event. The probability of such a primary event is dependent upon the accident sequence being analyzed. Given the initiating event of an accident sequence, such a primary event corresponding to the initiating event is treated as if it has a probability of one when quantifying the accident sequence. Therefore, when the truncated system fault tree minimal cut sets are being determined, these primary events are assigned a probability of one.

The result of the system fault tree analysis is a set of minimal cut sets which satisfy the truncation criteria for each system fault tree. The minimal cut sets of each system fault tree are in terms of primary events which represent component failures, human errors, test and maintenance events, and independent subtrees.

Each accident sequence to be quantified contains one or more front-line system failures. There are generally hundreds of accident sequences which must be quantified in the screening calculations. Therefore, it is efficient to solve the system fault trees once and to use the minimal cut sets of the fault trees in the accident sequence analysis.

The most common way of retaining and using the system fault tree minimal cut sets for the accident sequence analysis is to use a Boolean equation representation of the minimal cut sets. The left-hand side of the Boolean equation is a variable corresponding to the top event of the system fault tree. The right-hand side of the Boolean equation represents the minimal cut sets of the fault tree and is called the Boolean minimal cut set expression. Each minimal cut set is represented by the Boolean product (AND) of the primary events in the minimal cut set. The minimal cut sets are separated from one another by the Boolean sum (OR) operator. A comparison of the fault tree representation and the Boolean representation for minimal cut sets is provided in Figure 6.3-1.

	Fault Tree	Boolean Representation
Minimal Cut Set M_i With Primary Events, $P_{i,j}$	$M_i = \{P_{i,1}, P_{i,2}, \ldots, P_{i,n_i}\}$	$M_i = P_{i,1}*P_{i,2}*\ldots*P_{i,n_i}$
	$= \{P_{i,j} \mid 1 \le j \le n_i\}$	$= \prod_{j=1}^{n_i} P_{i,j}$
Set of All Mininal Cut Sets for Top Event T	$T = \{M_1, M_2, \ldots, M_m\}$	$T = M_1 + M_2 + \ldots + M_m$
	$= \{M_i \mid 1 \le i \le m\}$	$= \sum_{i=1}^{m} M_i$
	$= ((P_{1,1}, P_{1,2}, \ldots P_{1,n_1}),$ $(P_{2,1}, P_{2,2}, \ldots P_{2,n_2}), \ldots,$ $(P_{m,1}, P_{m,2}, \ldots, P_{m,n_m}))$	$= P_{1,1}*P_{1,2}*\ldots*P_{1,n_1} +$ $P_{2,1}*P_{2,2}*\ldots*P_{2,n_2} +$ $\ldots + P_{m,1}*P_{m,2}*\ldots*P_{m,n_m}$
	$= \{(P_{1,j} \mid 1 \le j \le n_1), (P_{2,j} \mid 1 \le j \le n_2),$ $\ldots, (P_{n,j} \mid 1 \le j \le n_m)\}$	$= \prod_{j=1}^{n_1} P_{1,j} + \prod_{j=1}^{n_2} P_{2,j} + \ldots + \prod_{j=1}^{n_m} P_{n,j}$
	$= ((P_{i,j} \mid 1 \le j \le n_i) \mid 1 \le i \le m)$	$= \sum_{i=1}^{m} \prod_{j=1}^{n_i} P_{i,j}$

Figure 6.3-1 Fault Tree and Boolean Representation

6.4 Accident Sequence Minimal Cut Sets

Each accident sequence contains an initiating event and one or more system failures and may contain system successes. An accident sequence fault tree is a fault tree with an AND gate as its top event. The inputs to the top gate are the initiating event and the top gates of the system fault trees for the system failures in the accident sequence. The minimal cut sets of the accident sequence fault tree represent all of the fundamental ways, in terms of the initiating event and the primary events of the system fault trees, that the accident sequence can occur. The minimal cut sets are checked for consistency with the system successes, if any, in the accident sequence. Minimal cut sets which cause the failure of a system defined to be in a success state in the accident sequences are eliminated. The remaining minimal cut sets are subsequently quantified to produce a frequency estimate for the accident sequence.

Actually forming the accident sequence fault trees and determining their minimal cut sets requires resolving the same system fault trees in various combinations, possibly hundreds of times. This is a time consuming and expensive process. Alternatively, the Boolean minimal cut set equations for the accident sequence fault trees can be formed by using the Boolean minimal cut set equations for the system fault trees. If any minimal cut set of any of the system fault trees contains a primary event which corresponds to the initiating event, drop the primary event from the minimal cut set. Forming the Boolean product (AND) of the Boolean minimal cut set expressions for the system failures and the initiating event, and applying the Boolean identities P*P = P and P + P*Q = P produces a Boolean minimal cut set expression for the accident sequence fault tree.

The number of minimal cut sets may be so large that determining all of them is not possible. Truncation may again be necessary. The truncation value should again be as small as possible, but it should not be any less than the truncation value used for the system fault trees times the frequency of the initiating event, since some of the accident sequence fault tree minimal cut sets with a frequency less than this product may have already been discarded when the system fault tree minimal cut sets were truncated. The same truncation value that was used for the system fault trees or the product of the truncation value used for the system fault trees and the initiating event frequency are the most common choices for the truncation value.

The system successes, if any, in the accident sequence are included in the analysis at this time to eliminate minimal cut sets of the accident sequence fault tree which are precluded by the logic associated with the system successes in the accident sequence.

Any minimal cut set of an accident sequence fault tree which causes the failure of a system defined to be in a success state in the accident sequence is eliminated. A system success which is independent of the system failures need not be included since no minimal cut sets will be dropped. However, in general a large number of minimal cut sets will be dropped when the system successes are considered, and it is often necessary to use a computer code. The computer code usually uses one of two approaches: a complement approach or a direct comparison approach.

The complement approach is best suited for small fault trees; it can be very difficult to determine the complement expression for a large fault tree. The Boolean minimal cut set expression for a system fault tree represents the ways the system can fail. The complement of this expression identifies combinations of primary events which ensure the success of the system. The complement expression can be simplified by the application of the identities $P + P^*Q = P$ and $P^*P = P$. Taking the Boolean product of the accident sequence fault tree minimal cut set expression and the complement expressions for each system success in the accident sequence, and applying the identity $P^*\overline{P} = \phi$, where, $\overline{P}$ designates success of event P, eliminates the minimal cut sets of the accident sequence fault tree which cause the failure of a system defined to be in a success state in the accident sequence. After the complements have been used to eliminate zero products, they are dropped from the minimal cut set expression. Although theoretically the complemented events could be carried throughout the remainder of the analysis, there are several reasons for not doing so. First, the inclusion of the complemented events in the Boolean expressions for the accident sequences greatly increases the size of the expressions. Second, the rare event approximation cannot be used on such an expression since the probabilities of the complemented events are close to one. Third, it can be shown that dropping the complemented events, after applying the $P^*\overline{P} = \phi$ identity, and applying the identity $P + P^*Q = P$ to the resulting expression produces a conservative approximation to the accident sequence expression with all of the complemented events retained. Experience has shown that the conservatism introduced by dropping the complement terms at this point is quite small.

The direct comparison approach compares the accident sequence fault tree minimal cut sets with the minimal cut sets of the system fault trees for the systems which are in a success state in the accident sequence. If a minimal cut set of a system fault tree for a system success is a subset of a minimal cut set for the accident sequence fault tree, the latter minimal cut set is dropped from the set of minimal cut sets for the accident sequence fault tree by application of the identity $P + P^*Q = P$. A description of this approach can be found in [20]. This approach is equivalent to the complement approach and has been used successfully on very large accident sequence Boolean expressions.

Whichever method is used, the end product is the same: the accident sequence fault tree minimal cut sets which do not cause the failure of any of the system successes in the accident sequence. These minimal cut sets will be called the accident sequence minimal cut sets (as opposed to the accident sequence fault tree minimal cut sets).

6.5 Accident Sequence Screening Quantification

The screening quantification identifies accident sequences which are candidates for being dominant accident sequences. The quantification at this step of the analysis relies on point values and the rare event approximation. Let the Boolean minimal cut set representation for accident sequence S be given by

$$S = N_1 + N_2 + ... + N_n.$$

The initiating event, IE, is in every minimal cut set N_i and can be factored out:

$$S = IE^*(M_1 + M_2 + ... + M_n)$$

where

$$IE^*M_i = N_i, \; i = 1, 2, ..., n$$

The M_i's are the Boolean minimal cut set representations without the initiating event. So the Boolean equation:

$$T = M_1 + M_2 + ... + M_n$$

is the Boolean minimal cut set equation for the accident sequence S without the initiating event.

Each minimal cut set M_i, $i = 1, 2, ..., n$, consists of the Boolean product of one or more primary events. Assuming statistical independence of each primary event, the probability of the minimal cut set M_i is the product of the probabilities of each primary event in M_i; i.e.,

$$P(M_i) = P(a_{i,1}) \cdot P(a_{i,2}) \cdot P(a_{i,k}) = \prod_{j=1}^{k} P(a_{i,j}) \; ,$$

where $P(a_{i,j})$ is the probability of primary event $a_{i,j}$.

The probability expression for P(T) is given by:

$$\begin{aligned}
P(T) = {} & P(M_1) + P(M_2) + \dots + (M_n)\} \; P_1 \\
& \left.\begin{aligned}
& - P(M_1 * M_2) - P(M_1 * M_3) - \dots - P(M_1 * M_n) \\
& - P(M_2 * M_3) - P(M_2 * M_4) - \dots - P(M_2 * M_n) \\
& - \dots - P(M_3 * M_n) - \dots - P(M_{n-1} * M_n)
\end{aligned}\right\} P_2 \\
& \left.\begin{aligned}
& + P(M_1 * M_2 * M_3) + P(M_1 * M_2 * M_4) + \dots \\
& + P(M_1 * M_2 * M_n) + P(M_1 * M_3 * M_4) + \dots \\
& + P(M_1 * M_3 * M_n) + \dots P(M_{n-2} * M_{n-1} * M_n)
\end{aligned}\right\} P_3 \\
& \left.\begin{aligned}
& - P(M_1 * M_2 * M_3 * M_4) - \dots - P(M_1 * M_2 * M_3 * M_n) \\
& - \dots - P(M_{n-3} * M_{n-2} * M_{n-1} * M_n)
\end{aligned}\right\} P_4 \\
& + \dots + (-1)^{n+1} P(M_1 * M_2 * M_3 * \dots * M_n)\} P_n
\end{aligned}$$

If we let the P_i represent the parts of the equation as shown, then P(T) is less than the minimum of P_1, $P_1 + P_2 + P_3$, ... and greater than the maximum of $P_1 + P_2$, $P_1 + P_2 + P_3 + P_4$, ... The P_1 value is an upper bound on P(T) and is also a good approximation for P(T), called the rare event approximation, when the primary events in the equation for P(T) have small probability values. The approximation P_1 is a conservative one since $P(T) \leq P_1$. Although the approximation may be too conservative, this is not of great concern in the screening quantification.

Initiating event frequency estimates are provided by the data base development task. Multiplying the initiating event frequency by the rare event approximation for P(T) produces an approximate frequency for S, the accident sequence.

The accident sequences are ranked based on their frequency, and accident sequences which have a negligible approximated frequency are eliminated. The remaining accident sequences are candidates for being dominant accident sequences.

6.6 Quantification of Candidate Dominant Accident Sequences

The primary event data used to quantify the candidate dominant accident sequences is subjected to a closer scrutiny, and the possibility of operator recovery action is also considered. The candidate dominant accident secuence minimal cut sets are examined to determine human errors for which point value estimates are to be computed and component failures whose point value estimates should be checked for accuracy in the light of plant-specific information. If the point value estimates for any of the primary events increase when the data is revised, it is necessary to again determine the truncated minimal cut sets of the system fault trees which contain any of these primary events since some of the system fault tree minimal cut sets were eliminated by truncation based on the data used for the screening quantification.

The minimal cut sets of the candidate dominant accident sequences are again determined using the minimal cut set expressions (some of which may differ from those used in screening calculations as discussed above) for the minimal cut sets of the system fault trees. Truncation is employed, if necessary, to keep the number of accident sequence minimal cut sets at a manageable level.

A candidate dominant accident sequence minimal cut set equation can be expressed as $S = IE * (M_1 + M_2 + \dots + M_n)$, where $T = M_1 + M_2 + \dots + M_n$ is the expression to be quantified. The M_i's can be ordered so that $T = M_1 + M_2 + \dots + M_K + M_{K+1} + \dots + M_n$ where $M_1, M_2, \dots, M_K$ are minimal cut sets comprised of only small probability primary events, i.e., $P(a_{i,j}) \leq N$, where the value of N is chosen by the analyst. The remaining minimal cut sets, $M_{K+1}, \dots, M_n$ each have at least one primary event with probability $> N$. Then $P(M_1 + M_2 + \dots + M_K)$ is approximated using the rare event approximation while $P(M_{K+1} + M_{K+2} + \dots + M_n)$ is approximated by computing successive upper and lower bounds, i.e., P_1, $P_1 + P_2$, $P_1 + P_2 + P_3$, ..., until a reasonable approximation can be made. The sum of these two approximations multiplied by the frequency of the initiating event gives the preliminary approximate frequency of the candidate dominant accident sequence. The final approximate frequency of each candidate dominant accident sequence is not obtained until the possibility of recovery is considered for the candidate dominant accident sequence minimal cut sets.

6.7 Treatment of Recovery

Each candidate dominant accident sequence minimal cut set represents one way the sequence may occur. The information available to the operator and the recovery action to be taken depends on the particular minimal cut set, so recovery actions are considered at the minimal cut set level rather than at the accident sequence level. Since there may be a large number of minimal cut sets for an accident sequence, it may be necessary to consider recovery for only the most significant minimal cut sets. A probability of nonrecovery is estimated for each minimal cut set which is recoverable by some operator recovery action. The frequency of the minimal cut set is then multiplied by its probability of nonrecovery to compute an estimate of the minimal cut set frequency with recovery. The final estimated frequency for a candidate dominant accident sequence is computed using these (reduced) minimal cut set frequencies with recovery.

The primary events of a particular accident sequence minimal cut set may or may not be recoverable by routine recovery actions. Heroic recovery actions or repairing components are not considered, but routine recovery actions are. For example, the overhaul of a pump or diesel generator is not considered, but the manual realignment of a valve, whether by handswitch in the control room or local turning, is. If a primary event can be recovered by a routine recovery action, the location of the recovery action is determined. In general, recovery actions can be separated into those which can be accomplished from the control room and those which can only be performed locally. If recovery can only be performed locally and the local site is inaccessible (i.e., inside containment), the primary event is considered nonrecoverable.

Once a primary event is deemed recoverable and the location of the recovery action is determined, a critical time for the recovery action is estimated. Two types of critical times are considered when determining the critical time for a recovery action. The primary event itself can have a critical recovery period which is independent of the accident sequence, or the state of the core or containment in an accident sequence can have a critical time period for restoration of the primary event.

An example of primary event critical time is that of lube-oil cooling for a pump. If the primary event is the loss of such cooling, there is a definite time interval during which the pump can operate without the cooling, and this time interval defines the critical time for the recovery of the primary event.

The second type of critical time considers the mitigative function in which the primary event is involved during the course of the accident sequence. In general, the accident sequences can be combined into groups with each group having its own set of critical times. For example, sequences initiated by large LOCAs have different time constraints for core recovery mitigation than do sequences initiated by small LOCAs. In this second type of critical time examination, the questions asked in determining the critical time for recovery are phenomenological in nature. For example, if neither containment spray pump receives an actuation signal, the critical time during which they can be manually actuated is determined by how long it takes in the sequence for the containment to be pressurized to the point of failure. When both types of critical times are applicable for a particular recovery action, the shortest critical time is used.

After the critical times and locations of the possible recovery actions are established, the probability of recovery is estimated for each recovery action. The probability of nonrecovery is one minus the probability of recovery. If a primary event is not recoverable, its probability of recovery is zero and its probability of nonrecovery is one. The following table is an example of a simple recovery model, where the probability of recovery is a function of the critical time and location of the recovery action. Note that if a primary event has a critical time of 18 minutes and can be recovered by a recovery action in the control room, the probability of nonrecovery is 0.1. If this primary event can also be recovered locally, its probability of nonrecovery is 0.25. For these cases, the probability of nonrecovery used in the analysis is the smallest one, 0.1 in this example.

Probability of Recovery and Nonrecovery

		Critical Time for Recovery Action	
P(R)	P(NR)	In Control Room	Locally
0.0	1.00*	<5 min	<15 min
.75	.25	5-10	15-20
.90	.10	10-20	20-30
.95	.05	20-30	30-40
.97	.03	30-60	40-70
.99	.01	>60	>70

*In addition, P(R) = 0.0 and P(NR) = 1.00 for faults which are nonrecoverable or whose location is inaccessible.

If more than one primary event in a minimal cut set is recoverable, the recovery action chosen for the minimal cut set is the one with the highest probability. For most minimal cut sets, recovery of a single primary event of the minimal cut set will restore the sequence to a success (no core melt). For these minimal cut sets, the freqency of the minimal cut set is multiplied by the probability of nonrecovery to estimate the frequency of the minimal cut set with recovery. In a small number of minimal cut sets (less than 1% of the minimal cut sets for the Arkansas Nuclear One IREP analysis [8]) more than one primary event in the minimal cut set requires recovery to restore the sequence to a success state. Recovery of just one primary event in these minimal cut sets alters the minimal cut set so that it becomes a minimal cut set of another sequence, but this other sequence still leads to core melt. The probability of nonrecovery for a minimal cut set which requires the recovery of more than one of its primary events is determined by

$$P(NR) = 1 - \prod_{i=1}^{n} (1 - P(NR)_i) \ ,$$

where n is the number of primary events requiring recovery and $P(NR)_i$, $1 \leq i \leq n$, is the individual probability of nonrecovery for each of the n primary events which must be recovered.

Minimal cut sets may contain primary events (which are developed events) that represent independent subtrees. One approach to applying recovery to the independent subtrees is to replace the developed events which represent independent subtrees by the minimal cut sets of the independent subtrees which were determined earlier in the analysis. Recovery can then be applied as previously described.

A recovery event is added to each probabilistically significant minimal cut set in the candidate dominant accident sequence expressions. The probability for each event is the nonrecovery probability associated with the particular cut set. The frequency estimates for the candidate dominant accident sequences are again computed using the minimal cut set frequencies including the nonrecovery probabilities for the minimal cut sets of the candidate dominant accident sequences. (The minimal cut set frequency with recovery is the original cut set frequency multiplied by the probability of nonrecovery for the cut set.) The candidate dominant accident sequences are ranked by their estimated frequency and the dominant accident sequences are selected. As an example, the following table gives the dominant accident sequences and their estimated frequencies for the Arkansas Nuclear One IREP analysis. The table also illustrates the importance of recovery in decreasing the estimated frequencies of the dominant accident sequences for Arkansas Nuclear One IREP analysis.

Table 6.7-1. Arkansas Nuclear One, Unit 1, Dominant Accident Sequences*

Dominant Accident Sequence**	Estimated Frequency/Yr w/o Recovery	Estimated Frequency/Yr w/ Recovery
T(LOP)LD_1YC	4.2E-5	9.9E-6
B(1.2)D_1C	2.0E-5	4.4E-6
T(D01)LQ-D_3	2.1E-5	4.0E-6
T(A3)LQ-D_3	7.0E-6	3.3E-6
T(D01)LD_1YC	5.2E-5	3.1E-6
T(FIA)KD_1	2.8E-6	2.8E-6
B(1.2)D_1	2.2E-5	2.8E-6
T(D02)LD_1YC	5.8E-6	2.5E-6
T(D01)LD_1	1.8E-5	2.2E-6
T(D01)LD_1C	9.7E-6	1.8E-6
B(4)H_1	3.8E-5	1.4E-6
T(A3)LD_1C	3.4E-6	1.4E-6
B(1.66)H_1	2.7E-5	1.2E-6
T(A3)LD_1	5.9E-6	9.5E-7

*Taken from Reference [8].

**Legend: Initiating Events

B(1.2) Reactor Coolant Pump Seal Rupture or Small-Small LOCA (0.38 in. < D ≤ 1.2 in.)

B(1.66) - Small LOCA (1.2 in. < D ≤ 1.66 in.)

B(4) - Small LOCA (1.66 in. < D ≤ 4 in.)

T(LOP) - Loss of Offsite Power Transient

T(PCS) - Loss of Power Conversion System Transient Caused by Other Than a Loss of Offsite Power

T(FIA) - Transients With All Front-Line Systems Initially Available

T(A3) - Transient Initiated by Failure of the ES Bus A3 (4160 Vac)

T(D01) - Transient Initiated by Failure of the ES Bus D01 (125 Vdc)

T(D02) - Transient Initiated by Failure of the ES Bus D02 (125 Vdc)

System Failures

C - Reactor Building Spray Injection System
D_1 - High Pressure Injection System (1 of 3 Pumps)
D_3 - High Pressure Injection System (2 of 3 Pumps)
H_1 - High Pressure Recirculation System
K - Reactor Protection System
L - Emergency Feedwater System
Q - Reclosure of Pressurizer Safety/Relief Valves
Y - Reactor Building Cooling System

7. Interpretation and Analysis of Results Methods

A Monte Carlo simulation is performed on the dominant accident sequences and the core melt expression to illustrate the variability in the accident sequence frequencies as a result of uncertainties in the point value estimates used in the accident sequence frequency calculations. The uncertainty analysis requires probability distributions for the human error, component failure, test and maintenance, and recovery events.

The Birnbaum and Fussell-Vesely measures of importance are computed for the individual events including initiating events, primary events from the fault trees, and recovery events. These probabilistic measures of event importance make it possible to rank the initiating events, human errors, component failures, test and maintenance, and recovery events to reflect their overall contribution to core melt.

For these calculations, it is convenient to replace the independent subtrees, which are represented by developed events in the dominant accident sequences, by their minimal cut sets, which were determined early in the analysis. This facilitates the uncertainty analysis since primary events which represent identical components have correlated data which should be accounted for in the uncertainty analysis. It is also useful for the probabilistic importance measures since these measures are usually computed for the original primary events instead of the developed events which represent independent subtrees.

7.1 Formation of the Core Melt Expression

Uncertainty, sensitivity, and importance calculations are performed not only for the dominant accident sequences but also for the core melt expression. This expression is formed by taking the Boolean sum (OR) of the minimal cut set expressions for all of the dominant accident sequences and applying the identity P + P*Q = P to the resulting expression. The Boolean products in the core melt expression represent the core melt minimal cut sets, i.e., all of the fundamental ways that core melt can occur as a result of one of the dominant accident sequences occurring.

7.2 Uncertainty Analysis

The frequencies of the dominant accident sequences were computed using point value estimates for the event probabilities. Similarly, the core melt expression could be quantified using only point estimates. The point value estimates are, however, imprecise. There are a variety of methods for assessing the impact of this imprecision on the computed frequencies for the dominant accident sequences and core melt. One common method is to perform a Monte Carlo simulation.

A median probability and an error factor are associated with each event (initiating events, primary events, and recovery events) represented in the dominant accident sequence and core melt expressions. The error factor is used to define a possible range of values for a particular random variable. If the median probability of occu-rence of some event X is $X_{0.5}$, then the possible values of the random variable representing the occurrence of X are between $X_{0.5}/f$ and $X_{0.5}\cdot f$, where f is the error factor for event X. The median probability and the error factor are used to calculate upper and lower bounds which are percentile points of some probability distribution. From this, the parameters of a probability distribution for the occurrence of the event are calculated. Values given in Part III, Section 5, for the primary events represent the assumed 90th and 10th percentile points of a lognormal distribution. A number of arguments are presented for the applicability of the lognormal distribution for describing the primary event data in the *Reactor Safety Study* (Reference 4, pp. II-42, II-43).

Some information regarding error factors for initiating events may be found in Reference 13. Error factors associated with recovery events are a matter of analyst judgment. Each trial in the Monte Carlo simulation consists of taking a random sample from the probability distributions for the primary events and recovery events and a random sample from the frequency distribution for the initiating event(s). The approximate frequency of the accident sequence (or of core melt) is computed as described in Part III, Section 6.5. After a certain number of trials (e.g., 1200 for the ANO-1 IREP analysis), the resulting distribution, the mean, standard deviation, 5th, 50th, and 95th percentile points are computed, which are then used to compute the equivalent median and error factor for the dominant accident sequence and core melt frequencies.

The computer codes which are currently available for the uncertainty analysis and the importance measures (discussed in the following section), do not allow values greater than one since they were designed to handle probabilities. The frequency of an initiating event is usually given for a time interval of one year. The median frequency or the product of the median frequency and the error factor for some initiating events may be greater than one. When this occurs, these events can be scaled to values less than 1 by choosir a sufficiently small time interval to ensure that there are no values greater than one. Upon completing the calculation, the results of the analysis and calculation can be converted to a time interval of one year by multiplying through by the scaling factor. For details of this approach see Reference 19.

A minimal cut set may contain two or more primary events whose probability distributions have been derived from the same data and are therefore identical. If different random samples from the same distribution are generated for each of these primary events, the resulting frequency for the minimal cut set, and hence the accident sequence, will be underestimated. This problem can be avoided by generating one random sample from the probability distribution and using it for all of the primary events with this probability distribution. In order to accomplish this, it is necessary to replace independent subtrees by their minimal cut sets in terms of their primary events so that primary events with the same distribution are identified and treated accordingly.

7.3 Importance Calculations

Probabilistic importance measures are used to estimate the contribution a particular event makes to the frequency of a dominant accident sequence or to the overall core melt frequency.

There are three principal types of measures corresponding to the Barlow-Proschan, Fussell-Vesely, and Birnbaum measures. These measures are defined and described in [21].

The Barlow-Proschan and Fussell-Vesely measures are more closely related to each other than to the Birnbaum measure. The exact nature of the relationships among these and other measures can be found in [22]. The Barlow-Proschan and Fussell-Vesely measures compute the probability that an event is contributing to the accident sequence frequency, and therefore provide information on which events, if made less probable or less frequent through improved quality or redundancy, will most decrease the accident sequence or core melt frequency. The principal difference between these two measures is that the Barlow-Proschan measure allows incorporation of time-dependent failure distributions. Although the Fussell-Vesely measure does not allow time-dependent failure distributions, it does incorporate a sense of contribution to failure in that it measures, for example, the probability that repairing a component restores the system, a slightly different interpretation than the Barlow-Proschan measure.

The Birnbaum measure is an indication of the sensitivity of accident sequence or core melt frequency to the probability or frequency of an individual event. Thus it measures the rate of change of accident sequence frequency to change in event probability or frequency.

As described in [22], these measures are intimately linked, and their differences are quite subtle. Thus it is difficult to make recommendations on which measures are appropriate to use in different situations. The choice between the Barlow-Proschan measure and the Fussell-Vesely measure only has meaning if time-dependent failure distributions are available; otherwise, these measures are the same under the assumptions used to calculate them in most available computer codes. The choice between Barlow-Proschan/Fussell-Vesely and the Birnbaum measure is more difficult since they measure different aspects of system reliability. However, the Birnbaum measure is not a function of the event's probability or frequency, so it is not as useful as the Fussell-Vesely measure for measuring the contribution of an individual primary event with a given point value probability estimate.

There are other probabilistic importance measures that are similar to the Fussell-Vesely measure, including the criticality measure and the upgrading function [21]. However, for reliable systems these measures all give the same ranking of events.

The ranking of events for each dominant accident sequence identifies the important primary events for that sequence. It does not, however, provide a measure of the overall importance of these event relative to all of the dominant accident sequences or relative to some group of accident sequences. Applying the probabilistic importance measures to the events in the core melt expression, however, allows the ranking of events to identify their relative contribution to core melt. The importance of classes of events, such as all test and maintenance events, is obtained by summing the importance measures of all of the events in the class.

References

[1] A. A. Garcia, R. T. Liner, P. J. Amico, and E. V. Lofgren, "Crystal River-3 Safety Study," Science Applications, Inc. NUREG/CR-2515, SAND81-7229 (Albuquerque, NM: Sandia National Laboratories, December 1981.)

[2] P. Cybulskis and R. Wooton, Battelle Columbus Laboratories, and G. J. Kolb, Sandia National Laboratories, "LWR Core Meltdown Accident Sequence Phenomenology," Transactions of the American Nuclear Society, Voi 41. Los Angeles, CA, June 1982.

[3] A. S. McClymont and B. W. Poehlman, Science Applications, Inc., "ATWS: A Reappraisal, Part 3. Frequency of Anticipated Transients," EPRI NP-2230, January 1982.

[4] "Reactor Safety Study, An Assessment of Accident Risks in US Commercial Nuclear Power Plants," US Nuclear Regulatory Commission, Wash-1400, NUREG-75/014, October 1975.

[5] A. D. Swain, H. E. Guttmann, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, SAND80-0200 (Albuquerque, NM: Sandia National Laboratories, September 1980). (A revised version will be published in early 1983.)

[6] G. J. Kolb, Sandia National Laboratories, "Systemic Event Tree Methodology Employed in the Interim Reliability Evaluation Program (IREP)," Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Vol 2, Port Chester, NY: September 1981.

[7] "ATWS: A Reappraisal—Part III, Frequency of Anticipated Transients," Prepared by Science Applications, Inc., EPRI NP-801, July 1978.

[8] G. J. Kolb, et. al., "Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One-Unit 1 Nuclear Power Plant," NUREG/CR-2787, SAND82-0978 (Albuquerque, NM: Sandia National Laboratories, June 1982).

[9] G. B. Varnado, Sandia National Laboratories, and W. Horton and P. Lobner, Science Applications Inc., "Fault Tree Analysis Procedures Using Modular Logic Modules," SAND81-0062 (Albuquerque, NM: Sandia National Laboratories) To Be Published (early 1983).

[10] M. E. Stewart, J. K. Rawlins, and R. H. Jeunings, "Test Reactor Risk Assessment Methodology," Aero Jet Nuclear Co. ANCR-1271, April 1976.

[11] W. E. Vesely, F. F. Goldberg, US Nuclear Regulatory Commission, N. H. Roberts, U. of Washington, and D. F. Haasl, Institute of System Sciences Inc., "Fault Tree Handbook," NUREG-0497, January 1981.

[12] B. J. Bell, A. D. Swain, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants," NUREG/CR-2254, SAND81-1655 (Albuquerque, NM: Sandia National Laboratories, December 1981). (A revised version will be published in early 1983.)

[13] A. J. Oswald, C. D. Gentillon, S. D. Matthews, and T. R. Meachum, "Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP) Guide," (EG&G Idaho, Inc. EGG-EA-5887, June 1982).

[14] G. J. Kolb, S. W. Hatch, Sandia National Laboratories, and P. Cybulskis, and R. O. Wooton, Battelle Columbus Laboratories, "Reactor Safety Study Methodology Applications Program: Oconce #3 PWR Power Plant," NUREG/CR-1659 (2 of 4), SAND80-1897 (Albuquerque, NM: Sanida National Laboratories, revised May 1981).

[15] S. W. Hatch, Sandia National Laboratories, and P. Cybulskis and R. O. Wooton, Battelle Columbus Laboratories, "Reactor Safety Study Methodology Applications Program: Grand Gulf #1 BWR Power Plant," NUREG/CR-1659 (4 of 4), SAND80-1897 (4 of 4) (Albuquerque, NM: Sandia National Laboratories, October 1981).

[16] Memorandum for D. G. Eisenhunt, NRC, From T. E. Murley, NRC. Subject: Reactor Coolant Pump Seal Failure. nd.

[17] "Military Handbook: Reliability Prediction of Electronic Equipment," Rome Air Development Center, Griffith AFB, NY, MIL-HDBK-217C, April 1979.

[18] "Military Handbook: Reliability Prediction of Electronic Equipment," Rome Air Development Center, Griffith AFB, NY, MIL-HDBK-217B.

[19] D. W. Stack, "Accident Sequence Analysis Using SETS," SAND82-2272 (Albuquerque, NM: Sandia National Laboratories, to be published.)

[20] R. B. Worrell, B. L. Hulme, "Algebraic Approximation of Event Tree Sequences," SAND82-1273 (Albuquerque, NM: Sandia National Laboratories, 1982).

[21] H. E. Lambert, F. M. Gilman, "Importance Computer Code," ERDA Report UCRL-79269 (Livermore, CA: Lawrence Livermore Laboratory, 1977).

[22] R. Engelbrecht-Wiggans, D. R. Strip, "On the Relation of Various Reliability Measures to Each Other and to Game Theoretic Values," SAND80-2624 (Albuquerque, NM: Sandia National Laboratories, 1981).