

NUREG/CR-4780  
EPRI NP-5613  
Vol. 1

---

---

# Procedures for Treating Common Cause Failures in Safety and Reliability Studies

Procedural Framework and Examples

---

---

Pickard, Lowe, and Garrick, Inc.

Prepared for  
U.S. Nuclear Regulatory Commission

Electric Power Research Institute

8802030161 880131  
PDR NUREG  
CR-4780 R PDR

## NOTICE

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

## NOTICE

### Availability of Reference Materials Cited in NRC Publications

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

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

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

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

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

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

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

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

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Information Support Services, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

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

---

# Procedures for Treating Common Cause Failures in Safety and Reliability Studies

Procedural Framework and Examples

---

Manuscript Completed: November 1987  
Date Published: January 1988

Prepared by  
A. Mosleh and K. N. Fleming, Pickard, Lowe, and Garrick, Inc.  
G. W. Parry, NUS Corporation  
H. M. Paula, JBF Associates, Inc.  
D. H. Worledge, Electric Power Research Institute  
D. M. Rasmuson, U.S. Nuclear Regulatory Commission

Pickard, Lowe, and Garrick, Inc.  
2260 University Drive  
Newport Beach, CA 92660

Prepared for  
Division of Reactor and Plant Systems  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555  
NRC FIN A1384

Electric Power Research Institute  
3412 Hillview Avenue  
Palo Alto, CA 94303

## ABSTRACT

This report presents a framework for the inclusion of the impact of common cause failures in risk and reliability evaluations. Common cause failures are defined as that subset of dependent failures for which causes are not explicitly included in the logic model as basic events. The emphasis here is on providing procedures for a practical, systematic approach that can be used to perform and clearly document the analysis.

The framework comprises four major stages:

1. System Logic Model Development. The basic system failure logic is modeled in terms of basic events that represent component status.
2. Identification of Common Cause Component Groups. The principal object is to identify, using quantitative and qualitative screening, the groups of components that are felt to have significant potential for common cause failures.
3. Common Cause Modeling and Data Analysis. Common cause basic events are defined for inclusion in the logic model, to represent the residual dependent failures and probability models are constructed for each new basic event. At this stage, the logic model is extended from a component state basis to a component group impact basis. Historical data on multiple failure events are analyzed and the parameters of the probability models for common cause basic events estimated.
4. System Quantification and Interpretation of Results. The results are integrated into the system and sequence analyses and the results are analyzed.

The framework and the methods discussed for performing the different stages of the analysis integrate insights obtained from engineering assessments of the system and the historical evidence from multiple failure events into a systematic, reproducible, and defensible analysis.

## ACKNOWLEDGMENTS

To obtain a wide degree of consensus on the principles to be incorporated into this report, the contributions of many experts and organizations in the U.S. and Europe were solicited and received. Part of this participation took the form of in-depth reviews and written comments on earlier drafts of this report. Comments were received from:

- Sandia National Laboratories
- National Centre for Systems Reliability, UKAEA
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- New Hampshire Yankee (a division of PSNH)
- Kraftwerk Union, Germany
- Joint Research Centre, ISPRA of the European Economic Community, Italy
- Saratoga Engineering Consultants
- Central Electricity Generating Board, United Kingdom
- Brookhaven National Laboratory
- Idaho National Engineering Laboratory

In addition to the above organizations, special appreciation is expressed to the following individuals who have helped in the development of this report with their review and comments.

- Michael P. Bohn, Sandia National Laboratories - Albuquerque
- William E. Vesely, Science Applications International Corporation
- Lee Abramson, USNRC
- Angela M. Games, Safety and Reliability Directorate, UKAEA
- David Campbell, JBF Associates, Inc.
- Patrick W. Baranowsky, USNRC

## CONTENTS - VOLUME I

<u>Section</u>	<u>Page</u>
1 INTRODUCTION AND SUMMARY	1-1
1.1 General Purpose	1-1
1.2 Background	1-2
1.3 Reliability Benchmark Exercise on Common Cause Failures	1-2
1.4 Perspective on Dependent Events	1-4
1.5 Overall Objectives	1-8
1.6 Report Guide	1-9
1.7 References	1-9
2 FUNDAMENTAL CONCEPTS AND OVERVIEW OF A PROCEDURAL FRAMEWORK FOR THE ANALYSIS OF COMMON CAUSE EVENTS	2-1
2.1 Dependent Events and Their Mechanisms	2-1
2.2 Classification of Dependent Events	2-4
2.3 Overviews of the Procedural Framework for Common Cause Failures Analysis	2-8
2.3.1 Stage 1: Logic Model Development	2-8
2.3.2 Stage 2: Identification of Common Cause Component Groups	2-10
2.3.3 Stage 3: Common Cause Modeling and Data Analysis	2-12
2.3.4 Stage 4: Quantification and Interpretation of Results	2-13
2.4 Summary	2-13
2.5 References	2-13
3 ANALYSIS FRAMEWORK AND METHODOLOGY	3-1
3.1 Stage 1: System Logic Model Development	3-1
3.1.1 Step 1.1 - System Familiarization	3-3
3.1.2 Step 1.2 - Problem Definition	3-3
3.1.3 Step 1.3 - Logic Model Development	3-4
3.2 Stage 2: Identification of Common Cause Component Groups	3-5
3.2.1 Step 2.1 - Qualitative Analysis	3-6
3.2.2 Step 2.2 - Quantitative Screening	3-10
3.3 Stage 3: Common Cause Modeling and Data Analysis	3-12
3.3.1 Step 3.1 - Definition of Common Cause Basic Events	3-12
3.3.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events	3-16
3.3.3 Step 3.3 - Data Classification and Screening	3-25
3.3.4 Step 3.4 - Parameter Estimation	3-46
3.4 Stage 4: System Quantification and Interpretation of Results	3-59
3.4.1 Step 4.1 - Quantification	3-59
3.4.2 Step 4.2 - Results Evaluation and Sensitivity Analysis	3-59
3.4.3 Step 4.3 - Reporting	3-60

## ILLUSTRATIONS

<u>Figure</u>		<u>Page</u>
2-1	Procedural Framework for Common Cause Analysis	2-9
3-1	Key Input and Products of the Framework for Common Cause Analysis	3-2
3-2	Example of Event Classification and Impact Assessment	3-32
3-3	Example of the Assessment of Impact Vectors Involving Multiple Interpretation of Event	3-33
3-4	Decision Tree for Assessing and Mapping Event Impact Vectors	3-44
3-5	Simplified Emergency Cooling and Containment Cooling Systems	3-61
3-6	The Event Tree for the Sample Problem	3-63
3-7	Inclusion of Common Cause Basic Events	3-67
4-1	Simplified Schematic of Major Components in an Example Auxiliary Feedwater System	4-3
4-2	Reliability Block Diagram of Auxiliary Feedwater System - Normal Alignment	4-6
4-3	Component-Level Fault Tree of Example System	4-7
4-4a	Extensions to the Component-Level Fault Tree of Figure 4-3 To Incorporate Common Cause Events - Motor-Operated Valve Group	4-18
4-4b	Extensions to the Component-Level Fault Tree of Figure 4-3 To Incorporate Common Cause Events - Mechanical Pump and Motor Drive Group	4-19
4-5	The Distribution of MGL Parameters for the EFW Pump (excluding driver)	4-37
4-6	Relative Importance of Terms in AFWS Algebraic Model	4-40
4-7	Uncertainty Range of the Example AFW System Unavailability	4-43
4-8	Simplified Schematic of 125/250V DC Power System - Unit 2	4-47
4-9	Simplified Schematic of 125/250V DC Power System - Unit 3	4-48
4-10	Staggered Intervals for Quarterly Checks on Station Batteries and 24/48V Batteries	4-51
4-11	Fault Tree for Core Damage Scenario: CCFs in the 125/250V DC Power System Result in Loss of HPIC, RCIC, and ADS	4-53
4-12	Fault Tree for Core Damage Scenario: CCFs in the 125/250V DC Power System Result in Loss of All EDGs	4-53
4-13	Extension of Sample DC Power System Fault Tree (Figure 4-12) To Incorporate CCF Events	4-64

## TABLES

<u>Table</u>		<u>Page</u>
1-1	Treatment of Common Cause Events in Selected PRAs	1-6
1-2	Summary of Events Classified in Reference 1-2	1-7
2-1	Different Approaches to Dependent Events Categorization	2-5
2-2	Types of Dependent Events Based on Their Impact on a PRA Model	2-6
3-1	Key Characteristics of the Parametric Models	3-19
3-2	Formulas for Mapping Down Event Impact Vectors	3-37
3-3	Mapping Down Binary Impact Vectors from Four-Train and Three-Train System Data	3-38
3-4	Formulas for Upward Mapping of Events Classified as Nonlethal Shocks	3-41
3-5	Examples of Upward Mapping of Impact Vectors	3-43
3-6	Simple Point Estimators for Various Parametric Models	3-49
3-7	Event Classification and Analysis Summary	3-58
3-8	Basic Events Probabilities	3-64
3-9	Cutsets for Sequence $IE\bar{C}$ without Common Cause	3-65
3-10	Cutsets for Sequence $IE\bar{C}$ without Common Cause	3-66
3-11	Cutsets for Sequence $IE\bar{C}$ with Common Cause Added	3-68
3-12	Cutsets for Sequence $IE\bar{C}$ with Common Cause Added	3-69
4-1	Maintenance and Test Procedures Applicable to the Auxiliary Feedwater System	4-4
4-2	Cause and Component Group Combinations Initially Defined for the Auxiliary Feedwater System	4-10
4-3	Summary of Root Cause Analysis for the AFWS	4-17
4-4	Minimal Cutset of the Expanded Fault Tree of the Auxiliary Feedwater System	4-21
4-5	Terms of the Algebraic Model for the AFWS in Normal Alignment Basic Parameter Model Form	4-22
4-6	Quantification Formulas for Three Parametric Common Cause Models	4-24
4-7	Component-Level Minimal Cutsets for Example System - Normal Alignment	4-26
4-8	Classification and Impact Assessment of Events Involving Dependent Failures and Unavailabilities of Auxiliary Feedwater Pumps	4-28
4-9	Bayesian Estimates of the Parameters for Three Common Cause Models of the Example System	4-32
4-10	System Quantification Results Based on Three Parametric Models	4-38
4-11	Comparison of Cause Tables for Three Auxiliary Feedwater Systems in Normal Alignment Evaluated Using MGL Model	4-45
4-12	Systems and Surveillance Test Procedures Applicable to the 125/250V DC Power System	4-50



TABLES (continued)

<u>Table</u>		<u>Page</u>
4-13	Root Cause and Component Group Combinations Initially Defined for the 125/250V DC Power System	4-54
4-14	Nonvital DC Loads That Are Disconnected from the 125V DC Buses as Required by Procedure 6	4-60
4-15	Root Cause and Component Group Combinations Identified in Step 3 and Designated for Further Analysis	4-62
4-16	Classification and Impact Assessment of Events Involving Failures of Station Batteries	4-66
4-17	Classification and Impact Assessment of Events That Illustrate Root Cause/Component Group Combinations 3 through 8	4-69
4-18	Quantification of CCF Contribution	4-75

## ACRONYMS

<u>Acronym</u>	<u>Definition</u>
ADS	automatic depressurization system
AFW	auxiliary feedwater
AFWS	auxiliary feedwater system
BFR	binomial failure rate
BWR	boiling water reactor
CCF	common cause failure
CCF-RBE	Common Cause Failure Reliability Benchmark Exercise
CCS	containment cooling system
CST	condensate storage tank
ECS	emergency cooling system
ECWS	emergency cooling water system
EDG	emergency diesel generator
EOP	emergency operations procedure
EPRI	Electric Power Research Institute
ESWS	emergency service water system
FMEA	failure mode and effects analysis
HPCI	high pressure coolant injection
ISI	in-service inspection
KWU	Kraftwerk Union, Federal Republic of Germany
LER	Licensee Event Report
LOCA	loss of coolant accident
LOSP	loss of offsite power
MCS	minimal cutset
MGL	multiple Greek letter
MOV	motor-operated valve
NPE	<u>Nuclear Power Experience</u>
PRA	probabilistic risk assessment
PSNH	Public Service of New Hampshire
PWR	pressurized water reactors
RBE-CCF	Reliability Benchmark Exercise in Common Cause Failures
RCIC	reactor core isolation cooling system
RHR	residual heat removal
UKAEA	United Kingdom Atomic Energy Authority
USNRC	U.S. Nuclear Regulatory Commission

## GLOSSARY OF TERMS AND DEFINITIONS

In order to better communicate the procedures and guidance presented in this report, it is necessary and useful to summarize in one place the definitions of terms used frequently in dependent events analyses. More in-depth definitions of some of these terms are provided at appropriate points of the report, as needed, to provide a clear description of the methodology. Concise definitions are presented below.

1. Component. A component is an element of plant hardware designed to provide a particular function. Its boundaries depend on the level of detail chosen in the analysis. The hierarchy of the level of detail of modeling a plant in risk and reliability analysis flows from plant, to system, to subsystem, to component, then to cause (see definition below). For system modeling purposes, a component is at the lowest level of detail in the representation of plant hardware in the models. Events that represent causes of one or more component states in a system logic model (e.g., fault tree) are found at the level of detail below component.
2. Component State. Component state defines the component status in regard to the function that it is intended to provide. In this context, the following two general categories of component states are defined (the same states apply to higher levels of plant hardware, such as system):
  - a. Available. The component is available if it is capable of performing its function according to a specified success criterion. (Not to be confused with availability, which is defined below.)
  - b. Unavailable. The component is unable to perform its intended function according to a stated success criterion. It is important to note that the success criterion defined by the analyst to enable him to distinguish between available and unavailable states is not unique. This is because there are cases of several functions and operating modes for a given component, each with a different success criterion. Also, a given event in one plant may be classified differently for a similar component in another plant with different success criteria. Therefore, the specification and documentation of the success criteria and the reconciliation of potential mismatches between the data base and systems models become important tasks of the systems analyst.

Two subsets of unavailable states are failure and functionally unavailable. Note that "unavailable" should not be confused with "unavailability," which is defined below.

- (1) Failure. The component is not capable of performing its specified operation according to a success criterion. In order to restore the component to a state in which it is capable of operation, some kind of repair or replacement action is necessary. Additionally, the event may also be considered a failure when a component performs its function when not required or performs its function as required, but does not stop operating once meeting its success criteria. The latter is equivalent to saying that stopping when required is part of the success criterion. Therefore, failure encompasses functioning when not required, as well as not functioning when required.
- (2) Functionally unavailable. The component is capable of operation, but the function normally provided by the component is unavailable due to lack of proper input, lack of support function from a source outside the component (i.e., motive power, actuation signal), maintenance, testing, the improper interference of a person.

Sometimes, although a given success criterion has been met and the component has performed its function according to the success criterion, some abnormalities are observed that indicate that the component is not in its perfect or nominal condition. Although a component in such a state may not be regarded as unavailable, there may exist the potential of the component becoming unavailable with time, other changing conditions, or more demanding operational modes. Events involving these potentially unavailable states provide valuable information about causes and mechanisms of propagation of failures and thus should not be ignored. The concept of potentially unavailable states also serves a practical need to enable the consistent classification of "grey area" cases and difficult-to-classify situations. The following component state category is defined for this situation.

- c. Potentially Unavailable. The component is capable of performing its function according to a success criterion, but an incipient or degraded condition, as defined below, exists.
  - (1) Degraded. The component is in such a state that it exhibits reduced performance but insufficient degradation to declare the component unavailable according to the specified success criterion. Examples of degraded states are relief valves opening prematurely outside the technical specification limits but within a safety margin and pumps producing less than 100% flow but within a stated performance margin.

- (2) Incipient. The component is in a condition that, if left unremedied, could ultimately lead to a degraded or unavailable state. An example is the case of an operating charging pump that is observed to have excessive lube oil leakage. If left uncorrected, the lube oil could reach a critical level and result in severe damage to the pump.

A key to distinguishing between degraded and incipient conditions is the knowledge that an incipient condition has not progressed to the point of a noticeable reduction in actual performance, as is the case with a degraded condition.

It is important to recognize that potentially unavailable is not synonymous with hypothetical. Both incipient and degraded conditions are indicative of observed, real component states that, without corrective action, would likely lead to unavailable component states.

Although the above potentially unavailable states are often used in event report classification in support of parameter estimation, system models (e.g., fault trees) generally do not model states other than success or unavailable. Therefore, how potential states are "mapped" into two state models is an important subject of this procedures guide.

3. Cause. A cause is simply an explanation for why a component became unavailable or potentially unavailable. In complete, traditional system logic models, the cause level is the most detailed level of analysis and is almost always implicit in the quantification model, being located below the component level. With every cause, there exists a mechanism fully or partially responsible for the state of a component when an event includes a single component state; the cause of the component state is referred to (loosely) as a root cause. In more complex events involving two or more component states, a particular component state or set of component states can result from either a root cause or can be caused by the state of another component; i.e., component cause.
4. Event. An event is the occurrence of a component state or a group of component states.
5. Independent Event. An independent event is an event in which a component state occurs, causally unrelated to any other component state. Two events, A and B, are independent if and only if  $P(A \text{ and } B) = P(A) \cdot P(B)$ .

6. Dependent Event. If an event is not independent, it is defined as a dependent event. Two events, A and B, are dependent only if

$$P(A \text{ and } B) = P(A) \cdot P(B|A) = P(B) P(A|B) \neq P(A) \cdot P(B)$$

7. Common Cause Event. It is not the purpose of this report to resolve, once and for all, the issues associated with attempts to provide a clear and unambiguous definition of the term common cause event. The only way to treat these issues is to adopt a cause-effect event classification system, such as that described in detail in Reference 2-4 and summarized in Appendix A. Here, we define what common cause events mean to the systems analyst. In the context of system modeling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are a direct result of a shared cause. It is also implied that the shared cause is not another component state because such cascading of component states is normally due to a functional coupling mechanism. Such functional dependencies are normally modeled explicitly in systems models without the need for special common cause event models. The special models that have been developed to model common cause events, such as the beta factor, binomial failure rate, multiple Greek letter, basic parameter, common load, and other models, all apply to root-caused events branching to impact multiple components, but are generally not applied to component-caused events. A more focused definition of common cause events is presented in Section 2.
8. Root Cause. Ideally, the cause of an event can be traced to an event that occurred at some distinct but possibly unknown point in time. These causal events are known as "root cause." There are four general types of root causes.
- a. Hardware. Isolated random equipment failures due to causes inherent in the affected component.
  - b. Human. Errors during plant operations (dynamic interaction with the plant), errors during equipment testing or maintenance, and errors during design, manufacturing, and construction.
  - c. Environmental. Events that are external to the equipment but internal to the plant that result in environmental stresses being applied to the equipment.
  - d. External. Events that initiate external to the plant that result in abnormal environmental stresses being applied to the equipment.

9. Coupling Mechanism. A coupling mechanism is a way to explain how a root cause propagates to involve multiple equipment items; e.g., components. The three broad categories of coupling mechanisms are functional, spatial, and human.
- a. Functional Couplings
    - (1) Connected equipment. Encompasses plant design involving shared equipment, common input, and loop dependencies plus situations in which the same equipment provides multiple functions.
    - (2) Nonconnected equipment. Encompasses interrelated success criteria, such as the relationship between a standby system and the system it is supporting. More subtle forms of nonconnected equipment couplings are environmental conductors, such as heating, ventilation, and air conditioning systems.
  - b. Spatial Couplings
    - (1) Spatial proximity. Refers to equipment found within a common room, fire barriers, flood barriers, or missile barriers.
    - (2) Linked equipment. Equipment in different locations that, although not functionally related, is similarly affected by an extreme environmental condition possibly due to the breach of a barrier.
  - c. Human Couplings. Refers to activities, such as design, manufacturing, construction, installation, quality control, plant management, station operating procedures, emergency procedures, maintenance, testing and inspection procedures, and implementation, etc.
10. Unavailability. The probability (relative frequency) that a system or component occupies the unavailable state at a point in time. In applied risk and reliability evaluations, this point in time is when a randomly occurring initiating event or system or component challenge occurs. Availability is the complement of unavailability.
11. Unreliability. The probability (relative frequency) that a system or component fails (in regard to specified success criteria) during a specified time interval. This time interval is often referred to as the "mission time."
12. Shock. A concept used to explain how component states other than intrinsic, random, independent failures occur that is used in some common cause models, such as the EFR model. A shock is an event that occurs at a random point in time and acts on the system; i.e., all the components in the system simultaneously. There are two kinds of shocks distinguished by the potential impact of the shock event, as defined below.

- a. Lethal Shock. A lethal shock is a shock in which all the components in a system are failed, with certainty, any time the shock occurs.
  - b. Nonlethal Shock. A nonlethal shock is a shock that has some independent chance that each component in the system fails as a result of the shock. The range of possible outcomes (each having a different probability of occurrence) of a nonlethal shock range from no component failures to all the components failed.
13. Common Cause Component Group. A group of (usually similar) components that are considered to have a high potential of failing due to the same cause.
  14. Common Cause Basic Event. An event involving common cause failure of a specific subset of components within a common cause component group.
  15. Impact Vector. An assessment of the impact an event would have on a common cause component group. The impact is usually measured as the number of failed components out of a set of similar components in the common cause component group.
  16. Defensive Strategy. A set of operational, maintenance, and design measures taken to diminish the frequency and/or the consequences of common cause failures. Common cause design review, surveillance testing, and redundancy are therefore examples of tactics contributing to a defensive strategy.



## Section 1

### INTRODUCTION AND SUMMARY

#### 1.1 GENERAL PURPOSE

The purpose of this report is to provide a framework for common cause event analysis in applied risk and reliability evaluations. The term common cause events refers to a specific class of dependent events encountered by the system analyst in the performance of a plant-level PRA or a system-level reliability analysis. The methods for analyzing these events have historically been applied unsystematically and usually with little justification by individual analysts. Furthermore, the methods have recently undergone much development. These characteristics, in a field that can severely limit the reliability performance of redundant systems and contribute significantly to the risk of nuclear plant accidents, have resulted in the need for this report. Although much work has been published in this field, it is widely recognized that the available literature is lacking with respect to procedures and guidance for the current and prospective system analyst. Hence, it is a particularly appropriate time to take a "snapshot" of the current state of the art and to integrate the available tried and tested methods into a systematic framework for performing a system-level common cause analysis.

This report is the culmination of many years of research by the authors and others in the treatment of dependent failures in reliability and risk studies. The work reported here organizes the products of this research into a unified framework. This framework integrates qualitative and quantitative aspects of operating experience and design characteristics into a multi-step procedure that can be followed by systems analysts with a moderate level of experience. It is not the purpose of this report to advance or promote a particular method or technique. Nor is the intention to rigidly constrain the analyst to a prescribed recipe for common cause analysis.

The purpose of the procedural framework advanced here is to allow the analyst to make intelligent choices along the way, while obliging him to consider the issues involved, the consequences of his decisions, and the need to document the process very carefully. Although the choice of particular techniques and models is left to the discretion of the analyst, the framework will provide the structured approach needed to make future common cause analysis contributions to risk or reliability studies (1) more tractable from the point of view of the analyst, (2) more consistent and scrutable to peer and regulatory reviewers, (3) more realistic from the point of view of plant operators, and (4) more defensible by study sponsors. The framework proposed goes further than providing procedural guidance; together with the technical appendices that explain the relationship between the various models and the demands made by them on the data analysis, the procedure presents a fairly complete conceptual, as well as practical, framework for dealing with common cause failures.

## 1.2 BACKGROUND

The major vehicle for the production of the procedural framework was the invitation extended by the Electric Power Research Institute to the U.S. Nuclear Regulatory Commission Office of Research, to jointly collaborate on integrating the results of EPRI and USNRC research during the closing phase of EPRI Research Project RP2169, "A Study of Common Cause Failure." This collaboration was considered essential to make the most informed use of the available research products and to create a powerful industry consensus on the most reasonable treatment for a significant contributor to the probability of nuclear plant accidents.

The USNRC had sponsored research in the area of common cause failures for many years. Quantitative methods for treating common cause events were first investigated, followed by work on data analysis. More recently, the research has focused on qualitative screening methods.

EPRI, through RP2169, had sponsored such research since 1981. Initially the project addressed the definition of common cause events and developed a classification system to aid the interpretation and use of plant data; i.e., historical common cause events. The method proposed for using the data developed into a preliminary version of the procedural framework. Subsequent work, again emphasizing data analysis, focused on the effectiveness of various defensive tactics that could be employed in plant design and operation to lessen the susceptibility to common cause failures.

Others have also done relevant research, especially in Europe. From the beginning, the EPRI project liaised closely with this work. The final product, described in this report, has benefited greatly from the recently completed "Reliability Benchmark Exercise in Common Cause Failures," sponsored by the Euratom Joint Research Centre in Ispra, Italy. The U.S. participation was jointly sponsored by EPRI and USNRC. Insights gained from the RBE-CCF have influenced the preparation of this report. These insights and the collaboration that led to them are reported in Section 1.3.

A concerted effort was then required to pull together what had been developed internationally and within the United States into a cohesive and useful framework to aid the analyst. To obtain a wide degree of consensus on the principles to be incorporated into this guide, the contributions of many experts and organizations in the United States and Europe were solicited and received.

Most topics presented in this report have received wide peer review. However, some topics have not, such as the mapping of failure events, but are presented here because of their importance.

## 1.3 RELIABILITY BENCHMARK EXERCISE ON COMMON CAUSE FAILURES

The international benchmark exercise, organized by the Joint Research Centre of the European Economic Community at Ispra, Italy, had, as a principal objective, the testing of methods for system-level common cause analysis.

The Common Cause Failure Reliability Benchmark Exercise (Reference 1-1) was carried out over a 2-year period, 1984 to 1986, and comprised 10 teams representing 8 countries, including Belgium, Denmark, France, Federal Republic of Germany, Italy, Sweden, United Kingdom, and the United States.

In this benchmark exercise, each team performed a PRA-type systems analysis of the same system, an emergency feedwater system at the Grohnde PWR plant in the Federal Republic of Germany built by KWU. The independent events analysis, data base, systems boundaries, and success criteria were fixed, and each team was asked to perform a systems analysis that included common cause events using whatever methods and data bases deemed appropriate by each team.

The benchmark exercise was structured into phases and tasks that focused on particular issues, such as the definition of boundary conditions and success criteria, the roles of explicit and parametric models, the selection of a parametric model, the analysis of event data in support of parameter estimation, the use of computer programs, and the identification of principal contributors to the results. As one part of the exercise, each team provided its own independent assessment of the same set of classified event reports from U.S. operating experience (Reference 1-2) to support the quantification of common cause parameters.

The CCF-RBE had a major impact on this report. In providing its contribution (Reference 1-3) to the benchmark exercise, the U.S. team used a set of procedures and analytical framework that conformed to an earlier draft of this report. This provided an opportunity to test the basic steps of the procedural framework and to identify aspects of the draft procedures that needed improvement. Among the lessons learned from the CCF-RBE that the authors found to be particularly useful in the development of this procedures guide are the following.

- There are important roles for both explicit and parametric modeling of common cause events, and care must be taken not to double count the same events with both approaches.
- The importance of a thorough, systematic qualitative analysis as a prerequisite to a meaningful quantitative analysis cannot be overstated. Most of the variations in the results that are introduced by the analyst are so introduced in the qualitative phase of the analysis.
- Because of the practical limitations associated with efforts to ensure adequate completeness, procedures for both qualitative and quantitative screening of potential dependent events are necessary, important, and must be carefully documented.
- Once the qualitative analysis and system logic model are fixed and the available data are interpreted consistently, the selection of a parametric model among a relatively large set of tried and tested models is not particularly important and does not introduce an appreciable level of uncertainty.

- The greatest sources of uncertainty in common cause analysis lie in the areas of data collection and interpretation. There should be structured procedures for reducing these uncertainties. Every effort should be made to quantify the impact of these uncertainties i. the estimation of common cause event frequency parameters.
- Care must be taken to account for the impact common cause events have on the Boolean reduction of a system fault tree.

#### 1.4 PERSPECTIVE ON DEPENDENT EVENTS

Dependent events have long been recognized as a source of difficulty facing those responsible for the safe design and operation of nuclear energy systems. Dependent failures are those failures that defeat the redundancy or diversity that is employed to improve the availability of some plant function such as coolant injection. In the absence of dependent failures, separate trains of a redundant system, or diverse methods of providing the same function, are regarded as independent so that the unavailability of the function is essentially the product of the unavailabilities of the separate trains or diverse systems. However, a dependent failure arises from some cause that fails more than one system, or more than one train of a system, simultaneously. Thus, the effect of dependent failures is to increase the unavailability of the function with respect to the situation of true independence.

Reactor operating experience has shown that dependent events are major contributors to reactor incidents and accidents (References 1-2 and 1-4). This result, in one respect, is due to the success achieved in minimizing the frequency of potential accidents caused by the unfortuitous coincidence of independent events. It is also indicative of the high degree of reliability that has been achieved through the use of the design principle of redundancy, which has been particularly effective in reducing the impact of single independent equipment failures. On the other hand, the operating experience indicates that enhanced defenses against dependent events may sometimes be needed. Hence, it is appropriate that current priorities in risk management be aimed toward controlling the risk contribution of dependent events.

Over the past decade since the Reactor Safety Study (Reference 1-5), we have seen the completion of a couple of dozen probabilistic risk assessments and a rapid increase in the application of risk and reliability methods. We have also seen a consistent pattern emerging in the results of these applications that reinforces the importance of dependent events that is apparent in accounts of reactor operating experiences. These results consistently include a finding that various types of dependent events dominate plant risk and system unavailability.

System analysts generally try to include most explicit dependencies in the basic system or plant logic model. So, for example, functional dependencies arising from the dependence of frontline systems on support systems, such as power or service water, are included in the logic model by including basic events, which represent component failure modes associated with failures of these support systems. Failures resulting

from the failure of another component (cascading or propagating failures) are also modeled explicitly. Operator failures to respond in the manner called for by the operating procedures are included as branches on the event trees or as basic events on fault trees. Some errors made during maintenance are usually modeled explicitly on fault trees, or they may be included as contributors to overall component failure probabilities or rates.

The logic model constructed initially has basic events that to a first approximation are considered independent. This is a step that is necessary to enable the analyst to construct manageable models. However, many dependencies among component failures are not accounted for explicitly in the logic model, and this means that the basic events are not, in fact, independent. This is accounted for by introducing the concept of common cause basic events, which represent the class of residual dependent failures whose root causes are not explicitly modeled. In a PRA model, a common cause event is defined as the failure or unavailable state of more than one component at the same time and due to the same shared cause. Common cause events require the existence of some cause-effect relationship that links the failures of a set of components to a single shared root cause.

As the examples in Table 1-1 show, there has been a lack of consistency in the treatment of common cause failures in PRAs. The inconsistency appears in a variety of ways. For example, some studies have not modeled common cause failures, and where they have been modeled, the degree of modeling and the methods used for quantification have differed. One of the most significant differences has been in the collection, interpretation, and use of data.

Several independent data analysis projects have compiled dependent failure events. One of these, sponsored by the USNRC, has identified common cause events in the course of quantifying CCF parameters for various components (References 1-13 to 1-17). Another, sponsored by the Electric Power Research Institute, produced a dependent events data base in Reference 1-2 with the use of a classification system that was a product of the same research project (References 1-18 and 1-19). Some gross statistics of this EPRI-sponsored data base are provided in Table 1-2. Included in this table are 113 common cause events out of a total of 2,654 events that were analyzed from a 10-year period (1972 through 1981). A key point emphasized in this report is that there is not enough plant-specific common cause data to provide reliable estimates of common cause failure probabilities, and the total industry data base must be used. However, statistical data like those in Table 1-2 cannot be incorporated into a plant-specific systems analysis without a careful event-by-event evaluation to determine the applicability and impact of each event on the system being analyzed and without taking into account the various sources of uncertainty, such as modeling assumptions and analyst's judgment in interpretation and use of the available evidence.

Many of the dependent failure events identified thus far do not fit in the plant and system logic models that rely on explicit modeling. The reason is that explicit models generally do not model failures at the subcomponent-level or at the level of "root" causes that impact two or

Table I-1

## TREATMENT OF COMMON CAUSE EVENTS IN SELECTED PRAs

PRA	Year Completed	Method Used for Subcomponent Level Common Cause Failure Analysis	Reference
Reactor Safety Study	1975	"Square root method" used in selected cases.	(1-5)
HTGR AIPA Study	1976	Beta factor method used for all redundant active components; parameters quantified from LWR and GCR operating experience.	(1-6)
Zion PSA	1978	Beta factor method used for selected components; parameters quantified judgmentally.	(1-7)
RINGHALS 2	1981	C-factor method used for most redundant active components; parameters quantified from plant-specific and generic data.	(1-8)
IREP PRAs	1983	Selected CCF events were modeled explicitly in the fault trees, and their frequencies were estimated directly from operational data or using human reliability analysis.	(1-9)
Seabrook PSA	1983	Multiple Greek letter, beta factor, and their variations used for all redundant active and some diverse components. Parameters estimated from 500 reactor years of U.S. operating experience data.	(1-10)
Sizewell PRA	1984	CCF not modeled; cutoff probabilities used and sensitivities to arbitrary changes calculated.	(1-11)
Oconee PRA	1984	CCF not modeled and not reflected in quantification.	(1-12)

Table 1-2

## SUMMARY OF EVENTS CLASSIFIED IN REFERENCE 1-2

Component	Reactor Years	Number of Events Classified*	Event Distribution		
			Independent	Dependent	Generic Common Cause Events
Reactor Trip Breakers	563	72	56	16	11
Diesel Generators	394	674	639	35	22
Motor-Operated Valves	394	947	842	105	42
Safety/Relief Valves					
PWR	318	54	30	24	0
BWR	245	172	136	36	14
Pumps					
Safety Injection	394	112	77	35	8
RHR	394	117	67	50	5
Containment Spray	394	48	32	16	2
Auxiliary Feedwater	394	255	194	61	5
Service Water	394	203	159	44	4
Total	-	2,654	2,232	422	113

\*Events classified include those having one or more actual or potential component failures or functionally unavailable states.

more components because they cannot conveniently be made to do so. The analysis framework of this report does represent the specific combinations of groups of components that can fail due to shared causes. Root causes are considered in deciding which historical events apply to the case in question. The way these shared causes affect the component groups is treated by using implicit modeling. This is the main justification for including common cause basic events explicitly in the model.

## 1.5 OVERALL OBJECTIVES

The overall objectives of this guidebook are to:

1. Provide a procedural framework for common cause analysis for use in applied risk and reliability evaluations by and for the nuclear industry.
2. Provide a comprehensive and integrated systems analysis framework for common cause analysis that includes a proper balance between qualitative and quantitative aspects.
3. Provide guidance and analysis techniques to circumvent some of the practical problems facing the common cause analyst.
4. Account for advances that have been made in the state of the art in common causes and thereby serve to update previously published PRA procedures guides.
5. Identify important interfaces between the various tasks, including qualitative analysis, systems modeling, event classification, parameter estimation, and quantitative analysis tasks.
6. Provide the flexibility of choice among alternative systems modeling approaches and techniques for parameter estimation and data handling when alternatives exist and when the superior choice cannot be easily determined.
7. Solicit a sufficiently broad base of input to achieve a consensus on the principles of common cause failure analysis to the extent possible within the constraints of schedule and budget.

In addressing objective 6, it was not felt necessary to include all the various models that have been proposed for common cause event quantification. A specific set of parametric modeling techniques was selected to provide adequate representation of the variety of methods that have been proposed, with an emphasis on those that have been actually used to a significant extent on published risk or reliability evaluations.

While the selection and incorporation of the appropriate parametric model is an important objective of this report, a more important one is to address important interfaces among the tasks of a systems analysis that are necessary to fully address the effects of common cause events on



plant and system performance. The full implications of common cause events in tasks such as fault tree construction, minimal cutset determination, and data analysis have generally not been recognized in previous procedure guides as deserving special attention in the case of common cause events, but these tasks are emphasized in the present procedure.

A key requirement was to present the procedure in a manner that facilitated its practical application, while providing in the appendices the depth and details required for understanding special technical topics related to modeling details, assumptions, and theoretical backgrounds.

The objective of the main body of the report is to present the procedural framework, analysis steps, and practical guidelines to enable an experienced PRA/reliability analysis practitioner to perform a defensible common cause failure analysis that considers all of the elements of the analysis that have a significant impact on the results. The presentation is supported by a series of appendices that provide more precise understanding of the analytical techniques, their conceptual origin, assumptions, and their interrelationships. The appendices enable the analyst to have a better appreciation of the reasons for the various steps of the analysis and the implications of the assumptions made in each step. It also provides additional practical guidelines for a more detailed analysis and for the cases where certain variations of the main techniques might be needed.

## 1.6 REPORT GUIDE

The procedures and guidance presented in this report are based on experience and selected case studies in dependent events analysis, as well as detailed probabilistic methodology. Some fundamental concepts and an overview of the procedural framework are presented in Section 2. Section 3 provides a discussion of the basic elements of the systematic approach supported by a series of appendices in Volume II for methodological details.

The major presentation of guidance on how to apply the methodology is made in terms of application to two example systems in Section 4.

Finally, Section 5 discusses areas in which enhancements can be made in the analysis of common cause failures through further refinement in models and data bases.

## 1.7 REFERENCES

- 1-1. Poucet, A., A. Amendola, P. C. Cacciabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Center Report, PER 1133/86, Ispra, Italy, April 1986.
- 1-2. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," Pickard, Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

- 1-3. Fleming, K. N., et al., "Common Cause Failure Reliability Benchmark Exercise, United States Team Contribution," prepared for Electric Power Research Institute, PLG-0426, July 1985.
- 1-4. G. M. Ballard, "An Analysis of Dependent Failures in the ORNL Precursor Study," Proceedings of the ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, pp. 6-1 to 6-10, San Francisco, California, February 24-March 1, 1985.
- 1-5. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, NUREG-75/014, October 1975.
- 1-6. Fleming, K. N., et al., "HTGR Accident Initiation and Progression Analysis Phase II Risk Assessment," United States Department of Energy Report, GA-A15000, UC-77, April 1978.
- 1-7. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, September 1981.
- 1-8. NUS Corporation, "Ringhals 2 Probabilistic Risk Assessment," NUS-4635, May 1983.
- 1-9. U.S. Nuclear Regulatory Commission, "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, January 1983.
- 1-10. Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, December 1983.
- 1-11. Vavrek, K. J., and G. R. Andre, "Sensitivity Study of Common Mode Failure Rates for Sizewell B," Proceedings of the ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, Vol. 2, pp. 102-1 to 102-8, San Francisco, California, February 24-March 1, 1985.
- 1-12. Nuclear Safety Analysis Center, "Oconee PRA, A Probabilistic Risk Assessment of Oconee Unit 3," cosponsored by the Nuclear Safety Analysis Center, Electric Power Research Institute, and Duke Power Company, NSAC 60-SY, June 1984.
- 1-13. Bari, R. A., et al., "Probabilistic Safety Analysis Procedures Guide," Brookhaven National Laboratory, NUREG/CR-2815, Rev. 1, August 1985.
- 1-14. Atwood, C. L., "Common Cause Fault Rates for Pumps," NUREG/CR-2098, prepared for the U.S. Nuclear Regulatory Commission by EG&G Idaho Inc., February 1983.

- 1-15. Steverson, J. A., and C. L. Atwood, "Common Cause Fault Rates for Valves," NUREG/CR-2770, prepared for the U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.
- 1-16. Atwood, C. L., "Common Cause Fault Rates for Diesel Generators," NUREG/CR-2099, prepared for the U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., June 1982.
- 1-17. Meachum, T. R., and C. L. Atwood, "Common Cause Fault Rates for Instrumentation," NUREG/CR-3289, prepared for the U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., May 1983.
- 1-18. Los Alamos Technical Associates, Inc., "Common Cause Failures--Phase I: A Classification System," EPRI NP-3383, January 1984.
- 1-19. Los Alamos Technical Associates, Inc., "A Study of Common Cause Failures--Phase II: A Comprehensive Classification System for Component Fault Analysis," EPRI NP-3837, May 1985.

## Section 2

### FUNDAMENTAL CONCEPTS AND OVERVIEW OF A PROCEDURAL FRAMEWORK FOR THE ANALYSIS OF COMMON CAUSE EVENTS

The purpose of this guide is to provide a framework to guide experienced analysts in the performance of systems analyses that adequately account for common cause events. Common cause events are a subset of the more general class of dependent events whose causes are not normally explicitly modeled as basic events in the system logic models, especially when these models are developed only to the level of detail that defines component failure modes. In principle, the system logic models can be developed further to include a larger number of basic events that correspond with common cause events. Each common cause basic event in such a logic model would be indicated as resulting in failure of two or more specific components in the system. One of the important tasks in a common cause analysis is to define, unambiguously, the appropriate combination of explicit and implicit or parametric modeling techniques and the appropriate analysis of the data in support of those techniques to ensure adequate completeness, while avoiding the double counting of any basic event. A clear understanding of the mechanisms by which dependent events occur is essential to performing this task.

Given the definition of the events, it is necessary to categorize and interpret experience data to identify occurrences of the defined set of common cause events and use the data to estimate the probability of common cause events for use in reliability evaluations. Section 2.1 discusses in general terms the mechanisms of dependent events and how an understanding of the mechanisms can be used to define common cause failure events. Section 2.2 is a brief description of event classification schemes that have been developed to provide a framework to help provide a systematic interpretation of the data. These classification schemes help to distinguish between such component states as failure, functional unavailability, and various degraded states. They also help to distinguish between independent and dependent failures, of which common cause failures are identified as a subset. Section 2.3 is a brief review of the procedural framework, discussed in detail in Section 3, that has been developed to incorporate common cause failures into systems analysis and that is the subject of this guide.

#### 2.1 DEPENDENT EVENTS AND THEIR MECHANISMS

To understand dependent events and to model them, it is necessary to answer such questions as: Why do components fail or why are they unavailable? What is it that can lead to multiple failures? Is there anything at a particular facility that could prevent such multiple failures occurring?

These questions lead to the consideration of three concepts. The first is the root cause of failure or unavailability. A root cause is a mechanism of a transition of state from available to that of failed or functionally unavailable. Several different classification schemes for root causes have been developed; some are hierarchical (see for example

Reference 2-1), others are not (Reference 2-2), and some root cause classification schemes (References 2-3 and 2-4) were developed particularly for dependent failure and common cause analysis. These classification schemes will be discussed in Section 2.2. One thing is clear, however, a dependent event root cause classification scheme is simply a special case of the more general root cause classification scheme that covers all events; i.e., both dependent and independent events. Although each of the available classification schemes has its own advantages and disadvantages, a meaningful common cause analysis requires proper identification of the root cause. The degree of detail in specifying the root cause is dictated by how specific an analysis needs to be, but it is clear that a thorough understanding of dependent events and how they can be prevented can only come from a very detailed specification of the types of root causes. Ideally, the root cause categories should be exhaustive and mutually exclusive to avoid ambiguity in classification.

Given the existence of the root cause, the second concept of importance is that of a linking or coupling mechanism, which is what leads to multiple equipment failure. The coupling mechanism explains why a particular cause impacts several components. Obviously, each component fails because of its susceptibility to the conditions created by the root cause, and the role of the coupling mechanism or link is in making those conditions common to several components.

For example, suppose that two components are susceptible to high humidity and that they are located in the same room. A common cause failure could occur as a result of an event at the plant, which results in high humidity in this room. High humidity is the root\* cause of failure of each of the two components. One immediately recognizable coupling mechanism is the fact that both components are located in the same room.

Another example of a dependent event that occurred at a U.S. nuclear power plant is the case of a redundant safety injection system that failed to actuate because of a design error in which the motor-operated valves in the redundant pump trains were undersized and unable to open against the differential pressure created by the operation of the pumps. In this example, the root cause of failure of each valve is an undersized motor due to error in the design process. The use of identical valves and common demand conditions form the coupling mechanism, together with the inability of the surveillance tests to reveal this condition prior to the actual demand.

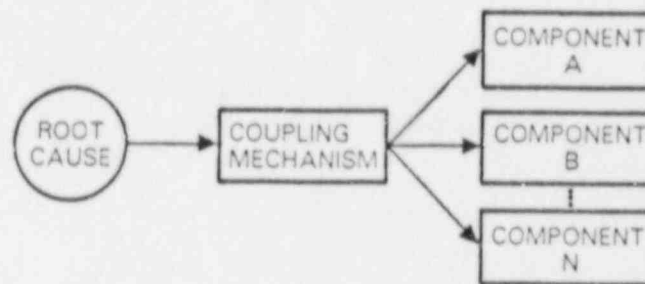
Dependent failures therefore can be thought of as resulting from the coexistence of two factors, one that provides a susceptibility for components to fail or to be unavailable from a particular root cause of

---

\*Depending on how far back the identification of failure causes goes, high humidity could be considered as the immediate cause, being caused itself by some other cause or causes; e.g., pump leakage. Hence, the term "root cause" can imply different levels of deductive reasoning in establishing the cause. In one of the classification schemes discussed below, root cause is defined as that entire set of sequential steps that precedes the occurrence of a component state.

failure and a coupling mechanism that creates the conditions for multiple components to be affected by the same cause. This is illustrated by the following figure.

There is a third factor that enters into determining the potential for dependent failures, including common cause failures, and it is arguably the key determinant. This factor is the existence or lack thereof of engineered or operational defenses against unanticipated equipment failures. Typical tactics adopted in a defensive scheme include design control, segregation of equipment, well-designed test and inspection



Physical Elements of a Dependent Event

procedures, maintenance procedures, review of procedures, training of personnel, manufacturing and construction quality control, and installation and commissioning quality control. The different tactics may be particularly effective for mitigating specific types of dependent or common cause failures.

As an example of a defensive strategy, physical separation of redundant equipment reduces the chance of simultaneous failure of the equipment due to certain environmental effects. In this case, the defense acts to remove the coupling mechanism. Other tactics may be effective at reducing the likelihood of independent failures as well as dependent failures by reducing the susceptibility of components to certain types of root causes. Thus, it can be argued that a complete treatment of dependent failures should not be performed independently of an analysis of the independent failures; rather, the treatment of all failures should be integrated. Indeed, the procedural framework advocated in this report places emphasis on the proper integration of the treatment of dependent and independent events.

Although the preceding discussion applies to all types of dependent failures, the thrust of this document is the treatment of common cause failures. Many types of dependent failures, failures of components resulting from failures of support systems or cascade type failures, for example, in which failure of one component implies unavailability of another because of some functional dependency, can be and usually are modeled explicitly. Thus, in logic models, one of the contributors to the event, "unavailability of component A," can be the unavailability of the support systems on which operation of component A depends. However, it is not, in general, practical to attempt to model all dependent failures explicitly, especially when the cause is not the failure of another component.

That group of dependent events whose failure mechanisms are not normally modeled explicitly in the system logic model and whose cause does not involve failure or unavailability of another component are known as common cause events. Having excluded the occurrence of multiple functional unavailabilities of components resulting from failure of another component from this definition, all common cause events of practical interest are also common cause failures. The concepts of root cause and coupling mechanism are used below to identify types of dependent failures that can be modeled explicitly and that are not to be included in the common cause events. As discussed later, these concepts, and those of defenses, are crucial to the systematic interpretation of historical data to identify and quantify the potential for common cause failure.

From a probabilistic point of view, the importance of common cause failures is that their existence implies that failures of two or more components, symbolically represented by A and B, are not probabilistically independent;

and, indeed,

$$P(A \text{ and } B) > P(A) \cdot P(B)$$

It is the purpose of this document to provide an analyst with a procedural framework and some guidance on how to use this framework to estimate the significance of this dependence in applied risk and reliability evaluations.

## 2.2 CLASSIFICATION OF DEPENDENT EVENTS

The categorization scheme of the PRA Procedures Guide summarized in Table 2-1 provides a convenient way to identify the nature and scope of dependent events analysis in a PRA. The logic of this categorization scheme is based on the observation that dependent events must be considered not only in the quantification, but also in the definition of accident sequences in a PRA. Accident sequences are defined by initiating events and event trees. Hence, dependent events can: (1) cause initiating events and interact with one or more event tree top events, (2) interact with two or more top events in the event tree, or (3) interact with components within a given event in the event tree. Based on this observation, the PRA Procedures Guide defined a corresponding set of categories: (1) common cause initiating events, (2) intersystem dependencies, and (3) intrasystem dependencies. The dependent events categories determined by these three possibilities were further subdivided, as described in Table 2-1.

To make effective use of the historical data in support of common cause analysis, it is important to clearly distinguish between dependent events that are to be modeled explicitly and those that are contributors to the class of common cause events. A great degree of success in a systematic approach to this screening of data has resulted from attempts to develop a taxonomy (i.e., a systematic, "top-down" categorization scheme for these events) for the broad and all-encompassing notion of a dependent event. The PRA Procedures Guide scheme described above provided one such taxonomy.

Table 2-1

## TYPES OF DEPENDENT EVENTS BASED ON THEIR IMPACT ON A PRA MODEL

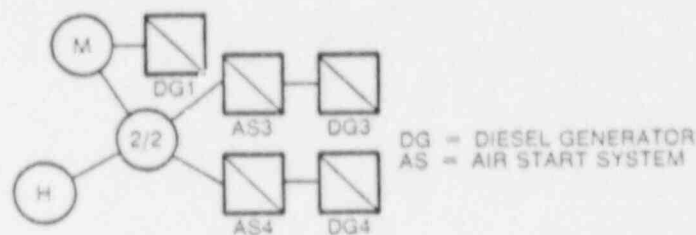
Dependent Event Type	Characteristics	Subtypes (coupling mechanisms)	Examples (trigger events)
1. Common Cause Initiating Event	Causes a plant transient and increases unavailability of one or more mitigating systems.	<ul style="list-style-type: none"> <li>● Functional</li> <li>● Spatial</li> <li>● Human</li> </ul>	<ul style="list-style-type: none"> <li>● Loss of offsite power.</li> <li>● Earthquake.</li> <li>● Maintenance error shorting out instrument bus.</li> </ul>
2. Intersystem Dependency	Causes a dependency in a joint event probability involving two or more systems.	<ul style="list-style-type: none"> <li>● Functional</li> <li>● Spatial</li> <li>● Human</li> </ul>	<ul style="list-style-type: none"> <li>● Coolant charging fails because component cooling fails.</li> <li>● Fire causes loss of equipment of two systems.</li> <li>● Operator error causes loss of two systems.</li> </ul>
3. Intercomponent (intrasystems) Dependency	Causes a dependency in a joint event probability involving two or more components.	<ul style="list-style-type: none"> <li>● Functional</li> <li>● Spatial</li> <li>● Human</li> </ul>	<ul style="list-style-type: none"> <li>● Battery loses charge after it is run beyond capacity.</li> <li>● Fire causes loss of redundant pumps.</li> <li>● Design error present in redundant pump controls.</li> </ul>



Some of the better known attempts to develop a taxonomy for dependent events are summarized in Table 2-2. Although there is much in common with the different approaches listed, each provides a unique perspective of the various attributes of dependent events, and, taken as a whole, all contribute to a better understanding of their nature, causes, and possible defenses. Each of these schemes incorporates to some degree the concepts of root causes and coupling mechanisms either implicitly or explicitly.

The EPRI event classification scheme was developed as an alternative to the unachievable task of developing a coherent and unambiguous definition of a common cause failure. It has proved useful in the classification of event reports for the purpose of delineating the logical interrelationships among the cause or causes of an event and the event impacts, as determined by the failure or functional unavailability of specific components. A key feature of this system is a cause-effect logic diagram.

A typical cause-effect diagram is shown in the following:



Example Cause-Effect Logic Diagram

The diagram represents an event that happened at the Peach Bottom plant in June 1977 when three out of four diesel generators became inoperable. Air start systems of diesel generators 3 and 4 were cross-tied with the air start of diesel generator 1 to "correct" a previous failure. Later, when diesel generator 1 was taken out of service for maintenance, air supply to diesel generators 3 and 4 was lost, making both diesels inoperable. In the above figure, circles with letters represent causes encoded with the letters "H" for human and "M" for maintenance. Component states are represented by squares. In general, all components are classified as either available or unavailable with respect to a particular success criterion. An unavailable component is either failed (☒) or functionally unavailable (☑) to cover cases in which the nonfunctioning is due to the lack of required input. To cover degraded performance short of violating the success criteria, incipient failures, ambiguous event reports, and difficult-to-classify situations, each component state can be classified as either actual or potential. This classification is extremely useful in screening events for use in a common cause analysis. A fuller description of the classification system is found in Appendix A.

In the EPRI event classification system, events can be classified according to the structure of the cause-effect logic diagram. Of particular concern are the branched events, such as the event described above in which there is a branching or propagation between a given node

Table 2-2

## DIFFERENT APPROACHES TO DEPENDENT EVENTS CATEGORIZATION

Dependent Events Categorization Scheme	Basis of Categorization	Reference
Edwards and Watson	Hierarchy of engineering and operational activities to identify specific categories of causes.	(2-3)
Generic Cause	Comprehensive set of causes and conditions that lead to dependent events with emphasis on spatial interactions.	(2-5)
PRA Procedures Guide	Categories and subcategories defined by different ways dependent events impact a PRA model.	(2-6)
EPRI Systems Interaction Procedure Guide	Logical breakdown of different types of trigger events and coupling mechanisms that cause the events.	(2-7)
EPRI Event Classification Scheme	Categories based on different key structures of cause-effect logic diagrams developed for experienced events.	(2-4), (2-8)

and two or more component states. When the causes feeding into the branching node are root causes (i.e., other than component states), the event is classified as a root-caused branched event.

There is an obvious relationship between the EPRI event classification scheme and the root cause coupling mechanism. The chief difference is that the latter concept breaks down the cause in the EPRI scheme into two components: the root cause and the coupling mechanism. Hence, in terms of the root cause coupling mechanism representation, a common cause event is simply a dependent event in which the root cause and coupling mechanism are other than failure or functional unavailability of another component. In terms of the PRA Procedures Guide scheme, common cause events can be defined in each of the three main categories although, in most practical cases, they are limited to the intrasystem dependency category. The key characteristics of a common cause event shared by all these classification schemes is that two or more components must be affected by a single, shared cause and that this cause must not be failure or functional unavailability of another component.

## 2.3 OVERVIEWS OF THE PROCEDURAL FRAMEWORK FOR COMMON CAUSE FAILURES ANALYSIS

The previous two sections have provided some basic tools with which to analyze common cause failures. This section is a brief description of the procedural framework that has been developed to perform such an analysis. There are four major stages each of which contains a number of steps. They are summarized in Figure 2-1.

### 2.3.1 Stage 1: System Logic Model Development

The objective of this stage is to construct a logic model that identifies the contributions of component states that lead to the undesired system state.

2.3.1.1 Step 1.1 - System Familiarization. This is an essential element of any system analysis. To be able to model a system, the analyst must understand what the intended function of the system is, what components it is composed of, and what procedures govern its operation, testing, and maintenance. In addition, the analyst needs to know the relation of the system being analyzed to other systems as well as to its physical environment in the broader picture of a plant model.

From a common cause failure standpoint, particular attention needs to be paid to identifying those elements of design, operation, and maintenance and test procedures that could influence the chance of multiple component failures. The information collected in this step is essential in the identification of potential sources of dependence and grouping of components in the screening phases of the analysis (Steps 2.1 and 2.2).

2.3.1.2 Step 1.2 - Problem Definition. In this step, the analysis boundary conditions, such as the physical and functional systems boundaries of the system, functional dependencies on other systems (support systems), functional interfaces with other systems, and, finally, system success criteria, need to be defined. This determines what equipment should be modeled, how it should operate for the system to

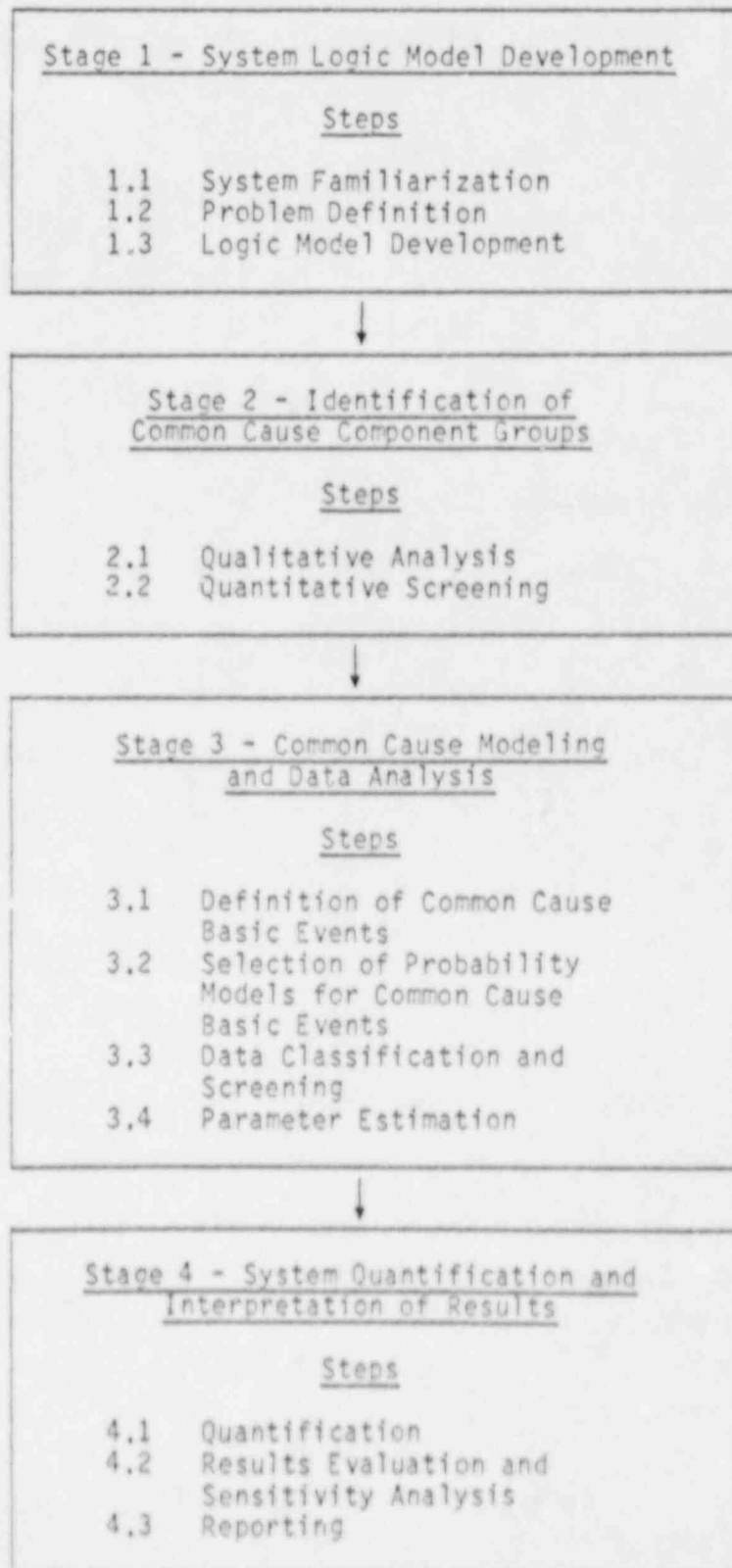


Figure 2-1. Procedural Framework for Common Cause Analysis

perform its intended function (which failure modes to consider), what are the success criteria, and what are the applicable mission time and possible initial system alignments. In this process, potential operator actions, the impact of test and maintenance requirements, and other assumptions and ground rules imposed on the analysis in the context of the overall plant model should be identified.

From the point of view of dependent failures, those root causes of dependency that are to be explicitly modeled should be identified. Examples of causes that are frequently modeled explicitly are fire, flood, or earthquake. Similarly, certain categories of human errors, such as calibration errors and errors to return equipment and system to their original configuration after test and maintenance, are typically modeled explicitly. This process then defines the scope of the residual common cause failure analysis. It cannot be overemphasized that extra care is needed in the application of parametric common cause models in order not to double count for causes explicitly modeled.

2.3.1.3 Step 1.3 - Logic Model Development. The first step in any system analysis is the development of a logic model that relates a system state, such as system unavailable, to lower component-level states. By convention, the lowest level of input to the logic model represents single-component unavailable events. This will be called a component-level logic model and can be used to generate minimal cutsets. It is when this logic model is used to construct a probability model that the question of independence of events arises. The remaining stages are concerned with the assessment of the significance of this dependence on the evaluation of probabilistic measures of system performance, such as reliability or unavailability.

### 2.3.2 Stage 2: Identification of Common Cause Component Groups

The objectives of this screening stage include:

- Identifying the groups of system components to be included in or eliminated from the CCF analysis.
- Prioritizing the groups of system components identified for further analysis so that time and resources can be best allocated during the CCF analysis.
- Providing engineering arguments to aid in the data analysis step (Step 3.3).
- Providing engineering insights for later formulation of defense alternatives and stipulation of recommendations in Stage 4 (Quantification and Interpretation of Results) of the CCF analysis.

These objectives are accomplished through the qualitative analysis and quantitative screening steps. These two steps are presented separately, but they can be and often are performed interactively.

2.3.2.1 Step 2.1 - Qualitative Analysis. In this step, a search is made for common attributes of components and mechanisms of failure that can

lead to common cause events. Past experience and understanding of the engineering environment are used to identify signs of potential dependence among redundant components. Also, experience is used to identify the effectiveness of defenses that may exist to preclude or reduce the probability of the occurrence of certain CCF events. This search identifies initial groups of system components to be included in the analysis.

Then, a formal analysis of the root causes of equipment failure is performed to substantiate and improve the initial identification. For increased efficiency, the root cause analysis can be performed following the quantitative screening (Step 2.2). In this way, the analyst can focus on dominant CCF contributors to system unavailability as he performs the root cause analysis. The root cause analysis will also provide engineering arguments that will aid in (1) the data analysis (Step 3.3) and (2) formulating defense alternatives and recommendations (Stage 4).

2.3.2.2 Step 2.2 - Quantitative Screening. In this step, a conservative value is assigned to the probability of each basic event in the system fault tree, including the independent as well as the CCF events. The system unavailability is evaluated using conservative values, and the dominant contributors to the system unavailability are identified. These dominant contributors will be emphasized in Stages 3 and 4.

The quantitative screening step is useful in a system CCF analysis, and it is an almost essential step for performing an efficient CCF analysis at the plant level; i.e., an accident sequence CCF analysis. This is due to the fact that an accident sequence CCF analysis involves a large number of CCF events and a large number of accident sequences; thus, prioritizing CCF events for allocating time and resources increases the efficiency of the overall analysis.

Finally, several factors involved in the quantitative analysis of accident sequences will affect the contribution of CCFs to the accident sequence frequency. Some of these factors tend to affect different CCF contributors in different ways. In particular, recovery considerations will affect the relative contribution of CCF scenarios not only to accident sequence frequencies but also to system unavailabilities. Thus, recovery considerations (even if only of a preliminary nature) can play an important role in the quantitative screening step since the purpose of this step is to allow focusing on dominant CCF scenarios as early in the analysis as possible.

The two steps of this stage permit the analyst to separate potentially important cause and component group combinations from unimportant combinations based on qualitative and quantitative arguments as early in the analysis as such judgments are possible. As the analysis progresses, more information is collected and the cause and component group combinations that survived the previous screening tasks are then analyzed in greater detail. The end result of the screening is a list of CCF groups that the analyst feels confident, due to the wide range of postulated causes of CCF events and the carefully selected screening

arguments, represents the failures that contribute most to system unavailability or accident sequence frequency in the larger context of PRA.

### 2.3.3 Stage 3: Common Cause Modeling and Data Analysis

At the completion of Stage 2, the analyst has developed a component-level logic model of the system and has defined the scope of the common cause analysis in terms of component groups. The purpose of this stage is to modify the logic model to incorporate common cause events, convert this logic model to a probability estimation model, and to analyze the data for quantifying the parameters of this model.

2.3.3.1 Step 3.1 - Definition of Common Cause Basic Events. To model common cause failures, it is convenient to define common cause basic events; that is, basic events that represent multiple failures of components from shared root causes. This step also leads to a redefinition of the single-component basic events. Definition of new basic events leads to a redefinition of the structure of the logic model to include the new events.

2.3.3.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events. The objective of this step is to provide a transition from the logic model in Step 3.1 to a model that can be quantified. This is done by associating a probability model, such as the constant failure rate model or the constant probability of failure with demand model with each basic event (common cause or independent). Each model has one or more parameters and estimators for these parameters that, in terms of measurements of numbers of failure events and number of components failed, are based on specific assumptions. Some models are purely parametric (e.g., MGL, Reference 2-8), while others attempt to relate probabilities of common cause failures of two, three, or more components through the assumption of a specific causal mechanism (Reference 2-9). This step and Step 3.1 are closely connected because the choice of model affects the definition of the basic events and vice versa.

2.3.3.3 Step 3.3 - Data Classification and Screening. The purpose of this step is to evaluate and classify event reports to provide input to parameter estimation. It is necessary to take care to distinguish between events whose causes are explicitly modeled and those that are to be included in the residual common cause event models. The sources of data available to an analyst are event reports on both single and multiple equipment failures. Since plant-specific data on multiple equipment failures are rare, it is necessary to extend the search to other plants. However, since other plants may be designed or operated differently, events that occurred at one plant may not be possible at another. Thus, the data should not be used blindly, but should be carefully reviewed for applicability. This review concentrates on root causes, coupling mechanisms, and defensive strategies in place at the plant of interest. Since the event reports are generally not as detailed as an analyst would like, analysis of these reports requires a great deal of judgment; a systematic approach to this screening is essential for scrutability and reproducibility of the analysis. One such approach is described in Appendix A.

2.3.3.4 Step 3.4 - Parameter Estimation. The purpose of this step is to use the information obtained in Step 3.3 about the number of applicable events of single and multiple failures and the number of failed components to estimate the parameters of the common cause probability models. There are several sources of uncertainty, including the interpretation of the data to elicit causal mechanisms, the assessment of their impact at the plant being modeled, and uncertainty about how the data were obtained. Consequently, it is essential to not only provide a point estimate but also to characterize this uncertainty numerically.

#### 2.3.4 Stage 4: System Quantification and Interpretation of Results

The purpose of this stage is to synthesize the key output of the previous stages to effect a quantification of system failure frequency, the performance of sensitivity analyses, and the interpretation of results.

2.3.4.1 Step 4.1 - Quantification. The event probabilities obtained for the common cause events as a result of Stage 3 of the analysis are incorporated in the solution for the unavailability of the systems or into event sequence frequencies in the usual way cutsets are quantified. The results of this step include the numerical results and the identification of key contributors.

2.3.4.2 Step 4.2 - Results Evaluation and Sensitivity Analysis. As pointed out above, there is considerable uncertainty in the estimation of common cause failure probabilities. An uncertainty analysis is done to integrate the individual uncertainties into a combined result. It is also useful to see how significant such uncertainties can be by using sensitivity analyses to determine the direct relationship between the input values for the common cause basic events and the overall system results.

2.3.4.3 Step 4.3 - Reporting. The final step is the reporting of the analysis. It is particularly important to be clear in specifying what assumptions have been used and to identify the consequences of using these and other assumptions.

#### 2.4 SUMMARY

This section has provided an overview of some concepts that are useful in the definition and analysis of common cause failures. The procedural framework that has been developed has been described briefly. In the next chapter, this will be described in greater detail.

#### 2.5 REFERENCES

- 2-1. Satterwhite, D. G., et al., "Root Cause of Component Failures Program: Methods and Applications," U.S. Nuclear Regulatory Commission, NUREG/CR-4616, 1986.
- 2-2. Drago, J. P., et al., "The In-Plant Reliability Data Base for Nuclear Power Plant Components: Data Collection and Methodology Report," prepared for the U.S. Nuclear Regulatory Commission, Oak Ridge National Laboratory, NUREG/CR-2641, ORNL/TM-8271, November 1982.



- 2-3. Edwards, G. T., and I. A. Watson, "A Study of Common Mode Failures," United Kingdom Atomic Energy Authority Report SRD R146, July 1979.
- 2-4. Smith, A. M., et al., "A Study of Common Cause Failure--Phase II: A Comprehensive Classification System for Component Fault Analysis," prepared for the Electric Power Research Institute, by Los Alamos Technical Associates," EPRI NP-3837, May 1985.
- 2-5. Rasmuson, D. M., et al., "COMCAN II-A - A Computer Program for Automated Common-Cause Failure Analysis," TREE-1361, EG&G Idaho, Inc., INEL, 1979.
- 2-6. American Nuclear Society and Institute of Electrical and Electronics Engineers, "PRA Procedures Guide; A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG/CR-2300, 1983.
- 2-7. Fleming, K. N., et al., "Systems Interaction Identification Procedures - Volume 5 Application of PRA to the System Interaction Issue," prepared for the Electric Power Research Institute by Pickard, Lowe and Garrick, Inc., EPRI-NP 3834, July 1985.
- 2-8. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," prepared for Electric Power Research Institute by Pickard, Lowe and Garrick, Inc., EPRI NP-3967, June 1985.
- 2-9. Vesely, W. E., "Estimating Common Cause Failure Probabilities in Reliability and Risk Analysis: Marshall-Olkin Specialization," IL-0454, 1977.

## Section 3

### ANALYSIS FRAMEWORK AND METHODOLOGY

The purpose of this section is to describe each step of the framework introduced in Section 2 in more detail and to present some techniques and models that are commonly used. The emphasis in this section is, however, on presenting the basic elements of the framework depicted in Figure 3-1 and on the methodology. The examples used are not intended to be exhaustive. More details on technical issues briefly discussed in this section are provided in the appendices. Two example applications are given in Section 4 to provide additional detail.

It must be mentioned that the number of steps and the particular order in which they are presented here should be viewed in the context of a general guideline and an overall framework. As will be seen from the more detailed presentation, there can be considerable interaction, overlap, and iteration among these steps; some analysis techniques require a somewhat different order of steps. An experienced analyst may be able to skip some of the steps or take a different approach in achieving the objectives of a given step. However, Figure 3-1 and this section present the steps in a logical sequence that is applicable to the majority of situations and is based on extensive experience in actual application.

#### 3.1 STAGE 1: SYSTEM LOGIC MODEL DEVELOPMENT

This stage involves steps that are familiar to systems analysts. The three basic steps of this stage are:

- Step 1.1 - System Familiarization
- Step 1.2 - Problem Definition
- Step 1.3 - Logic Model Development

Although the above steps are the essential elements of any systems analysis, the emphasis of the following discussion will be on those aspects that are more directly relevant to the treatment of common cause events. Consequently, some of the details about those elements of analysis that are considered routinely in system analysis work are not presented. Similarly, the available systems modeling techniques [e.g., fault tree (Reference 3-1), GO methodology (Reference 3-2), etc.] are not discussed. The reader must familiarize himself with the fundamentals of

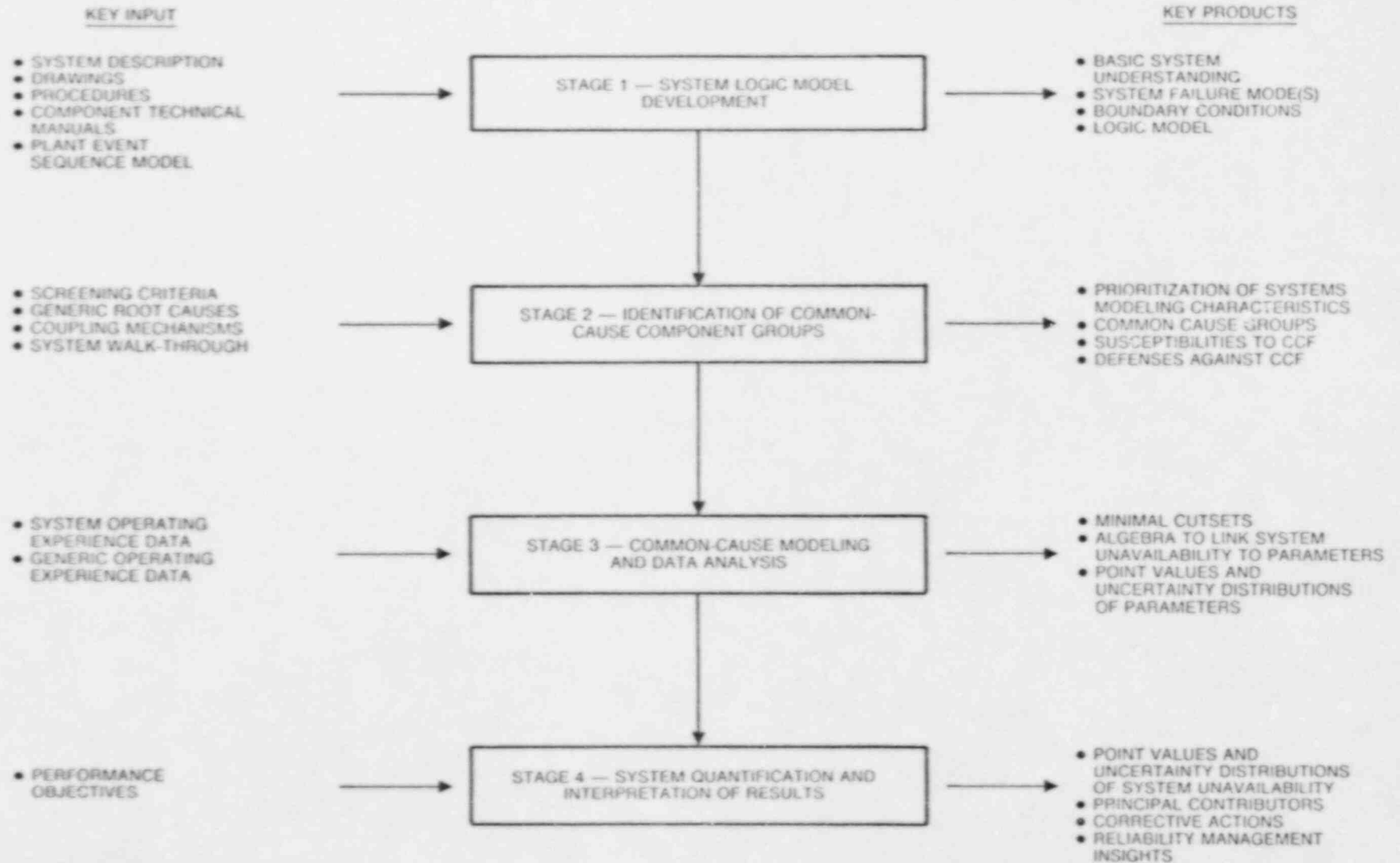


Figure 3-1. Key Input and Products of the Framework for Common Cause Analysis

system reliability analysis and the use of fault trees and/or reliability block diagram modeling techniques before attempting to use the methods of this report.

### 3.1.1 Step 1.1 - System Familiarization

To model a system, the analyst must understand what the intended function of the system is, of what components it is composed, and what procedures govern its operation, testing, and maintenance. In addition, the analyst determines the relation of the system being analyzed both to other systems and to its physical environment in the broader picture of a plant model.

From a common cause failure standpoint, particular attention must be paid to identifying those elements of design, operation, maintenance, and test procedures that could increase the chance of multiple component failures. The information collected in this step is essential for identifying potential sources of dependence and grouping components in the screening phase of the analysis (Stage 2).

### 3.1.2 Step 1.2 - Problem Definition

In this step, such analysis boundary conditions as the physical and functional boundaries of the system, functional dependencies on other systems (support systems), functional interfaces with other systems, and, finally, system success criteria are defined. This determines what equipment is modeled, how it should operate for the system to perform its intended function (which failure modes to consider), and what the applicable mission time and initial system alignments are. In this process, potential operator actions, the impact of test and maintenance requirements, and other assumptions and ground rules imposed on the analysis in the context of the overall plant model are identified.

From the point of view of common cause failures, those root causes of dependency that are to be explicitly modeled are identified. For instance, if they are to be modeled, most analyses include some external root causes, such as fire, flood, or earthquake, in the system-level analysis in terms of explicit models. Similarly, certain categories of human errors, such as calibration errors and errors in returning equipment and system to their original configuration after test and maintenance, are typically modeled explicitly using human reliability analysis techniques. This process, then, defines the scope of the residual common cause failure analysis; i.e., those root causes of multiple failures that are not modeled explicitly, but could contribute to system unavailability. It is these residual common cause events that are treated using the parametric common cause models discussed later.

The CCF-RBE (Reference 3-3) concluded that among the participants there was a consensus about the general approach toward the modeling of the different types of dependent events in a systems reliability analysis. The set of guidelines is reproduced here verbatim as an example of the level of detail normally expected.

1. Multiple failure events for which a clear cause-effect relationship can be identified should be explicitly modeled in the system model: the root cause events should be included in the system fault tree so that no further special dependent failure model is necessary. This applies to multiple failures caused by internal equipment failure (such as cascade failures and component caused functional unavailability events) and multiple failures due to clearly identifiable human errors (such as human errors in steps of a prescribed procedure).
2. Multiple failure events for which no clear root cause event can be identified can be modeled using implicit methods such as the parametric models.
3. Between the two previous extremes, there is a set of multiple failure events for which the explicit modeling of the cause, even if in principle feasible, is not performed because this would be too onerous and it is rather preferred to encapsulate them in a parametric model. The decision to do this is taken by the analyst based on his experience and judgement, and taking into consideration the aim and scope of the analysis. Moreover, explicit modeling may in some cases be impracticable because the component failure data do not allow to distinguish between different failure causes.

Explicit modeling should in principle go as far as reasonable, depending on the resources for the analysis, the level of detail, etc.... For the remaining dependencies, at least an upper bound should be assessed and for this parametric modeling can be used.

Anyway, the analyst should clearly document what has gone into his parametric modeling and what has been modeled explicitly.

### 3.1.3 Step 1.3 - Logic Model Development

The key step in any systems analysis is the development of a logic model that relates a system state, such as "system unavailable," to a combination of more elementary events, such as component states. There are a number of techniques for logical representation of a system. These include fault trees, reliability block diagrams, or GO diagrams. The most commonly used logic model is the fault tree. Specific guidance on how to use fault trees for system analysis can be found in Reference 3-1. The form of the logic model is not fundamental, but rather is based on such practical considerations as style, familiarity, and ability to interface with available software. The logic model simply reflects the analyst's understanding of the system that is developed in Steps 1.1 and 1.2.

Representing the logic model down to the level of component failure modes is clearly adequate for identifying the groups of component states that

lead to system unavailability; i.e., the minimal cutsets. It is not necessary for this purpose to further reduce these component states to a finer level of detail that specifies the causes of the components being in their undesired states. However, it will be seen that identifying causes is an essential part of analyzing event data to create a data base for estimating event probabilities.

### 3.2 STAGE 2: IDENTIFICATION OF COMMON CAUSE COMPONENT GROUPS

The objectives of this stage include:

- Identifying the groups of system components to be included in or eliminated from the CCF analysis.
- Prioritizing the groups of system components identified for further analysis so that time and resources can be best allocated during the CCF analysis.
- Providing engineering arguments to aid in the data analysis step (Step 3.3).
- Providing engineering arguments to formulate defense alternatives and stipulate recommendations in Stage 4 (interpretation of results) of the CCF analysis.

The screening process results in the identification of those components and failure causes in the system that will be included in, or eliminated from, the common cause analysis subject to the analysis boundary conditions, level of detail, etc., identified in Step 1.2. The end result of this stage is a definition of the components for which common cause failures are to be included in the model and a determination of which root causes and coupling mechanisms should be included in the common cause events for the purposes of quantification. Much of the information collected in Step 1.1 and the analysis boundary conditions defined in Step 1.2 are directly relevant to the process of identifying common cause component groups, which involves an engineering evaluation of failure causes, coupling mechanisms, and existing defenses against common cause failure in the system being analyzed. A common cause component group is usually a group of similar or identical components that have a significant likelihood of experiencing a common cause event. In principle, any combination of components could be postulated as having a potential for being involved in such an event.

Since detailed common cause analysis is a very time-consuming exercise and, in addition, it is desirable to keep the size of the model to a manageable level, it is essential to reduce the scope of the analysis through prioritizing root causes and coupling mechanisms and defining only those groups of components that are judged to have a significant likelihood of dependence that contributes to the overall system unavailability. Hence, by selectively defining these groups, the number of potential common cause events that could be postulated is reduced by the analyst.

There are two types of screening that are useful in this step: qualitative and quantitative screening. These types, identified as separate screening steps, permit the analyst to separate potentially important cause and component group combinations from unimportant combinations, based on qualitative and quantitative arguments, as early in the analysis as such judgments can reasonably be made. As the analysis progresses, more information is collected and the cause and component group combinations that survived the previous screening tasks are then analyzed in greater detail. The end result of the screening is a list of CCF groups that the analyst feels confident, in light of the wide range of postulated causes of CCF events and the carefully selected screening arguments, adequately bound the common cause event possibilities that will be subjected to further study.

### 3.2.1 Step 2.1 - Qualitative Analysis

In this step, a search is made for common attributes of components and mechanisms of failure that can lead to potential common cause failures. Analysts in the past have relied on a variety of factors, including engineering insight, obvious signs of dependence, and the perceived effectiveness of certain defenses to identify component groups for common cause analysis.

This process can be enhanced by developing a checklist of such key attributes as design, location, operation, etc., for which the analyst can assess the degree of similarity of the various components. A partial list of such attributes is the following:

- Component type (e.g., motor-operated valve, swing check valve, etc.), including any special design or construction characteristics; e.g., component size, material, etc.
- Component use; e.g., system isolation, flow modulation, parameter sensing, motive force, etc.
- Component manufacturer.
- Component internal conditions; e.g., absolute or differential pressure range, temperature range, normal flow rate, chemistry parameter ranges, power requirements, etc.
- Component external environmental conditions; e.g., temperature range, humidity range, barometric pressure range, atmospheric particulate content and concentration, etc.
- Component location name and/or location code.
- Component initial conditions (e.g., normally closed, normally open, energized, deenergized, etc.) and operating characteristics; e.g., normally running, standby, etc.

- Component testing procedures and characteristics; e.g., test interval, test configuration or lineup, effect of test on system operation, etc.
- Component maintenance procedures and characteristics; e.g., planned, preventive maintenance frequency, maintenance configuration or lineup, effect of maintenance on system operation, etc.

The above list or a similar one is simply a tool to help account for factors affecting component interdependence and to readily identify the presence of identical redundant components. It provides a method of documenting the qualitative analysis required to support the selection of common cause groups. Based on experience in performing these evaluations and in analyzing U.S. operating experience data (References 3-4, 3-5, and 3-6), additional guidance can be provided in the assignment of component groups. The most important guidelines follow:

- When identical, functionally nondiverse, and active components are used to provide redundancy, these components should always be assigned to a common cause group, one group for each group of identical redundant components. In general, as long as these are common cause groups of identical active components already identified, the assumption of independence among diverse components is a good one and is supported by operating experience data.
- When diverse redundant components have piece parts that are identically redundant, the components should not be assumed to be fully independent. One approach in this case is to break down the component boundaries and identify the common piece parts as a common cause component group. For example, pumps can be identical except for their drivers.
- In systems reliability analysis, it is frequently assumed that certain passive components can be omitted, based on arguments that active components dominate. In applying this principle to common cause analysis, care must be exercised to not exclude such important events as debris blockage of redundant pump strainers, etc.

Susceptibility of a group of components to common cause failures not only depends on their degree of similarity to such attributes as those listed here, but also on the existence or lack of defensive measures against common cause and the degree of their effectiveness.

Although much work is needed to determine the relation between various root causes, coupling mechanisms, and defensive tactics, valuable insight can be gained by considering, in a qualitative fashion, the effectiveness of some broad categories of defenses for various general groups of causes. Such an analysis can be useful in the evaluation of common cause event data for plant-specific applications. As an example, physical



separation of redundant equipment may reduce the chance of simultaneous failure of the equipment due to some environmental effects (see Appendix B). In this case, the defense acts to weaken the coupling mechanism. Other tactics may be effective at reducing the likelihood of root causes resulting in independent failures as well as common cause failures. Thus, it can be argued that a complete treatment of common cause failures should not be performed independently of an analysis of the independent failures, but rather the treatment of all failures should be integrated.

Another structured and systematic way for identifying and categorizing groups of components for common cause analysis in larger and more complex problems (e.g., accident sequence analysis) is called the generic cause approach (Reference 3-7). This method, which is described in more detail in Appendix B, begins with the identification of a wide range of postulated causes of CCF events, events that each involve a particular group of components; e.g., a group of components that would all be affected by a common design error or a group of components that would all be susceptible to a harsh environment in a certain location.

The six tasks of this approach permit the analyst to separate potentially important cause and component group combinations from unimportant combinations, based on qualitative and quantitative arguments, as early in the analysis as such judgments are possible. As the analysis progresses, more information is collected and the cause and component group combinations that survived the previous screening tasks are then analyzed in greater detail.

Specifically, the six screening tasks an analyst can use to identify the most important CCF scenarios of a plant are:

- Task 1. Identifying important root causes of component failures and defining the groups of components that are susceptible to each root cause of failure.

These failure causes usually fall into a few general categories, such as those defined in Reference 3-6. At least three types of these root cause and component group combinations are considered:

- Root causes that affect similar kinds of equipment.
- Root causes that affect any equipment operated according to the same procedures.
- Root causes that affect any equipment in the same location.

- Task 2. Screening the root cause and component group combinations initially defined for analysis and eliminating from the analysis those component groups that can be determined to be unimportant when compared to other failures for the system.

- Task 3. Determining those component groups that can cause system failures.
- Task 4. Screening each harsh environment scenario that survived the screening in Task 3 to determine if there is a root cause event that can trigger the scenario.
- Task 5. Determining the component minimal cutsets that are involved in each scenario retained for analysis.
- Task 6. Screening the scenarios that have been retained for analysis and eliminating unimportant scenarios by considering details of the relationships between the root causes of failure and the component failures in the MCSs.

The following is a description of some additional criteria that can be used to identify common cause scenarios involving errors in the installation, maintenance, testing, or operation of components and scenarios involving harsh environments. These criteria are only examples of how engineering insight can be applied to the screening of scenarios. For any given case, there may be other powerful screening criteria.

- In the screening of installation, maintenance, testing, and operating error scenarios, determine if there are any plausible errors either in performing the task or in the procedures defining the task that could result in component unavailability. If there are none, the scenario may be discarded. For example, if a procedure does not call for removing a component from service, there is little chance that the component will be left in a disabled state at the end of the task.
- Common cause scenarios associated with plant testing and maintenance schedules should be examined to determine whether the scenario is credible. For example, consider a minimal cutset involving three pumps. A common preventive maintenance task is to be performed at 1-month intervals on each of the three pumps. The plant maintenance schedule calls for this maintenance to be staggered among the three pumps; i.e., pump 2 is to be serviced 1 month after pump 1, and pump 3 is to be serviced 2 months after pump 1. A functional test of the pumps is also to be performed monthly, and it too is to be staggered. Each pump is to be tested 1 month after its preventive maintenance. Therefore, an error that occurs during the maintenance of pump 1 will probably be discovered and corrected before the same error can fail pump 3 and, possibly, even pump 2. Thus, the MCS will likely never occur due to errors in this maintenance task, and the scenario may be eliminated from the analysis. In general, it is only necessary to consider MCSs whose basic events are all affected by the same procedure within one testing interval.

- Also, scenarios in which different personnel perform a task on multiple components in an MCS may be screened out. The systematic repetition of task-related errors is highly dependent on the interpretation of the working procedure and on the effects of stress, fatigue, and personnel abilities. These factors can vary considerably among individuals.
- Finally, a plant visit is required for making a detailed survey to determine the spatial relationships of components, sources of harsh environments, barriers to harsh environments of interest, and any other pertinent factors. The plant visit may determine some scenarios are incredible in light of these details.

For example, an analyst may discover several penetrations with unsealed conduits connecting equipment in different locations. Moisture in one location (e.g., at an upper floor) could propagate through the conduits and cause the components connected to these conduits in the other locations (e.g., at a lower floor) to fail. Since operating experience indicates several component failures due to moisture propagating through conduits, moisture could cause CCFs of components in these locations. A detailed analysis of the locations, however, may reveal that the unsealed conduits do not connect equipment in the same MCS to a common source of moisture. Thus, the scenario can be screened out.

Several computer codes are available to support the above tasks (References 3-7, 3-8, and 3-9).

### 3.2.2 Step 2.2 - Quantitative Screening

After the qualitative screening of Step 2.1 has been completed, the analyst has identified groups of components that, by virtue of similarity, environment, etc., have been judged to be susceptible to common cause failures. One can further reduce the list of important common cause candidate groups by performing quantitative screening. This step is useful for systems reliability analysis and may be essential for an accident sequence-level analysis in which exceedingly large numbers of cutsets may be generated in solving the fault tree logic models.

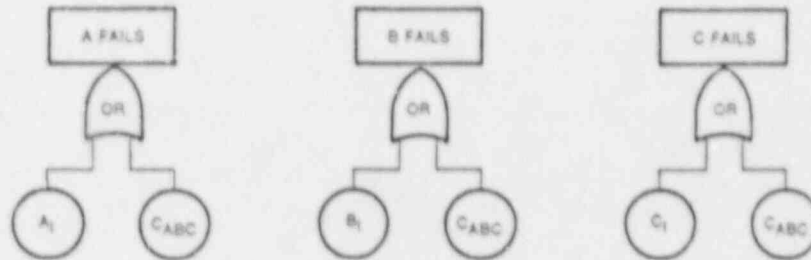
In performing quantitative screening for common cause failure candidates, one is actually performing a complete quantitative common cause analysis except that a conservative and very simple quantification model is used. The procedure is as follows:

1. The fault trees are modified to explicitly include a single common cause failure event for each component in a common cause group that fails all members of the group. For example, if components A, B, and C have been identified as a

common cause component group, the basic events on the fault tree shown below



are expanded to include the basic event  $C_{ABC}$ , defined as the concurrent failure of A, B, and C due to a common cause, as shown below:



(Here  $A_i$ ,  $B_i$ , and  $C_i$  denote the independent failure of components A, B, and C, respectively.) This substitution is made at every point on the fault trees where the events "A FAILS," "B FAILS," or "C FAILS" occur.

2. The fault trees are now solved, either by hand for simple systems, or more commonly by using a fault tree reduction code (e.g., WAM, FTAP, SETS, IRRAS, etc.) to obtain the minimal cutsets for the system or accident sequence. Any resulting cutset involving the intersection  $A_i B_i C_i$  will (because of the rules of Boolean algebra) have an associated cutset involving  $C_{ABC}$ . The significance of this process is that, in large systems or accident sequences, some truncation of cutsets on failure probability must usually be performed to obtain any solution at all, and the product of independent failures  $A_i B_i C_i$  is often lost in the truncation process due to its small value, while the (numerically larger) common cause term  $C_{ABC}$  will survive.

3. Numerical values for the CCF basis events can be estimated using the simple beta factor model (see Section 3.3.2.1)

$$P(C_{ABC}) = \beta P(A)$$

For screening purposes, the analysis may use  $\beta = 0.1$  or some other conservative value (see Section 3.3).  $P(A)$  is the total random failure frequency that would be used in the absence of any common cause considerations.

The beta factor model provides a conservative approximation to the common cause event frequency regardless of the number of redundant components in the common cause basic event being considered.

Those common cause basic events that are found to (quantitatively) contribute little to the system (or accident sequence) frequency (or

which do not survive the truncation process) can be dropped from further consideration. Those common cause basic events that are found to be significant contributors to the system frequency are retained and often further analyzed using a more refined logical or quantitative model and a detailed analysis of event data to support realistic estimates of model parameters, as described in the sections to follow.

As mentioned above, this process of adding common cause basic events to the fault tree(s) and solving the trees for the minimal cutsets is necessary because high-ordered cutsets involving groups of components susceptible to common cause failures are often lost if only independent failure rates are prescribed. However, experienced analysis familiar with the systems logic may sometimes use cutsets based only on independent failures and add the final common cause cutsets by observation. This latter process, however, requires considerable experience and judgment, and is not, in general, recommended because it is easy to overlook a significant common cause event.

The end result of the screening is a list of CCF groups that the analyst feels confident, due to the wide range of postulated causes of CCF events and the carefully selected screening arguments, represents the failures that contribute most to system unavailability or accident sequence frequency in the larger context of PRA.

### 3.3 STAGE 3: COMMON CAUSE MODELING AND DATA ANALYSIS

The key output of Stages 1 and 2 is the identification of the groups of components for which common cause failures may be important. The objective of Stage 3 is to complete the system quantification by incorporating the effects of common cause events for component groups that survive the screening process of Stage 2. This is achieved through four steps:

- Step 3.1 - Definition of Common Cause Basic Events
- Step 3.2 - Selection of Probability Models for Common Cause Basic Events
- Step 3.3 - Data Classification and Screening
- Step 3.4 - Parameter Estimation

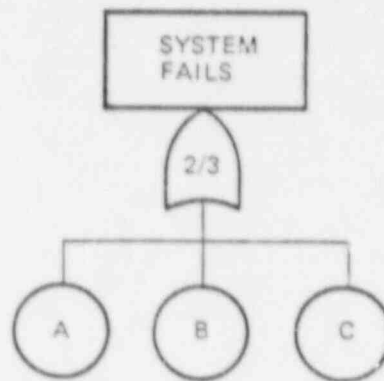
Each of these steps is described in the following sections. More detailed discussion of various technical topics is provided in the appendices.

#### 3.3.1 Step 3.1 - Definition of Common Cause Basic Events

To facilitate subsequent application of data on historical independent and dependent failure events to the estimation of model parameters, it is convenient to define common cause basic events; that is, basic events that represent failures of specific components in a common cause component group. This step is equivalent to a redefinition of the logic model basic events from a component-level basis to a lower level of

detail that identifies the particular impacts that common cause events of specified multiplicity may have on the system. Thus, the common cause basic events are written in terms of the particular combination of components affected. The common cause basic events also provide an unambiguous and useful technical vocabulary for discussing each of the models in Section 3.2. At this lower level of detail, the specific causes of multiple failures are not explicitly included, but the impacts of those causes on the particular number of components failed are.

As an example of this breakdown, consider a system of three identical components, A, B, and C, with a two-out-of-three success logic. These components form a single common cause component group. The component-level fault tree that would be developed in Step 1.3 is:



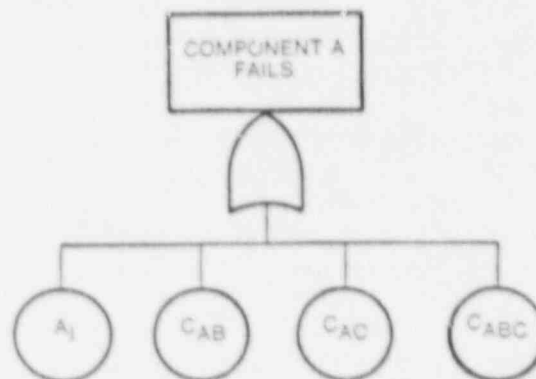
with the following minimal cutsets:

{A, B}; {A, C}; {B, C}

The reduced Boolean representation of the system failure in terms of the above minimal cutsets of the component-level fault tree is

$$S = A * B + A * C + B * C \quad (3-1)$$

The expansion of this component-level Boolean expression down to the common cause impact level can be illustrated by representing each component-level basic event as a subtree, such as that shown below, in which it is assumed that common cause failures can lead to either two or three components failing simultaneously.



The equivalent Boolean representation of total failure of component A is

$$A_T = A_I + C_{AB} + C_{AC} + C_{ABC} \quad (3-2)$$

where

$A_T$  = total failure of component A.

$A_I$  = failure of component A from independent causes.

$C_{AB}$  = failure of components A and B (and not component C) from common causes.

$C_{AC}$  = failure of components A and C (and not component B) from common causes.

$C_{ABC}$  = failure of components A, B, and C from common causes.

When all the components of our two-out-of-three example system are expanded similarly, the following minimal cutsets are obtained

$\{A_I, B_I\}; \{A_I, C_I\}; \{B_I, C_I\}$

$\{C_{AB}\}; \{C_{AC}\}; \{C_{BC}\}$

$\{C_{ABC}\}$

The reduced Boolean representation of the system failure in terms of these cutsets is

$$S = A_I * B_I + A_I * C_I + B_I * C_I + C_{AB} + C_{AC} + C_{BC} + C_{ABC} \quad (3-3)$$

Had the success criterion for this example been only one out of three instead of two out of three, it is clear that a substitution of subtrees, like those shown above, into the system fault tree would produce cutsets of the type,  $C_{AB} * C_{AC}$ . These cutsets have questionable validity unless the events  $C_{AB}$  and  $C_{AC}$  are defined more precisely. One option is to define the events  $C_{AB}$  and  $C_{AC}$  to be mutually exclusive. Then, the Boolean expression in Eq. 3-2 would represent a partition of the failure space of A into mutually exclusive parts based on the impact on other components in the common cause component group of the underlying set of causes. This would imply that the probabilities of cutsets like  $C_{AB} * C_{AC}$  are identically zero. An alternative option is to construct the events  $C_{AB}$ ,  $C_{AC}$ , and  $C_{ABC}$  as sums of contributions from specific root causes so that, for example,

$$C_{AB} = \sum_i C_{AB}^{(i)}$$

where  $C_{AB}(i)$  represents the common cause failures of components A and B from root cause i.

In this case, it is clear that cutsets of the form  $C_{AB} \cdot C_{AC}$  could occur from combinations of such root causes as  $C_{AB}(i) \cdot C_{AC}(j)$ , but all combinations  $C_{AB}(i) \cdot C_{AC}(i)$  would be eliminated since component A would be supposed, in this cutset, to have been failed twice by the same root cause. Thus, the events  $C_{AB}$  and  $C_{AC}$  in this picture are neither mutually exclusive nor exactly independent, and the probability of  $C_{AB} \cdot C_{AC}$  cannot be calculated directly without using the decomposition into cause contributions.

It will be seen later that the causes are considered in classifying events in terms of their impact on components. If in this process, events that could have been identified as  $C_{AB}(i) \cdot C_{AC}(j)$  are classified (as is most likely) as  $A_i \cdot C_{BC}$ ,  $C_i \cdot C_{AB}$ ,  $B_i \cdot C_{AC}$ , or  $C_{ABC}$ , then cutsets like  $C_{AB} \cdot C_{AC}$  should be eliminated to avoid double counting. Such a counting process then makes this option equivalent to the previous, mutually exclusive definition of the events. This is discussed in more detail in Volume II. It is clear that the definition of the events, the counting process by which event reports are classified, and the way the results are used to estimate the parameters of common cause models are closely intertwined.

Although complete agreement has not been reached on the most appropriate definition of these events, it fortunately does not make a significant numerical difference to the results because, in general, the contribution of cutsets like  $C_{AB} \cdot C_{CD}$  is considerably smaller than that of cutsets like  $C_{ABC}$ .

Note that this procedure does not, at this point, require the identification of specific common cause events; e.g., a fire that damages a specific set of components. At this stage, the common cause events are only identified by the impact they have on specific sets of components. Since all possible combinations of components within the groups identified in Stage 2 are included, this formulation of the fault tree is complete with respect to all possible ways that the common cause events could impact the system.

Although this procedure of expansion can be generalized, it can be seen immediately that this results in proliferation of the cutsets, which may create practical difficulties when dealing with complex problems. The above fault tree illustrates the fundamental logic of how common cause events impact systems. This logic structure provides the analyst with a systematic and disciplined framework by which he can include and exclude possible events and make his assumptions and approximations that justify these inclusions and exclusions visible and explicit, based on the screening analysis (Stage 2).

Simplification can be achieved by quantitative and qualitative screening to prevent the rapid and unmanageable expansion of the fault tree. For example, if, based on conservative assessments of the probability of the basic events, the likelihood of certain component-level cutsets involving



those basic events is expected to be dominated by others, those basic events may be eliminated from the expansion of the fault tree. Also, once the common cause events are included in this way, standard fault tree analysis techniques, such as cutset order or probability truncation, can be safely applied without any concern about common cause events because they are fully represented in the fault tree.

If the number of cutsets appears to be unmanageable although screening has been done, a practical solution to the problem is to delay the common cause impact expansion until after the component-level fault tree is solved, at which time those terms in the component-level Boolean expression that had not been expanded would be expanded through a process similar to that in Eq. 3-2, and the new Boolean expression would be reduced again. Other techniques include reducing the level of detail of the original component-level tree to the supercomponent level and assuming the common cause events always have a global impact. Care, however, must be exercised so that no terms in the expansion of the reduced Boolean expressions would be missed or ignored.

In short, the process of developing the logic model at the common cause impact level should be viewed as an iterative process through which the proper balance between completeness and practicality is achieved. In Section 4 and in Appendix F, additional guidance is provided on how to implement this procedure.

### 3.3.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events

The primary objective of this step is to select the common cause model that will be used in the quantification of the common cause basic events. The cutset Boolean equation is transformed so that the probabilities of the basic events can be substituted directly into the resulting algebraic expression.

For example, in the three-component example system of Section 3.3.1, the algebraic equivalent of Eq. 3-3 in terms of the probabilities of the basic events, using the rare events approximation,\* is

$$\begin{aligned}
 P(s) = & P(A_1) \cdot P(B_1) + P(A_1) \cdot P(C_1) + P(B_1) \cdot P(C_1) \\
 & + P(C_{AB}) + P(C_{AC}) + P(C_{BC}) + P(C_{ABC})
 \end{aligned}
 \tag{3-4}*$$

where

$P(x) \equiv$  probability of event  $x$

---

\*According to rare events approximation for two events,  $a$  and  $b$ , we have  $P(a \cdot b) \approx 0$ . Consequently,

$$\begin{aligned}
 P(a + b) &= P(a) + P(b) - P(a \cdot b) \\
 &\approx P(a) + P(b)
 \end{aligned}$$

It is a common practice in risk and reliability analysis to assume that the probabilities of similar events involving similar types of components are the same. This approach takes advantage of the physical symmetries associated with identically redundant components in reducing the number of parameters that need to be quantified. For example, in Eq. 3-4 it is assumed that

$$\begin{aligned} P(A_1) &= P(B_1) = P(C_1) = Q_1 \\ P(C_{AB}) &= P(C_{AC}) = P(C_{BC}) = Q_2 \\ P(C_{ABC}) &= Q_3 \end{aligned} \tag{3-5}$$

Note that the probability of failure of any given basic event within a common cause component group depends only on the number and not on the specific components in that basic event. This is called the symmetry assumption.

Continuing with our example, the system failure probability (Eq. 3-4) can be written as

$$Q_s = 3Q_1^2 + 3Q_2 + Q_3 \tag{3-6}$$

Here, the cutset information is lost, but quantification is easier.

Generalization of this concept is straightforward; for the basic events corresponding to a common cause group of  $m$  components, one can define the following probabilities.

$$\begin{aligned} Q_k &= \text{probability of a basic event involving } k \text{ specific components} \\ 1 &\leq k \leq m \end{aligned} \tag{3-7}$$

Note that the total probability of failure of a specific component can be obtained from the  $Q_k$ 's. This can be seen, for example, from Eq. 3-2 where the failure of component A due to all causes is expanded in terms of the basic events. Transforming Eq. 3-2 into its equivalent probability model and using  $Q_1$ ,  $Q_2$ , and  $Q_3$ , as defined in Eq. 3-5, we get

$$Q_t = Q_1 + 2Q_2 + Q_3 \tag{3-8}$$

where, in this case,  $Q_t$  is the total failure probability of component A. In general, the total failure probability of a component in a common cause group of  $m$  components is

$$Q_t = \sum_{k=1}^m \binom{m-1}{k-1} Q_k \tag{3-9}$$

where the binomial term

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(m-k)! (k-1)!} \quad (3-10)$$

represents the number of different ways that a specific component can fail with  $(k - 1)$  other components in a group of  $m$  similar components.

The model that uses  $Q_k$ 's defined in Eq. 3-7 to calculate system failure probability is called the basic parameter model (Reference 3-4). Ideally,  $Q_k$ 's can be calculated from data in which case there is no need for further probabilistic modeling. Unfortunately, as we will see in Step 3.4, the data required to estimate  $Q_k$ 's directly, are not normally available. Other models have been developed that put less stringent requirements on the data. This, however, is only done at the expense of making additional assumptions that address the incompleteness of the data (see Appendix C). Several of these models are summarized in Table 3-1 and explained in the following. These models can be categorized in several different ways, based on the number of parameters, their assumptions regarding the cause, coupling mechanism, and impact of common cause failures.

The categories for the number of parameters required for modeling common cause events are:

- Single Parameter Models
- Multiple Parameter Models

With respect to how multiple failures occur, there are two categories:

- Shock Models
- Nonshock Models

The "shock models" estimate the frequency of multiple component failures by assuming that the system is subject to common cause "shocks" at a certain rate and estimating the conditional probability of failure of components within the system, given the occurrence of shocks. The common cause failure frequency is the product of the shock rate and the conditional probability of failure, given a shock.

Finally, as mentioned before, except for the basic parameter model, all common cause models discussed in this report estimate the probability of basic events indirectly; i.e., through the use of other parameters. In general, the types of parameters, estimation method, and data requirements vary from one model to another. However, with the current state of data that involve large uncertainties, the numerical impact of selecting one model over another is not significant, given a consistent treatment of data in all cases. These points become clearer in the following sections. The remainder of this section deals with a brief description of the various parametric models summarized in Table 3-1.

Table 3-1  
KEY CHARACTERISTICS OF THE PARAMETRIC MODELS

ESTIMATION APPROACH		MODEL	MODEL PARAMETERS*	GENERAL FORM FOR MULTIPLE COMPONENT FAILURE FREQUENCY
NONSHOCK MODELS	DIRECT	BASIC PARAMETER	$Q_1, Q_2, \dots, Q_m$	$Q_k = Q_k \quad k = 1, 2, \dots, m$
	INDIRECT	SINGLE PARAMETER	$Q_t, \beta$	$Q_k = \begin{cases} (1 - \beta) Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$
		MULTIPARAMETER	$Q_t, \beta, \gamma, \delta, \dots$ $m - 1$ PARAMETERS	$Q_k = \frac{1}{(m-1)} \binom{k}{i-1} \rho_i (1 - \rho_{k+1}) Q_t$ $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \dots, \rho_{m+1} = 0$
		ALPHA FACTOR	$Q_t, \alpha_1, \alpha_2, \dots, \alpha_m$	$Q_k = \frac{k}{(m-1)} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \dots, m$ $\alpha_t = \sum_{k=1}^m k \alpha_k$
SHOCK MODELS		BINOMIAL FAILURE RATE	$Q_t, \mu, \rho, w$	$Q_k = \begin{cases} \mu \rho^k (1 - \rho)^{m-k} & k \neq m \\ \mu \rho^{m+w} & k = m \end{cases}$

\*REFER TO THE TEXT FOR DEFINITION OF VARIOUS PARAMETERS

3.3.2.1 Single Parameter Models. The single parameter models refer to those parametric models that use one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. The most widely used single parameter model, and the first such model to be applied to common cause events in applied risk and reliability analysis, is known as the beta-factor model (Reference 3-10). A variant of this model, called the C-factor method (References 3-11 and 3-12) employed the same model, but to address the incompleteness of the data sources, used a different method of estimating the parameter. The problem of estimating model parameters will be discussed in Section 3.3.4. According to the beta-factor model, a fraction ( $\beta$ ) of the component failure rate can be associated with common cause events shared by the other component in that group. According to this model, whenever a common cause event occurs, all components within the common cause component group are assumed to fail. Therefore, based on this model, for a group of  $m$  components, all  $Q_k$ 's defined in Eq. 3-7 are zero except  $Q_1$  and  $Q_m$ . The last two quantities are written as

$$\begin{aligned} Q_1 &= (1-\beta) Q_t \\ Q_m &= \beta Q_t \end{aligned} \tag{3-11}$$

This implies that

$$\beta = \frac{Q_m}{Q_1 + Q_m} \tag{3-12}$$

Note that  $Q_t$ , the total failure probability of one component, is given as

$$Q_t = Q_1 + Q_m \tag{3-13}$$

which is the special case of Eq. 3-9 when  $Q_2 = Q_3 = \dots = Q_{m-1} = 0$ .

As an example, using the beta-factor model, the terms representing the basic event in Eq. 3-6 are written as

$$\begin{aligned} Q_1 &= (1-\beta) Q_t \\ Q_2 &= 0 \\ Q_3 &= \beta Q_t \end{aligned} \tag{3-14}$$

which gives

$$Q_s = 3(1-\beta)^2 Q_t^2 + \beta Q_t \tag{3-15}$$

As can be seen, the beta factor model requires that an estimate of the total failure rate of the component be provided from generic sources of data and that a corresponding estimate for the beta factor also be provided. A practical and useful feature of this model is that the estimators of  $\beta$ , as will be shown in Step 3.4, do not explicitly depend

on system or component success data, which are not generally available. This feature, the fact that estimates of the  $\beta$  parameter for widely different types of components vary much less than estimates of  $Q_k$  and the simplicity of the model are the main reasons for wide use of this method in risk and reliability studies. It should be noted, however, that estimating  $\beta$  factors, just as with any reliability analysis parameter, requires specific assumptions concerning the interpretation of data (Reference 3-13). This and several related issues regarding the assumption behind the various models and the implications of those assumptions are discussed briefly in Section 3.3.4 and further in Appendix C.

Although historical data collected from the operation of nuclear power plants indicate that common cause events do not always fail all redundant components, experience from using this simple model shows that, in many cases, it gives reasonably accurate (only slightly conservative) results for redundancy levels up to about three or four items. However, beyond such redundancy levels, this model generally yields results that are conservative. When interest centers around specific contributions from third or higher order trains, more general parametric models are recommended.

3.3.2.2 Multiple Parameter Models. For a more accurate analysis of systems with higher levels of redundancy, models that represent the range of impact levels that common cause events can have are more appropriate. These models involve several parameters with which to quantify the specific contribution of various basic events.

Four such models are selected here to provide adequate representation of the methods that have been proposed. In the nonshock model category, the MGL model (Reference 3-14) and the alpha-factor model (Reference 3-15) are discussed. The shock model category is represented by the binomial failure rate model (References 3-16 and 3-17). These models are briefly described in the following paragraphs.

3.3.2.2.1 Multiple Greek letter model. The MGL model (Reference 3-14) is the most general of a number of recent extensions of the beta-factor model. The MGL model was the one used most frequently in the International Common Cause Failure Reliability Benchmark Exercise (Reference 3-3). In this method, other parameters in addition to the  $\beta$ -factor are introduced to distinguish among common cause events affecting different numbers of components in a higher order redundant system.

The MGL parameters consist of the total component failure frequency, which includes the effects of all independent and common cause contributions to that component failure, and a set of failure fractions, which are used to quantify the conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components in the same group, given component failure has occurred. For a system of  $m$  redundant components and for each given failure mode,  $m$  different parameters are defined. For example, the first four parameters of the MGL model are, as before

$Q_t$  = total failure frequency of the component due to all independent and common cause events.

plus

- B = conditional probability that the common cause of a component failure will be shared by one or more additional components.
- Y = conditional probability that the common cause of a component failure that is shared by one or more components will be shared by two or more components additional to the first.
- δ = conditional probability that the common cause of a component failure that is shared by two or more components will be shared by three or more components in addition to the first.

The general equation that expresses the frequency of multiple component failures due to common cause,  $Q_k$ , in terms of the MGL parameters, is given in Table 3-1.

To see how these parameters can be used in developing the probabilities of the basic events, consider the three-component system represented by Eq. 3-6.

The maximum number of components that can share a common cause is three ( $m = 3$ ). Therefore,  $\gamma$  is the conditional probability that the common cause of failure of a component will be shared by exactly two additional components, and  $\delta = 0$ .

Then, from Table 3-1,

$$\begin{aligned} Q_1 &= (1-B)Q_t \\ Q_2 &= (1/2)B(1-\gamma)Q_t \\ Q_3 &= B\gamma Q_t \end{aligned} \tag{3-16}$$

The above expressions for  $Q_1$ ,  $Q_2$ , and  $Q_3$  can be used, for example, in Eq. 3-16 to obtain the unavailability of a two out of three system in terms of the MGL parameters:

$$Q_s = 3(1-B)^2 Q_t^2 + \frac{3}{2} B(1-\gamma)Q_t + B\gamma Q_t \tag{3-17}$$

Note that the beta factor model is a special case of the MGL model. For this example, the MGL model reduces to the beta factor model if  $\gamma = 1$ . In particular, Eq. 3-17 reduces to Eq. 3-15 if  $\gamma = 1$ .

**3.3.2.2.2 Alpha-factor model.** As explained in References 3-18 through 3-20 and in Appendices C and E, rigorous estimators for the B-factor model and its generalization, the MGL model parameters, are fairly difficult to obtain although approximate methods have been developed and used in practice (Reference 3-21). A rigorous approach

to estimating  $\beta$ -factors is presented in Reference 3-19 through introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference 3-15 uses the multiparameter generalization of event-based parameters directly to estimate the common cause basic event probabilities. This multiparameter common cause model is called the  $\alpha$ -factor model.

The difference between the  $\alpha$ -factor parameters and the MGL parameters is that the former are system failure based, while the latter are component failure based. This difference and its implications are described more fully in Appendices C and E in which estimators for the MGL and  $\alpha$ -factor models are developed. The  $\alpha$ -factor parameters are thus more directly related to the observable number of events than are the MGL parameters.

Like the MGL model, the  $\alpha$ -factor model develops common cause failure frequencies from a set of failure ratios and the total component failure rate. The parameters of the  $\alpha$ -factor model are defined.

As before,

$Q_t \equiv$  total failure frequency of each component due to all independent and common cause events

plus

$\alpha_k \equiv$  fraction of the total frequency of failure events that occur in the system involving the failure of  $k$  components due to a common cause

and

$$\alpha_1 + \alpha_2 + \dots + \alpha_m = 1$$

The general equation relating the basic event probabilities,  $Q_k$ 's to the  $\alpha$ -factor model parameter is given in Table 3-1. As we can see, the key difference between  $\alpha$  in this model and the parameters of the MGL and  $\beta$ -factor models is that the former is a fraction of the events that occur within a system, whereas the latter are fractions of component failure rates.

Again, as an example, the probabilities of the basic events of the three-component system of Eq. 3-6, in terms of the  $\alpha$ -factor model parameters, are written as (from the general equation in Table 3-1, with  $m = 3$ )

$$Q_1 = \frac{\alpha_1}{\alpha_t} Q_t$$

$$Q_2 = \frac{\alpha_2}{\alpha_t} Q_t$$



$$Q_3 = 3 \frac{\alpha_3}{\alpha_t} Q_t \quad (3-18)$$

where

$$\alpha_t = \alpha_1 + 2\alpha_2 + 3\alpha_3, \text{ a normalizing factor.}$$

Therefore, the system unavailability for our example (Eq. 3-6) is given by

$$Q_s = 3 \left( \frac{\alpha_1}{\alpha_t} \right)^2 Q_t^2 + 3 \frac{\alpha_2}{\alpha_t} Q_t + 3 \frac{\alpha_3}{\alpha_t} Q_t \quad (3-19)$$

3.3.2.2.3 Binomial failure rate model. The BFR model (References 3-16 and 3-17) considers two types of failures. The first represents independent component failures; the second type is caused by shocks that can result in failure of any number of components in the system. According to this model, there are two types of shocks, lethal and nonlethal. When a nonlethal shock occurs, each component within the common cause component group is assumed to have a constant and independent probability of failure. The name of this model arises from the fact that, for a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution. The BFR model is therefore more restrictive because of these assumptions than all other multiparameter models presented in Table 3-1. When originally presented and applied, the model only included this nonlethal shock. Because of its structure, the model tended to underestimate the probabilities of failure of higher order groups of components in a highly redundant system; therefore, the concept of lethal shock was included. This version of the model is the one recommended.

When a lethal shock occurs, all components are assumed to fail with a conditional probability of unity. Application of the BFR model with lethal shocks requires the use of the following set of parameters:

- $Q_i$  = independent failure frequency for each component.
- $\omega$  = frequency of occurrence of nonlethal shocks.
- $p$  = conditional probability of failure of each component, given a nonlethal shock.
- $\omega$  = frequency of occurrence of lethal shocks.

The general form of the probability of basic events according to the BFR model is given in Table 3-1. oe

As an example, using this model, the probabilities of the basic events in Eq. 3-6 are written as

$$\begin{aligned}Q_1 &= Q_I + \mu p (1-p)^2 \\Q_2 &= \mu p^2 (1-p) \\Q_3 &= \mu p^3 + \omega\end{aligned}\tag{3-20}$$

Therefore,

$$Q_S = 3[Q_I + \mu p(1-p)^2]^2 + 3\mu p^2(1-p) + \mu p^3 + \omega\tag{3-21}$$

It should be noted that the basic formulation of the BFR model was introduced in terms of the rate of occurrence of failures in time, such as failure of components to continue running while in operation. Here, consistent with our presentation of other models, the BFR parameters are presented in terms of general frequencies that can apply to both failures in time and to failure on demand for standby components.

### 3.3.3 Step 3.3 - Data Classification and Screening

Ideally, the numerical value of the parameters of the various models described in Step 3.2 should be estimated in a manner that makes the maximum possible use of event data; i.e., reports of operating experience. This requires review, evaluation, and classification of the available information to obtain specialized failure data. Because common cause failures can dominate the results of reliability and safety analysis, it is extremely important that this analysis of data is performed within a context that represents the engineering and operational aspects of the system being modeled.

Due to the rarity of common cause events and the limited experience of individual plants, the amount of plant-specific data for common cause analysis is very limited. Therefore, in almost all cases, we need to use data from the industry experience and a variety of sources to make statistical inferences about the frequencies of the common cause events. However, due to the fact that there is a significant variability in plants, especially with regard to the coupling mechanisms and defenses against common cause events, the industry experience is not, in most cases, directly applicable to the specific plant being analyzed although much of it may be indirectly applicable. Also, and perhaps equally important, the analysis boundary conditions that dictate what category of components and causes should be analyzed, requires careful review and screening of events to ensure consistency of the data base with the assumptions of the system model, its boundary conditions, and other qualitative aspects delineated in Stage 2 of the analysis.

The significance of this step cannot be overemphasized. An important conclusion of the Common Cause Failure Reliability Benchmark Exercise (Reference 3-3) is that the most important source of uncertainty and variation in the numerical results is data interpretation. Thus, careful attention and documentation must be given to this step.

3.3.3.1 Data Sources. The first step in data analysis is the data gathering task. The existing data sources generally fall into one of the following categories:

- Generic Raw Data Compilations
- Plant-Specific Raw Data Records
- Generically Classified Event Data and Estimated Parameters

Typical data sources within the above categories are briefly described in the following.

3.3.3.1.1 Generic raw data compilations.

- Licensee Event Report System. This source is a compilation of "safety significant" event reports submitted to the U.S. Nuclear Regulatory Commission by nuclear power plant licensees in accordance with the U.S. government regulations. Various summaries of the LERs are published by different organizations. For instance, summaries of all reported events sorted by plant name are published on a monthly basis by Oak Ridge National Laboratory. In addition, the USNRC has published a compilation of one-line summaries of events involving several categories of components. These are:
  - Diesel Generators (NUREG/CR-1362; Reference 3-22)
  - Pumps (NUREG/CR-1205; Reference 3-23)
  - Valves (NUREG/CR-1363; Reference 3-24)
  - Selected instrumentation and Control Components (NUREG/CR-1740; Reference 3-25)
  - Primary Containment Penetrations (NUREG/CR-1730; Reference 3-26)
  - Control Rods and Drive Mechanisms (NUREG/CR-1331; Reference 3-27)

These reports also provide statistical analysis of the data and give estimates of component failure rates. These rates are based on the number of reported events and estimates of the population, number of demands, and

exposure time for each category of components and each plant. No attempt is made in this report to obtain estimates for the parameters of dependent failure models.

It is reported in Reference 3-28 that the LERs do not report all the independent events and that the underreporting could be as high as a factor of 2 or 3. LERs are available in the public literature.

- Nuclear Power Experience. This source is an LER-based compilation of event reports supplemented by information from other sources. It includes a large number of LERs and is updated monthly (Reference 3-29). NPE is available on a subscription basis only.

The above two sources provide information about abnormal occurrences and are not particularly designed to be used as data bases for model parameter estimation. Nevertheless, they are often the only sources of data available to the analyst. The event reports should be reviewed and classified to extract information about the parameters of interest. The degree of usefulness of the LER and NPE data sources for the purpose of estimating dependent failure parameters depends on the type of model being used. For instance, either of the two sources form a sufficient basis for estimating the parameters of the MGL and alpha factor methods, whereas additional information, such as system success data, is needed to estimate BFR parameters. Furthermore, under the new LER reporting rules, single component failures, in general, are not recorded. Hence, the data base is considerably less useful than it was under the old rules. It will be seen later that consistent recording of single and multiple failure events is required for most parameter estimates.

3.3.3.1.2 Plant-specific raw data records. For a plant-specific analysis, the most applicable sources of data are the plant records, such as operator log books and maintenance request records. Review of the plant-specific records can provide a much more accurate account of failure as well as success data compared with generic raw data sources, but this depends on the quality of the plant record-keeping activity and on such a factor as how well the root causes of various events have been pinpointed. The statistical significance of plant-specific data, however, is a direct function of the number of years of operation of the plant, and, as mentioned before, for plants with even a few years of operating history, the plant-specific data alone will, in general, be insufficient for a common cause analysis.

3.3.3.1.3 Data sources specifically developed for dependent failure analysis. Results of systematic efforts directly aimed at extracting qualitative as well as quantitative information about dependent failures can be found in the following reports:

- Pumps (NUREG/CR-2098; Reference 3-30)

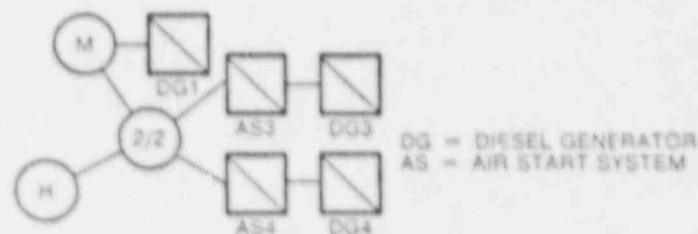
- Valves (NUREG/CR-2770; Reference 3-31)
- Instrumentation and Control Assemblies (NUREG/CR-3289; Reference 3-32)
- Pumps, Valves, Diesel Generators, and Breakers (EPRI NP-3967; Reference 3-4)

The first three of the above reports provide the result of event classification and parameter estimation for the BFR and beta-factor models.

The EPRI-dependent events data classification study (Reference 3-4) presents the results of applying EPRI's detailed and systematic approach (Reference 3-33) for classifying events on a large number of NPE events for the purpose of identifying common cause events. Additionally, another EPRI report and data base (Reference 3-28) contain dependent and independent events data that are systematically classified from LER reports, primarily to provide statistical information on industry defenses against common cause failures and on the distribution of causes for the events.

3.3.3.2 Data Classification. Once the raw data (event reports) are collected, the next step is a review and classification of the events to identify where each event fits in a set of predefined categories describing the type of the event, its cause(s), and its impact; e.g., number of components failed. For this purpose, a data classification approach, such as one developed for EPRI (Reference 3-33) and summarized in Appendix A, is needed. This approach is briefly reviewed in the following.

The EPRI classification system makes use of a cause-effect logic diagram to portray the interactions between root causes and component states in an event. Once the event scenario deduced from an event report is modeled in this way, dependent events are easily identified and their impact on the original system can be readily seen. A typical cause-effect diagram is shown in the following figure.



The diagram represents an event that happened at the Peach Bottom plant in June 1977 in which three out of the four diesel generators became inoperable. Air start systems for diesel generators 3 and 4 were cross-tied with the air start system of diesel generator 1 to correct a

previous failure. Later, when diesel generator 1 was taken out of service for maintenance, air supplies to diesel generators 3 and 4 were lost, making both diesels inoperable.

In the preceding figure, circles with letters represent causes encoded with the letters "H" for human and "M" for maintenance. Component states are represented in squares. In general, all components were classified as either available or unavailable according to a particular success criterion. An unavailable component is either failed (☒) or functionally unavailable (☐) to cover cases in which the nonfunctioning was due to the lack of required input. To cover degraded performance short of violating the success criteria, or incipient failures, component states may be classified as potential failures. Potential failure states are degraded states and incipient failures that had not progressed to the point of failure at the time the event report was prepared.

The cause-effect diagram is constructed by connecting symbols for those causes and component states that produce the event. The symbol (2/2) in the example cause-effect diagram is a logic node, which is introduced to explain cases in which more than one cause is identified. Put together, the diagram of the above example shows how maintenance made one diesel unavailable and, at the same time, contributed to the air start systems of two other diesels becoming unavailable. This led to the functional unavailability of two additional diesels.

It is worth mentioning that the focus of this classification system is on the identification of common cause events and their immediate cause(s) and impact(s). Therefore, some important characteristics of common cause events, such as coupling mechanisms, are not explicitly addressed and represented by the classification system.

This screening of event reports is a rather subjective exercise, particularly in light of the quality of many of the event reports. In an attempt to reduce subjectivity in the screening of event data to identify common cause failures, the CCF-RBE identified the following rules, which have been somewhat modified.

1. Component-caused functional unavailabilities were screened out since it was assumed that this kind of dependency is modeled explicitly.
2. If a specific defense exists that clearly precludes a class of events, all specific events belonging to that class can be screened out.
3. If the cause of the reported event is a train interconnection that, in the plant under consideration, does not exist, the event is considered as an independent failure of one train.

4. Events related to inapplicable plant conditions (e.g., preoperational testing, etc.) can be screened out unless they reveal general causal mechanisms capable of occurring during power operation.
5. If the event occurred during shutdown and would be restored before resuming power operation because of preservice testing or if it cannot occur during power operation, the event is screened out.
6. If a second failure in an event happened after the restoration of the first, both failures are considered as independent failures.
7. Events regarding incipient failure modes (e.g., packing leak, etc.) that clearly do not violate component success criteria can be screened out.
8. Only the events regarding the failure modes of interest were taken into consideration; events regarding failure modes that are irrelevant to the system logic model can be screened out.

Rules 2 and 3 are more directed to the screening of events for applicability to other plants.

3.3.3.3 Event Impact Assessment. The outcome of the event classification process up to this point can be summarized in a form similar to the example given in Figure 3-2(a).

To complete the description of the event impact at the original plant, the analyst needs to identify the following:

1. Component Group Size. The number ( $m$ ) of (typically similar) components that are believed to have been exposed to the root cause and coupling mechanism of the event.
2. Number of Components Affected. The number of components within the component group that were affected (e.g., failed) in the event.
3. Shock Type. Whether the cause(s) and coupling mechanism(s) involved were of the type that typically results in the failure of all components within the component group (lethal shock) or not (nonlethal shock).
4. Failure Mode. The particular component function affected; e.g., failure to open on demand.

Figure 3-2(b) summarizes the information about the event for the example event described in Figure 3-2(a) and introduces the representation called the impact vector (References 3-21 and 3-34).

The binary impact vector of an event that has occurred in a component group of size  $m$  has  $m + 1$  elements. Each element represents the number of components that can fail in an event. If, in an event,  $k$  components are failed, then a 1 is placed in the  $F_k$  position of the binary impact vector, with 0 in other positions. In the example of Figure 3-2, the component group size is 2; therefore, the binary impact vector has three elements:  $\{F_0, F_1, F_2\}$ . Since two components were failed, we have  $F_0 = F_1 = 0$  and  $F_2 = 1$ . A condensed representation is

$$I = \{0, 0, 1\} \quad (3-22)$$

Often, the picture is not as clear as the example in Figures 3-2(a) and 3-2(b) may imply. Most of the time, the event descriptions are not clear, the exact states of components are not always known, and root causes are seldom identified. Therefore, the interpretation of the event [i.e., the translation of the event descriptions into a form similar to the example in Figures 3-2(a) and 3-2(b)] may require establishing several hypotheses, each representing a different interpretation of the event.

As an example, consider the event classified in Figure 3-3(a). Since it is not clear whether the third diesel was also actually failed, the binary impact vector is assessed under two different hypotheses [Figure 3-3(b)]. Under the first hypothesis, only two diesels are considered failed, while, according to the second hypothesis, all three diesels were failed. The analyst at this point needs to assess his or her degree of confidence in each of the two hypotheses. In the example of Figure 3-3(b), a weight of 0.9 is given to the first hypothesis, reflecting a very high degree of confidence that only two diesels were actually failed. The weight for the second hypothesis is obviously 0.1 since the weight should add up to 1. This property of the weighting factors assumes all reasonable hypotheses are accounted for. Note that the data analyst must be in a position to defend and document this assessment.

The expectation values for the impact vectors, taken over the two hypotheses, are

$$\begin{aligned} T &= \{P_0, P_1, P_2\} \\ &= (0.9)I_1 + (0.1)I_2 \\ &= \{0, 0.9, 0.1\} \end{aligned} \quad (3-23)$$

which is also shown in Figure 3-3(b). Note that  $F_k$  refers to a single binary impact vector and  $P_k$  refers to an average impact vector.

This may be used for point estimation.

3.3.3.4 Reinterpretation of Events: Creation of "Plant-Specific" Data Base. Up to this point, the event has been analyzed for the original plant. The next step is to determine what that event implies for the plant and system that are being analyzed. As was mentioned earlier, the



Plant (Date)	Status	Event Description	Cause-Effect Diagram
Pilgrim (September 1976)	95% Power	Two residual heat removal torus cooling valves failed to operate. It was found that the failure was due to excessive pressure differential across the valves, which exceeded the capacity of the valve motors.	

a) Event Classification

Component Group Size	Impact Vector			Shock Type	Fault Mode
	F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>		
2	0	0	1	Nonlethal (L)	Fail To Open on Demand

(b) Event Impact Assessment

Figure 3-2. Example of Event Classification and Impact Assessment

Plant (Date)	Status	Event Description	Cause-Effect Diagram
Maine Yankee (August 1977)	Power	Two diesel generators failed to run due to plugged radiator. The third unit radiator was also plugged.	

(a) Event Classification

Component Group Size	Hypothesis	Probability	$F_0$	$F_1$	$F_2$	$F_3$	Shock Type	Failure Mode
3	$I_1$	0.9	0	0	1	0	Nonlethal (N)	Failure during Operation
	$I_2$	0.1	0	0	0	1		
	Average Impact Vector (I)			$P_0$	$P_1$	$P_2$	$P_3$	
			0	0	0.9	0.1		

(b) Multiple Hypothesis Impact Vector Assessment

Figure 3-3. Example of the Assessment of Impact Vectors Involving Multiple Interpretation of Event

For example, assume that after considering all the qualitative differences between the example plant of Figure 3-2 and our plant, we decide that we are about 75% confident that the event is not applicable to our plant. The average impact vector for our plant (ignoring quantitative differences) can be summarized as follows:

Plant	Not Applicable	Average Impact Vector		
		P0	P1	P2
Pilgrim	--	0	0	1
Our Plant	0.75	0	0	0.25

Note that  $P_0 + P_1 + P_2 + P_{NA} = 1$ .

3.3.3.4.2 Adjustments for size difference. The next step is to consider the system size differences. The objective is to estimate or infer what the data base of applicable events would look like if it all was generated by systems of the same size (i.e., the number of components in each common cause group) as the system being analyzed. This is done by simulating, in a thought experiment, the occurrence of causes of failures (both independent and dependent) in the system of interest and observing how the impact of these causes changes due to difference in system size. Appendix D provides a detailed discussion of the background and justification of the need for adjustment in an impact assessment based on system size differences.\* Appendix D also develops a set of rules and equations for changing the event impact vectors of the original system to a corresponding set for the system being analyzed.

A key assumption behind these rules and equations is that the independent failures are mainly associated with internal component failure mechanisms and that the common cause events are mainly associated with the failure mechanisms external to the components. In view of this general distinction, one can conclude that the causes of common cause events are independent of the number of components. It follows that the same cause will have different impacts depending on the number of components present. For example, any of the causes impacting two or more specific components in a system with two or

---

\*The numerical importance of this adjustment was first explained by Peter Doerre of KWU, Federal Republic of Germany, as part of a contribution to the CCF Reliability Benchmark Exercise (Reference 3-3). The particular mapping method presented here is one of several different ways that the impact vectors can be mapped (see Reference 3-35 for an example).

same qualitative and quantitative information obtained, based on the event at the original plant, may not be directly applicable to the plant and system of interest due to several reasons, such as differences in design, operation, common cause defenses, etc. It is therefore essential to reinterpret the event in light of the specific characteristics of the system under consideration.

In general, the differences between the system in which the data originated and the system being analyzed arise in two ways: First, even for systems of the same size, there are physical differences in system design, component type, operating conditions, environment, etc.; second, there can be a difference in system size (degree of redundancy).

In the following, a framework is described with which these two types of differences can be taken into account explicitly in reinterpretation of the event and the assessment of the impact vector for the system of interest.

3.3.3.4.1 Systems of the same size. First, we consider the differences, given the assumption that the system size is the same. The question to be answered is the following: given all the qualitative differences between the two systems, could the same root cause(s) and coupling mechanism(s) occur in the system being analyzed?

The qualitative information collected about the system in Stages 1 and 2 and about the original system obtained in the initial data classification form the basis of the answer to this question.

If the answer is yes about the applicability, then the event is applicable to the system being analyzed and the analyst can go to the next step to consider the quantitative difference between the two systems. If the answer is no, the event is not applicable and will not be considered as statistical evidence in the estimation of the common cause model parameters and the reasons for elimination will be suitably documented.

In reality, this step involves a considerable amount of judgment. There are a number of sources of uncertainty. These include the lack of detailed information about the event, its circumstances, the nature of its causes, the nature of defenses in the original system, and the effectiveness of defenses in the system being analyzed. Yet, because of the sparsity of data, there is strong motivation to avoid tossing the data out and to extract from it that evidence that is applicable. Due to uncertainties involved and the important implications of screening events out of the data base by declaring them inapplicable, the analyst must have a concrete reason for his judgment. In the cases in which the analyst is uncertain about whether an event is applicable or not, the impact vector of the original system may be modified by a weight reflecting the degree of applicability of the event, as viewed by the analyst. This is similar to the multiple hypothesis situation discussed earlier. Hence, the alternative hypotheses are: (1) applicable with probability  $p$  and (2) not applicable with probability  $(1 - p)$ .

more components can only impact up to one component if only one is present, and some causes may have no impact at all. Similarly, the notion that independent events are due to internal causes leads to the conclusion that the number of independent events observed in the data base is proportional to the number of components in the system. Therefore, if we add more components for the same level of system experience, we add a like amount of opportunities for occurrence of independent events. These and other observations and assumptions lead to the following set of "mapping rules" for adjusting impact vectors for system size. Details are provided in Appendix D.

The rules are presented for the following cases:

1. Mapping Down. The case in which the component group size in the original system is larger than in the system being analyzed.
2. Mapping Up. The case in which the component group size in the original system is smaller than in the system being analyzed.

3.3.3.4.3 Mapping down impact vectors. A complete set of formulas for mapping down data from systems having four, three, or two components to any identical system having fewer  $(m)$  components is presented in Table 3-2. In this table,  $P_k^{(m)}$  represents the  $k$ -th element of the average impact vector in a system (or component group) of size  $m$ . The formulas show how to obtain the elements of the impact vector for smaller size systems when the elements of the impact vector of a larger system are known. Table 3-3 provides several examples of the application of these formulas to binary impact vectors; i.e., impact vectors whose entries are either zero or one. Generalization of the formulas of Table 3-2 to system sizes larger than 4 is straightforward, following the approach described in Appendix D.

3.3.3.4.4 Mapping up impact vectors. It can be seen from the results presented above that downward mapping is deterministic; i.e., given an impact vector for an identical system having more components than the system being analyzed, the impact vector for the same size system can be calculated without introducing any new uncertainties. Mapping up, however, as shown in Appendix D, is not deterministic.

To reduce the uncertainty inherent in upward mapping of impact vectors, use is made of a powerful concept that is the basis of the BFR common cause model. This concept is that all events can be classified into one of three categories:

1. Independent Events. Causal events that act on components singly and independently.

Table 3-2

FORMULAS FOR MAPPING DOWN EVENT IMPACT VECTORS

		SIZE OF SYSTEM MAPPING TO (NUMBER OF IDENTICAL TRAINS)		
		3	2	1
SIZE OF SYSTEM MAPPING FROM	4	$P_0^{(3)} = \frac{1}{4} P_1^{(4)} + P_0^{(4)*}$ $P_1^{(3)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)}$ $P_2^{(3)} = \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)}$ $P_3^{(3)} = \frac{1}{4} P_3^{(4)} + P_4^{(4)}$	$P_0^{(2)} = \frac{1}{2} P_1^{(4)} + \frac{1}{6} P_2^{(4)}$ $P_1^{(2)} = \frac{1}{2} P_1^{(4)} + \frac{2}{3} P_2^{(4)} + \frac{1}{2} P_3^{(4)}$ $P_2^{(2)} = \frac{1}{6} P_2^{(4)} + \frac{1}{2} P_3^{(4)} + P_4^{(4)}$	$P_0^{(1)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} + \frac{1}{4} P_3^{(4)}$ $P_1^{(1)} = \frac{1}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)} + P_4^{(4)}$
	3		$P_0^{(2)} = P_0^{(3)} + \frac{1}{3} P_1^{(3)}$ $P_1^{(2)} = \frac{2}{3} P_1^{(3)} + \frac{2}{3} P_2^{(3)}$ $P_2^{(2)} = \frac{1}{3} P_2^{(3)} + P_3^{(3)}$	$P_0^{(1)} = P_0^{(3)} + \frac{2}{3} P_1^{(3)} + \frac{1}{3} P_2^{(3)}$ $P_1^{(1)} = \frac{1}{3} P_1^{(3)} + \frac{2}{3} P_2^{(3)} + P_3^{(3)}$
	2			$P_0^{(1)} = P_0^{(2)} + \frac{1}{2} P_1^{(2)}$ $P_1^{(1)} = \frac{1}{2} P_1^{(2)} + P_2^{(2)}$

\*THE TERM  $P_0^{(4)}$  IS INCLUDED FOR COMPLETENESS, BUT IN PRACTICE, ANY EVIDENCE THAT MIGHT EXIST ABOUT CAUSES THAT IMPACT NO COMPONENTS IN A FOUR-TRAIN SYSTEM WOULD BE "UNOBSERVABLE."

Table 3-3

## MAPPING DOWN BINARY IMPACT VECTORS FROM FOUR-TRAIN AND THREE-TRAIN SYSTEM DATA

SYSTEM	IMPACT VECTOR*				
	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>

## MAPPING OF EVENT 1

ORIGINAL FOUR-TRAIN SYSTEM	0	0	0	0	1.00
IDENTICAL THREE-TRAIN SYSTEM	0	0	0	1.00	---
IDENTICAL TWO-TRAIN SYSTEM	0	0	1.00	---	---
IDENTICAL ONE-TRAIN SYSTEM	0	1.00	---	---	---

## MAPPING OF EVENT 2

ORIGINAL FOUR-TRAIN SYSTEM	0	0	0	1.00	0
IDENTICAL THREE-TRAIN SYSTEM	0	0	.75	.25	---
IDENTICAL TWO-TRAIN SYSTEM	0	.50	.50	---	---
IDENTICAL ONE-TRAIN SYSTEM	.25	.75	---	---	---

## MAPPING OF EVENT 3

ORIGINAL FOUR-TRAIN SYSTEM	0	0	1.00	0	0
IDENTICAL THREE-TRAIN SYSTEM	0	.50	.50	0	---
IDENTICAL TWO-TRAIN SYSTEM	.17	.67	.17	---	---
IDENTICAL ONE-TRAIN SYSTEM	.50	.50	---	---	---

## MAPPING OF EVENT 4

ORIGINAL FOUR-TRAIN SYSTEM	0	1.00	0	0	0
IDENTICAL THREE-TRAIN SYSTEM	.25	.75	0	0	---
IDENTICAL TWO-TRAIN SYSTEM	.50	.50	0	---	---
IDENTICAL ONE-TRAIN SYSTEM	.75	.25	---	---	---

## MAPPING OF EVENT 5

ORIGINAL FOUR-TRAIN SYSTEM	1.00	0	0	0	0
IDENTICAL THREE-TRAIN SYSTEM	1.00	0	0	0	---
IDENTICAL TWO-TRAIN SYSTEM	1.00	0	0	---	---
IDENTICAL ONE-TRAIN SYSTEM	1.00	0	---	---	---

SYSTEM	IMPACT VECTOR			
	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>

## MAPPING OF EVENT 6

ORIGINAL THREE-TRAIN SYSTEM	0	0	0	1.00
IDENTICAL TWO-TRAIN SYSTEM	0	0	1.00	---
IDENTICAL ONE-TRAIN SYSTEM	0	1.00	---	---

## MAPPING OF EVENT 7

ORIGINAL THREE-TRAIN SYSTEM	0	0	1.00	0
IDENTICAL TWO-TRAIN SYSTEM	0	.67	.33	---
IDENTICAL ONE-TRAIN SYSTEM	.33	.67	---	---

## MAPPING OF EVENT 8

ORIGINAL THREE-TRAIN SYSTEM	0	1.00	0	0
IDENTICAL TWO-TRAIN SYSTEM	.33	.67	0	---
IDENTICAL ONE-TRAIN SYSTEM	.67	.33	---	---

## MAPPING OF EVENT 9

ORIGINAL THREE-TRAIN SYSTEM	1.00	0	0	0
IDENTICAL TWO-TRAIN SYSTEM	1.00	0	0	---
IDENTICAL ONE-TRAIN SYSTEM	1.00	0	---	---

\*FOR EACH EVENT, THE "ORIGINAL" IMPACT VECTOR IS ASSUMED TO BE AVAILABLE FROM AN EVENT REPORT TAKEN FROM A GIVEN SIZE SYSTEM. THEN, WITHIN THE SAME BOX, DIFFERENT EXAMPLES OF NEW IMPACT VECTORS FOR ANALYZED SYSTEMS OF A SMALLER SIZE THAN (BUT OTHERWISE IDENTICAL TO) THE "ORIGINAL" SYSTEM ARE GIVEN.

\*\*(-) MEANS THE IMPACT CATEGORY IS INAPPLICABLE

2. Nonlethal Shocks. Causal events that act on the system as a whole with some chance that any number of components within the system can fail. Alternatively, nonlethal shocks can occur when a causal event acts on a subset of the components in the system.
3. Lethal Shocks. Causal events that always fail all the components in the system.

When enough is known about the cause (i.e., root cause and coupling mechanism) of a given event, it can usually be classified in one of the above categories without difficulty. If, in the course of upward mapping, each event can be identified as belonging to one of the above categories, the uncertainty associated with upward mapping can be substantially reduced (but not eliminated). To be able to categorize an event into one of the above categories requires the analyst to understand the nature of the cause. Random, independent failures (category 1) are usually due to internal causes or external causes isolated to a specific component. Of the remaining external causes, lethal shocks can often be identified as having a certain impact on all components present. Design errors and procedural errors form common examples of lethal shocks. What is left are external causes that have an uncertain impact on each component and these are the not necessarily lethal--or nonlethal--shocks.

If an event is identified as being either an independent event or lethal shock, the impact vectors can be mapped upward deterministically, as shown below. It is only in the case of nonlethal shocks that an added element of uncertainty is introduced on mapping upward. How each event is handled is separately summarized below.

3.3.3.4.5 Mapping up independent events. In this case, since the number of independent events in the data base is simply proportional to the number of components in the system, it can be shown that  $P_I^{(l)}$  and  $P_I^{(k)}$ , the number of independent events in systems with sizes  $l$  and  $k$ , respectively, are related by the following equation:\*

$$P_I^{(l)} = \frac{l}{k} P_I^{(k)} \quad (3-24)$$

The numerical impact of the upward mapping of the independent events on the value of the common cause parameters is shown in Section 4.1 in the context of an example system.

---

\*Because it adds events that were not actually observed, this approach decreases the statistical uncertainty associated with the frequency of independent events. However, the impact on the uncertainty analysis is generally negligible compared to other sources of uncertainty.



3.3.3.4.6 Mapping up lethal shocks. By definition, a lethal shock wipes out all the redundant components present within a common cause group. The key underlying assumption in the following simple formula for upward mapping of impact vectors involving lethal shock is that the lethal shock rate acting on the system is constant and independent of system size. From it follows the following simple relationship:

$$p_{\ell}^{(\ell)} = p_j^{(j)} \quad (3-25)$$

Hence, for lethal shocks, the impact vector is mapped directly. The probability that all  $j$  components in a system of  $j$  components have failed due to a lethal shock is mapped directly to the probability of failing all  $\ell$  components in an  $\ell$  component system without modification.

3.3.3.4.7 Mapping up nonlethal shocks. Nonlethal shock failures are viewed as the result of a nonlethal shock that acts on the system at a rate that is independent of the system size. For each shock, there is a constant probability,  $\rho$ , that each component fails. The quantity  $\rho$  is the conditional probability of each component failure, given a shock.

The process of mapping a nonlethal shock that occurs in a one-component system up to a four-component system is illustrated in Appendix D. Table 3-4 includes formulas to cover all the upward mapping possibilities with system sizes up to four. In the limiting cases of  $\rho = 0$  and  $\rho = 1$ , the formulas in Table 3-4 became identical to Eq. 3-24 (mapping up independent events) and Eq. 3-25 (mapping up lethal shocks), respectively.

By making use of the powerful concepts of the BFR model, the uncertainty inherent in mapping up impact vectors is reduced to the uncertainty in estimating the parameter  $\rho$ , which is the probability that the nonlethal shock or cause would have failed a single hypothetical component added to the system. The formulas in Table 3-4 take care of all the bookkeeping problems of enumerating the possibilities and factoring in the system size effects.

While it is the analyst's responsibility to assess, document, and defend his assessment of the parameter  $\rho$ , some simple guidelines should help in its quantification.

- If an event is classified as a nonlethal shock and it fails only one component of a group of three or more components, it is reasonable to expect that  $\rho$  is small ( $\rho < .5$ ).
- If a nonlethal shock fails a number of components intermediate to the number present, it is unreasonable to expect that  $\rho$  is either very small ( $\rho \rightarrow 0$ ) or very large ( $\rho \rightarrow 1$ ).

Table 3-4

FORMULAS FOR UPWARD MAPPING OF EVENTS CLASSIFIED AS NONLETHAL SHOCKS

		SIZE OF SYSTEM MAPPING TO		
		2	3	4
SIZE OF SYSTEM MAPPING FROM	1	$P_1^{(2)} = 2(1 - \rho)P_1^{(1)}$ $P_2^{(2)} = \rho P_1^{(1)}$	$P_1^{(3)} = 3(1 - \rho)^2 P_1^{(1)}$ $P_2^{(3)} = 3\rho(1 - \rho)P_1^{(1)}$ $P_3^{(3)} = \rho^2 P_1^{(1)}$	$P_1^{(4)} = 4(1 - \rho)^3 P_1^{(1)}$ $P_2^{(4)} = 6\rho(1 - \rho)^2 P_1^{(1)}$ $P_3^{(4)} = 4\rho^2(1 - \rho)P_1^{(1)}$ $P_4^{(4)} = \rho^3 P_1^{(1)}$
	2		$P_1^{(3)} = (3/2)(1 - \rho)P_1^{(2)}$ $P_2^{(3)} = \rho P_1^{(2)} + (1 - \rho)P_2^{(2)}$ $P_3^{(3)} = \rho P_2^{(2)}$	$P_1^{(4)} = 2(1 - \rho)^2 P_1^{(2)}$ $P_2^{(4)} = (5/2)\rho(1 - \rho)P_1^{(2)} + (1 - \rho)^2 P_2^{(2)}$ $P_3^{(4)} = \rho^2 P_1^{(2)} + 2\rho(1 - \rho)P_2^{(2)}$ $P_4^{(4)} = \rho^2 P_2^{(2)}$
	3			$P_1^{(4)} = (4/3)(1 - \rho)P_1^{(3)}$ $P_2^{(4)} = \rho P_1^{(3)} + (1 - \rho)P_2^{(3)}$ $P_3^{(4)} = \rho P_2^{(3)} + (1 - \rho)P_3^{(3)}$ $P_4^{(4)} = \rho P_3^{(3)}$

- If a nonlethal shock fails all the components present in a system, it is reasonable to expect that  $\rho$  is large ( $\rho > .5$ ).

Examples of upward mapping for several different events are shown in Table 3-5.

A final observation to be aware of is that, based on the example problem presented in Section 4.1, the final results of a common cause analysis are much more sensitive to uncertainties in the classification of lethal shocks than nonlethal shocks. Hence, the conservative approach of simply assuming that  $\rho = 1$  would not have an appreciable impact in most practical cases.

3.3.3.4.8 Summary of impact vector mapping. The impact vector mapping concepts of this section are summarized in the form of a decision tree for the data analyst in Figure 3-4. This decision tree guides the analyst through the important tasks of assessing the applicability of each event, determination of system size for the events in the data base and for the system being analyzed, and the use of the appropriate mapping formulas derived in this section.

Once the impact vectors of all the events in the data base are assessed for the system being analyzed, the number of events in each impact category can be calculated by adding the impact vectors. That is,

$$n_k = \sum_{i=1}^m P_k(i) \quad (3-26)$$

where

$n_k$  = total number of basic events involving failure of  $k$  similar components.

$P_k(i)$  = the  $P_k$  element of the impact vector.

As an example, consider the following data base of four events with the associated average impact vectors assessed for a system of four components.

Table 3-5

EXAMPLES OF UPWARD MAPPING OF IMPACT VECTORS

EVENT NO.	SYSTEM-SIZE	IMPACT VECTOR*			
		P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>
INDEPENDENT EVENT CASES					
1	ORIGINAL - ONE TRAIN	1	—**	—	—
	IDENTICAL - TWO TRAIN	2	0	—	—
	IDENTICAL - THREE TRAIN	3	0	0	—
	IDENTICAL - FOUR TRAIN	4	0	0	0
2	ORIGINAL - TWO TRAIN	1	0	—	—
	IDENTICAL - THREE TRAIN	1.5	0	0	—
	IDENTICAL - FOUR TRAIN	2	0	0	0
3	ORIGINAL - THREE TRAIN	1	0	0	—
	IDENTICAL - FOUR TRAIN	1.33	0	0	0
NONLETHAL SHOCK CASES (p = .10)					
4	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	1.8	.1	—	—
	IDENTICAL - THREE TRAIN	2.43	.27	.01	—
	IDENTICAL - FOUR TRAIN	2.915	.486	.036	.001
5	ORIGINAL - TWO TRAIN	1	0	—	—
	IDENTICAL - THREE TRAIN	1.35	1	0	—
	IDENTICAL - FOUR TRAIN	1.62	.225	.01	0
6	ORIGINAL - TWO TRAIN	5	5	—	—
	IDENTICAL - THREE TRAIN	675	5	.05	—
	IDENTICAL - FOUR TRAIN	81	.5175	.095	.005
7	ORIGINAL - THREE TRAIN	25	.5	.25	—
	IDENTICAL - FOUR TRAIN	3	.475	.275	.025
LETHAL SHOCK CASE					
8	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	0	1	—	—
	IDENTICAL - THREE TRAIN	0	0	1	—
	IDENTICAL - FOUR TRAIN	0	0	0	1
NONLETHAL SHOCK CASES (p = .9)					
9	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	2	.9	—	—
	IDENTICAL - THREE TRAIN	.03	.27	.81	—
	IDENTICAL - FOUR TRAIN	.004	.054	.324	.729
NONLETHAL SHOCK CASES (p = .5)					
10	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	1	.5	—	—
	IDENTICAL - THREE TRAIN	.75	.75	.25	—
	IDENTICAL - FOUR TRAIN	.5	.75	.5	.125
11	ORIGINAL - TWO TRAIN	0	1	—	—
	IDENTICAL - THREE TRAIN	0	.5	.5	—
	IDENTICAL - FOUR TRAIN	0	.25	.5	.25
12	ORIGINAL - TWO TRAIN	.5	.5	—	—
	IDENTICAL - THREE TRAIN	.375	.50	.25	—
	IDENTICAL - FOUR TRAIN	.25	.4375	.375	.125
13	ORIGINAL - THREE TRAIN	.25	.5	.25	—
	IDENTICAL - FOUR TRAIN	.1667	.375	.375	.125

\*FOR EACH EVENT, THE "ORIGINAL" IMPACT VECTOR IS ASSUMED TO BE AVAILABLE FROM AN EVENT REPORT TAKEN FROM A GIVEN SIZE SYSTEM THEN, WITHIN THE SAME BOX, DIFFERENT EXAMPLES OF NEW IMPACT VECTORS FOR ANALYZED SYSTEMS OF A LARGER SIZE THAN (BUT OTHERWISE "IDENTICAL" TO) THE "ORIGINAL" SYSTEM ARE GIVEN.

\*\*[—] MEANS THE IMPACT CATEGORY IS INAPPLICABLE

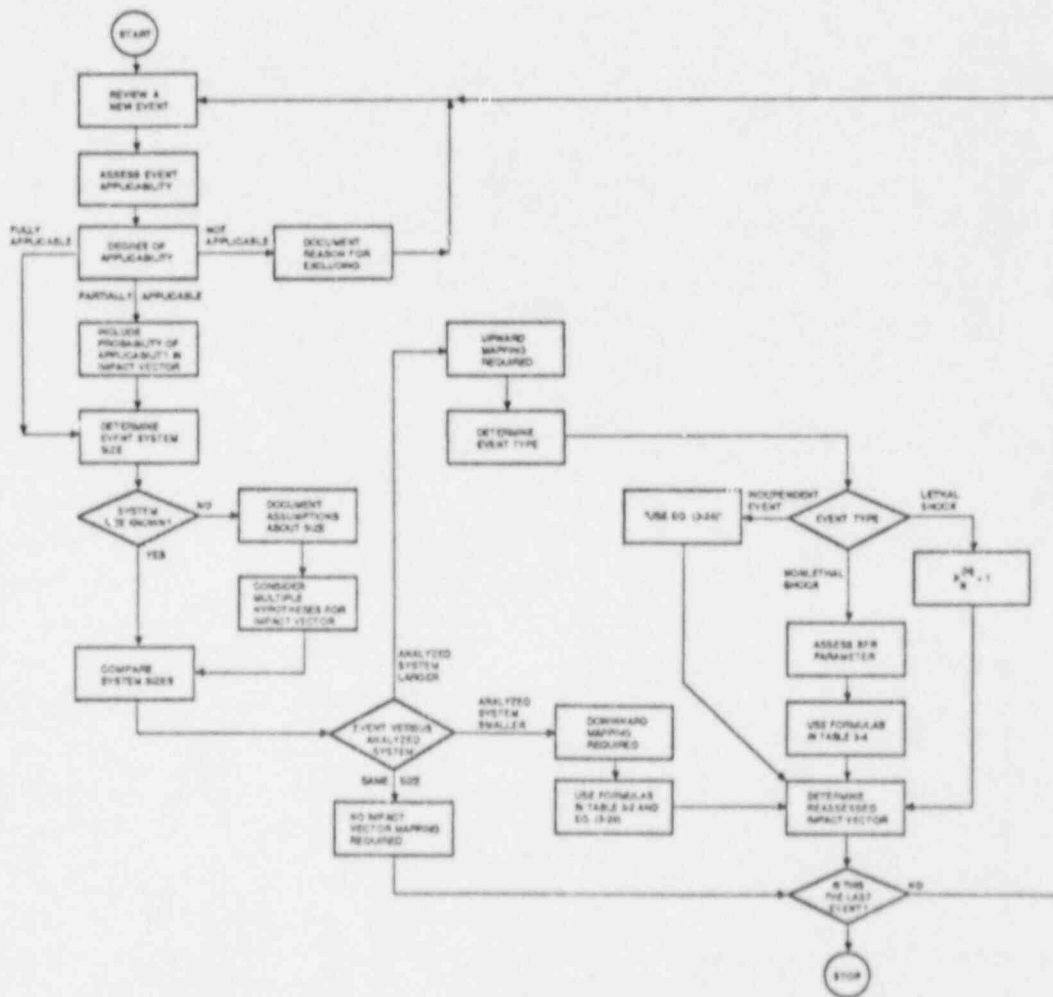


Figure 3-4. Decision Tree for Assessing and Mapping Event Impact Vectors

Event Number	Impact Vector					
	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	NA
1	0	0.1	0	0.9	0	0
2	0	0.8	0.1	0.05	0.05	0
3	0	0	0	0	0	1
4	0.7	0	0.3	0	0	0
Total	n <sub>0</sub>	n <sub>1</sub>	n <sub>2</sub>	n <sub>3</sub>	n <sub>4</sub>	n <sub>NA</sub>
	0.7	0.9	0.4	0.95	0.05	1

In this data base, for example, the value of n<sub>3</sub> (number of events involving failure of three components) is calculated as

$$\begin{aligned} n_3 &= 0.9 + 0.05 \\ &= 0.95 \end{aligned}$$

Note also that

$$\sum_{k=1}^4 n_k = 4 \quad (3-27)$$

which is the total number of events in the data base.

**3.3.3.5 Summary of Event Screening.** The result of this process is a set of impact vectors that summarizes the translation of industry experience to the plant of interest. It is stressed that, for this to be complete, the exercise has to be performed not only for the potential dependent events but also for the independent events. In this process, some events have been screened out as being inapplicable. The validity of this screening out has been questioned because it implies that the plant in question is somehow better than the "generic" plant that possesses all characteristics of all plants and that it has no hidden causes of failure that other plants do not. Although it is clearly not reasonable to assume each plant has all the characteristics of all plants in the data base this screening must be done with care and with specific justifiable reasons for excluding any event.

The natural way to deal with the question is to compensate for the deletion of events by also reducing the exposure and for the number of independent events. As an example, suppose that it is felt that because of significant design differences, the events occurring in one or more plants in the generic data base are not applicable. One approach then is to exclude events for the affected components at these plants from the

data base. This implies a smaller exposure, which affects the direct estimation of the basic event probabilities. Additionally, if the parametric models are used, this implies that the associated independent failure events also be excluded. This smaller data base leads to larger uncertainties in the parameter estimates, which may increase or decrease.

An intermediate case but less practical solution is one in which some of the failure causes of a component apply while others do not. In this case, the events could be modeled or excluded depending on the cause. For example, events relating to failures of diesel generators due to electric start motor problems do not apply to diesel generators with air start systems. On the other hand, generic causes like human error would still be held to apply to systems with such specific design differences. Each source of events would then be related to the relevant exposure. This process is probably beyond the capability of current data systems to support, and the former procedure of deleting plants from the data base for rejected events is recommended.

#### 3.3.4 Step 3.4 - Parameter Estimation

The purpose of this step is to use the "pseudo-data" generated in the previous step to provide estimates of either the basic event probabilities themselves (using the basic parameter model) or the parameters of the common cause failure models (beta, BFR, etc.). These estimates are subject to many sources of uncertainty and the ways in which these are addressed are also discussed here.

The information provided by the set of impact vectors is the numbers of events in which 1, 2, 3, and up to  $n$ , where  $n$  is the degree of redundancy, components failed. To proceed further, it is necessary in the case of the direct estimation of the basic event probabilities to have estimates of the exposure of the events to the failures. The exposure may be measured in terms of the number of demands or the total time, depending on which reliability model is appropriate for the failure mode of interest. In the case of the parameters of common cause failure models, it is also necessary to have at least an estimate of the relative exposures in order to derive estimators. This is illustrated in the following example, which is included for two reasons: first and most important is to illustrate how assumptions made about the way the events in the data base arose affects the estimation of common cause event probabilities, and second is to illustrate the way by which this pseudo-data base can be anchored to preexisting estimates of single-component failure probabilities. The example is the derivation of the estimator for the beta factor for the case of a two-train redundant system in the failure to start mode. The illustration given is for the case in which the reliability model chosen is that of a constant probability of failure on demand. An alternative model, the assumption of a constant failure rate while on standby is somewhat different, as discussed in Appendix C.

3.3.4.1 Example - Beta Factor Estimator. Suppose that the evidence from the pseudo-data base is that there are  $n_1$  failures of single components and  $n_2$  failure events in which both components failed. Suppose further that an estimate of the total single-component failure probability,  $Q_T$ ,

already exists. Then, the unknown number of single-component demands,  $N$ , in the pseudo-data base can be estimated by making the identification,  $Q_T = (n_1 + 2n_2)/N$ . Now, all that is unknown is the number of times,  $N_2$ , that there was an effective test in the pseudo-data base for the common cause failure. For most redundant systems in nuclear power plants, the greatest number of demands comes from surveillance testing so that the answer to this question can come from knowing the testing strategy, as illustrated below. Consider the following two strategies, both of which comply with a technical specification requirement that says that each train must be tested once a month.

- Strategy 1. Both components are tested at the same time (or at least the same shift). In this case, the number of tests against the common cause can be said to be  $N/2$ . The common cause failure probability therefore is  $2n_2/N$ , and an appropriate beta factor estimator, consistent with Eq. 3-12, is

$$\beta = \frac{2n_2}{n_1 + 2n_2} \quad (3-28)$$

This is the familiar estimator found in the PRA Procedures Guide for example.

- Strategy 2. The components are tested at staggered intervals, one every 2 weeks, and, if there is a failure, the second component is tested immediately. In this case, the number of tests against the common cause is higher because each successful test of a component is a confirmation of the absence of the common cause. The number of tests against the common cause failure  $N_2$  is related to  $N$  by the following equation:

$$N = N_2 + n_1 + n_2 \quad (3-29)$$

The terms  $n_1$  and  $n_2$  arise because of the failure of the first component, which occurs  $n_1$  times on its own and  $n_2$  times in conjunction with the failure of the other. In this case, therefore, the common cause failure probability is given by  $n_2/N_2$ , which is approximately  $n_2/N$  when  $n_1$  and  $n_2$  are small compared to  $N$ . This is approximately half of the failure probability that results from assuming the first strategy is correct. The appropriate beta factor in this case is

$$\beta = \frac{n_2}{n_1 + n_2} \quad (3-30)$$

This example therefore illustrates the importance of recognizing that specific estimators are based on particular assumptions about such things as testing strategy. In general, the testing strategies at the plants in



the pseudo-data base may not be known and will probably be mixed. The two extreme cases here should bound the real situation. Although the numerical uncertainty introduced may not be large compared with that introduced by the interpretation of the data, this is an important point to recognize for consistency in modeling. This question is discussed at greater length in Appendix C.

3.3.4.2 Point Estimates. Table 3-6 presents simple point estimates for the various parametric models described in this report, based on the assumption that the data are from plants in which nonstaggered testing is adopted. The estimators are provided in terms of the number of basic events observed in each common cause impact category (i.e.,  $n_1, n_2, \dots, n_m$ ) and, if necessary, the number of system demands,  $N_D$ , which is related to the number of component demands,  $N$ , in the following way:  $N = mN_D$ . To obtain the time-based parameters (e.g., failure during operation), the quantity  $N_D$  should be replaced by  $T$ , the cumulative system exposure time; e.g., total number of system operating hours. More detail about the development of these estimators is provided in Appendix E.

Note that, for a fixed single-component total failure probability, the estimates of common cause failure probabilities are conservative if staggered versus nonstaggered testing is assumed (Table 3-6). If all the plants in the data base use staggered testing, the conservatism would be a factor of two for two train systems and somewhat larger for higher redundancies. In practice, the conservatism is less than this.

These point estimates rely on the fact that there exist in the data base some multiple failure events. If there are none, these simple estimators are zero. In this case, an estimator, such as the C-factor (Reference 3-11), can be useful for screening purposes. This estimator is essentially the fraction of root causes of events in the event data base for which it is judged, on the basis of the impact of these root causes on the plant of interest, could have led to multiple failures at that plant. It will be noted that, in contrast to screening out events, this method may in fact introduce multiple failure events. The method is based on the assumption that the observed spectrum of root causes is a good representation of the true spectrum.

3.3.4.3 Assessment of Uncertainty in Parameter Estimates. Point estimates developed above only provide single values for the parameters of the models. However, there are numerous sources of uncertainties that must be taken into account to present a realistic picture of what the analyst knows about the value of these parameters. In performing uncertainty analysis, it is often sufficient to develop distributions only for the most important contributors to the system unavailability, identified through ranking the contributors on the basis of point estimates.

The following provides a brief discussion of the most important elements of uncertainty and some available techniques for incorporating these

Table 3-6

## SIMPLE POINT ESTIMATORS FOR VARIOUS PARAMETRIC MODELS

Sheet 1 of 3

Method	Point Estimator (a,b,c)	Remarks
Basic Parameter	$Q_k = \frac{n_k}{\binom{m}{k} N_D} \quad k=1, \dots, m$	<ul style="list-style-type: none"> <li>Estimator is a maximum likelihood estimator.</li> <li>For time-based failure rates, replace system demands (<math>N_D</math>) with total system exposures time <math>T</math>.</li> </ul>
Multiple Greek Letter	$Q_t = \frac{1}{mN_D} \sum_{k=1}^m k n_k$ $\beta = \left( \sum_{k=2}^m k n_k \right) / \left( \sum_{k=1}^m k n_k \right)$ $\gamma = \left( \sum_{k=3}^m k n_k \right) / \left( \sum_{k=2}^m k n_k \right)$ $\delta = \left( \sum_{k=4}^m k n_k \right) / \left( \sum_{k=3}^m k n_k \right)$	<ul style="list-style-type: none"> <li>Estimators are only provided for three parameters (<math>\beta</math>, <math>\gamma</math>, and <math>\delta</math>). Estimators for higher order parameters are derived similarly.</li> <li>Generic values of <math>Q_t</math>, the total component failure frequency, are usually available from risk and reliability data sources.</li> <li>The estimators are based on approximate method described in Appendix C.</li> </ul>

## NOTES:

- All estimators assume that, in every system demand, all components and possible combinations of components are challenged. Consequently, system tests are assumed to be nonstaggered (see discussion in Appendix C).
- For the definition of various parameters, see Section 3.3.2.
- Estimates are developed for a system of  $m$  redundant components.

Table 3-6 (continued)

Sheet 2 of 3

Method	Point Estimator (a,b,c)	Remarks
Beta Factor	$Q_t = \frac{1}{mN_D} \sum_{k=1}^m kn_k$ $R = \left( \sum_{k=2}^m kn_k \right) / \left( \sum_{k=1}^m kn_k \right)$	<ul style="list-style-type: none"> <li>• Generic values of <math>Q_t</math>, the total failure frequency are usually available from generic risk and reliability data sources.</li> <li>• The estimator is based on approximate method described in Appendix C.</li> </ul>
Alpha Factor	$Q_t = \frac{1}{mN_D} \sum_{k=1}^m kn_k$ $\alpha_k = \frac{n_k}{\sum_{k=1}^m n_k} \quad k=1, \dots, m$	<ul style="list-style-type: none"> <li>• Generic values of <math>Q_t</math>, the total failure frequency are usually available from generic risk and reliability data sources.</li> <li>• The estimator is a maximum likelihood estimator, described in Appendix C.</li> </ul>

## NOTES:

- (a) All estimators assume that, in every system demand, all components and possible combinations of components are challenged. Consequently, system tests are assumed to be nonstaggered (see discussion in Appendix C).
- (b) For the definition of various parameters, see Section 3.3.2.
- (c) Estimates are developed for a system of  $m$  redundant components.

Table 3-6 (continued)

Sheet 3 of 3

Method	Point Estimator (a,b,c)	Remarks
Binomial Failure Rate	$Q_I = \frac{n_I}{mN_D}$ $Q'_t = \left( \sum_{k=1}^m n_k \right) / N_D$ $\omega = \frac{n_L}{N_D}$ $\frac{p}{1-(1-p)^m} = \frac{\sum_{k=1}^m kn_k}{m \sum_{k=1}^m n_k}$ $\mu = \frac{Q'_t}{1-(1-p)^m}$	<ul style="list-style-type: none"> <li>• Estimators are maximum likelihood estimators.</li> <li>• For time-based failure rates, replace system demands with total system exposure time.</li> <li>• <math>n_I</math> is the number of single component failures due to common cause shocks. The quantity <math>n_I</math> represents number of independent failures.</li> </ul>

## NOTES:

- (a) All estimators assume that, in every system demand, all components and possible combinations of components are challenged. Consequently, system tests are assumed to be nonstaggered (see discussion in Appendix C).
- (b) For the definition of various parameters, see Section 3.3.2.
- (c) Estimates are developed for a system of  $m$  redundant components.

elements in assessing parameter distributions. The uncertainties stem from one or more of the following reasons:

1. Uncertainty in data classification and impact vector assessment.
2. Uncertainty in estimating success (exposure) data and incompleteness of failure event data sources; e.g., underreporting of independent events.
3. Statistical uncertainty dictated by the size of data sample.
4. Variation among plants in equipment, system design, and operations.

Uncertainties about PRA parameters are typically represented in the form of probability distributions, and it is the mean value of these distributions that is the most suitable "point estimate" for point calculations. Therefore, it is recommended that the parameters be estimated with the associated uncertainty distributions even when uncertainty propagation is not intended in system quantification.

The distribution of the parameters is estimated on the basis of evidence. The evidence could be statistical when data are available or based on expert opinion. Bayes' theorem provides a very flexible and powerful framework for incorporating various types of information in parameter estimation. It is particularly useful when the evidence is of an uncertain nature as is the case with PRA data in general and common cause failure data in particular. For this reason, parameter estimation techniques in this report are presented in the Bayesian framework. The way Bayes' theorem is used for this purpose is discussed in Appendix E.

The distributions presented in Appendix E assume that the required data (e.g.,  $n_k$ 's for the MGL model) are known. However, as discussed in the previous sections, such is not the case and the full representation of all uncertainties requires some refinements in the uncertainty models. In fact, the uncertainties are mostly driven, not by the usual statistical uncertainties, but rather by such factors as judgment used in data classification, assumptions made about the population from which failure and success data are obtained, and completeness of the data bases.

3.3.4.4 Uncertainty in Data Classification and Impact Vector Assessment. The uncertainties due to judgments required in interpretation and classification of failure events and the assessment of impact vectors, as described before, are perhaps the most significant of all sources of uncertainty. Using the impact vector, the analyst's judgment about how a given event should be counted in estimating parameters is encoded in his probability for each of several hypotheses set forth by him about the possible impact of the event (number of components failed), for the system being analyzed.

Formally, this type of uncertain data can be represented as

$$E = \{ \langle P_{ij}, I_{ij} \rangle \quad i=1, \dots, N; \quad j=1, \dots, M_i \} \quad (3-31)$$

where  $P_{ij}$  is the analyst's probability for hypothesis  $j$  about event  $i$ , and  $I_{ij}$  is the corresponding binary impact vector.  $N$  represents the number of events in the data base, and  $M_i$  is the number of hypotheses about the  $i$ th event. Note that

$$\sum_{j=1}^{M_i} P_{ij} = 1 \quad (3-32)$$

As an example, consider a data base composed of two events, with the following hypotheses and impact vectors:

Event	Hypothesis	Probability	Impact Vector				
			F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	NA
Event 1	I <sub>11</sub>	P <sub>11</sub>	0	0	1	0	0
	I <sub>12</sub>	P <sub>12</sub>	0	0	0	1	0
Event 2	I <sub>21</sub>	P <sub>21</sub>	1	0	0	0	0
	I <sub>22</sub>	P <sub>22</sub>	0	1	0	0	0
	I <sub>23</sub>	P <sub>23</sub>	0	0	1	0	0

There are six possible data sets that can be obtained from the above set of hypotheses by taking all possible combination of hypotheses. These data sets and the associated probabilities are listed in the following.

Data Set	Probability	Event Statistics				
		N <sub>0</sub>	N <sub>1</sub>	N <sub>2</sub>	N <sub>3</sub>	NA
D <sub>1</sub>	w <sub>1</sub> = P <sub>11</sub> P <sub>21</sub>	1	0	1	0	0
D <sub>2</sub>	w <sub>2</sub> = P <sub>11</sub> P <sub>22</sub>	0	1	1	0	0
D <sub>3</sub>	w <sub>3</sub> = P <sub>11</sub> P <sub>23</sub>	0	0	2	0	0
D <sub>4</sub>	w <sub>4</sub> = P <sub>12</sub> P <sub>21</sub>	1	0	0	1	0
D <sub>5</sub>	w <sub>5</sub> = P <sub>12</sub> P <sub>22</sub>	0	1	0	1	0
D <sub>6</sub>	w <sub>6</sub> = P <sub>12</sub> P <sub>23</sub>	0	0	1	1	0

An uncertainty distribution for a given common cause parameter,  $\lambda$ , can be found by taking any of the six possible data sets listed in the above table as evidence. If  $\pi_i(\lambda|D_i)$  is such a distribution based on data set  $D_i$ , then the distribution of  $\lambda$ , taking into account all possible data sets, will be given by

$$\pi(\lambda) = \sum_{i=1}^6 w_i \pi_i(\lambda|D_i) \quad (3-33)$$

where  $w_i$  is the probability associated with data set  $D_i$ .

In reality, the number of data sets that can be generated by considering all possible combinations of various hypotheses about events is very large. As a result, the implementation of the rigorous procedure described here is extremely difficult. An approximate way of including these effects, at least in the mean values, is to obtain an "average" impact vector for each event, as recommended in Section 3.3.3, before combining them to obtain the total number of events in each impact category. Formally,

$$\bar{E} = \{\bar{I}_i; \quad i=1, \dots, N\} \quad (3-34)$$

where

$$\bar{I}_i = \sum_{j=1}^{M_i} P_{ij} I_{ij} \quad (3-35)$$

For instance, in our two-event example, this averaging process result, in:

Event	$P_0$	$P_1$	$P_2$	$P_3$	NA
Event 1	0	0	$P_{11}$	$P_{12}$	0
Event 2	$P_{21}$	$P_{22}$	$P_{23}$	0	0

Then, the resulting data set (by adding  $\bar{P}_i$ 's from each event) is

Data Set	$\bar{n}_0$	$\bar{n}_1$	$\bar{n}_2$	$\bar{n}_3$	$\bar{NA}$
$\bar{D}$	$P_{21}$	$P_{22}$	$P_{11} + P_{23}$	$P_{12}$	0

The implications of this approximation and comparison with the rigorous treatment according to Eq. 3-33 are discussed in Reference 3-36.

Another practical approximation that attempts to incorporate the uncertainty more completely is choosing two bounding cases, one with a consistently pessimistic view (and nonstaggered estimators), the other with a consistently optimistic view (and staggered testing assumptions) to provide a measure of the range. A "best estimate" may also be provided using, perhaps, an average or expected value of the impact vectors. It is recognized that more work is required for a practical and more complete treatment of uncertainty.

3.3.4.5 Uncertainty due to Success and Failure Data Completeness. The problems associated with estimating success (exposure) data (e.g., the number of system demands or operating hours) needed by some of the parametric models directly and all others indirectly are not specific to common cause failure analysis. It is, in general, very difficult to obtain an accurate estimate of the success data because no success data recording and reporting system exists for the nuclear industry. Even reconstruction of the success data from plant-specific records, as is often done in plant-specific PRAs, is not only a major task, but also heavily involves the judgment of the data analyst. However, the problem is exacerbated in the case of common cause failures because of the problem of estimating the success data for groups of components taken together. Since the data on which the estimates are based are from groups of plants that probably have different surveillance test strategies, it is unlikely that "exact" estimators can even be found, thus adding another dimension to the uncertainty.

Similar uncertainties exist about the completeness of the failure event sources. It is believed, for instance, that a substantial proportion of all independent failure events are not reported to the LER system. Both of these uncertainties can be represented explicitly in the parametric distributions through Bayes' theorem by assuming uncertainty distributions for both the success and failure data.

3.3.4.6 Statistical Uncertainty. This source of uncertainty is a well-known subject in statistics. It stems from the fact that parameters are estimated only on a subset of the entire population of failure and success data. Larger sample sizes result in a higher degree of confidence in the estimated parameters simply because they are better representative of the general population. The mathematical models of Appendix E explicitly handle this type of uncertainty; as more data become available, the posterior distributions become narrower, indicating a higher degree of confidence. For instance, the variance of the distributions of the basic parameter model decreases as  $n_k$  and  $N_0$  (for demand-based parameters) increase. Similar behavior is observed in the distributions of other models.

3.3.4.7 Plant-to-Plant Variability. The fourth source of uncertainty is the familiar concept of variation of the value of the parameters from plant to plant. This type of variability stems from the fact that similar equipment and systems in various plants may show inherently



different failure rates due to a variety of reasons, such as minor design differences within the same category of equipment, variation in system designs, and operating philosophies leading to different coupling mechanisms.

Conceptually, there are two approaches for dealing with this issue. One approach is to assess the variability of the parameters that are based on statistical evidence from each plant, without screening events based on their applicability to the situation under consideration. If it were practical, this would result in a wider range of possible values for the parameters than if this variation were ignored. In the second approach, which is adopted in this report for estimation of the common cause parameters, failure events from various plants are reclassified and mapped for the plant or system of interest. The result is the formation of a data base much larger than one based only on the records of the specific plant under consideration. The resulting statistical uncertainty range for the estimated parameters will obviously be smaller in this case, compared with a distribution representing differences in plants. This reduction in uncertainty is the result of applying the additional information about the specific characteristics of the system being analyzed and obviates the need for separate consideration of the plant-to-plant variation for the common cause parameters. This decrease in statistical uncertainty is bought at the expense of another uncertainty, that in the impact vector assessment. It is however still essential to consider plant-to-plant variation for total failure rates.

3.3.4.8 Use of Generic Values of Common Cause Parameters. The systematic procedures for dependent events analysis presented in Step 3.3 require the analyst to screen and classify event data, use estimators provided, and develop uncertainty distributions and/or point estimates of model parameters for each specific analysis. This procedure is recommended instead of using published numerical data for these parameters for several important reasons. One reason is to prevent the use of data that are inapplicable to the system being analyzed. Another is to provide a consistent framework for combining data from systems having different numbers of components and for accounting for differences between the number of components being analyzed and those associated with systems providing the data. In addition, event screening can eliminate all inconsistencies between the data and the assumptions built into the common cause event models. Finally, the event screening and classification process provides qualitative insights about possible approaches to defending against future occurrences of these events in the system.

A formidable obstacle to the adoption of an approach based on event screening in prior analyses was the amount of time needed to sift and sort through such event reports as the Licensee Event Reports and the numerous problems associated with extracting quantitative information from the review of these reports. A useful contribution to lessening the work has been the development and application of the EPRI-dependent events classification system. The final form of this classification system (Reference 3-33) has been and is currently being applied to a large fraction of the accumulated LERs covering U.S. power reactor

experience. As mentioned earlier, an initial data base of classified event reports, including several hundred dependent events, is provided in Reference 3-4. Numerous examples of this classified data base are presented in this section and in Section 4. This EPRI data base was expanded in a companion project (Reference 3-28). The availability of these classified data bases greatly reduces the time required to incorporate event screening as an integral part of systems analysis if one is willing to accept the classification of the authors of the report. It should be remembered that this classification is subjective. However, at the very least, the report provides a prescreening of the data to identify event reports worth looking at in detail.

Despite the availability of classified event reports, the authors recognize the continuing need to support analysts who may need to bypass the event screening step and use published numerical values of common cause event parameters. For these analysts, a list of what the authors call "generic beta factors" are provided in Table 3-7. This table provides an update of a similar table in Reference 3-4. (Appendix H presents a compilation of generic beta factors that have been derived worldwide from nuclear, chemical, aircraft, and other industries.) Although the use of these generic factors is strongly discouraged as a substitute for the event screening approach, the use of these generic beta factors may be used as a coarse and conservative screen for common cause analysis, provided suitable qualification of the results is indicated. Implicit assumptions in the use of these parameters include the following:

- The analyzed system is susceptible to all the same (unspecified) common cause events experienced by all the plants in the data base.
  - The analyzed system has the same, yet unspecified, success criteria as those assumed by the analyst who classified the data in Reference 3-4.
  - The Table 3-7 values of the beta factor include both failures to start on demand and failure to run for all components except breakers and valves. Hence, they represent an average of these modes weighted by their relative frequency of occurrence.
- The beta-factor estimates have been developed from systems of different sizes. Their application implicitly assumes that the system being analyzed has an "average" number of components.
- The values do not account for underreporting of independent events. The beta factors are therefore additionally conservative.

Included in this table is a generic beta factor for a "generic component." This factor can be used with components not listed in the table but identified by the analyst as being in a common cause group. It

Table 3-7

## EVENT CLASSIFICATION AND ANALYSIS SUMMARY

Component	Reactor Years	Number of Events Classified <sup>a</sup>	Event Distribution <sup>b</sup>				Generic Beta Factor
			Independent	Dependent	Generic Common Cause Events		
					Potential	Actual	
Reactor Trip Breakers	563	72	56	16	3	8	.19
Diesel Generators	394	674	639	35	9	13	.05
Motor-Operated Valves	394	947	842	105	17	25	.08
Safety/Relief Valves							
PWR	318	54	30	24	0	0	.07
BWR	245	172	136	36	7	7	.22
Check Valves	654	254	242	12	3	5	.06
Pumps							
Safety Injection	394	112	77	35	2	6	.17
RHR	394	117	67	50	2	3	.11
Containment Spray	394	48	32	16	1	1	.05
Auxiliary Feedwater	394	255	194	61	2	3	.03
Service Water	394	203	159	44	2	2	.03
Chillers	654	33	27	6	2	2	.11
Fans	654	59	49	10	2	3	.13
All	-	3,000	2,550	450	52	78	.10 <sup>c</sup>

<sup>a</sup>Events classified include those having one or more actual or potential component failures or functionally unavailable states.

<sup>b</sup>Independent events are those in category LS (linear, single unit); dependent events are those in the following categories: LM (linear, multiple unit), BSR (branched, single unit, root-caused), and BSC (branched, single unit, component-caused); generic common cause events are a subset of event category BSR that meets screening criteria to be modeled in a systems analysis as a common cause event. Actual common cause events have at least two actual component states.

<sup>c</sup>Average of all component beta factors.

should be used for screening purposes only. It is the responsibility of the analyst to defend any conclusions derived from generic beta factors in light of the above severe limitations. The authors generally discourage this approach and would prefer that each analyst perform his own evaluation of the data to base each analysis on.

### 3.4 STAGE 4: SYSTEM QUANTIFICATION AND INTERPRETATION OF RESULTS

The final stage of the analysis involves quantification of the system unavailability, performing uncertainty sensitivity analyses, interpretation of the results, and documentation. The objectives of this stage are achieved through the steps described in the following.

#### 3.4.1 Step 4.1 - Quantification

In this step, the parameter estimates obtained in Step 3.4 are used along with the algebraic (probability) equations developed in Step 3.2 to quantify the system unavailability. This quantification is performed for each of the sets of system boundary conditions. Both point estimates and complete uncertainty distributions may be computed. Reference 3-3 discusses a number of computer programs that can be used for this purpose. The specific program used for quantification depends on the form of the algebraic equations developed and the specific logic models employed. Many programs, such as GO, SETS, and the WAM series (Reference 3-10), can be used to reduce the Boolean logic, to develop the algebraic equations, then to quantify these resulting expressions by using parameter estimates supplied by the user from data. Each such computer program has its own advantages and disadvantages.

As was mentioned in Step 3.4, the most appropriate point estimate of the parameters for point calculation is the mean value of their uncertainty distribution.

#### 3.4.2 Step 4.2 - Results Evaluation and Sensitivity Analysis

The final step of system analysis prior to documentation is the interpretation of the results of the quantification results. In addition to the overall top event frequency and its uncertainty estimate, the results also should summarize the relative contributions of independent hardware failures, failures involving tests or maintenance, and common cause failures. Such results should be presented for each separate set of system boundary conditions (i.e., states of support systems) evaluated. Although the system analysis alone can be useful in identifying what limits the system failure frequency and hence point the way to improvements, the reader is again cautioned. For effective risk management, recommendations for improvements must be based on an overall plant perspective. Suggested improvements to individual systems, which at the system level may appear very effective, may instead have only a very small impact on plant risk.

As was discussed in Steps 3.3 and 3.4, there is considerable uncertainty in the estimation of common cause failure probabilities. Although an uncertainty analysis can express the significance of this in an integral sense, it is also useful to see how significant such uncertainties can be

by using sensitivity analyses to illustrate the direct relationship between the input values for the common cause basic events and the overall system results.

Another factor to be considered in the process of evaluation of the results is an assessment of the possibilities and impact of the recovery from failures. This subject, in relation to the analysis of common cause failures, is briefly addressed in Appendix G.

### 3.4.3 Step 4.3 - Reporting

The final step is the reporting and documentation of the analysis. Although all assumptions should be documented, the most crucial are those concerning the analysis, classification, and reinterpretation of the data for plant-specific conditions because it is this area of the analysis that is the source of greatest uncertainty. The impact vectors serve to document the assumptions made, but need to be supplemented by comments explaining on what basis the assumptions are made; for instance, why the particular mechanism for linking failures was felt to be well defended against. The importance of this cannot be overstated because it is a key to understanding the occurrence of and potential for defenses against common cause failures at the plant.

## 3.5 APPLICATION OF THE PROCEDURAL FRAMEWORK: A SIMPLIFIED EXAMPLE

The preceding four subsections of this section have described in detail the steps involved in each of the four stages of the procedural framework. The purpose of this section is to provide a summary of the procedure by using a simple tutorial example. The intent is to illustrate in a simple way, without providing any detailed evaluation, the main features and products of the different stages of the analysis. These examples are for the analysis of the unavailability of specific systems, an auxiliary feedwater system, and station batteries. Since this guide is applicable to common cause analysis at the accident sequence, as well as system unavailability level, the example chosen here is the analysis of a simple event tree and shows more explicitly than do the examples of Section 4 the application of quantitative screening. The example event tree has two branch points and two accident sequences of interest. Although the solution was solved using the event tree linking method, the intention is not to endorse any particular method for the treatment of support system dependencies (in this case, AC power). The same logical cutsets would arise using a support state methodology.

### 3.5.1 Stage 1: System Logic Model Development

A simplified diagram of the plant and its systems is given in Figure 3-5. There are two safety systems; the emergency cooling system that is designed to prevent core melt in the case of loss of normal cooling, and a containment cooling system, which can mitigate radioactivity release. The example should not be interpreted as a complete or accurate model of any particular plant; the sole intent is to

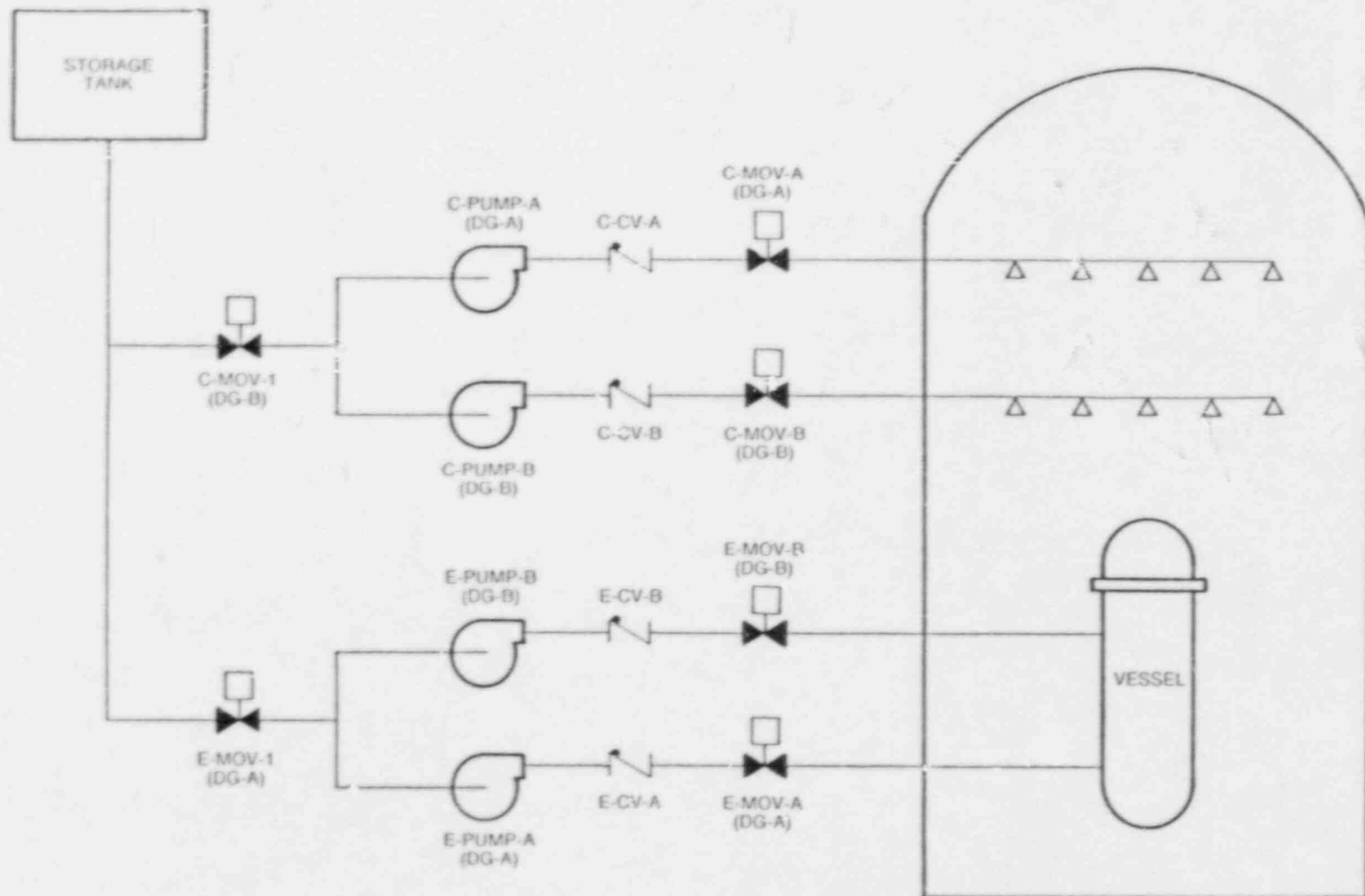


Figure 3-5. Simplified Emergency Cooling and Containment Cooling Systems

provide a model for which cutsets can be simply evaluated and that can therefore be used to demonstrate the procedure for inclusion of common cause failures.

The system dependencies modeled explicitly are the common supply tank and the dependency on diesel generators.

The problem to be solved is the estimation of the frequencies of accident sequences IEC and IEC in the event tree of Figure 3-6, with an initiating event of loss of offsite power. The logical solution was obtained by constructing fault trees for the ECS and CCS systems, explicitly including the dependency of each component on diesel generators and combining the appropriate fault trees (or complements) to get the accident sequence cutsets. The parametric values for the basic events are given in Table 3-8. The cutsets for the two sequences are given in Tables 3-9 and 3-10. The cutset frequencies are included for comparison. The cutsets give the complete logical description of the combinations of failures that can lead to the sequences, but because the frequencies in Tables 3-9 and 3-10 are evaluated on the basis of the assumption that the failures are independent, they are underestimated, as will be seen later. This has completed Steps 1.1 through 1.3 of the procedure.

### 3.5.2 Stage 2: Identification of Common Cause Component Groups

It is assumed that, on the basis of a qualitative screening following Step 2.1 of the procedural framework, the following common cause component groups have been identified for consideration:

(DGA, DGB), (E-PUMP-A, E-PUMP-B)  
(C-PUMP-A, C-PUMP-B), (C-MOV-A, C-MOV-B),  
(E-MOV-A, E-MOV-B)

As described in Section 3.2.1, the qualitative screening consists of a search for the common attributes of components and mechanisms of failure that can lead to a potential for common cause failure.

The next step is to perform a quantitative screening (Step 2.2). The mechanics of this step use a simplified version of the common cause modeling described and performed in Step 3 and illustrate the iterative nature of application of the procedure. In fact, since the common cause groups involve only two components, the beta-factor model will be used both in the screening and in the detailed analysis (Stages 2 and 3). In accordance with Step 3.1, the following common cause basic events are defined: DG-CCF, E-PUMP-CCF, E-MOV-CCF, C-PUMP-CCF, C-MOV-CCF.

They are included in the logic model by substitution of fault trees, similarly to those in Figure 3-7, into the original system fault trees. The screening analysis was carried out by using a beta factor of .1 to estimate all CCF contributions. The results of this analysis are shown in Tables 3-11 and 3-12.

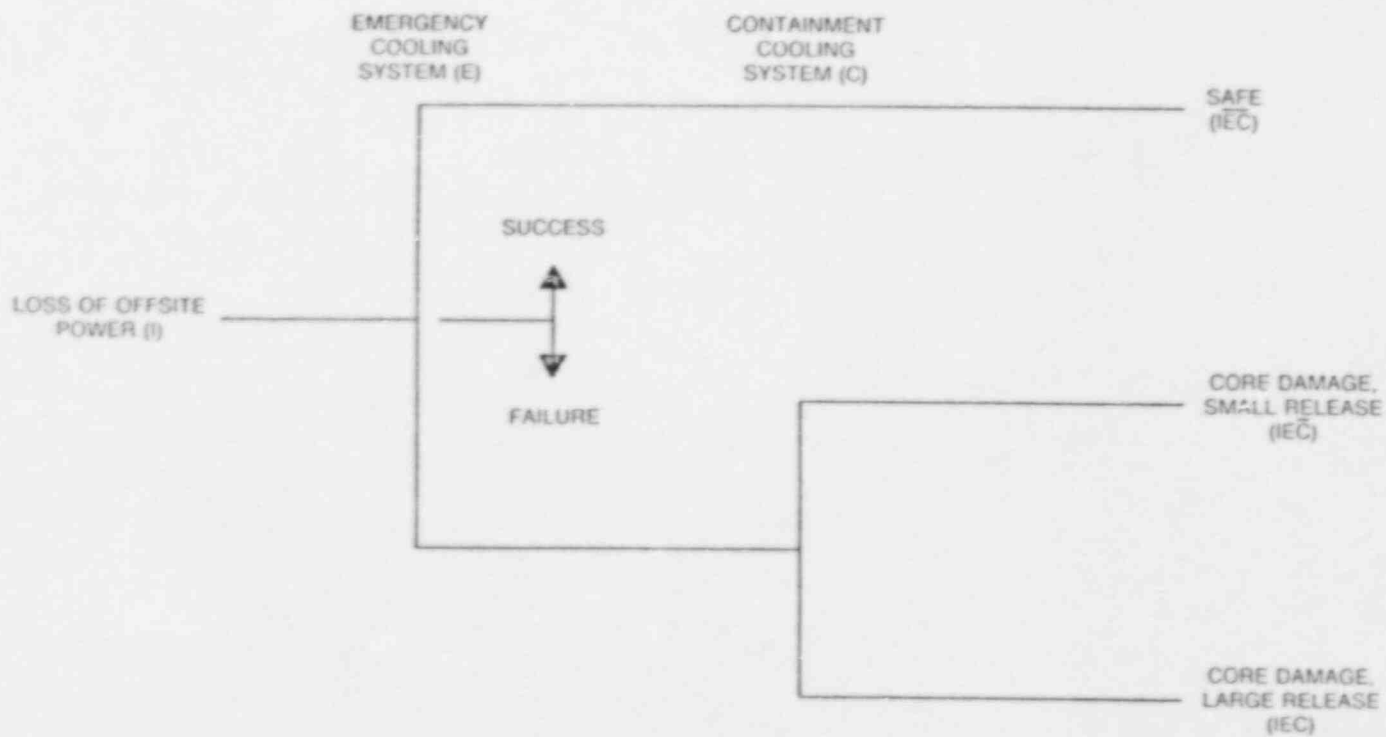


Figure 3-6. The Event Tree for the Sample Problem



Table 3-8

## BASIC EVENTS PROBABILITIES

Primary Name	Probability
C-CV-A	1.0-4
C-CV-B	1.0-4
C-MOV-1	1.0-3
C-MOV-A	5.0-3
C-MOV-B	5.0-3
C-PUMP-A	3.0-3
C-PUMP-B	3.0-3
DG-A	2.0-2
DG-B	2.0-2
TANK	1.0-7
E-CV-A	1.0-4
E-CV-B	1.0-4
C-MOV-1	1.0-3
E-MOV-A	5.0-3
E-MOV-B	5.0-3
E-PUMP-A	3.0-3
E-PUMP-B	3.0-3
LOSP	2.2-2

NOTE: Exponential notation is indicated in abbreviated form; i.e., 1.0-4 =  $1.0 \times 10^{-4}$ .

Table 3-9

## CUTSETS FOR SEQUENCE IEC WITHOUT COMMON CAUSE

Number	Percent of Sequence Total	Frequency	Event Names	
1	94.94	4.4-4	DG-A	LOSP
2	4.75	2.2-5	E-MOV-1	LOSP
3	0.12	5.5-7	E-MOV-A	E-MOV-B LOSP
4	0.07	3.3-7	E-PUMP-A	E-MOV-B LOSP
5	0.07	3.3-7	E-MOV-A	E-PUMP-B LOSP
6	0.07	1.9-7	E-PUMP-A	E-PUMP-B LOSP
7	0.00	1.10-8	E-CV-A	E-MOV-B LOSP
8	0.00	1.10-8	E-MOV-A	E-CV-B LOSP
9	0.00	6.60-9	E-CV-A	E-PUMP-B LOSP
10	0.00	6.60-9	E-PUMP-A	E-CV-B LOSP
11	0.00	2.20-10	E-CV-A	E-CV-B LOSP
Total		4.63-4		

NOTE: Exponential notation is indicated in abbreviated form;  
 i.e., 4.4-4 =  $4.4 \times 10^{-4}$ .

Table 3-10

## CUTSETS FOR SEQUENCE IEC WITHOUT COMMON CAUSE

Number	Percent of Sequence Total	Frequency	Event Names			
1	52.27	8.80-6	DG-B	DG-A	LOSP	
2	13.07	2.20-6	DG-A	C-MOV-B	LOSP	
3	13.07	2.20-6	DG-B	E-MOV-A	LOSP	
4	7.84	1.32-6	DG-A	C-PUMP-B	LOSP	
5	7.84	1.32-6	DG-B	C-PUMP-A	LOSP	
6	2.61	4.40-7	C-MOV-1	DG-A	LOSP	
7	2.61	4.40-7	DG-B	E-MOV-1	LOSP	
8	0.26	4.40-8	DG-B	E-CV-A	LOSP	
9	0.26	4.40-8	DG-A	E-CV-B	LOSP	
10	0.13	2.20-8	C-MOV-1	E-MOV-1	LOSP	
11	0.01	2.20-9	TANK	LOSP		
12	0.00	5.50-10	CCS-MOV-A	C-MOV-B	E-MOV-1	LOSP
Total		1.68-5				

NOTE: Exponential notation is indicated in abbreviated form;  
i.e., 8.80-6 =  $8.80 \times 10^{-6}$ .

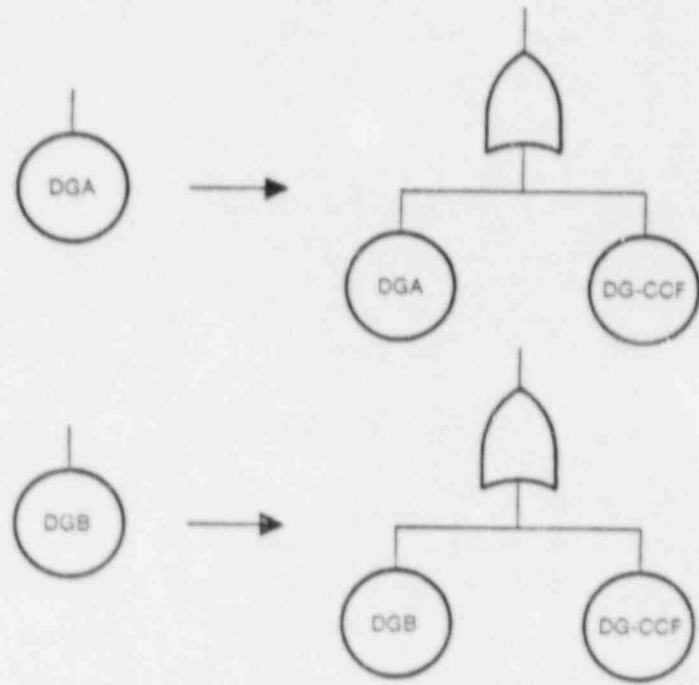


Figure 3-7. Inclusion of Common Cause Basic Events

Table 3-11

## CUTSETS FOR SEQUENCE IEC WITH COMMON CAUSE ADDED

Number	Percent	Frequency	Event Names		
1	91.47	4.40-4	DG-A	LOSP	
2	4.57	2.20-5	E-MOV-1	LOSP	
3	2.29	1.10-5	E-MOV-CCF	LOSP	
4	1.37	6.60-6	E-PUMP-CCF	LOSP	
5	0.11	5.50-7	E-MOV-A	E-MOV-B	LOSP
6	0.07	3.30-7	E-MOV-A	E-PUMP-B	LOSP
7	0.07	3.30-7	E-PUMP-A	E-MOV-B	LOSP
8	0.04	1.98-7	E-PUMP-A	E-PUMP-B	LOSP
9	0.03	1.10-8	E-MOV-A	E-CV-B	LOSP
10	0.00	1.10-8	E-CV-A	E-MOV-B	LOSP
11	0.00	6.60-9	E-PUMP-A	E-CV-B	LOSP
12	0.00	6.60-9	E-CV-A	E-PUMP-B	LOSP
Total		4.81-4			

NOTE: Exponential notation is indicated in abbreviated form;  
i.e., 4.40-4 =  $4.40 \times 10^{-4}$ .

Table 3-12

## CUTSETS FOR SEQUENCE IEC WITH COMMON CAUSE ADDED

Number	Percent	Frequency	Event Names		
1	71.44	4.40-5	DG-CCF	LOSP	
2	14.29	8.80-6	DG-B	DG-A	LOSP
3	3.57	2.20-6	DG-A	C-MOV-B	LOSP
4	3.57	2.20-6	DG-B	E-MOV-A	LOSP
5	2.14	1.32-6	DG-B	E-PUMP-A	LOSP
6	2.14	1.32-6	DG-A	C-PUMP-B	LOSP
7	0.71	4.40-7	DG-B	E-MOV-1	LOSP
8	0.71	4.40-7	C-MOV-1	DG-A	LOSP
9	0.36	2.20-7	C-MOV-CCF	DG-A	LOSP
10	0.36	2.20-7	DG-B	E-MOV-CCF	LOSP
11	0.21	1.32-7	DG-B	E-PUMP-CCF	LOSP
12	0.21	1.32-7	C-PUMP-CCF	DG-A	LOSP
13	0.07	4.40-8	DG-B	E-CV-A	LOSP
14	0.07	4.40-8	DG-A	C-CV-B	LOSP
15	0.04	2.20-8	C-MOV-1	E-MOV-1	LOSP
16	0.02	1.10-8	C-MOV-CCF	E-MOV-1	LOSP
17	0.02	1.10-8	C-MOV-1	E-MOV-CCF	LOSP
18	0.01	6.60-9	C-MOV-1	E-PUMP-CCF	LOSP
19	0.01	6.60-9	C-PUMP-CCF	E-MOV-1	LOSP
20	0.01	5.50-9	C-MOV-CCF	E-MOV-CCF	LOSP
21	0.01	3.30-9	C-MOV-CCF	E-PUMP-CCF	LOSP
22	0.01	3.30-9	C-PUMP-CCF	E-MOV-CCF	LOSP
23	0.00	2.20-9	TANK	LOSP	
24	0.00	1.98-9	C-PUMP-CCF	E-PUMP-CCF	LOSP

NOTE: Exponential notation is indicated in abbreviated form;  
i.e., 4.40-5 =  $4.40 \times 10^{-5}$ .

A screening criterion of 1% of the severe core damage frequency was adopted; i.e., if a CCF event existed in a cutset contributing to more than 1% of the sequence frequency, it was retained for further analysis.

For sequence  $IE\bar{C}$ , two events remain after this screening: E-MOV-CCF and E-PUMP-CCF (see Table 3-11) and, for sequence  $IE\bar{C}$ , only one remains - DG-CCF (see Table 3-12).

This simple example illustrates the important fact that, depending on the result of interest, the requirements for detailed evaluation do vary.

### 3.5.3 Stage 3: Common Cause Modeling and Data Analysis

As remarked previously, the definition and modeling of basic events (Steps 3.1 and 3.2) are the same as those performed for the screening analysis. (An example in Section 4 illustrates the use of higher order models.) Pursuing Step 3.3 will result in a set of pseudo-data for use in estimating the beta factor. As discussed in Section 3.3, there are several sources of uncertainty in analyzing and interpreting this data. It is assumed therefore that the data analysis resulted in two sets of pseudo-data, one corresponding to an optimistic, the other to a pessimistic, view of the data. An optimistic interpretation can be obtained by screening out any event for which there is an element of doubt of its applicability, while a pessimistic interpretation should include any event about which there was a doubt. Using these sets of pseudo-data, the following estimates for the beta factors are obtained.

Component	Beta Factor	
	Low Value	High Value
Diesel Generators	.03	.12
ECS MOVs	.06	.11
ECS Pumps	.04	.17

The two values are used to define a range of values, this being the simplest representation of uncertainty. An alternative would have been to also provide a best estimate interpretation of the data.

### 3.5.4 Stage 4: System Quantification and Interpretation of Results

The results of the quantification of sequence frequencies using the beta factors obtained in Stage 3 are:

Sequence	Zero Value	Low Value	High Value
$IE\bar{C}$	$4.63 \times 10^{-4}$	$4.726 \times 10^{-4}$	$4.357 \times 10^{-4}$
$IE\bar{C}$	$1.68 \times 10^{-5}$	$3.08 \times 10^{-5}$	$7.04 \times 10^{-5}$

Comparing the results of the evaluation with the results that were obtained without common cause failures, it can be seen that the inclusion of common cause failures, makes little difference to the frequency of sequence IEC but is significant for sequence IEC. The reason is easy to understand; in sequence IEC, there is a single-component failure cutset that is dominant, whereas, in sequence IEC, the dominant cutsets are of the order 2 before inclusion of common cause failure. Also, the dominant common cause failure contribution is excluded from sequence IEC because of the success in C, the containment cooling system.

An important fact to check is if the more detailed common cause failure analysis results in a significant reduction in leading contributions so that, with the new values, other common cause failure contributions become significant. This is not the case in this example.

Except for the crude representation of uncertainty given by the range of values, no detailed uncertainty analysis has been performed in this example. Neither has an importance or sensitivity analysis been performed. It is clear, however, that had the common cause groups been identified differently [for example, if (C-MOV-1, E-MOV-1) or (C-MOV-A, C-MOV-B, E-MOV-A, E-MOV-B) had been identified as common cause groups] the results of the analysis would have been very different. Inclusion of such groups is a candidate for a sensitivity study. In this example, no best estimate of the beta factors was provided. Such an estimate could be obtained using a best estimate interpretation of data, or might arise naturally out of a full-blown uncertainty analysis as the mean values of the probability distributions on the beta factor values.

### 3.5.5 Conclusions

The tutorial example presented here has illustrated, in a simple way uncluttered by calculational details, the application of the procedural framework. The next chapter provides a more detailed guide for using the procedure and in particular addresses one of the most time-consuming aspects, the collection and evaluation of event data.

## 3.6 APPLICATION OF THE PROCEDURAL FRAMEWORK TO FUTURE PLANTS

The framework in this section has been presented in the context of plants that have been built and/or operating. From the previous discussion, it can be seen that the complete framework provides a detailed mechanism for assessing the impact of common cause failures on a system or plant. When a plant or system is in the design stage, common cause failure considerations are harder to evaluate, especially from a quantitative perspective. The data evaluation and screening cannot be performed as effectively in the design stage. Therefore, the qualitative analysis has a more important role and can assist in the design process to identify potential defenses against common cause failures.

For example, location of equipment can be checked for common cause failure from harsh environments. The impact of procedures can also be assessed. As the system design progresses, the impacts can be further refined and finally quantified.



### 3.7 REFERENCES

- 3-1. U.S. Nuclear Regulatory Commission, "Fault Tree Handbook," NUREG-0497, January 1981.
- 3-2. Rees D., and S. Lainoff, "GO Methodology - Modeling Manual," NP3123, Vol. 3, June 1985.
- 3-3. Poucet, A., A. Amendola, P. C. Cacciabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Centre Report, PER 1133/86, Ispra, Italy, April 1986.
- 3-4. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," Electric Power Research Institute, EPRI NP-3967, February 1985.
- 3-5. Paula, H. M., and D. J. Campbell, "Analysis of Dependent Failure Events and Failure Events Caused by Harsh Environmental Conditions," JBFA-LR-111-85, JBF Associates, Inc., Knoxville, Tennessee, August 1985.
- 3-6. Edwards, G. T., and I. A. Watson, "A Study of Common Mode Failures," SRD-R-146, United Kingdom Atomic Energy Authority, Safety and Reliability Directorate, July 1979.
- 3-7. Rasmuson, D. M., et al., "Use of COMCAN III in System Design and Reliability Analysis," EGG-2187, EG&G Idaho, Inc., Idaho Falls, Idaho, October 1982.
- 3-8. Worrell, R. P., SETS Reference Manual, NUREG/CR-4213, SAND83-2675, Sandia National Laboratories, Albuquerque, New Mexico, 1985.
- 3-9. Putney, B., "WAMCOM, Common-Cause Methodologies Using Large Fault Trees," EPRI NP-1851, Electric Power Research Institute, Palo Alto, California, May 1981.
- 3-10. Fleming, K. N., "A Reliability Model for Common Mode Failure in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A13234, April 23-25, 1975.
- 3-11. Evans, M., G. Parry, and J. Wreathall, "On the Treatment of Common Cause Failures of System Analysis," Reliability Engineering, Vol. 9, pp. 107-115, 1984
- 3-12. Parry, G. W., "Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty," SRA 1984 Annual Meeting, 1984.
- 3-13. Parry, G. W., "Technical Note: Modeling Uncertainty in Parameter Estimation," Nuclear Safety, Vol. 27, p. 212, 1986.

- 3-14. Fleming, K. N., and A. M. Kalinowski, "An Extension of the Beta Factor Method to Systems with High Levels of Redundancy," Pickard, Lowe and Garrick, Inc., PLG-0289, June 1983.
- 3-15. Mosleh, A., and N. O. Siu, "A Multi-Parameter, Event-Based Common-Cause Failure Model," Paper M7/3, Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 1987.
- 3-16. Vesely, W. E., "Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin Specialization," IL-0454, 1977.
- 3-17. Atwood, C. L., "Common Cause Fault Rates for Pumps," NUREG/CR-2098, prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.
- 3-18. Apostolakis, G., and P. Moieni, "On the Correlation of Failure Rates," Reliability Data Collection and Use in Risk and Availability Assessment, proceedings of the Fifth EUREDATA Conference, Heidelberg, Germany, April 9-11, 1986, published by Springer-Verlag Berlin, Heidelberg, Germany, 1986.
- 3-19. Paula, H. M., "Comments on 'On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation'," Nuclear Safety, Vol. 27, No. 2, April-June 1986.
- 3-20. Apostolakis, G., and P. Moieni, "The Foundations of Models of Dependence in Probabilistic Safety Assessment," Reliability Engineering, Vol. 18, pp. 177-195, 1987.
- 3-21. Mosleh, A., "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data," Nuclear Engineering and Design, Vol. 93, 1986.
- 3-22. EG&G Idaho, Inc., "Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants, January 1, 1976 to December 31, 1978," prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-1362, EGG-EA-5092, March 1980.
- 3-23. EG&G Idaho, Inc., "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978," prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-1205, EGG-EA-5044, January 1982.
- 3-24. EG&G Idaho, Inc., "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants, Main Report, January 1, 1976 to December 31, 1978," prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-1363, EGG-EA-5125, October 1982.
- 3-25. Miller, J. L., W. H. Hubble, M. Trojovsky, and S. R. Brown, "Data Summary of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants,"

prepared for the U.S. Nuclear Regulatory Commission, EG&G Idaho, Inc., NUREG/CR-1363, EGG-EA-5816, Rev. 1, October 1982.

- 3-26. Sams, D. W., and M. Trojosky, "Data Summaries of Licensee Event Reports of Primary Containment Penetrations at U.S. Commercial Nuclear Power Plants, January 1, 1972 to December 31, 1978, prepared for the U.S. Nuclear Regulatory Commission, EG&G Idaho, Inc., NUREG/CR-1730, EGG-EA-5/88.
- 3-27. Hubble, W. H., and C. F. Miller, "Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978, prepared for the U.S. Nuclear Regulatory Commission, EG&G Idaho, Inc., NUREG/CR-1331, EGG-EA-5079.
- 3-28. Smith, M., et al., "Data Based Defensive Strategies for Reducing Susceptibility to Common Cause Failures," draft report, prepared for Electric Power Research Institute, Saratoga Engineering Consultants, 1987.
- 3-29. S. M. Stoller, Nuclear Power Experience, updated monthly.
- 3-30. Atwood, C. L., "Common Cause Fault Rates for Pumps," prepared for the U.S. Nuclear Regulatory Commission, EG&G Idaho, Inc., NUREG/CR-2098, EPRI-685-DOC-01, EGG-EA-5289.
- 3-31. Atwood, C. L., and J. A. Stevenson, "Common Cause Fault Rates for Valves: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants," prepared for the U.S. Nuclear Regulatory Commission, EG&G Idaho, Inc., NUREG/CR-2770, EGG-EA-5485, February 1983.
- 3-32. Meachum, T. R., and C. L. Atwood, "Common Cause Fault Rates for Instrumentation and Control Assemblies," prepared for U.S. Nuclear Energy Commission under Department of Energy Contract No. DE-AC07-761D01570, Idaho National Engineering Laboratory, EG&G, Idaho, Inc., NUREG/CR3289, EPRI-685-DOC-06, EGG-2258, May 1973.
- 3-33. Los Alamos Technical Associates, Inc., "A Study of Common Cause Failures--Phase II: A Comprehensive Classification System for Component Fault Analysis," EPRI NP-3337, May 1985.
- 3-34. Fleming, K. N., A. Mosleh, and R. K. Deremer, "A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models," Nuclear Engineering and Design, Vol. 93, pp. 245-273, 1986.
- 3-35. Doerre, P., "Possible Pitfalls in the Process of CCF Event Data Evaluation," Kraftwerk Union AG, Proceedings, PSA '87-- International Topical Conference on Probabilistic Safety Assessment Risk Management, August 30-September 4, 1987.

- 3-36. Mosleh, A., and N. O. Siu, "On the Use of Uncertain Data in Common Cause Failure Analysis," Proceedings, PSA '87--International Topical Conference on Probabilistic Safety Assessment Risk Management, August 30-September 4, 1987.



## Section 4

### EXAMPLE APPLICATIONS OF COMMON CAUSE ANALYSIS PROCEDURES

The methods and systematic procedures described in Section 3 can be better understood by their application to two sample systems analyzed in this section.

The first example is a three-train AFWS at an existing U.S. nuclear power plant. This type of system may be the one that has been subjected to more reliability analyses than any other because of the requirements imposed by the NRC after the accident at Three Mile Island. The common cause analysis of this system is described in Section 4.1 in terms of the steps of the systems analysis framework described in Section 3. This example emphasizes the screening process, identifying common cause component groups, and integrating those groups into the logic model of the system. It also shows how the different parametric models may be used and their parameters estimated. The relative significance of various common cause basic events is also investigated.

The second example is an actual analysis (Reference 4-1) of a system that is different from the AFWS in size (number of components) and types of equipment. The system is the DC electric power system in a U.S. BWR. The analysis emphasizes the common cause contribution of a subset of station batteries required to prevent core damage in some specific scenarios. The analysis includes a detailed review of root causes and coupling mechanisms of equipment failures; describes the qualitative screening process; and provides a detailed discussion of event data, screening, impact vector assessment, and parameter estimation. This analysis is included here only as a demonstration of the procedural framework for common cause analysis. No representation is made that the analysis and the results are adequately plant specific to include all of the essential characteristics of the subject plant.

The system is analyzed for scenarios that are characterized by transients that lead to station blackout (loss of all AC power) or substantial degradation of the AC power system as a result of coincident failures in the 125/250V DC power system. Loss of the 125/250V DC power system causes loss of the EDGs, the HPCI system, the RCIC system, and the depressurization system. Loss of these systems causes a loss of all core and containment cooling and, without recovery, would lead to core damage. This damage scenario was identified as a dominant scenario in a recent PRA study (Reference 4-2) in which generic CCF frequencies were assigned to a variety of components in several systems. The accident sequences were then quantified and the dominant scenarios identified. Finally, the dominant scenarios were analyzed for recovery potential and, whenever appropriate, the scenario frequencies were reduced according to the recovery likelihood. Following the recovery analysis, the PRA

results indicated that 51% of the frequency of severe core damage accidents was due to the scenario considered in this section. The PRA study, however, recognized the limitations of using generic CCF data and strongly recommended a more detailed CCF analysis of this major contributor to the core damage frequency before any actions be taken based on the PRA results.

The analysis of this scenario, presented in Section 4.2, provides a plant-specific estimation of the occurrence frequency of the scenario that is conservatively estimated to be at least five times less than the frequency estimated using the generic data. In addition, the detailed qualitative analysis gives indications of how safety improvements associated with this scenario could be pursued if desired.

#### 4.1 AUXILIARY FEEDWATER SYSTEM EXAMPLE

##### 4.1.1 Stage 1: System Logic Development

4.1.1.1 Step 1.1 - System Familiarization. A simplified P&ID of the example auxiliary feedwater system is shown in Figure 4-1. The system is typical for PWRs in the U.S. and consists of three pump trains, which take suction from a common condensate storage tank and supply header and provide auxiliary feedwater flow to four steam generators. This system has two identical electric motor-driven pumps and a steam turbine-driven pump. There are four motor-operated valves at the pump discharge that are normally closed. Each motor-driven pump can supply flow through successful valve openings to two dedicated steam generators, and the steam turbine-driven pump can supply flow to up to four steam generators, depending on how many MOVs open. An important characteristic of this system is that, although diversity is employed in pump drives, all three mechanical pumps are otherwise identical.

Table 4-1 shows the maintenance, test, and emergency procedures applicable to this system. Each pump is tested quarterly (Procedure 1 in Table 4-1) by opening a miniflow valve (not shown in Figure 4-1) and pumping water back to the condensate storage tank in a recirculation loop (also not shown in Figure 4-1). If a system actuation signal is received during a pump test, the miniflow line should isolate automatically but need not be isolated to meet the system success criteria. Each isolation valve undergoes a monthly stroke test (Procedure 2 in Table 4-1) that consists of cycling the valve once from the control room and recording the time required for cycling. Each isolation valve also undergoes quarterly preventive maintenance (Procedure 3 in Table 4-1) that includes adjustment of torque and limit switch settings and lubrication. A stroke test is required immediately following maintenance. The pumps are located in a common location with no environmental barriers between the pumps. The pumps are maintained according to Procedure 4 in Table 4-1. Although pump maintenance is a complex activity, the technical specifications for the AFWs do not require a complete flow test (Procedure 1 in Table 4-1) to be performed immediately following maintenance. Finally, the AFW is fully automatic, and the operator must verify its proper operation following automatic initiation. If the AFW control system fails, the operator must manually control proper flow to the steam generator (Procedure 5 in Table 4-1).

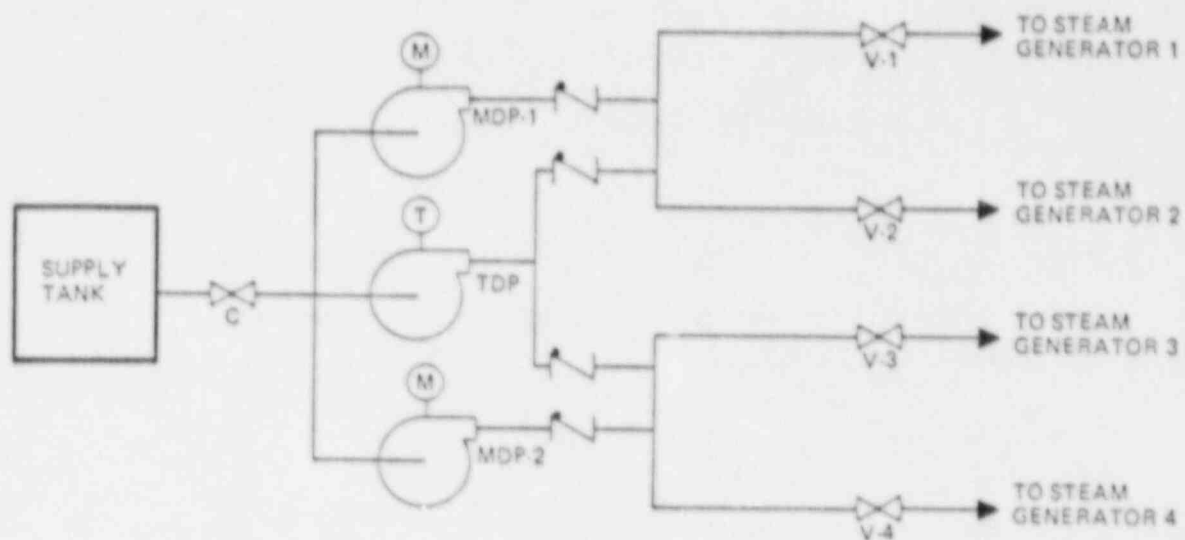


Figure 4-1. Simplified Schematic of Major Components in an Example Auxiliary Feedwater System



Table 4-1

MAINTENANCE AND TEST PROCEDURES APPLICABLE TO THE  
AUXILIARY FEEDWATER SYSTEM

Procedure Identification Number	Procedure Title
1	Auxiliary Feedwater Pump Quarterly Flow Test
2	Auxiliary Feedwater Isolation Valve Monthly Stroke Test
3	Auxiliary Feedwater Isolation Valve Quarterly Maintenance
4	Auxiliary Feedwater Pump Annual Maintenance
5	Station Emergency Operating Procedure

4.1.1.2 Step 1.2 - Problem Definition. As noted in Section 3, this step in the common cause analysis procedure involves the definition of analysis objectives, boundary conditions, mission time, system alignments, environmental hazards (including such external events as earthquakes), basic events (component breakdown-failure mode combination), potential operator actions, and any other assumptions or ground rules imposed on the analysis.

The objectives of this analysis are to determine the frequency of failure (i.e., failure frequency per demand) of the system and to determine the principal contributors to system failure. A probabilistic quantification of uncertainty is to be performed; hence, both point estimates and uncertainty distributions are to be provided.

For practical reasons, only major components of the system (i.e., the CST, pumps and drivers, actuation circuitry, and MOVs) are being considered. Component boundaries are defined as follows. The MOVs include:

- Motor/Operator (including limit switches and torque switches)
- Breaker
- Indication Circuit
- Control Circuit, Panel, and Switch
- Torque Limit Bypass Switch
- Valve Hardware (body, disc, stem, etc.)

Pumps include:

- Driver (motor and turbine)
- Breaker
- Control Circuit, Panel, and Switch
- Pump Hardware

Electric power supply is outside the scope of this analysis, and it is assumed to be available. Basic events are to be considered at the component level. Although of great importance, external events (e.g., seismic, fire, and flood) are also assumed to be outside the scope of this analysis. No operator intervention or recovery actions are to be considered except as noted in the qualitative analysis. It is assumed that the system must operate for 24 hours following its demand.

Various possible system alignments are normally considered in typical PRA system analysis. However, to simplify the presentation, the system is only analyzed for the normal alignment in which no test or maintenance is performed.

4.1.1.3 Step 1.3 - Logic Model Development. The reliability block diagram and component-level fault tree for the system are presented in Figures 4-2 and 4-3, respectively.

4.1.2 Stage 2: Identification of Common Cause Component Groups

4.1.2.1 Step 2.1 - Qualitative Analysis. The purpose of this step is to determine which common cause events are important for the system and

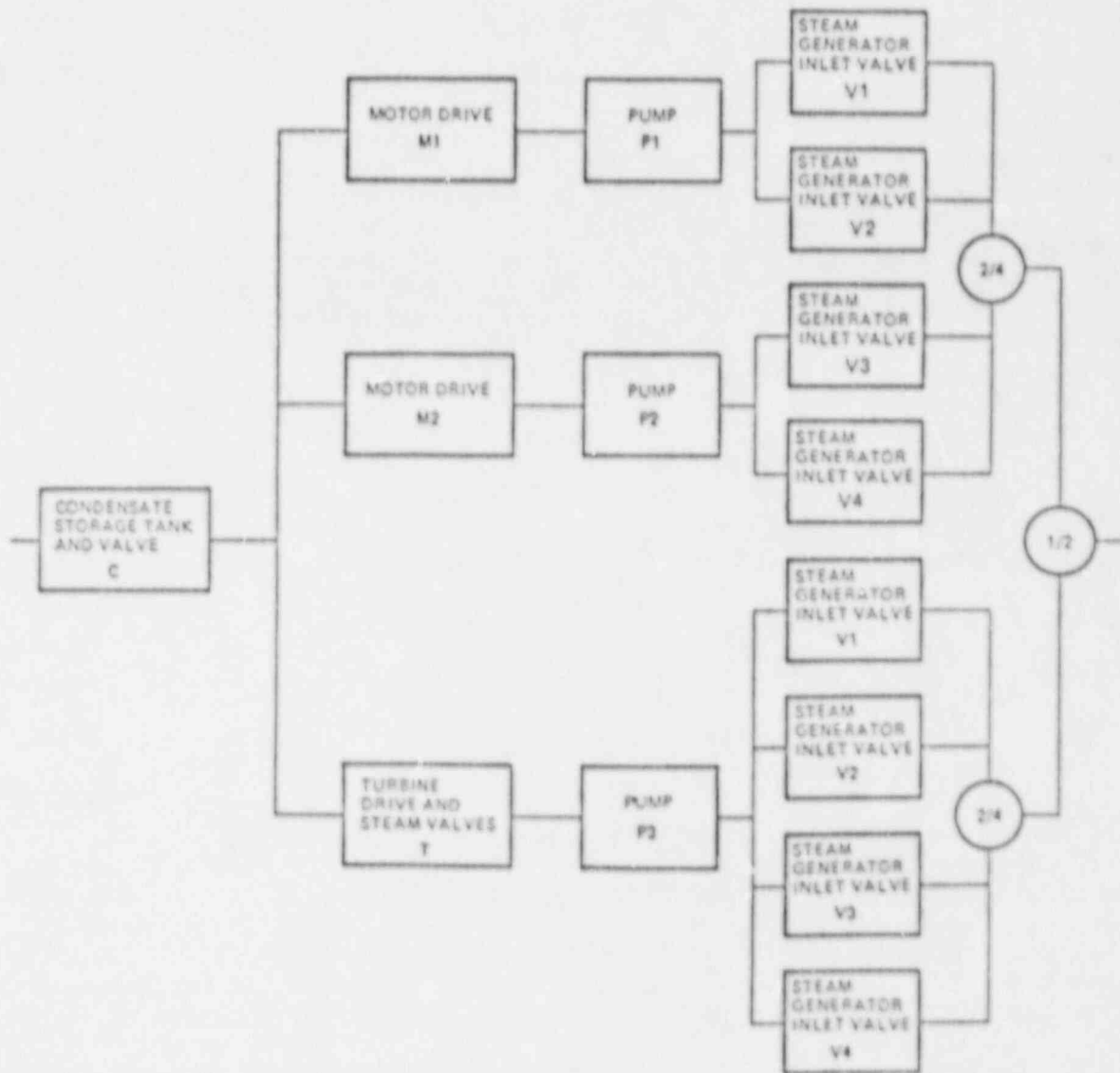


Figure 4-2. Reliability Block Diagram of Auxiliary Feedwater System - Normal Alignment

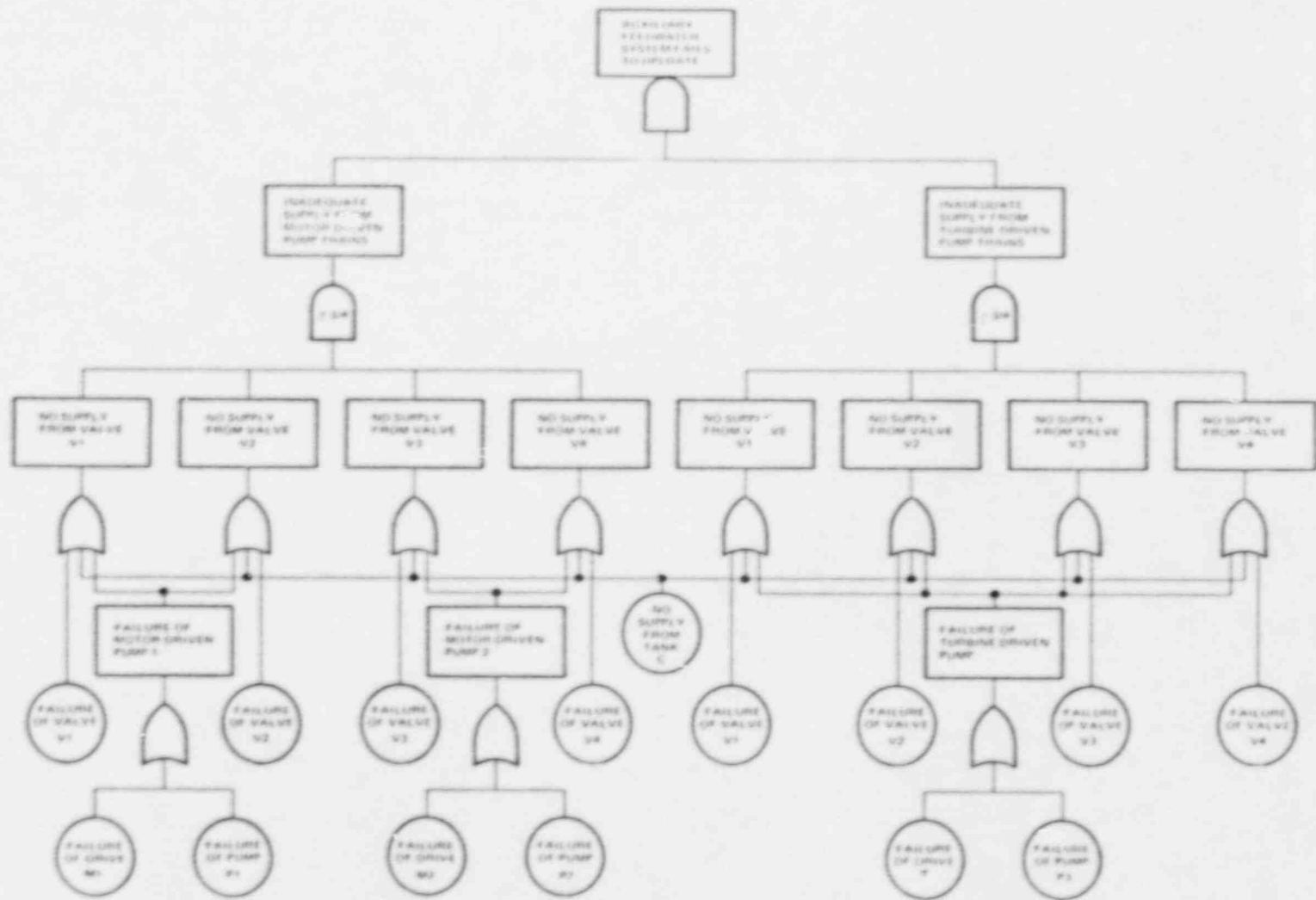


Figure 4-3. Component-Level Fault Tree of Example System

therefore should be included in the subsequent steps of the analysis. This objective is accomplished by first identifying an initial set of common cause events of interest. This identification relies on assumptions (based on judgment and feedback from operating experience) to keep the number of events of interest at a manageable level.

At this stage of the analysis, the analyst must decide which groups of components have a significant likelihood of experiencing a common cause event affecting two or more components within that group.

To incorporate common cause events into the systems analysis, it is necessary to understand the factors pointing to the independence, or lack thereof, among the components in the system. Such factors include whether groups of identical components are employed, the extent of diversity, if any, among components within a redundant group, the physical proximity or separation of the redundant components, and the capacities and susceptibilities of components to varied environmental stresses. An extremely important consideration is the potential for human errors in the design, manufacture, construction, plant management, and operation that could be shared by two or more components within a redundant group. All of these factors will be formally considered in the root cause analysis.

For our example system, there are three natural groups of components: the four identical motor-operated valves, the three identical pumps, and the two identical motor drives. Check valves are excluded to simplify the presentation of the example. However, in a more complete analysis, they should be included as a group. Combinations of components not within the selected groups are assumed to be independent. References 4-3 through 4-5 include hundreds of common cause events that affected sets of identical active components but very few, if any, that affected diverse components. Keeping the number of possibilities allowed for in the models at a manageable level will continue to require qualitative and quantitative judgment guided by feedback from operating experience. Such judgments, however, are not unlike the numerous judgments that need to be made by a systems analyst to account for independent events.

The three candidate common cause component groups of this example problem are:

<u>Pump Group</u>	<u>Motor Group</u>	<u>Valve Group</u>
P1	M1	V1
P2	M2	V2
P3		V3
		V4

The remainder of this section presents an analysis of the root causes and coupling mechanisms of failures for the equipment of interest in the system, with emphasis on the CCF potential associated with each root cause of failure. The main objective is to identify which one of the above candidate common cause component groups should be retained for analysis in the subsequent steps. This qualitative step also helps achieve the following two objectives: (1) to provide engineering

arguments that will aid in assessing the impact vectors in the data classification and screening step (Step 3.3) and (2) to provide engineering arguments to formulate defense alternatives and stipulate recommendations in the interpretation of results step (Stage 4).

The root cause and coupling mechanism analysis (referred to as root cause analysis in the rest of the discussion) is performed by first identifying an initial set of root causes of interest for the equipment in the AFWS and by also identifying the group of components affected by each root cause. Then, each root cause and component group combination is analyzed, based mostly on engineering arguments to assess how they could impact the AFWS. Some combinations may be "not applicable" to the AFWS. Other combinations may be easily detectable and easily repairable. In both of these cases, the combinations are labeled "unimportant," and this conclusion allows screening of related failure events in Step 3.3. Other combinations may be judged applicable to the AFWS. This conclusion supports assigning nontrivial impact vectors to related failure events in Step 3.3.

Three types of root cause and component group combinations must be addressed: type 1 consists of root causes that primarily affect similar equipment, type 2 consists of root causes that affect equipment operated according to the same procedures (with emphasis on misalignment errors), and type 3 consists of root causes that affect equipment in the same location.

The initial analysis of root causes of failure for the equipment of interest consists of a detailed review of (1) failure reports (e.g., LERs, NPE, plant logs, and so on), (2) other system reliability analyses (e.g., the FMEA), and (3) previous studies on similar systems. This initial effort indicates the fault categories that must be addressed in the analysis (e.g., valve internal failures, valve operator failures, loss of valve control signal, loss of valve power supply, and so on) and provides the basis for the root cause analysis. This review must be exhaustive to ensure that all the fault categories are adequately considered. The material that follows, however, was developed for illustrative purposes and is based on a limited data review. In an actual application, a more exhaustive data review would reveal additional root causes of failure to be considered. Nevertheless, the following discussion does cover the most commonly observed root causes of failure for the equipment of interest.

Table 4-2 summarizes the root cause and component group combinations defined for the auxiliary feedwater system. There are five type 1 combinations (the first three and the sixth and seventh root cause and component group combinations in Table 4-2). Most causes of AFW pump (excluding driver) failure are potential CCFs of interest because of the similarity of the three pumps (combination 1 in Table 4-2). Similarly, most causes of pump drive motor and AFW isolation valve faults will also be considered a type 1 combination (combinations 2, 3, 6, and 7 in Table 4-2).

There are five type 2 combinations (combinations 4, 5, and 8 in Table 4-2) because Procedures 1, 2, and 5 in Table 4-1 and the equipment

Table 4-2

CAUSE AND COMPONENT GROUP COMBINATIONS INITIALLY DEFINED  
FOR THE AUXILIARY FEEDWATER SYSTEM

Combination Identification Number	Cause of Interest	Affected Equipment	Type of Combination
1	All but procedure and environment-related causes.	AFW Pumps	1
2	All but procedure and environment-related causes.	Pump Drive Motors	1
3	All but procedure and environment-related causes.	AFW Isolation Valves	1
4	Errors committed during pump flow test.	Equipment Addressed in Procedure 1:* AFW Pumps	2
5	Errors committed during valve stroke test.	Equipment Addressed in Procedure 2:* AFW Isolation Valves	2
6	Errors committed during valve maintenance.	Equipment Addressed in Procedure 3:* AFW Isolation Valves	1
7	Misalignment errors committed during pump maintenance.	Equipment Addressed in Procedure 4:* AFW Pumps	1
8	Errors committed in operating the auxiliary feedwater system during a transient.	Equipment Addressed in Procedure 5:* All Pumps, Motor Drivers, and Isolation Valves	2
9	Energetic harsh environments in pump room.	All Equipment in Pump Room	3

\*Procedure titles are listed in Table 4-1.

addressed in these procedures will be considered a type 2 combination. This permits a closer scrutiny of the plant testing and operational activities.

Since all three pumps are located in the same room, energetic harsh environments (e.g., pipe ruptures, missiles, etc.) are potential causes of multiple failures within the AFWs. Therefore, energetic harsh environments and all the equipment in the pump room are also identified in Table 4-2 for additional analysis (combination 9).

Some nonenergetic harsh environments (e.g., moisture and contamination) are readily identified as possible causes of failures of some of the AFW equipment. However, since all pump equipment is environmentally qualified, failures due to these environments are more likely to occur as a result of improperly performed human-related activities; e.g., failure to properly seal the equipment following maintenance. These failures will be addressed for the applicable equipment when analyzing the type 1 combinations in Table 4-2. Thus, no additional type 3 combination has been identified for further analysis.

Each root cause and component group combination identified in the initial effort and summarized in Table 4-2 will now be analyzed, based mostly on engineering judgments.

#### 4.1.2.1.1 Root cause and component group combination 1: AFW pumps.

A review of operating experience reveals that multiple failures of auxiliary feedwater pumps are most often caused by (1) a partial or complete loss of flow from a common suction line, (2) maintenance errors that are systematically repeated for each pump, or (3) design deficiencies.

Loss of suction flow is most often caused by introducing air into the supply tank or suction line. Air can be introduced into the system during maintenance that requires disassembly of piping or other components or during transfer operations involving the supply tank. Although these activities take place infrequently, they do pose a threat to pump operability at this plant. Plugged strainers can also cause loss of suction to all three pumps, but this type of event is more readily recognizable (operational experience indicates that a reduced flow condition is often observed before sufficient plugging causes pump failure).

Maintenance is performed on the three auxiliary feedwater pumps once per year. All three pumps are serviced during the same shift by a single maintenance crew, so the potential for repeating an error (e.g., installing the seal packing too tightly) on all three pumps does exist. The faulted condition of the pumps would not be detected until a system demand occurred or until the next flow test of one of the pumps. Due to flexibility in the scheduling of maintenance at this plant, the faulted condition could exist for up to 1 month.

Design deficiencies are most often associated with control circuitry, but some events have been observed involving the fluid system. Some design deficiencies go undetected for several years, and system modifications often introduce additional design deficiencies into the



systems. Therefore, design deficiencies cannot be ruled out even for older plants. Diversity does provide defense against most of the observed design-related CCF events. Since the control systems for the two motor-driven pumps differ from the control system for the turbine-driven pump, dependencies due to control circuitry design deficiencies are judged to affect the motor-driven pumps only. However, dependencies due to pump (excluding driver) and fluid system design deficiencies are likely to affect all three trains.

Since a number of credible root causes that affect the three auxiliary feedwater pumps have been identified, root cause and component group combination 1 is judged credible at this plant.

4.1.2.1.2 Root cause and component group combination 2: pump drive motors. The review of operational experience revealed only a few events involving pump drive motors. This limited experience, however, indicates that the CCF potential exists and is most often associated with design deficiencies (e.g., undersized motor) or harsh environments, such as moisture and low temperature (another harsh environment, high temperature steam, will be analyzed later).

These harsh environments should not be a problem at this plant because the equipment in the AFWS is environmentally qualified, and the plant maintains an appropriate winter provisions program to ensure adequate room temperatures for all safety-related equipment. Obviously, failure to properly maintain equipment according to maintenance programs will result in failures. This root cause and component group combination is judged less likely than combinations 1 or 3 (discussed next), but it is still a credible root cause of CCFs.

4.1.2.1.3 Root cause and component group combination 3: AFW isolation valves. A large number of multiple failure events involving motor-operated valves have resulted from design deficiencies, manufacturing defects, and installation errors. Some of these faults and errors occur early in the life of a power plant, but others go undetected for several years. Also, system modifications and equipment replacement occur often in most systems, thus creating additional opportunities for introducing the fault events into the system. Therefore, these root causes of valve failures are of great CCF potential in this system.

Finally, several CCF events have resulted from such environmental causes as contamination and moisture. However, closer scrutiny reveals that these events are actually the result of design, manufacturing, and installation deficiencies and maintenance errors. For example, excessive grease may be introduced by the vendor (manufacturing deficiency) and moisture intrusion is usually associated with failure to properly seal equipment following maintenance (maintenance error) or failure to specify properly qualified equipment (design deficiency). Thus, these events represent a subset of the causes previously discussed.

Root cause and component group combination 3 is judged credible at this plant since several root causes with high CCF potential have been identified.

4.1.2.1.4 Root cause and component group combination 4: equipment addressed in Procedure 1. The AFW pump quarterly flow test consists of pumping water back to the condensate storage tank by opening a miniflow valve in a recirculation loop and starting the pump. Realignment errors following the test are unimportant because the miniflow lines need not be isolated to meet the system success criteria. Thus, root cause and component group combination 4 is discarded from further analysis.

4.1.2.1.5 Root cause and component group combination 5: equipment addressed in Procedure 2. The auxiliary feedwater isolation valve monthly stroke test involves cycling each valve once from the control room and recording the time required for cycling. The only potential error associated with this test is failure to return valves to their normal (closed) position. Since having these valves open would not prevent the system from functioning properly if demanded, this potential error is not of concern. Thus, root cause and component group combination 5 is discarded from further analysis.

4.1.2.1.6 Root cause and component group combination 6: equipment addressed in Procedure 3. Errors introduced when performing maintenance activities can result in CCF of the isolation valves.

Errors introduced during maintenance activities (mostly improper torque or limit switch settings, but also improper lubrication and improper seal packing) are also major contributors to valve CCF events. These faults are of particular concern at this plant for two reasons:

- Maintenance activities on all four valves are performed sequentially by the same crew. Thus, the potential for systematically repeated human errors is significant.
- Failures due to these root causes may not occur the first time the valve is cycled. Thus, the stroke test performed after maintenance may not detect the problem.

Some additional possibilities are examined now with emphasis on errors of alignment that may be committed when performing Procedure 3.

Procedure 3 addresses maintenance on the valve operator and the associated power and control equipment. (Maintenance requiring disassembly of the valve body is only allowed during shutdown because it involves isolating and draining the AFWS.) The following misalignment possibilities are considered:

1. Incorrect alignment of equipment resulting in valve unavailability(ies) during maintenance.
2. Incorrect alignment of equipment resulting in valve unavailability(ies) following maintenance.

3. Spurious operator actions resulting in valve unavailability(ies). This possibility is not directly associated with Procedure 3 but with erroneously misaligning equipment in the AFW when attempting to align equipment in other systems.

Procedure 3 requires that maintenance be performed on only one valve at a time. The valve must be locked open during maintenance, and both control signal and power supply must be removed before starting maintenance activities. Failures to open the valve before starting maintenance is judged unimportant because it would result in a single valve failure only. A CCF error of possible interest is performing an incorrect tagout (leaving the valve closed and removing control signal and power supply) on one valve and starting maintenance activities on a different valve (note that this scenario involves two human errors). This scenario is judged unimportant because it is very unlikely and because it would disable at most two valves (the system would still succeed, barring no additional failures). Thus, item 1 above is discarded.

Item 2 is also discarded because Procedure 3 calls for a stroke test immediately following maintenance on a valve and before starting maintenance on another valve. This test is accomplished from the control room and involves at least two plant operators [the operator(s) at the valve location and the control room operator]. The stroke test cannot be satisfactorily accomplished unless control signal and power supply have been properly restored to the valve. (Note that although alignment errors following maintenance are judged unimportant, some other errors are important, as discussed in root cause and component group combination 3.)

Finally, operational experience shows several instances in which valves were mistakenly deenergized, locked closed, or left with their control signals removed. In these cases, the operators were attempting to align equipment in other systems or even in other units and mistakenly removed from service the valves in the system of interest. The utility's administrative controls on tagouts were reviewed to verify if these spurious actions can credibly occur at this plant. Sufficient evidence of better-than-average administrative controls was not found however, and item 3 above is judged credible at this plant.

4.1.2.1.7 Root cause and component group combination 7: equipment addressed in Procedure 4. Procedure 4 was reviewed with emphasis on misalignment problems resulting from the annual maintenance activity. The findings associated with this procedure are identical to those associated with the isolation valves (combination 6). The only identified cause of multiple failures is a spurious operator action resulting in removal of the AFW pumps from service when attempting to remove pumps in a different system from service.

4.1.2.1.8 Root cause and component group combination 8: equipment addressed in Procedure 5. The AFW is normally actuated by an automatic control system, but Procedure 5 (EOP) calls for manual actuation if the control system does not initiate AFW in a timely

manner. Review of operational experience identified a problem that has existed at some plants. Starting all AFW pumps at once causes a temporary pressure drop in the common suction header that initiates the low suction pressure trip function for all pumps. The low pressure trip is prevented by starting the pumps sequentially, allowing enough time between starts for the suction header pressure to build back up. Normally, plants have these time delays built into their AFW control systems, but problems have occurred during manual actuation. At this plant, the control system uses time delays for starting the pumps, and the EOP explicitly instructs the operators to start the pumps one at a time, monitoring suction header pressure after starting each of the first two pumps. Therefore, this root cause and component group combination is judged unimportant in this analysis.

4.1.2.1.9 Root cause and component group combination 9: energetic harsh environments affecting equipment in the pump room. A complete search for credible sources of energetic harsh environments (e.g., pipe ruptures, missile impacts, etc.) that could disable the AFWS revealed only one scenario of potential interest. Since all three pumps are indeed located in the same room, a break in the steam supply line to the turbine-driven pump could potentially fail the two motor-driven pumps in addition to disabling the turbine-driven pump (the steam supply line break renders the turbine-driven pump unavailable by disrupting the supply of steam to the turbine driver). The contribution of this scenario to system unavailability is judged to be low for the following reasons:

- The motor-driven pumps are environmentally qualified; i.e., the motor and support equipment; e.g., junction boxes, conduits, cooling system equipment to motor bearings, and so on.
- An examination of the equipment layout revealed that only one of the motor-driven pumps is in the vicinity of the steam supply line. The other pump is at the opposite side of the room with its equipment further protected from steam impingement by a missile barrier. Thus, this other pump can only fail due to the steam supply line break if a sustained steam release fills the entire room with high temperature steam. Even in this case, failure of the pump is unlikely because it is qualified for such an environment.
- The steam generator isolation system would isolate the steam supply line almost immediately on an indication of a high steam supply line flow or on an indication of a low steam generator pressure. Thus, a sustained steam release is highly unlikely.
- The utility maintains an augmented ISI program for the steam supply line. An augmented ISI program is judged to greatly reduce the probability of a line rupture.

Therefore, root cause and component group combination 9 is judged unimportant in the CCF analysis. Table 4-3 summarizes the results of the root cause analysis for the AFWS.

This completes the qualitative analysis of this example. There are different types of additional qualitative analyses that may be performed but that are not included in this example. Such additional qualitative analyses include those to support the explicit modeling of external events; e.g., seismic events. These additional qualitative analyses have the potential for identifying new common cause events for incorporation into the logic model in Step 4.

The conclusion of the preceding discussion is that, from a qualitative standpoint, all three common cause component groups listed earlier should be modeled in this analysis since, for each group, one or more root cause and coupling mechanism of common cause failure have been identified.

4.1.2.2 Step 2.2 - Quantitative Screening. This step is usually taken to further reduce the number of common cause component groups by evaluating, in a conservative fashion, their numerical significance. However, in the present analysis, the system size and the number of common cause component groups are small and manageable, making the quantitative screening unnecessary.

#### 4.1.3 Stage 3: Common Cause Modeling

4.1.3.1 Step 3.1 - Definition of Common Cause Basic Events. The incorporation of the common cause events into the component-level logic model of Figure 4-3 is illustrated in Figures 4-4a and 4-4b for the fault tree logic form. The notation used to encode the common cause basic events, which are now defined at a level of detail below the component level (i.e., at the common cause impact level), uses the first letter to denote the common cause group (i.e., V, P, or M); the second letter to denote the impact of the cause (i.e., S for single component, D for double component, T for triple component, and G for global or all components in that group); and numbers to identify either the specific component or the specific combinations of components affected by that cause. This notation will be helpful in developing the algebraic equations after Boolean reduction is completed. Common cause basic events are now incorporated into the fault tree, based on the methodology of Section 3.

The enumeration of the events, facilitated by the special notation defined above, is simply the identification of all the component combinations involving 1, 2, ..., or N components. The fault subtree for each component then includes those and only those events that affect that particular component. Therefore, for the pump example, the following events would first be enumerated:

Single Component Events:	PS1, PS2, and PS3
Double Component Events:	PD12, PD23, and PD13
Triple (global) Component Events:	PG

Hence, the fault subtree for pump P1 would include all the events for which the name includes a 1 and the global event: PS1, PD12, PD13, and PG.

Table 4-3

## SUMMARY OF ROOT CAUSE ANALYSIS FOR THE AFW

Combination Identification Number	Equipment Affected	Comments
1	AFW Pumps	Important in CCF analysis; several root causes identified with significant CCF potential.
2	Pump Drive Motors	Important in CCF analysis; judged less likely than combinations 1 or 3.
3	AFW Isolation Valves	Important in CCF analysis; several root causes identified with significant CCF potential.
4	Equipment Addressed in Procedure 1: AFW Pumps	Unimportant in CCF analysis; no root cause identified with significant CCF potential.
5	Equipment Addressed in Procedure 2: AFW Isolation Valves	Unimportant in CCF analysis; no root cause identified with significant CCF potential.
6	Equipment Addressed in Procedure 3: AFW Isolation Valves	Important in CCF analysis; spurious operator actions could disable AFW system. Also, maintenance-related causes were identified.
7	Equipment Addressed in Procedure 4: AFW Pumps	Important in CCF analysis; spurious operator actions could disable AFW system.
8	Equipment Addressed in Procedure 5: All Pumps, Motor Drivers, and Isolation Valves	Unimportant in CCF analysis; Procedure 5 includes provisions to avoid root cause of concern.
9	All Equipment in Pump Room	Unimportant in CCF analysis; system well protected against identified harsh environment.

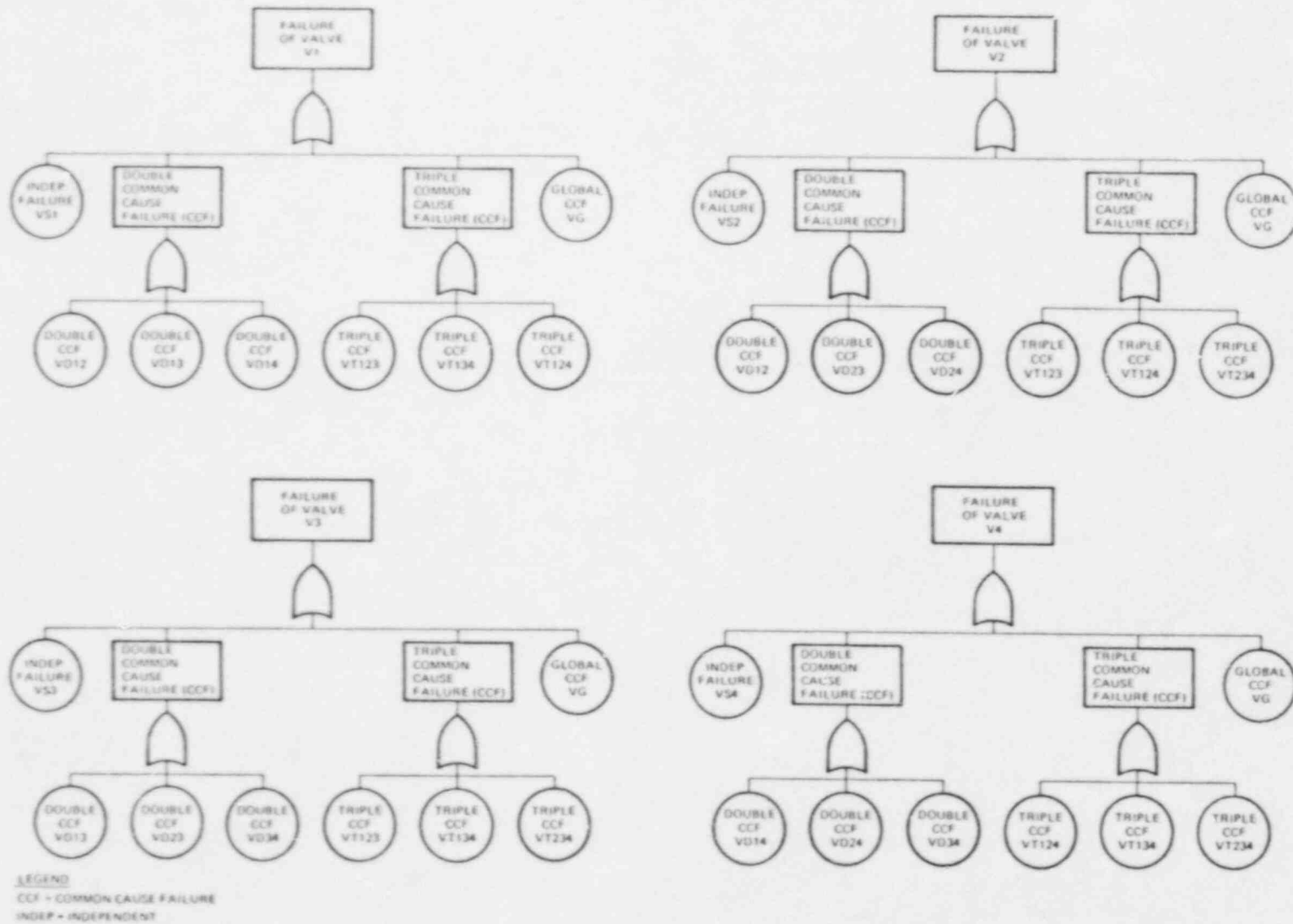


Figure 4-4a. Extensions to the Component-Level Fault Tree of Figure 4-3 To Incorporate Common Cause Events - Motor-Operated Valve Group

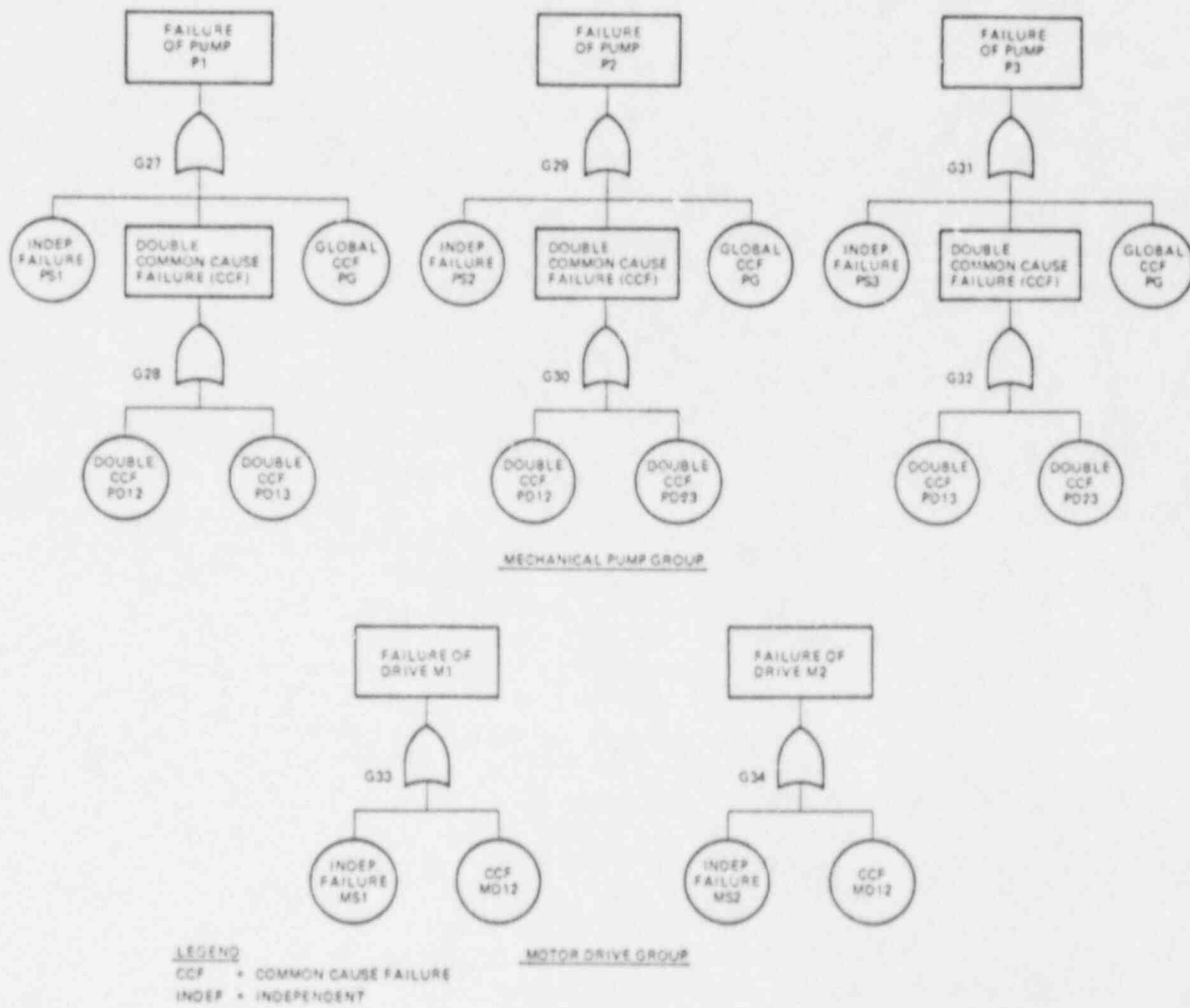


Figure 4-4b. Extensions to the Component-Level Fault Tree of Figure 4-3 To Incorporate Common Cause Events - Mechanical Pump and Motor Drive Groups



The minimal cutsets of the fault tree, expanded to include the common cause events, are presented in Table 4-4. Any fault tree software can be used to do this once the common cause events are properly incorporated. Note that the controversial cutsets that were discussed in Section 3.3.1 are presented separately in Table 4-4. As noted in that section, these controversial cutsets make negligible numerical contribution to the results and subsequently are either deleted or left in the analysis. Of the total of 129 cutsets listed that include 15 controversial cutsets, the 29 that are underlined are the only ones that would appear without the common cause events.

4.1.3.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events. After finding the minimal cutsets for each alignment, we make the transition from Boolean algebra to normal algebra. This transition is necessary to quantify the frequencies of the top event and all its contributors.

Table 4-5 shows the algebraic terms corresponding to the fault tree evaluation for the normal alignment case. Note that the assumption of symmetry of basic common cause events discussed in Section 3 in the context of the parametric models has been used in developing the algebraic equations of Table 4-5. For example, there are six different common cause events that fail two valves, each event failing a different pair of valves. According to the assumption of symmetry, all these are assumed to have the same probability, and so forth. For basic events associated with a common cause group, the notation,  $X_j$  is used where  $j$  represents the number of components of type  $X$  failed due to the corresponding cause and basic event in the fault tree. All the basic events with  $j = 1$  are independent events, while those with  $j \geq 2$  are common cause events. This notation does not reveal information about particular components. Such information is necessary in the fault tree basic event notation to properly identify minimal cutsets. However, from this point, it is only necessary to retain what is needed to compute frequencies and identify the contributors.

A very important result noted earlier and shown in Table 4-5 is the proliferation of cutsets associated with the introduction of the common cause events into the fault tree. For this example, the impact is more than a four-fold increase in the number of cutsets. Had we done any quantitative screening, the number of cutsets would not have become as high. An alternative to the incorporation of the common cause events into the fault tree is to leave them out and somehow incorporate them while developing the algebraic models. Experience has shown, however, that there is a high risk that not all the cutsets will be picked up and some may well be overlooked if this important step is buried in the algebraic formulas. For example, there is a definite relationship between the independent and common terms in Table 4-5.

Consider the term  $4V_1^3$  that represents the four minimal cutsets in the fault tree involving combinations of three independent valve failures. The common cause terms,  $V_4$ ,  $4V_3$ ,  $12V_2V_1$ ,  $15V_2^2$ ,\* all represent additional

---

\*This coefficient of 15 will be 3 if the controversial cutsets listed in Table 4-4 are deleted. Refer to Section 3.3.1 for the discussion of this controversy.

## MINIMAL CUTSET OF THE EXPANDED FAULT TREE OF THE AUXILIARY FEEDWATER SYSTEM

First Order Cutsets (a total of 7)

C, VG, PG, VT123, VT124, VT134, VT234

Second Order Cutsets (a total of 54)VD12\*VS3, VD12\*VS4, VD13\*VS2, VD13\*VS4, VD14\*VS2, VD14\*VS3  
VD23\*VS1, VD23\*VS4, VD24\*VS1, VD24\*VS3, VD34\*VS1, VD34\*VS2

VD12\*VD34, VD13\*VD24, VD14\*VD23

PD23\*VD12, PD23\*VD13, PD23\*VD14, PD23\*VD23, PD23\*VD24  
PD13\*VD34, PD13\*VD23, PD13\*VD24, PD23\*VD14, PD13\*VD13

PS1\*PD23, PS2\*PD13, PS3\*PD12

PD23\*MS1, PD13\*MS2, PD12\*T, PD23\*MD12, PD13\*MD12

PD23\*VS1, PD23\*VS2, PD13\*VS3, PD13\*VS4, MD12\*PS3, MD12\*T

VD12\*VC13, VD12\*VD14, VD12\*VD23, VD12\*VD24, VD13\*VD14,  
VD13\*VD23, VD13\*VD34, VD14\*VD24, VD14\*VD34, VD23\*VD24,  
VD23\*VD34, VD24\*VD34, PD12\*PD23, PD12\*PD13, PD13\*PD23

\*

Third Order Cutsets (a total of 68)VS1\*VS2\*VS3, VS1\*VS2\*VS4, VS1\*VS3\*VS4, VS2\*VS3\*VS4, PS1\*PS2\*PS3MS1\*PS2\*PS3, MS2\*PS1\*PS3, MS1\*MS2\*PS3, PS1\*PS2\*T, MS1\*PS2\*T,  
MS2\*PS1\*T, MS1\*MS2\*TVS1\*PS2\*PS3, VS2\*PS2\*PS3, V3\*P1\*P3, V4\*P1\*P3VS1\*PS2\*T, V2\*P2\*T, V3\*P1\*T, V4\*P1\*TVS1\*MS2\*PS3, V2\*M2\*P3, V3\*M1\*P3, V4\*M1\*P3VS1\*MS2\*T, V2\*M2\*T, V3\*M1\*T, V4\*M1\*P3PS2\*PS3\*VD12, PS2\*PS3\*VD13, PS2\*PS3\*VD14, PS2\*PS3\*VD23, PS1\*PS3\*VD24  
PS1\*PS3\*VD34, PS1\*PS3\*VD23, PS2\*PS3\*VD24, PS1\*PS3\*VD14, PS1\*PS3\*VD13MS2\*PS3\*VD12, MS2\*PS3\*VD13, MS1\*PS3\*VD14, MS2\*PS3\*VD23, MS2\*PS3\*VD24,  
MS1\*PS3\*VD13, MS1\*PS3\*VD23, MS1\*PS3\*VD24, MS2\*PS3\*VD14, MS1\*PS3\*VD34MS2\*T\*VD12, MS2\*T\*VD13, MS2\*T\*VD14, MS2\*T\*VD23, MS1\*T\*VD24,  
MS1\*T\*VD13, MS1\*T\*VD23, MS2\*T\*VD24, MS1\*T\*VD14, MS1\*T\*VD34PS2\*T\*VD12, PS2\*T\*VD13, PS2\*T\*VD14, PS2\*T\*VD23, PS2\*T\*VD24,  
PS1\*T\*VD34, PS1\*T\*VD23, PS2\*T\*VD24, PS1\*T\*VD14, PS1\*T\*VD13

\*For a discussion of these controversial cutsets, please refer to Sections 4.1.3.1 and 3.3.1.

Table 4-5

TERMS OF THE ALGEBRAIC MODEL FOR THE AFWs IN NORMAL ALIGNMENT  
BASIC PARAMETER MODEL FORM

Cutset Order	Independent Event Terms (account for 29 minimal cutsets)	Common Cause Event Terms (account for 100 minimal cutsets)
First Order Cutsets	C	$V_4 + P_3 + 4V_3$
Second Order Cutsets	None	$+ 12V_2V_1 + 15V_2^{2*} + 10V_2P_2 + 3P_1P_2 + 3P_2^{2*}$ $+ 2P_2M_1 + 2P_2M_2 + 4P_2V_1 + P_2T + M_2P_1 + M_2T$
Third Order Cutsets	$+ 4V_1^3 + P_1^3 + 2M_1P_1^2 + P_1M_1^2 + TP_1^2 + 2M_1TP_1$ $+ TM_1^2 + 4V_1P_1^2 + 4V_1TP_1 + 4V_1M_1P_1 + 4M_1V_1T$	$+ 10P_1^2V_2 + 10P_1V_2T + 10P_1V_2M_1 + 10V_2M_1T$

\*The coefficient of these terms are 3 and 0, respectively, when the controversial cutsets listed in Table 4-4 are eliminated. Refer to Section 3.3.1 for a discussion of these cutsets.

cutsets involving common cause events and combinations of common cause and independent events that would also fail combinations of three (or more) valves. Nevertheless, it should be noted that, as will be discussed later, not all the terms will have a significant contribution to the system unavailability and that the analyst might even be able to eliminate them at the initial quantitative screening level and the subsequent logic model expansion using quantitative arguments. This subject will be discussed more fully later.

It is important to note, however, that although many of the new cutsets introduced by the common cause events make small or insignificant contributions, the majority of the new cutsets added to this example have higher frequencies than most of the purely independent event cutsets. In Stage 4 below, we will return to this problem of cutset proliferation and examine some ways to simplify the analysis as well as the attendant pitfalls.

To complete the development of algebraic models to a form that is suitable for quantification, there are, as discussed in Section 3, alternative paths to follow depending on the type of parametric model selected. The following parametric models that are representative of the different categories of models described in Section 3 are selected:

- Basic Parameter Model
- Multiple Greek Letter Model
- Beta Factor Model (as special case of the MGL model)
- Binomial Failure Rate with Lethal Shocks Model

Application of the alpha factor model to this example will be discussed in Appendix E in the context of sensitivity analysis on certain characteristics of the selected models.

The correspondence between the algebraic terms of the example systems analysis and formulas for applying the three parametric common cause models is shown in Table 4-6. These can all be written down using Table 3-1; e.g., the term for  $V_2$ , using the MGL model, is

$$V_2 = \frac{1}{\binom{4-1}{2-1}} p_1 p_2 (1 - p_3) Q_t$$

where

$$p_1 = l, p_2 = B, \text{ and } p_3 = \gamma$$

Therefore,

$$V_2 = \frac{1}{3} B(1-\gamma) Q_t$$

There are a number of variations on the formulas that could have been used, depending upon how the data are analyzed. For example, in all three models, it is possible to reduce the number of parameters by not distinguishing between demand failures and failures during operation.

Table 4-6

## QUANTIFICATION FORMULAS FOR THREE PARAMETRIC COMMON CAUSE MODELS

Algebraic Term	Formulas for Applying Parametric Common Cause Models		
	Basic Parameter Model	Multiple Greek Letter Model	Binomial Failure Rate Model**
$V_1^*$	$\lambda_{V1}$	$(1-R)\lambda_V$	$\lambda_{V1}' + u_V p_V (1 - p_V)^3$
$V_2^*$	$\lambda_{V2}$	$\frac{1}{3}(1 - \gamma_V)^R \lambda_V$	$u_V p_V^2 (1 - p_V)^2$
$V_3^*$	$\lambda_{V3}$	$\frac{1}{3}(1 - \delta_V) \gamma_V^R \lambda_V$	$u_V p_V^3 (1 - p_V)$
$V_4^*$	$\lambda_{V4}$	$\delta_V \gamma_V^R \lambda_V$	$u_V p_V^4 + \omega_V$
$P_1$	$\lambda_{PS1} + \lambda_{PR1}t$	$(1 - R_{PS})\lambda_{PS} + (1 - R_{PR})\lambda_{PR}t$	$\lambda_{PS1}' + u_{PS} p_{PS} (1 - p_{PS})^2 + [\lambda_{PR1}' + u_{PR} p_{PR} (1 - p_{PR})^2]t$
$P_2$	$\lambda_{PS2} + \lambda_{PR2}t$	$\frac{1}{2} [(1 - \gamma_{PS})^R \lambda_{PS} + (1 - \gamma_{PR})^R \lambda_{PR}t]$	$u_{PS} p_{PS}^2 (1 - p_{PS}) + u_{PR} p_{PR}^2 (1 - p_{PR})$
$P_3$	$\lambda_{PS3} + \lambda_{PR3}t$	$\gamma_{PS}^R \lambda_{PS} + \gamma_{PR}^R \lambda_{PR}t$	$u_{PS} p_{PS}^3 + \omega_{PS} + (u_{PR} p_{PR}^3 + \omega_{PR})t$
$M_1$	$\lambda_{MS1} + \lambda_{MR1}t$	$(1 - R_{MS})\lambda_{MS} + (1 - R_{MR})\lambda_{MR}t$	$\lambda_{MS1}' + u_{MS} p_{MS} (1 - p_{MS}) + [\lambda_{MR1}' + u_{MR} p_{MR} (1 - p_{MR})]t$
$M_2$	$\lambda_{MS2} + \lambda_{MR2}t$	$R_{MS} \lambda_{MS} + R_{MR} \lambda_{MR}t$	$u_{MS} p_{MS}^2 + \omega_{MS} + (u_{MR} p_{MR}^2 + \omega_{MR})t$
$T$	$\lambda_{TS} + \lambda_{TR}t$	$\lambda_{TS} + \lambda_{TR}t$	$\lambda_{TS} + \lambda_{TR}t$
$C$	$\lambda_{C1}(t + \frac{T_C}{2})$	$\lambda_{C1}(t + \frac{T_C}{2})$	$\lambda_{C1}(t + \frac{T_C}{2})$
Total Number of Different Parameters	19	19	25

\*Time-based failure rates for these terms assumed to be negligible.

\*\*Prime is used to distinguish between the independent failure rate parameter (e.g.,  $\lambda_{V1}'$ ) in the binomial failure rate model and the single component failure frequency (e.g.,  $\lambda_{V1}$ ) in the basic parameter model.

Before jumping off to the next steps in the analysis, several important distinctions need to be made between the guidance given in Table 4-6 and different approaches that have been proposed for the incorporation of these common cause models into a systems analysis. Probably the most important such distinction is that, in contrast with procedures previously published, Table 4-5 specifies the incorporation of all three of the parametric models at the level of detail in the analysis below the component level; i.e., at the common cause impact level. It is instructive to backtrack a little and examine some of the difficulties that are encountered when common cause events are not incorporated into the logic model. In our example system for the normal alignment case, the component-level minimal cutsets are presented in Table 4-7. These correspond with the independent terms in Table 4-5.

The theoretically correct incorporation of the parametric models from the component-level minimal cutsets in Table 4-7 requires some nontrivial mental gymnastics. This is because the equivalent of the right-hand column of Table 4-5 must be generated in one's head while writing down the parametric formulas. For example, take the term  $4V^3$  in the grouping of minimal cutsets in Table 4-7. By identifying all the cutsets in Table 4-5 that affect combinations of three different valves, it is seen that the correct application of the parametric CCF models requires the analyst to develop the equivalent of the following intermediate step in his head.

$$4V^3 = V_4 + 4V_3 + 12V_1V_2 + 15V_2^{2*} + 4V_1^3 \quad (4-1)$$

If the above relationship is not accounted for by the analyst, either explicitly or implicitly, it is very likely that either overaccounting or underaccounting of system failure modes, or both, will result. In particular, it is very likely that the analyst would miss terms, such as  $4V_3$  (four possible combinations of common cause failure of three of the four valves), a term that could be numerically significant.

It must be mentioned, however, that not all the terms on the right-hand side of Eq. 4-1 are numerically important. Indeed, such terms as  $V_2^2$ , which involve simultaneous occurrence of two common cause failures, are generally dominated by other terms involving single common cause failures; e.g.,  $V_3$ . A quantitative screening, either as part of Step 2.2 or, as is often done, by defining a frequency cutoff in the fault tree code used to identify the cutsets, would reduce the number of terms to be carried through the rest of the analysis.

4.1.3.3 Step 3.3 - Data Classification and Screening. All three of the parametric common cause analysis approaches discussed in this section (basic parameter, MGL, BFR) require event data to be classified and categorized prior to parameter estimation. The mapping up and down requires classifying events into lethal and nonlethal shocks. Thus, the analysis is identical for all three models.

---

\*This coefficient of 15 will be 3 if controversial cutsets listed in Table 4-4 are deleted.

Table 4-7

COMPONENT-LEVEL MINIMAL CUTSETS FOR  
EXAMPLE SYSTEM - NORMAL ALIGNMENT

Number of Minimal Cutsets	Symbol*	Cutset Description
1	C	Common Suction Path
4	V <sup>3</sup>	Three valves
1	P <sup>3</sup>	Three Pumps
1	TP <sup>2</sup>	One Turbine and Two Pumps
2	MP <sup>2</sup>	One Motor and Two Pumps
2	MTP	One Motor, One Turbine, One Pump
1	M <sup>2</sup> P	Two Motors, One Pump
1	M <sup>2</sup> T	Two Motors, One Turbine
4	VP <sup>2</sup>	One Valve, Two Pumps
4	VTP	One Valve, One Turbine, One Pump
4	VPM	One Valve, One Pump, One Motor
4	VTM	One Valve, One Turbine, One Motor

\*In this notation, the exponents indicate the number of identical components of a given type in the cutset.

For the sample system, the dependent events data base for auxiliary feedwater pumps in Reference 4-1 includes 10 dependent events, each having 2 or more unavailable or potentially unavailable pumps. The classification and expected (average) impact vector for these data is shown in Table 4-8. Of the 10 event reports that were identified, 2 of the reports contained 2 separate, independent events each; hence, the table includes 12 events. This table does not show the several hundred independent events in the data base for this component.

The pump average impact vectors for the example system were assessed, based on the qualitative information from Stage 2 (Section 4.1.2) and the methods discussed in Section 3.

For instance, the impact vector for event 3 in Table 4-8 was analyzed as follows.

The impact vector for the original plant (Kewaunee) is based on two hypotheses:

Hypothesis	Probability	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>
H <sub>1</sub> : Clogging severe enough to cause failure of all three pumps.	0.1	0	0	0	1
H <sub>2</sub> : No significant reduction in flow (no failure).	0.9	1	0	0	0
Average Impact Vector		0.9	0	0	0.1

The assigned probability of 0.9 for the second hypothesis represents the degree of confidence that the component performance and success criteria were not violated in the event and that the flow reduction was minimal.

Since the pumps in the example AFWS take suction from the same source and the possibility of resin clogging exists for the plant analyzed, the cause of the event and its coupling mechanism apply with a probability of 1. Also, since both the original and the example systems have the same number of pumps, there is no need to modify the impact vector for system size difference. The resulting impact vector for the example system, therefore, is the same as the original impact vector.

Events classified as lethal shocks were based on the nature of the cause and the assessment that such a cause would have a high potential for failure of all redundant components present. Common cause events that affected two components, when it was known that three or more identical



Table 4-8

CLASSIFICATION AND IMPACT ASSESSMENT OF EVENTS INVOLVING DEPENDENT FAILURES AND UNAVAILABILITIES OF AUXILIARY FEEDWATER PUMPS

Sheet 1 of 2

Event Number	Plant (date)	Status	Event Description	Cause-Effect Diagram	Application	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	M/A	Shock Type	Failure Mode
1	Ginna (December 1973)	Critical	Two motor-driven auxiliary feedwater pumps inoperable due to air in common suction line.		Ginna	0	0	1	0	0	0	L	S
					Example System	0	0	0	1	0	0		
2	Zion 2 (February 1974)	Power Escalation Test	Two motor-driven auxiliary feedwater pumps inoperable due to air in suction lines.		Zion 2	0	0	1	0	0	0	L	S
					Example System	0	0	0	1	0	0		
3	Kewaunee (November 1975)	Shutdown	Resin clogged auxiliary feedwater pump strainers causing reduced flow.		Kewaunee	0.9	0	0	0	0.1	0	N	R
					Example System	0.9	0	0	0	0.1	0		
4	Turkey Point 3 (May 1974) (2 events)	98% Power	Auxiliary feedwater pumps A and B failed to start due to tight packing. Pump C started but tripped due to governor failure.		Turkey Point 3	0	0	1	0	0	0	N	S
					Example System	0	0	1	0	0	0		
					Turkey Point 3	0	1	0	0	0	0	I	R
					Example System	0	0	0	0	0	1		
5	Point Beach 1 and 2 (April 1974)	Power	Preoperation strainers left in suction line plugged, making motor-driven auxiliary feedwater pump A on Unit 1 inoperable. Similar strainers were found in Unit 1 motor-driven auxiliary feedwater pump B and Units 1 and 2 turbine-driven auxiliary feedwater pumps.		Point Beach 1	0	0.9	0	0	0	0.1	L	R
					Example System	0	0.9	0	0	0.1	0		

Table 4-8 (continued)

Event Number	Plant (Date)	Status	Event Description	Cause-Effect Diagram	Application	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	N/A	Shock Type	Failure Mode
6	Zion 2 (September 1981) (2 events)	Shutdown	All three auxiliary feedwater pumps failed to start. Pumps 2B and 2C failed due to a backfeed circuit that resulted from pumps' control switch modification. Failure of pump 2B was due to a pressure switch drift.		Zion 2	0	0	1	0	0	0	N	S
					Example System	0	0	1	0	0	0	0	0
7	Zion 2 (November 1979)	Power	Auxiliary feedwater pumps 2B and 2C failed to start due to miscalibrated pressure gauges.		Zion 2	0	0	1	0	0	0	N	S
					Example System	0	0	1	0	0	0	0	0
8	Zion 2 (December 1975)	Power	Auxiliary feedwater pumps 2B and 2C failed to start due to start circuitry design problem.		Zion 2	0	0	1	0	0	0	N	S
					Example System	0	0	1	0	0	0	0	0
9	Turkey Point 4 (June 1973)	Prior to Initial Power Testing	All three auxiliary feedwater pumps failed to start automatically due to missing fuses in pump autostart circuit.		Turkey Point 4	0	0	0	1	0	0	L	S
					Example System	0	0	0	0	0	0	1	0
10	Arkansas One 2 (April 1980)	On power	Two emergency feedwater pump - loss due to design problem.		AND 2	0	0	1	0	0	0	L	S
					Example System	0	0	0	1	0	0	0	0
Total Start Events						0	1	4	3	0	1	L = 3 N = 4	
Total Run Events						0.9	0.9	0	0.2	0	1	L = 1 N = 1	
						n <sub>0</sub>	n <sub>1</sub>	n <sub>2</sub>	n <sub>3</sub>	n <sub>4</sub>	n <sub>N/A</sub>		

LEGEND:

Cause-Effect Diagram:

- M - Maintenance
- P - Procedural Error
- D - Design Error
- E - Environmental
- I - Internal Failure
- H - Human Error

Shock Types and Failure Modes:

- L - Lethal Shock
- N - Nonlethal Shock
- I - Independent Event
- B - Fail to Run
- S - Fail to Start

components were present, were classified as nonlethal shocks. When design differences were noted to so justify, these events were classified as not applicable to the example system. In mapping the applicable events, all lethal shock events (or portions of events) were mapped directly to  $P_3$  since there are three pumps in the example system. In all cases of applicable nonlethal shock, it was known that the system size from which the data came also had three pumps. Hence, there was no need to make numerical corrections for mapping between different size systems, as discussed in Section 3.

4.1.3.4 Step 3.4 - Parameter Estimation. Numerical values of the various parameters of the three common cause models were developed for this example system by using the results of event classification for various components of the system. For all three models, the total failure frequency of the components was taken from generic estimates provided in Reference 4-6.

4.1.3.4.1 MGL parameters. In the case of the MGL model, the generic total failure frequency estimates and the classified set of events for pumps, valves, and other components were sufficient to estimate all the remaining parameters of the model. For instance, to estimate the beta factor for pump failure during operation using the data of Table 4-8, we have  $n_2 = 0$ ,  $n_3 = 0.2$ . In the process of reviewing and classifying events in the data base, 28 events were classified as independent pump failures. In six other cases, single pumps were in degraded condition and were classified as potential independent failures. Also in Table 4-8, there is one case of a common cause with 0.9 chance of impacting only one pump. The potential events must be weighted by the analysts' subjective probability that a recurrence of such an event would result in an actual component state in the system being analyzed. In this analysis, all the potential independent events were assigned a weight of 0.1. The effective number of independent failures therefore is

$$n_1 = 28 + 0.1(6) + 0.9(1) = 29.5 \quad (4-2)$$

We can now use these data in the estimator of Table 3-6 for the B-factor; i.e.,

$$\begin{aligned} B_{PR} &= \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \\ &= \frac{2(0) + 3(0.2)}{29.5 + 2(0) + 3(0.2)} \end{aligned} \quad (4-3)$$

However, most of the data are sparse, sometimes even nonexistent, resulting in parameter estimates that are equal or nearly equal to zero. We will therefore primarily adopt the Bayesian approach to estimation in this example (as described in Appendix E), which changes the estimates by integrating some prior or generic

information with the data. In this case, the mean value of the B-factor, for example, becomes

$$B = \frac{2n_2 + 3n_3 + a}{n_1 + 2n_2 + 3n_3 + a + b} \quad (4-4)$$

where a and b are the parameters of the prior distribution (see discussion in Appendix E regarding the approximate nature of the above estimator).

Assuming a uniform prior distribution (a=b=1), we obtain the following mean value

$$B_{PR} = \frac{2(0) + 3(0.2) + 1}{29.5 + 2(0) + 3(0.2) + 2} = 0.05 \quad (4-5)$$

This and other estimated parameters for this example are listed in Table 4-9.

We should be aware that one of the reasons the event count is so low is that events have been excluded because of their inapplicability for various sound reasons. This implies that, in our example, the dependencies should indeed be quite small. The Bayesian inclusion of generic information using a uniform prior opposes this trend and may therefore bias the results conservatively. Since our point estimate should not be unduly conservative, the influence of the prior should be investigated by sensitivity analysis. This is not done in this example.

The frequency of independent events is simply proportional to the number of components present. The above parameter estimates assume that all the evidence for independent failures,  $n_1$ , came from systems having the same number of pumps as the example system. To examine the sensitivity to this assumption, consider the following two alternative hypotheses. First, let us assume that the common cause event data are the same as indicated above, but that the independent event data all came from two-train systems. In this case, to correct for the size mismatch (see Section 3.3.3.4):

$$\begin{aligned} n_1(\text{three-train systems}) &= \frac{3}{2} n_1(\text{two-train systems}) & (4-6) \\ &= \frac{3}{2} (29.5) = 44.3 \end{aligned}$$

The resulting Bayesian mean value of  $B_{PR}$  now becomes

$$B_{PR} = \frac{2(0) + 3(0.2) + 1}{44.3 + 2(0) + 3(0.2) + 2} = .034 \quad (4-7)$$

Table 4-9

## BAYESIAN ESTIMATES OF THE PARAMETERS FOR THREE COMMON CAUSE MODELS OF THE EXAMPLE SYSTEM

Component (Failure Mode)	Failure Mode	Basic Parameter Model	Multiple Greek Letter Model	Binomial Failure Rate Model <sup>a, b</sup>
Pump (excluding driver)	Fail To Start on Demand	$\lambda_{PS1} = 8.68-4$ $\lambda_{PS2} = 2.17-4$ $\lambda_{PS3} = 5.21-4$	$\lambda_{PS} = 1.65-3$ $B_{PS} = 0.47$ $\gamma_{PS} = 0.53$	$\lambda'_{PS1} = 8.68-4$ $\mu_{PS} = 6.51-4$ $\omega_{PS} = 5.21-4$ $p_{PS} = 0.5$
	Fail During Operation	$\lambda_{PR1} = 1.62-5/hr$ $\lambda_{PR2} = 2.70-7/hr$ $\lambda_{PR3} = 1.13-6/hr$	$\lambda_{PR} = 1.71-5/hr$ $B_{PR} = 0.05$ $\gamma_{PR} = 0.62$	$\lambda'_{PR1} = 1.57-5/hr$ $\mu_{PR} = 9.72-7/hr$ $\omega_{PR} = 9.72-7/hr$ $p_{PR} = 0.5$
Motor (motor-driven pumps)	Fail To Start on Demand	$\lambda_{MS1} = 1.49-3/$ $\lambda_{MS2} = 2.98-4/$	$\lambda_{MS} = 1.65-3$ $B_{MS} = 0.1$	$\lambda'_{MS1} = 1.49-3$ $\mu_{MS} = 2.98-4$ $\omega_{MS} = 2.98-4$ $p_{MS} = 0.0$
	Fail During Operation	$\lambda_{MR1} = 1.61-5/hr$ $\lambda_{MR2} = 1.09-6$	$\lambda_{MR} = 1.71-5/hr$ $B_{MR} = 0.06$	$\lambda'_{MR1} = 1.61-5/hr$ $\mu_{MR} = 1.09-6/hr$ $\omega_{MR} = 1.09-6/hr$ $p_{MR} = 0.0$
Turbine (turbine- driven pump)	Fail To Start on Demand	$\lambda_{TS} = 3.15-2$	$\lambda_{TS} = 3.15-2$	$\lambda_{TS} = 3.15-2$
	Fail During Operation	$\lambda_{TR} = 1.01-3/hr$	$\lambda_{TR} = 1.01-3/hr$	$\lambda_{TR} = 1.01-3/hr$
Motor-Operated Valve	Fail To Operate on Demand	$\lambda_{V1} = 3.79-3$ $\lambda_{V2} = 4.49-5$ $\lambda_{V3} = 1.02-5$ $\lambda_{V4} = 3.80-4$	$\lambda_V = 4.30-3$ $B_V = 0.12$ $\gamma_V = 0.75$ $\delta_V = 0.95$	$\lambda'_{V1} = 3.75-3$ $\mu_V = 4.50-4$ $\omega_V = 3.80-4$ $p_V = 0.5$
Tank	Rupture	$\lambda_{C1} = 2.70-8/hr$	$\lambda_{C1} = 2.70-8/hr$	$\lambda_{C1} = 2.70-8/hr$

a. The prime on  $\lambda$  value is used to indicate that the parameter is generally different from a similar parameter in the basic parameter model.

b. Value of  $p$  is not Bayes' estimate. It is calculated from the procedure explained in the text.

NOTE: Exponential notation is indicated in abbreviated form; i.e.,  $8.68-4 = 8.68 \times 10^{-4}$ .

Conversely, if all the  $n_1$  data had come from four-train systems,

$$\begin{aligned} n_1(\text{three-train systems}) &= \frac{3}{4} n_1(\text{four-train systems}) & (4-8) \\ &= \frac{3}{4} (29.5) = 22.1 \end{aligned}$$

resulting in

$$B_{PR} = \frac{2(0) + 3(0.2) + 1}{22.1 + 2(0) + 3(0.2) + 2} = .065 \quad (4-9)$$

As a final sensitivity, assume all the  $n_1$  data came from two-train systems and that it is determined that the independent event data are preferentially underreported in the LER system in comparison to the common cause data to the extent that only one-third of the actual independent events are reported.

$$\begin{aligned} n_1(\text{three-train systems}) &= 3\left(\frac{3}{2}\right)n_2(\text{two-train systems}) & (4-10) \\ &= 3\left(\frac{3}{2}\right)(29.5) = 132.8 \end{aligned}$$

$$B_{PR} = \frac{2(0) + 3(0.2) + 1}{132.8 + 2(0) + 3(0.2) + 2} = .012 \quad (4-11)$$

Since it is almost certain that the independent event data came mainly from two and three-train systems and not principally from four train systems and since it is known that independent events are significantly underreported in LERs, it follows that the result in Ec. 4-11 properly represents the extent of these effects.

4.1.3.4.2 Basic parameters. In the case of basic parameter and BFR models, a set of success data, such as the total number of system demands ( $N_D$ ) and operating hours ( $T$ ), needs to be estimated. For the purpose of this example application, however, we estimate the success data by assuming that the generic total failure frequencies were based on the set of failure data presented in Reference 4-6. For instance, for pump failure during operation, we have the generic estimate of  $\lambda_{PR} = 1.71 \times 10^{-5}/\text{hour}^{-1}$ . The rate of independent failures can now be calculated from

$$\begin{aligned} \lambda_{PRI} &= (1 - B_{PR}) \lambda_{PR} \\ &= (1 - 0.05)(1.71 \times 10^{-5}) = 1.62 \times 10^{-5}/\text{hour}^{-1} & (4-12) \end{aligned}$$

The equivalent number of system operating hours,  $T$ , can now be calculated from

$$\lambda_{PRI} = \frac{n_1 + 0.5}{mT} \quad (4-13)$$

where  $m$  is the average number of pumps in the generic AFWs (assumed to be three) and 0.5 represents the parameter of the noninformative gamma prior distribution used to develop the Bayes' estimator (see Appendix E). Now, based on the data presented here,  $n_1 = 29.5$ , we have

$$T = \frac{29.5 + 0.5}{3 (1.62 \times 10^{-5})} = 6.17 \times 10^5 \text{ system exposure hours} \quad (4-14)$$

as the total exposure time of all of the systems and units in the data base.

Other success data for the parameters of the basic parameter and BFR models were similarly developed.

Using the success data, other parameters of the basic parameter model are estimated easily. For example, the rate of simultaneous failure of two pumps during operation,  $\lambda_{PR2}$ , is given by

$$\begin{aligned} \lambda_{PR2} &= \frac{n_2 + 0.5}{3T} \\ &= \frac{0 + 0.5}{3 (6.17 \times 10^5)} = 2.70 \times 10^{-7} / \text{hour} \end{aligned} \quad (4-15)$$

As before, sensitivity analysis of these results should be undertaken in a proper analysis.

4.1.3.4.3 BFR parameters. As mentioned earlier, obtaining Bayes' estimate for the parameter  $p$  in the BFR model requires numerical integration of Bayesian equations. A computer code has been developed to perform such calculations (Reference 4-7). Since the code was not available to the authors, a different approach was taken in this example to obtain approximate values of  $p$ . We first estimated the values of  $\lambda$ ,  $\lambda_t$ ,  $\omega$ , and  $\mu$  directly from the data, consistent with the estimates of the parameters of basic parameter and MGL models. For instance, the rate of lethal shocks for pump failure during operation was calculated from

$$\begin{aligned} \omega_{PR} &= \frac{n_L + 0.5}{T} \\ &= \frac{0.1 + 1/2}{6.17 \times 10^5} = 9.72 \times 10^{-7} / \text{hour} \end{aligned} \quad (4-16)$$

where  $n_L = 0.1$  is the expected number of lethal shocks based on the data of Table 4-8, and 0.5 is, as before, the parameter of the noninformative gamma prior distribution used in Bayes' theorem.

To obtain  $p$  (in this case  $p_{PR}$ ), we set the frequency of various failure events based on the BFR model equal to those obtained based on the basic parameter model. The result is the following set of equations (see Table 4-6).

$$\lambda_{PRI} = \lambda'_{PRI} + \mu_{PR} p_{PR} (1 - p_{PR})^2 \quad (4-17)$$

$$\lambda_{PR2} = \mu_{PR} p_{PR}^2 (1 - p_{PR}) \quad (4-18)$$

$$\lambda_{PR3} = \mu_{PR} p_{PR}^3 + \omega_{PR} \quad (4-19)$$

On substituting the numerical values for all parameters except  $p_{PR}$ , we get the following equations to solve for  $p_{PR}$ .

$$p_{PR}^2 - p_{PR} + 1.44 = 0 \quad (4-20)$$

$$p_{PR}^3 - p_{PR}^2 + 0.278 = 0 \quad (4-21)$$

$$p_{PR}^3 - 0.163 = 0 \quad (4-22)$$

When matching the numerical values of the basic parameter or MGL with the BFR model, as above, there is one important condition that must be satisfied for a unique and valid solution for the  $p$ -parameter to exist. The condition is that the evidence must fit the built-in assumption of the BFR model that the nonlethal shocks follow a binomial distribution over the number of components affected. In general, this assumption is not strictly satisfied in the data. In the above equations, the two solutions to Eq. 4-20 are complex numbers. Eqs. 4-21 and 4-22 each have one real and two complex solutions; the real solutions are  $p_{PR} = .23$  and  $p_{PR} = .55$ , respectively. To complete the example, a value of  $p = .5$  was assumed for each case in which a reasonable and consistent solution for the  $p$  parameter could not be found.

The above examples serve to illustrate some of the practical problems that need to be addressed in parameter estimation, even for a seemingly simple system such as the one used in the example. It is seen that a large amount of effort goes into the quantification of so many parameters, no matter which common cause model is selected. Numerous sources of uncertainty are also evident with the major ones consisting of sparsity of data, applicability and impact of each event in classification, and missing success data. A discussion of the impact of various sources of uncertainty in estimating various parameters was provided in Section 3. In this example, uncertainty distributions were developed for each of the parameters of various models using the Bayesian methods described in Appendix E.



Figure 4-5 shows, as an example, the cumulative distribution of two MGL parameters used for the run failure mode of AFW pumps. As can be seen, the uncertainty associated with the gamma factor is much larger than the beta factor. This, of course, is due to the greater sparsity of data for higher order parameters. It is important to note that these uncertainties do not include the effects of mapping independent events from different size systems, the effect of a possible bias in the data due to underreporting of independent events, and the impact of assumptions regarding system testing schemes and success data collection.

#### 4.1.4 Stage 4: System Quantification and Interpretation of Results

4.1.4.1 Step 4.1 - System Quantification. The next step in the analysis is the quantification of the system model. The recommended approach to quantification is to first perform a point estimate using the mean values of the uncertainty distributions for the parameters. The results can be used to identify significant contributors and to reduce the amount of effort and computation required to propagate the uncertainty distributions in the final results.

4.1.4.1.1 Point estimate results. The point estimate results using four parametric models are presented in Table 4-10 in a "cause table" format. This format permits an examination of the major contributors that can be easily identified with the minimal cutsets of the logic model. Recall that the letters denote the component group in which the event occurred, the subscripts define how many components are failed by the event, and the exponents indicate several occurrences of the same type of basic event. Note that the B-factor results are special cases of the corresponding MGL results when all higher order parameters (i.e.,  $\delta$  and  $\gamma$ ) are set as equal to 1. Consequently, the terms corresponding to intermediate basic events (e.g.,  $V_3$ ) vanish. This, of course, is expected because the B-factor approach only recognizes CCF events that result in failure of all components within a common cause component. As can be seen, the results are dominated by the common cause terms, particularly the global common cause events that fail all three pumps ( $P_3$ ) and all four motor-operated valves ( $V_4$ ). In fact, less than 1% of the point estimate result is due to purely independent terms. The fact that more than 99% of the system unavailability is due to cutsets involving common cause events fully justifies the added complexity of incorporating these events into the logic model. Hence, failure to include common cause events in this systems analysis would have resulted in a two orders of magnitude error on the optimistic side of the correct result.

It is instructive to examine the results in light of the complexity that was added in Step 3.1 by the direct incorporation of the common cause events into the system fault tree. It is obvious from a comparison of Tables 4-5 and 4-10 that only a small number of terms in the system algebraic model are significant in the overall results. To get a picture of which kind of terms contributed to the

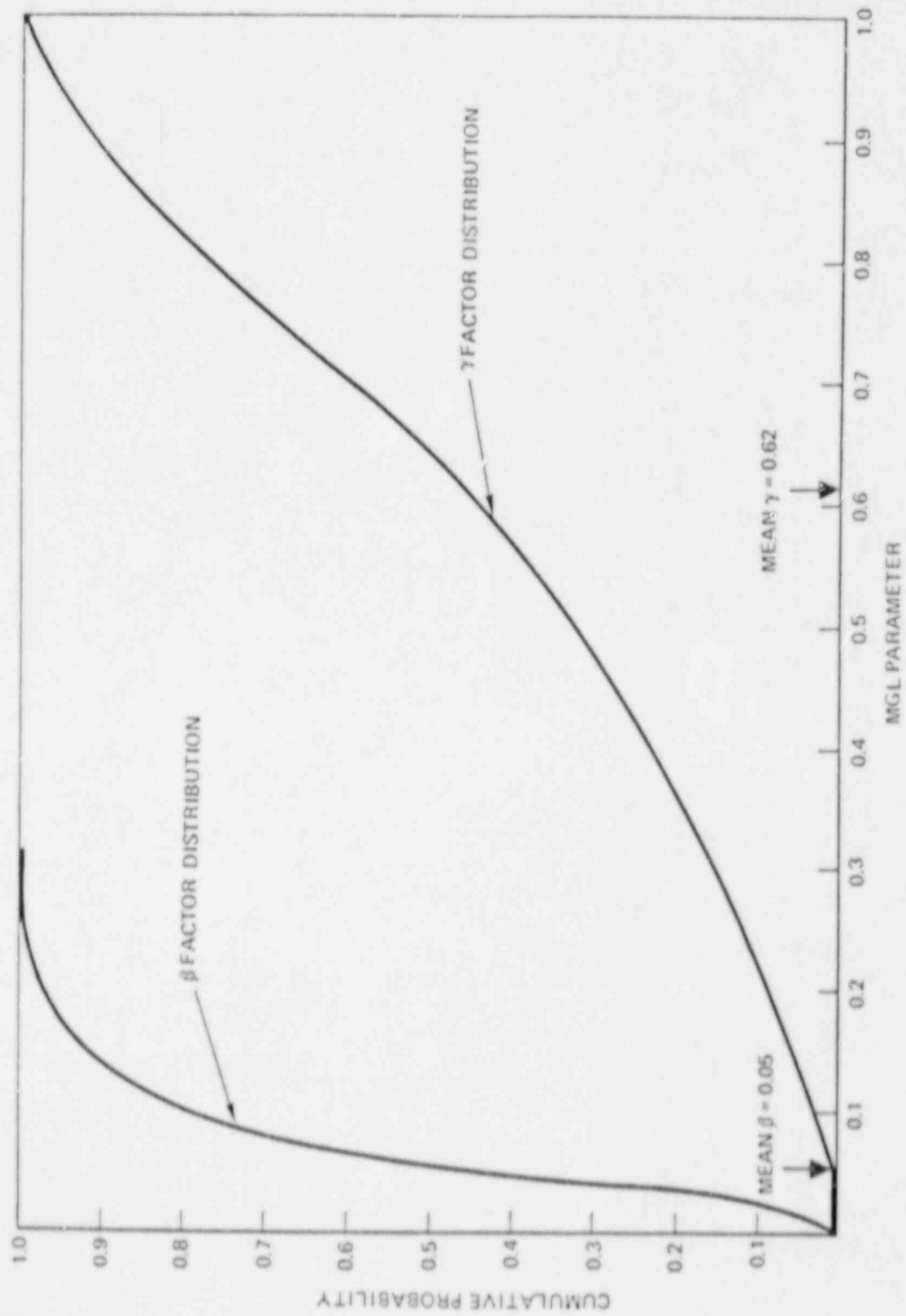


Figure 4-5. The Distribution of MGL Parameters for the EFW Pump (excluding driver)

Table 4-10

## SYSTEM QUANTIFICATION RESULTS BASED ON THREE PARAMETRIC MODELS

Algebraic Term	Basic Parameter Model	Multiple Greek Letter Model	Binomial Failure Rate Model	Beta Factor Model
$P_3$	5.5-4	4.2-4	6.5-4	8.8-4
$V_4$	3.8-4	3.7-4	4.1-4	6.2-4
$4V_3$	4.1-5	2.6-5	1.1-4	0
$M_2T$	1.8-5	1.1-5	1.8-5	1.1-5
$4P_2V_1$	3.4-6	2.8-6	1.2-6	0
C	2.3-6	2.3-6	2.3-6	2.3-6
$12V_2V_1$	2.0-6	2.0-6	2.6-6	0
Others	~ 2.0-5	~ 1.6-5	~ 2.0-5	2.7-5
Total	1.0-3	8.5-4	1.2-3	1.5-3

NOTE: Exponential notation is indicated in abbreviated form; i.e., 5.5-4 =  $5.5 \times 10^{-4}$ .

final results, an examination was made of each term in Table 4-5. This table includes 29 algebraic terms that cover the 129 minimal cutsets in the system fault tree. The smaller number of terms (29 versus 129) reflects the introduction of the symmetry assumption in Step 3.2, which results in grouping cutsets by frequency of occurrence in the algebraic terms.

The point estimates of the frequencies of all 29 terms in Table 4-5 were separately quantified using the MGL model and are plotted in Figure 4-6. The terms are first segregated by cutset order; then, categories are defined for each cutset order to enable the examination of six groups of terms, including:

1. First Order - Independent Event; e.g., C
2. First Order - Common Cause Event; e.g., V<sub>4</sub>
3. Second Order - Mixed Events; e.g., P<sub>1</sub> P<sub>2</sub>
4. Second Order - Common Cause Events; e.g., P<sub>2</sub> M<sub>2</sub>
5. Third Order - Independent Events; e.g., V<sub>1</sub><sup>3</sup>
6. Third Order - Mixed Events; e.g., V<sub>2</sub> M<sub>1</sub> T

Because of the particular logic of this problem, there were no fourth-order or higher order terms, no second-order independent event terms, and no third-order, purely common cause event terms.

The following distribution of failure frequency contribution (percent) was obtained when terms were grouped as in Figure 4-6.

Terms	Percent Contribution to Total Unavailability	
<u>First-Order Terms</u>	96.3	
1. Independent Events		0.3
2. Common Cause Events		96.0
<u>Second-Order Terms</u>	3.3	
3. Mixed Events		3.2
4. Common Cause Events		0.1
<u>Third-Order Terms</u>	0.4	
5. Independent Events		0.4
6. Mixed Events		<< 0.1
Total	100.	100.

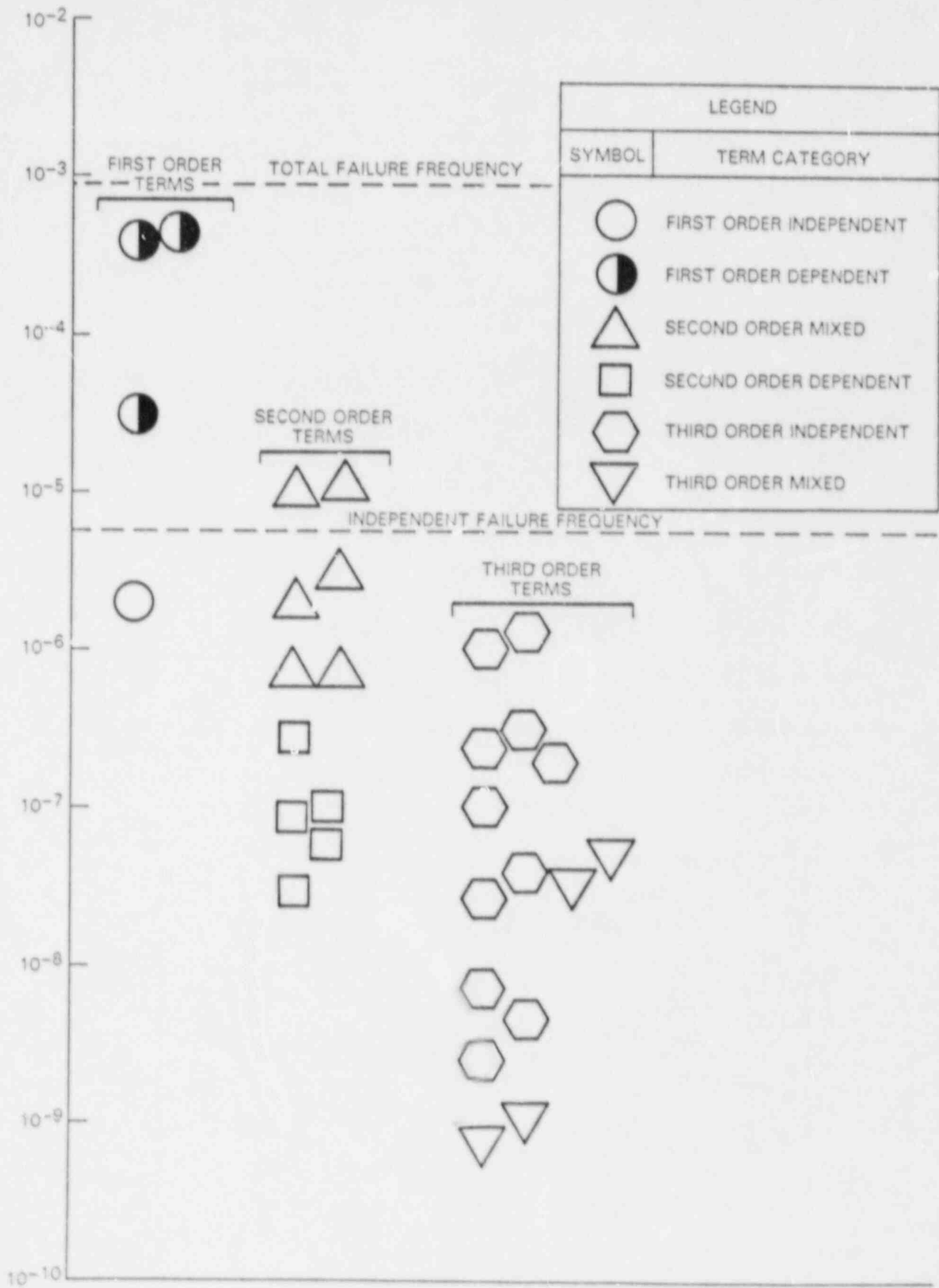


Figure 4-6. Relative Importance of Terms in AFWS Algebraic Model

Hence, more than 96% of the contribution comes from first-order cutsets, and most of this comes from common cause events.

As a class, the second-most important events were second order cutsets with one independent and one common cause event. The third ranking group was the third order cutset group with all independent events. From these results, the following observations can be made:

- System unavailability is dominated by far by first-order common cause events (these are the global CCF events). The first-order common cause events are about 25 times more likely to cause system failure than all other contributors combined.
- Most of the terms added by the common cause events have a higher frequency than most of the purely independent event terms.
- More than 99% of the total frequency is contained within two groups: number 2, first-order common cause, and number 3, second-order mixed events.
- With the exception of the first-order result, there is a tendency for the terms of order  $n$  to be dominated by the terms having the greatest number of independent events. This comes from the general rule that each common cause event tends to be less likely than each independent event.

The above insights may be useful to simplify the analysis of common cause events; i.e., limit the identification of minimal cutsets and the terms in the algebraic equations. Heuristic rules for a simplified analysis are discussed in Appendix F.

4.1.4.1.2 Uncertainty in system unavailability estimate. The uncertainty in system unavailability due to uncertainty in the numerical values used for the common cause model parameters can easily be obtained using one of the available techniques for uncertainty propagation (Reference 4-8). An uncertainty analysis, using a Monte Carlo sampling technique for the results obtained with the basic parameter and MGL methods, is presented in this section.

Uncertainties in the common cause parameters result from the following sources:

1. The size (or sparsity) of the data sample.
2. Uncertainty in the classification of data due to ambiguities and inaccuracies in the original event reports and in the interpretation of these reports for plant-specific applications.
3. Differences in system size and uncertainties about the sizes of systems in the data base.

4. Plant-to-plant variation relative to specific equipment, systems, and operating philosophy.
5. The selection of the type of probability distribution to represent the parameter; i.e., the modeling of one's state of knowledge about the values of these parameters, particularly in the choice of Bayesian priors when event data are sparse.

The first of these sources is a well-known subject in statistics. Access to a large set of failure and success data results in statistical estimates with a high degree of confidence simply because they are more representative of the general population. Due to sparsity of data, estimates of the common cause parameters are extremely sensitive to the judgments that are made during the process of data classification. As described in Sections 1 and 2 and in Appendix A, the concepts of functionally unavailable, potentially unavailable, incipient failure and degraded states play important roles in data classification, and their implementation relies heavily on analyst judgment. The uncertainty due to plant-to-plant variability stems from the fact that, for a variety of reasons, similar equipment and systems in various plants may exhibit different failure characteristics. These reasons include design differences within the same category of equipment and variation in system design and operating philosophy that result in different coupling mechanisms. In this analysis, the plant-to-plant variability is accounted for in the distributions for the total component failure frequencies ( $Q_T$ ). Uncertainties 2, 3, and 4 contribute to the overall uncertainty in the assignment of impact vectors when screening event data.

The fifth source of uncertainty involves the assumption that one needs to make regarding the appropriate mathematical form for representing the evidence. When significant data exist, "goodness-of-fit" techniques can be used to help the analyst objectively select a family of distributions based on the behavior of the data. Such techniques, however, are of little value when dealing with rare events. Most PRAs have used lognormal distributions for component failure rates but the gamma and beta distributions have also been used.

Figure 4-7 shows the uncertainty range of the total calculated system unavailability based on the basic parameter and the MGL models. There are certain aspects of the uncertainty that are not quantified in the uncertainties of the model parameters and thus are not represented in Figure 4-7. These include items 3 and 5 above. Item 2 has been accounted for in the mean values, but not in the dispersion of the distribution. For a more detailed discussion of the treatment of uncertainties, especially those stemming from impact vector assessment (items 2 and 3), the reader is referred to Appendix E.

4.1.4.2 Step 4.4 - Results Evaluation. The final step in the common cause analysis is the evaluation and interpretation of results. It is

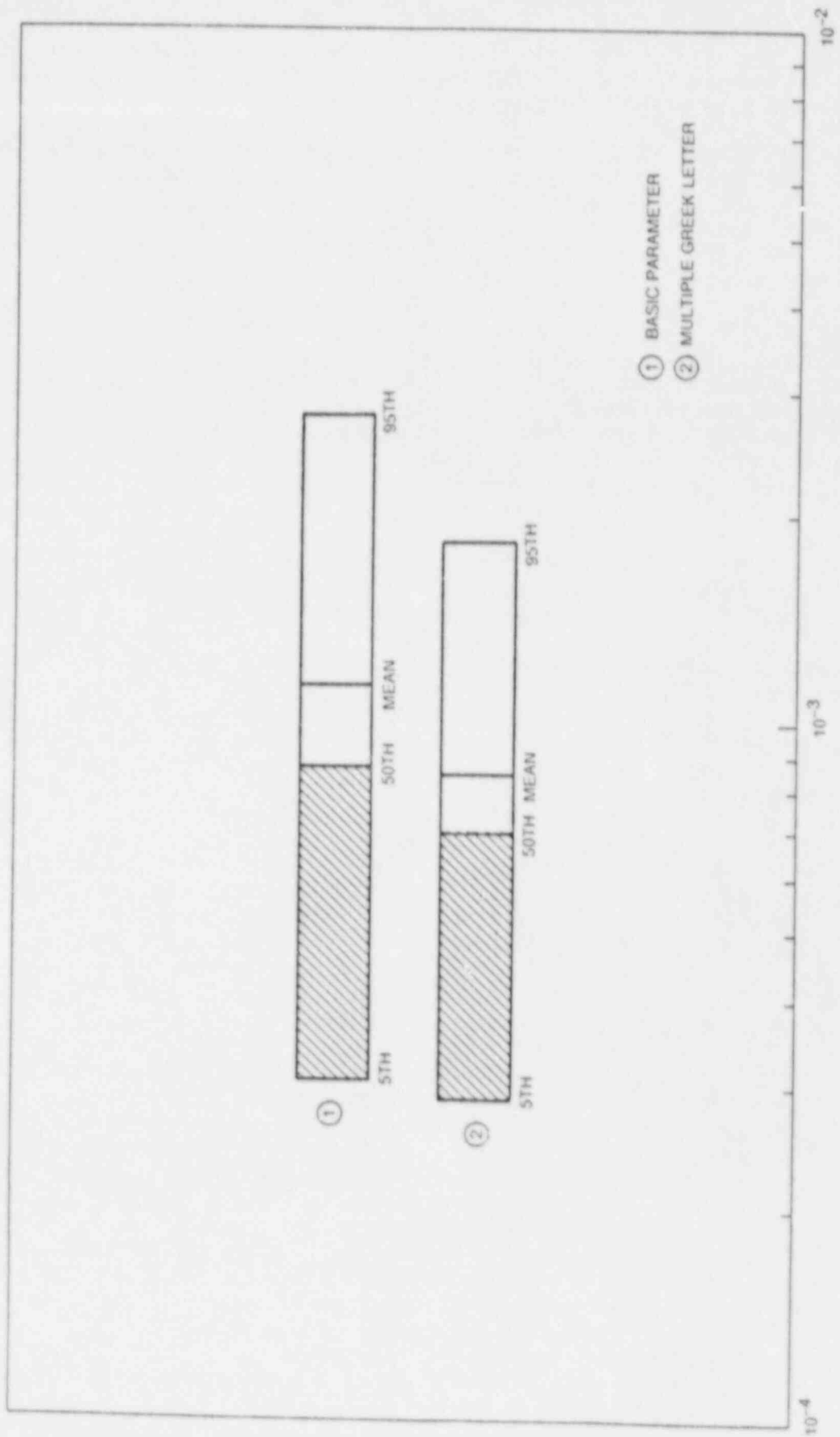


Figure 4-7. Uncertainty Range of the Example AFW System Unavailability



important to note that the good agreement among the three CCF models was made possible only through a consistent general framework for systems analysis and a consistent interpretation of the same underlying data base.

Interesting insights into these results can be obtained by rerunning the example problem twice, once assuming all three pumps in the system are motor-driven and once assuming the turbine-driven pump train is deleted from the original system. A comparison of these cases presented in Table 4-11 provides an indication of the benefits of redundancy and diversity. For comparison purposes, all three sets of results were obtained using the MGL method. In comparing the first two sets of results, it is seen that the net effect of pump driver diversity is a reduction in system unavailability by about 10%. This net effect reflects a reduction in common cause failure contribution of motor drives (the M<sub>3</sub> term) and an increase in the pump-driver failure rate in replacing an electric motor with a steam turbine driver. Not shown in this table is the added capability of the steam drive to operate without electric power, provided the motor-operated valves can be opened manually.

In comparing the second and third sets of results in Table 4-11, the benefits of the third train of redundancy are assessed to cause about a 50% decrease in system unavailability, much smaller than would be the case without consideration of common cause events.

It is important to recognize an important factor not shown in Table 4-11 that bears on the questions of the benefits of redundancy and diversity. The common cause data analysis that was performed in Step 3.3 evaluated the common cause data under the assumption that a common suction path for the redundant pump trains exists. A significant number of the common-cause events in the data base, particularly those for AFW pumps, would not have been common cause events in alternative designs with physically separated train and suction paths without crossties. For example, the events in the data base involving steam binding, air binding, and clogged strainers would not have affected more than one power train unless the suction paths were headered together or had shared a common source of steam or air leakage or debris clogging, as in the example system. Therefore, the conclusions drawn from Table 4-11 might have been different for designs with physically separated, redundant trains including separate suction paths and water supplies.

The three-train auxiliary feedwater system analyzed in this example is a rather typical configuration found in several existing U.S. power plants. The system was analyzed using U.S. industrywide experience data that were screened for applicability to a specific plant design. The results indicate that a realistic failure frequency for this system, when challenged with all support systems available, is about  $1 \times 10^{-5}$  per demand. Note that the results do not attempt to quantify the degree of plant-to-plant variability in AFWS reliability. Although the conclusions that are derived from these results are indicative of the type of results obtained in a common cause analysis, they strictly apply only to the example system. The results for this system are corroborated by three different parametric models: the basic parameter, MGL, and BFR (with lethal shocks) models. For the types of challenges considered (i.e.,

Table 4-11

COMPARISON OF CAUSE TABLES FOR THREE AUXILIARY FEEDWATER SYSTEMS  
IN NORMAL ALIGNMENT EVALUATED USING MGL MODEL

Two Motor-Driven; One Turbine-Driven (example system)		Three Motor-Driven		Two Motor-Driven (two steam generators per train)	
Contributor	Frequency	Contributor	Frequency	Contributor	Frequency
P <sub>3</sub>	4.2-4	P <sub>3</sub>	4.2-4	P <sub>2</sub>	8.0-4
V <sub>4</sub>	3.6-4	V <sub>4</sub>	3.6-4	V <sub>4</sub>	3.6-4
4V <sub>3</sub>	2.5-5	M <sub>3</sub>	9.5-5	M <sub>2</sub>	1.9-4
M <sub>2</sub> (P <sub>1</sub> + T)	1.1-5	4V <sub>3</sub>	2.5-5	4V <sub>1</sub> (P <sub>1</sub> + M <sub>1</sub> )	4.7-5
4V <sub>1</sub> (P <sub>1</sub> + T)(P <sub>1</sub> + M <sub>1</sub> )	2.7-6	4P <sub>2</sub> V <sub>1</sub>	2.8-6	(P <sub>1</sub> + M <sub>1</sub> )(P <sub>1</sub> + M <sub>1</sub> )	9.8-6
C	2.3-6	C	2.3-6	C	2.3-6
12V <sub>2</sub> V <sub>1</sub>	1.9-6	12V <sub>2</sub> V <sub>1</sub>	1.9-6	12V <sub>2</sub> V <sub>1</sub>	1.9-6
Others	~ 2.0-6	Others	~ 4.0-6	Others	~ 1.0-6
Total	8.2-4	Total	9.1-4	Total	1.4-3
Common Cause/ Total	.996	Common Cause/ Total	.997	Common Cause/ Total	.958

NOTE: Exponential notation is indicated in abbreviated form; i.e., 4.2-4 =  $4.2 \times 10^{-4}$ .

those with all support systems available), it is apparent that the incremental benefit of the third level of redundancy for pump trains is much smaller than would be indicated if common cause events had been ignored. Although the use of a steam-driven pump provides a capability to operate during loss of AC power scenarios, its benefits in terms of added diversity for scenarios in which all support systems are available are, in fact, mostly offset by the added unreliability of a steam turbine drive versus a motor drive. This observation is very dependent on the fact that, with this design, the advantages of redundancy and diversity are masked by the contribution of common cause events. It is important to note that this conclusion may have been much different for designs that employ fully separated pump trains. A significant number of the pump and valve common cause events in the data base would have been independent events in systems with physically separated pump trains without common suction and supply headers. The data would need to be reclassified to examine the implications of physical separation as a defense against common cause events.

#### 4.2 DC ELECTRIC POWER SYSTEM SAMPLE PROBLEM

This section applies the systematic procedures discussed in Section 3 to a second sample problem. The example used in this demonstration is the 125/250V DC system that serves a two-unit nuclear power station. This section emphasizes a detailed engineering analysis of a specific core damage scenario in Unit 2 involving the 125/250V DC power system. The scenario is characterized by transients leading to station blackout (loss of all AC power) or substantial degradation of the AC power system as a result of coincident failures in the 125/250V DC power system. A complete loss of the 125/250V DC power system causes loss of the EDGs, the HPCI system, the RCIC system, and the depressurization system. Loss of these systems causes a loss of all core and containment cooling and, without recovery, would lead to core damage.

##### 4.2.1 Stage 1: System Logic Model Development

This section is limited to identifying and quantifying CCFs that can occur within the 125V DC power system. Independent failures of equipment within redundant power divisions are not addressed because it has been shown that they contribute negligibly to the total severe core damage frequency of the plant (Reference 4-2).

4.2.1.1 Step 1.1 - System Familiarization. The 125/250V DC power system consists of four (two per unit) 125/250V DC power divisions, as illustrated in Figures 4-3 and 4-9. The four power divisions provide four physically separated sources of 250V DC power (buses 2AD10, 2BD18, 3AD10, and 3BD18) and eight physically separated sources of 125V DC power (buses 20D21, 20D22, 20D23, 20D24, 30D21, 30D22, 30D23, and 30D24). The

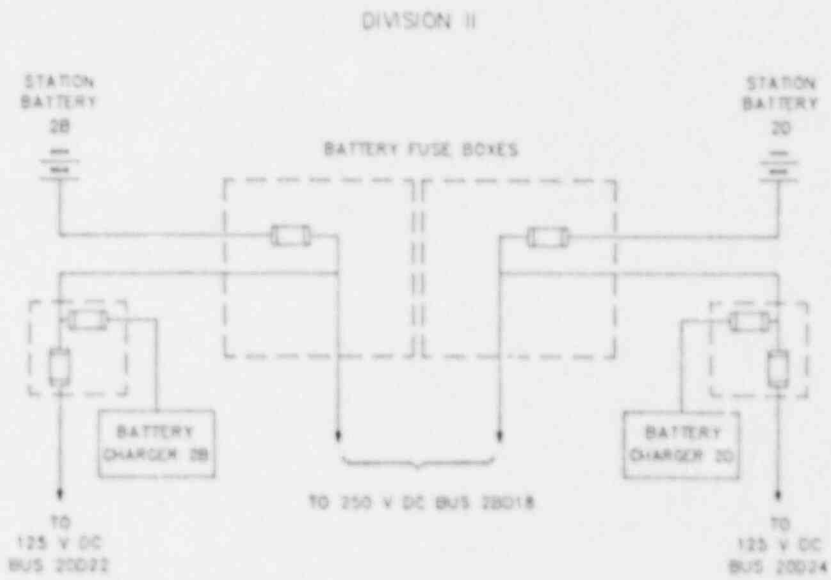
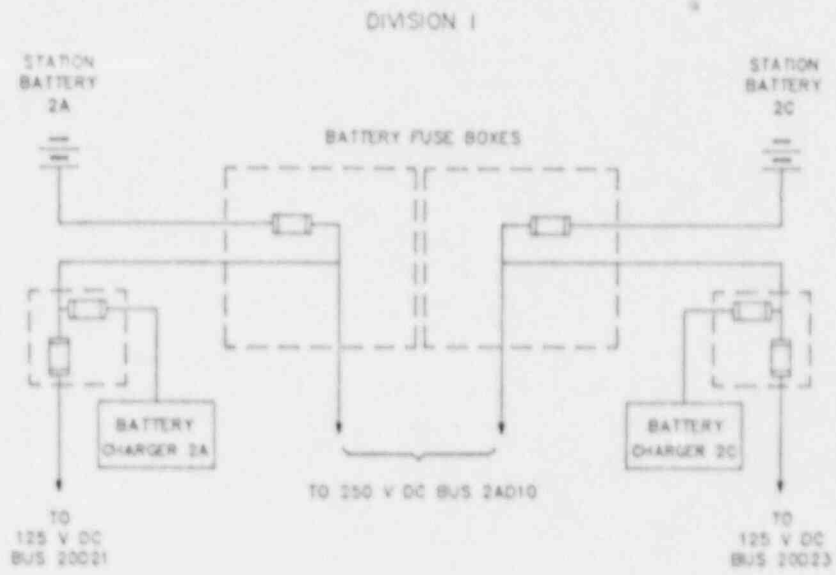


Figure 4-8. Simplified Schematic of 125/250V DC Power System - Unit 2

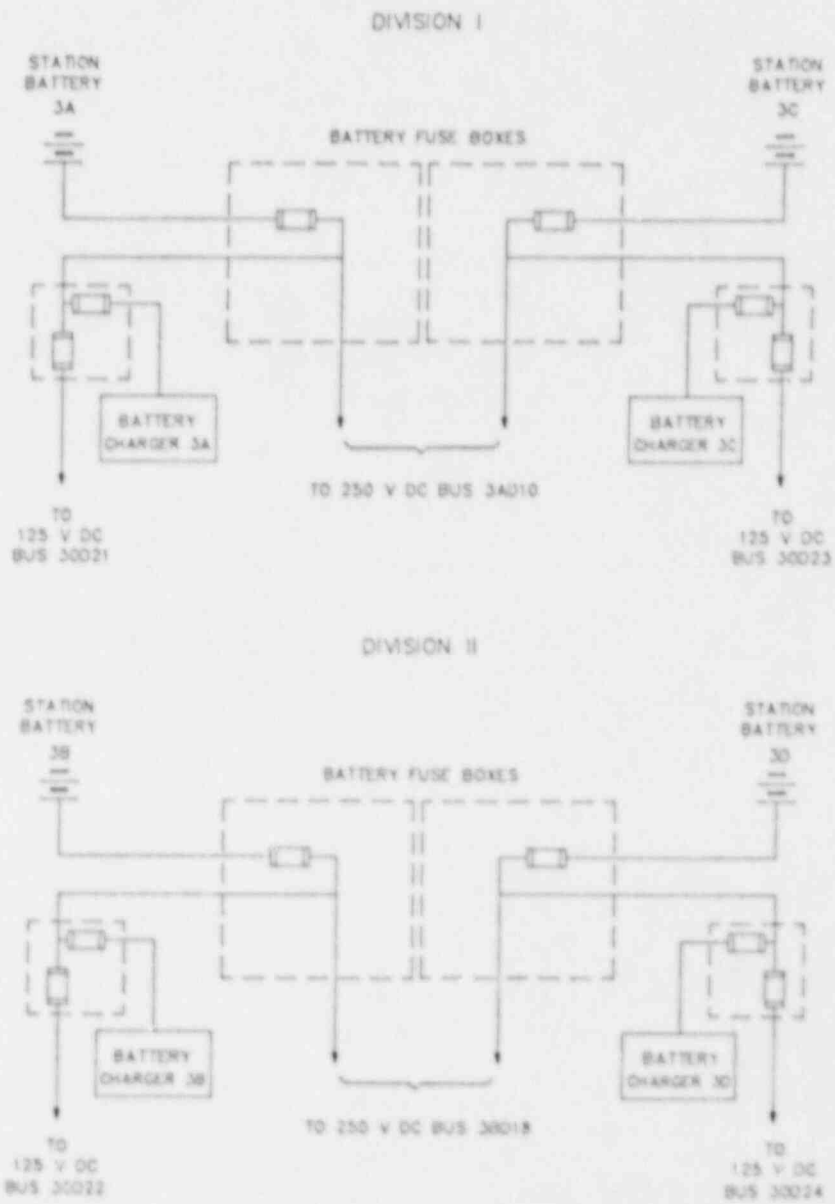


Figure 4-9. Simplified Schematic of 125/250V DC Power System - Unit 3

125V DC buses power some safety-related equipment, including the starting and loading of the four EDGs, as shown in the table that follows.

EDG (total of four EDGs serving both units)	125V DC Bus
EDG 1	20D21
EDG 2	20D22
EDG 3	30D23
EDG 4	30D24

The 250V DC buses serve larger loads, such as DC motor-driven valves in the HPCI and RCIC systems. All DC power divisions operate ungrounded, with a ground detector alarm in the main control room. The main control room is also equipped with trouble alarms for each battery charger and with undervoltage alarms for each DC power bus.

Table 4-12 shows the systems procedures and surveillance test procedures that are applicable to the 125/250V DC power system. The battery chargers are routinely inspected during operation for excessive heat and for proper output voltage. Each station battery undergoes a weekly check that includes measuring and recording the specific gravity, temperature, and voltage of the pilot cell in addition to measuring and recording the terminal voltage of the battery. Each station battery also undergoes a quarterly check that includes measuring and recording the voltage and specific gravity of each cell, and measuring and recording the temperature of every fifth cell in the battery. The battery terminal voltage and the charger output voltage are also recorded at this time. Other checks performed during the quarterly check are room temperature; ventilation system; general condition of the battery racks, posts, and connectors; and battery charger output current. The quarterly checks are performed at staggered intervals, as indicated in Figure 4-10. Station batteries 2A and 2C are tested on the same day, station batteries 2B and 2D are tested about 1.6 weeks (an eighth of a quarter) later, and so on. As the figure indicates, the quarterly check of the 24/48V DC batteries is also staggered with the station battery checks. (The 24/48V DC batteries are not analyzed in this section.)

Each station battery undergoes a capacity test during every refueling outage. This is accomplished through either a performance test (every third refueling outage) or a service test (all other refueling outages). In both of these capacity tests, the batteries are discharged until the terminal voltage drops to 105V. In the performance test, the battery discharge current is kept constant at 800 amps, while, in the service test, the current is adjusted to verify the ability of the battery to satisfy the design requirements of the DC system (the maximum current demanded from the battery is 650.2 amps in the first minute).

Table 4-12

SYSTEMS AND SURVEILLANCE TEST PROCEDURES APPLICABLE  
TO THE 125/250V DC POWER SYSTEM

Procedure Identification Number	Procedure Title
1	Routine Inspection of Battery Chargers
2	Station Battery Weekly Check
3	Station Battery Quarterly Check
4	Station Battery Service Test
5	Station Battery Performance Test
6	Loss of 125V Station Battery Charger
7	Startup of Battery Charger
8	Shutdown of Battery Charger
9	Loss of AC Feed to a 125V Battery Charger
10	Procedure for Investigating DC Battery Grounds
11	Procedure for Reducing and Isolating Unnecessary DC Loads Following Station Blackout

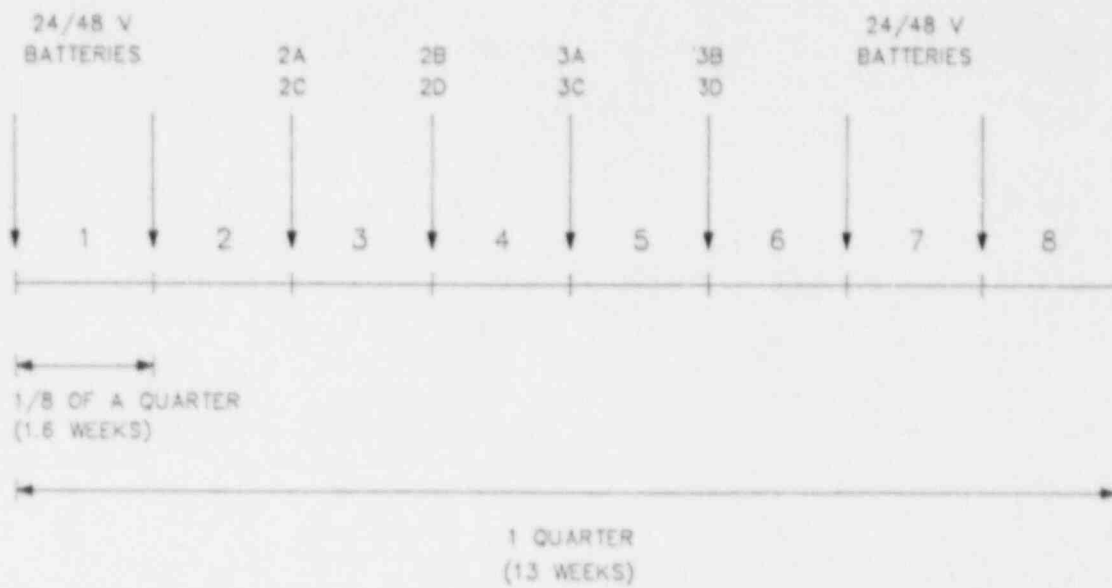


Figure 4-10. Staggered Intervals for Quarterly Checks on Station Batteries and 24/48V Batteries



4.2.1.2 Step 1.2 - Problem Definition. This sample problem analyzes the 125/250V DC system in the context of a specific core damage scenario in Unit 2 characterized by transients leading to station blackout (loss of all AC power) or substantial degradation in the AC power system as a result of coincident failures in the 125/250V DC power system. The initiating event is an LOSP or another transient event followed by LOSP. Following LOSP, the four EDGs should automatically start and load on the corresponding AC buses (there are four AC buses per unit that are fed by the common four EDGs). The DC buses 20D21, 20D22, 30D23, and 30D24 provide the necessary DC power to start and load EDGs 1, 2, 3, and 4, respectively. The inability of a DC bus to provide enough power to start and load an EDG results in the loss of that EDG.

If the EDGs start and load successfully, they energize the corresponding battery chargers and the station batteries are then no longer needed (unless additional failures develop). Therefore, the CCFs of interest in this example are those that result in failure to start and load the EDGs. The core damage scenario analyzed in this example is based on coincident failures in the 125/250V DC power system that result in (1) direct loss of HPCI, RCIC, and reactor depressurization systems or (2) loss of sufficient safety-related systems to prevent core cooling following reactor depressurization. In either case, loss of core cooling capability would result in core damage in about 30 to 40 minutes. The coincident failures in the 125/250V DC power system cause at least two EDGs (in case 1) or three EDGs (in case 2) to fail to start and load.

The success criteria for the 125/250V DC power system is difficult to specify. This is a result of the complex dependencies of the several systems on AC and DC power, and the complex interdependencies within the AC and DC power systems. For example, the ADS requires DC power from either DC bus 20D21 or 20D24 (all ADS valves would fail closed if both buses were unavailable). The AC feed to battery charger 2D, however, comes from an AC bus that is dependent on EDG 4 if offsite power is lost. EDG 4 gets starting and loading DC power from bus 30D24. Therefore, if offsite power is lost, failure of both station batteries 2A and 2D would not by itself cause failure of the ADS, but a failure of all three of station batteries 2A, 2D, and 3D is sufficient to cause complete loss of the ADS.

As another example, all EDGs are cooled by two ESWS trains and by one ECWS train. Loss of cooling from all three trains results in EDG failure within a few minutes. The motor-driven pump in each train is powered by EDG 2, 3, or 4, respectively, when offsite power is lost (EDG 1 is not used to power either ESWS or ECWS). Thus, LOSP followed by a failure of station batteries 2B, 3C, and 3D would result in failure to start EDGs 2, 3, and 4 and eventually would lead to the loss of EDG 1 even if station battery 2A remains available to start and load EDG 1.

Although the success criteria for the 125/250V DC power system depend on the systems that require DC power, a detailed analysis of all accident sequences involving LOSP revealed that, following LOSP, at least three station batteries must fail to result in core damage (barring any additional failures). Also, at least one of the station batteries is in

a different unit from the others (this fact is important for quantification purposes in the following analysis steps). Therefore, this example focuses on failure events within the DC power system that would result in failure or functional unavailability of specific combinations of three station batteries.

4.2.1.3 Step 1.3 - Logic Model Development. Figures 4-11 and 4-12 present component-level fault trees for station battery failure contributions to two core damage scenarios considered here. The first scenario involves batteries 2A, 2D, and 3D; the second requires failure of batteries 2B, 3C, and 3D. In this fault tree, "station battery" represents both the battery and the associated fuse box.

#### 4.2.2 Stage 2: Screening of Common Cause Component Groups

4.2.2.1 Step 2.1 - Qualitative Screening. The preliminary effort consisted of identifying important root causes and coupling mechanisms of component failures and defining the groups of components that are susceptible to each root cause of failure. This was accomplished through a detailed review of all LERs covering the period from early 1969 through mid-1986 and a review of previous studies on similar systems (References 4-9 through 4-11 and other unpublished studies). This preliminary effort indicated three general fault categories that must be addressed in this analysis. These general fault categories encompass all mechanisms that could result in failure or functional unavailability of one or more station batteries within the context of this analysis:

- Battery-Related Faults - This category includes battery internal faults, terminal connection faults, battery fuse faults, maintenance downtime, etc.
- Battery Charger-Related Faults - This category includes overcharging and undercharging conditions of the battery.
- Bus Alignment Faults - This category includes battery functional unavailability due to misalignment within the DC power system.

These faults were analyzed to determine combinations of root causes and component groups of interest in the CCF analysis. Three types of root cause and component group combinations must be addressed: type 1 consists of root causes that primarily affect similar equipment, type 2 consists of root causes that affect equipment operated according to the same procedures, and type 3 consists of root causes that affect equipment in the same location.

Table 4-13 summarizes the root causes and component group combinations initially identified for additional analysis. All causes of battery charger (including fuses) faults are potential CCFs of interest because of the similarity of the equipment in all DC power buses (the first five combinations in Table 4-13). In addition, the equipment addressed by each of the procedures numbered 6, 9, 10, and 11 in Table 4-12 will be considered a type 2 combination in this task (the last four combinations in Table 4-13). This permits the investigation of such possibilities as

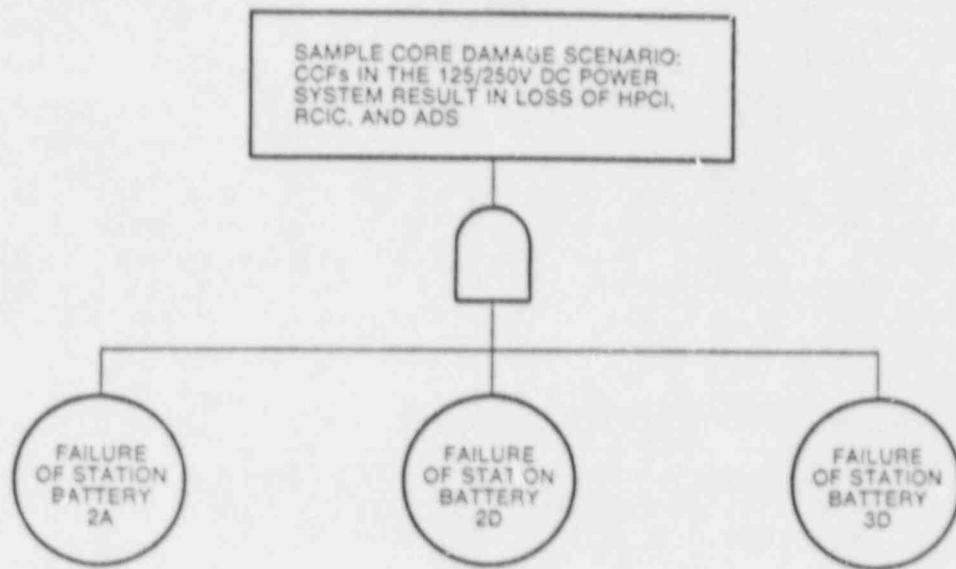


Figure 4-11. Fault Tree for Core Damage Scenario: CCFs in the 125/250V DC Power System Result in Loss of HPIC, RCIC, and ADS

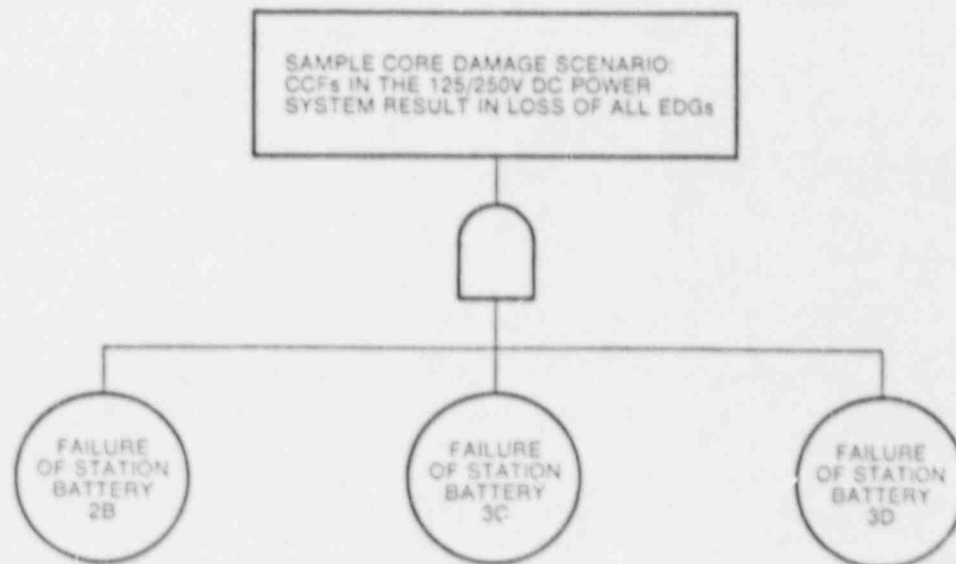


Figure 4-12. Fault Tree for Core Damage Scenario: CCFs in the 125/250V DC Power System Result in Loss of All EDGs

Table 4-13

ROOT CAUSE AND COMPONENT GROUP COMBINATIONS  
INITIALLY DEFINED FOR THE 125/250V DC POWER SYSTEM

Combination Identification Number	Root Cause of Interest	Affected Equipment	Type of Combination
1	All Causes*	Station Batteries	1
2	All Causes*	Battery Fuses	1
3	All Causes*	Battery Chargers	1
4	All Causes*	Battery Charger Fuses	1
5	All Causes*	125V Bus Fuses (in the same fuse box with the battery charger fuses)	1
6	Errors Committed Following Loss of a Station Battery Charger(s)	Equipment Addressed in Procedure 6:** All Breakers in Corresponding 125V DC Bus	2
7	Errors Committed Following Loss of Feed to Battery Charger(s)	Equipment Addressed in Procedure 9:** Alternate Feed Breakers plus All Equipment Addressed in Procedure 6	2
8	Errors Committed during Investigation of Battery Ground(s)	Equipment Addressed in Procedure 10:** a Number of Annunciator Feeds in the Corresponding Power Division	2
9	Errors Committed in Isolating DC Loads Following Station Blackout	Equipment Addressed in Procedure 11:** Most Breakers in the DC Power System	2

\*Similar components are usually affected by certain commonalities (similar installation, maintenance, and testing procedures and common design and manufacturing processes) that permit multiple failures due to repeated human errors. Therefore, all causes of component failures are potential causes of CCFs.

\*\*Procedures are described in Table 4-12.

inadvertently disabling a bus when following a procedure that calls for removing unavailable equipment from a DC power bus. Another type 2 possibility that must be considered at power plants with crosstie breakers between the DC power buses is an error committed when the buses are crosstied (a possibility mentioned for illustrative purposes only since the plant considered here has no crosstie breakers in its DC power system). Finally, with respect to type 3, root causes that affect equipment in the same location, no harsh environments (e.g., fires, floods, and explosions) were identified that could affect more than one station battery. Therefore, no type 3 root cause and component group combinations were identified in this sample problem. The nine root cause and component group combinations in Table 4-13 will now be analyzed in detail.

4.2.2.1.1 Root cause and component group combination 1 - station batteries. The causes of battery failures include internal faults and faults associated with the terminal connection detail (connections made between rows of cells or at the positive and negative terminals of the battery). Terminal connection detail faults generally result from corrosion at the connection interface or from improper torquing of the fasteners during installation. The likelihood of this failure mechanism is directly related to the quality of the plant checking, testing, and maintenance program.

Most internal faults take the form of gradual degradation (Reference 4-12). They may be related to the electrolyte (contamination or stratification), to the grid (loss of conductive path for the reaction current), to the active material (loss of contact and falling away from the plate), to the jar (loss of electrolyte), and to several others. These degradation mechanisms slowly build up to a point at which they could result in a catastrophic failure or in highly degraded battery performance. However, they are generally revealed by the quarterly checks, performance tests, or service tests. Therefore, actual battery failures due to internal faults are also related to the quality of the checking, testing, and maintenance program of the plant.

Another possible cause of battery unavailability is unscheduled maintenance. Unscheduled maintenance activities are generally started when discrepancies (e.g., a low specific gravity on a cell and a subsequent failure to hold a charge) are detected during the weekly and quarterly checks or during the refueling performance tests and service tests. According to plant personnel, the station batteries are not made inoperable for unscheduled maintenance. The practice of the plant consists of bypassing (jumping out) the affected cells to perform the necessary actions. Thus, the station battery remains operable during this time, and battery unavailability due to unscheduled maintenance is considered a negligible contributor to overall battery unavailability.

Root cause and component group combination 1 is to be retained for further analysis, and the fact that these root causes of battery failure are strongly associated with the checking, testing, and maintenance program should be emphasized. (This fact is crucial to quantification purposes in the following analysis steps.)

4.2.2.1.2 Root cause and component group combination 2 - battery fuses. A station battery can become functionally unavailable due to the spurious opening of the corresponding fuse either before or when the battery is demanded. However, the station battery fuse is a 1,200 amp fuse, which is substantially higher than the current expected from the battery under any circumstances. Any current strong enough to blow the battery fuse would cause noticeable disturbances in the DC power bus, including activation of the undervoltage relay. Thus, in the unlikely event of failure of a fuse due to operational abnormalities, such a failure would be self-announced and is therefore not significant to this study.

The only root cause of concern involving battery fuses would be failure mechanisms that might develop during the long time period (18 months) between refueling outages during which the fuse is subjected to only a small floating current. If a degradation mechanism (e.g., corrosion or contamination) builds up internally or at the fuse external contacts, a catastrophic failure may result (due to the heat generated at poor connections) when a high battery current is imposed on the battery fuse following an LOSP.

This root cause and component group combination is also to be retained for further analysis, with the stipulation that only one specific failure mechanism is of concern--a mechanism that might develop during the long time period between refueling outages. This same concern does not exist for battery charger fuses and 125V bus fuses (both in the same fuse box illustrated in Figures 4-8 and 4-9) because these fuses are constantly subjected to higher currents; therefore, their failure would be more readily announced.

4.2.2.1.3 Root cause and component group combination 3 - battery chargers. There are two basic types of battery charger-related failures to be addressed: (1) battery charger-related failures that result in degradation (undercharging condition) of the station batteries and (2) battery charger-related failures that result in damage of the station batteries due to an overcharging condition. These two types of failures are most likely to occur in the FLOAT and EQUALIZE modes, respectively.

Battery charger-related failures that could result in degradation of the station batteries include battery charger hardware failures, battery charger AC input and DC output circuit breaker faults (these include circuit breaker hardware failures as well as spurious opening of the circuit breaker by an operator), and failure to recharge the battery following battery charger maintenance. Battery charger hardware failures and circuit breaker faults are announced in the control room by a battery charger trouble alarm or, if the voltage on the DC bus drops below 115V, by an undervoltage alarm. On loss of a battery charger, the station battery serves all of its DC loads. After some time, the battery will discharge so that it is able to handle LOCA loads only; e.g., HPCI and RCIC systems. The time required to reach this condition is at least 12 hours and is extended by removing nonvital DC loads from the bus (the nonvital DC loads to

be disconnected are tabulated in Procedure 6, Table 4-12). If the charger is not recovered by this time, the operator has two options, as required by the technical specifications: (1) declare the battery system inoperable and shut down the plant, or (2) disconnect the LOCA loads and declare the RCIC (for batteries 2A or 2C) and/or the HPCI (for batteries 2B or 2D) inoperable. In this case, the battery system remains operable for an additional 24 hours.

In addition, a standby charger is available for each unit to supply the corresponding DC load in case one of the four dedicated battery chargers fails. Utility personnel indicated the operator would attempt to recover a troubled charger first. Then, if recovery is not successful, he would bring in the standby charger.

The technical specifications prevent the utility from operating the reactor with one or more station batteries in a condition that would make them incapable of starting and loading the EDG. In addition, the removal of nonvital DC loads from the DC bus and the availability of a standby charger make this loss of starting and loading capability very unlikely. Thus, battery charger-related failures that result in degradation of the station batteries are negligible contributors to battery unavailability.

Battery charger-related failures due to overcharging conditions can also result in damage to the station batteries. An equalizing charge is applied to each station battery following performance tests or service tests during refueling outages. Otherwise, an equalizing charge is applied only on an "as needed" basis. The equalizing charge is applied directly from the dedicated battery charger, and the charger simultaneously supplies DC power to the respective buses. The station battery is available to supply the DC loads during the equalizing charge period. (No realignment is needed if the charger trips or if offsite power is lost.) Thus, no downtime exists during the equalizing period, and no unavailability results from misalignment errors during the same period.

Also, when the battery charger is started following a performance test or a service test, it will automatically begin charging in the EQUALIZE mode. If the charger is operating in the FLOAT mode, it may be manually transferred to the EQUALIZE mode by momentarily moving the mode switch to the EQUALIZE position. In either case, once the battery charger is in the EQUALIZE mode, it automatically charges at the appropriate charging rate, continues charging for 72 hours, and then automatically shifts to the FLOAT mode. In addition, whenever the charger is put into the EQUALIZE mode, an operator is required to check that the charger output voltage is adequate. Any battery charger hardware failure (e.g., a very high output voltage) is detectable by the operator. Operator-induced failures are unlikely because no adjustments are required by the operator. Also, a complete check of the voltage and of the specific gravity of each cell is performed following the outage discharge test (performance test or service test), and the weekly and quarterly checks are very effective in detecting damage due to overcharging. Therefore, damage due to overcharging conditions is both very unlikely and easily

detectable. Battery charger-related failures that result in damage to a station battery due to overcharging conditions are thus also negligible contributors to battery unavailability.

In summary, all causes of battery charger-related failures have been analyzed and deemed unimportant with respect to other failure modes for the station batteries. Root cause and component group combination 3 is therefore discarded.

4.2.2.1.4 Root cause and component group combinations 4 and 5 - battery charger fuses and 125V bus fuses. These two root cause and component group combinations are similar to combination 2 (battery fuses). However, the battery charger and 125V bus fuses are constantly subjected to high currents (e.g., during testing of RCIC and HPCI systems), and the concern raised for the station battery fuses is not applicable here. These root cause and component group combinations are discarded in this task.

4.2.2.1.5 Root cause and component group combinations 6 and 7 - equipment addressed in Procedures 6 and 9. Loss of a station battery charger or loss of AC feed to the battery charger can lead to degradation (undercharging condition) of the corresponding station battery. This possibility has been analyzed in connection with root cause and component group combination 3, battery chargers. Some additional possibilities are examined now with emphasis on errors that may be committed when performing Procedure 6 or 9. For example, operational experience with other U.S. nuclear power plants shows instances in which a station battery was mistakenly removed from a DC power bus when attempting to remove an inoperable battery charger from the bus.

The station batteries at the subject plant do not have circuit breakers connecting them to the DC buses. The only elements between the station batteries and the 125V DC buses are the fuses, as indicated in Figures 4-8 and 4-9. The fuses at this plant are not used as switches to isolate equipment, as has been done at some other U.S. plants. Thus, it is reasonable to disregard the possibility of misalignment of one or more station batteries.

Procedure 6 does call for opening circuit breakers to some nonvital DC loads, and some of these circuit breakers are on the same 125V DC buses that feed the EDGs and the depressurization systems. It is conceivable that an operator would mistakenly open the circuit breakers to an EDG or to a depressurization system when following Procedure 6. Table 4-14 shows the nonvital DC loads that are disconnected from 125V DC power buses, as required by Procedure 6. These loads are removed from the respective buses only if the associated battery charger fails.

The misalignment of circuit breakers when performing Procedure 6 or 9 can only be triggered by an inoperable battery charger or by a loss of feed to a battery charger (Procedure 9 does not directly call for opening circuit breakers, but, if the alternate AC feed is



Table 4-14

NONVITAL DC LOADS THAT ARE DISCONNECTED  
FROM THE 125V DC BUSES  
AS REQUIRED BY PROCEDURE 6

125V DC Bus	Nonvital DC Load Description
20021	None
20022	Maintenance Shop DC Feed
20023	SAMAC Inverter
20024	Laboratory DC Feed
30021	None
30022	None
30023	None
30024	Remote Computer Data Terminal

unavailable, Procedure 9 does call for performing Procedure 6). The spurious opening of circuit breakers in different DC power buses, therefore, must be triggered by multiple battery charger failures. The CCF potential associated with root cause and component group combinations 6 and 7 is judged to be low for the following reasons:

- Operational experience supports the contention that battery charger failures are generally independent.
- The probability of opening a wrong circuit breaker in a bus is independent of having made a similar mistake in a previous bus.
- Root cause and component group combinations 6 and 7 would not affect buses 20D21 and 30D23. As Table 4-14 shows, buses 20D21 and 30D23 are not addressed by Procedure 6; therefore, even if the operator makes a mistake in every 125V DC power bus addressed in Procedure 6, the depressurization systems would have DC power available from bus 20D21, and EDGs 1 and 3 would have DC power available from buses 20D21 and 30D23, respectively. The availability of these buses would preclude the core damage scenario of interest in this sample problem.

Root cause and component group combinations 6 and 7 are eliminated from further analysis.

4.2.2.1.6 Root cause and component group combinations 8 and 9 - equipment addressed in Procedures 10 and 11. Root cause and component group combination 9 in Table 4-13 can be eliminated as inconsequential to further analysis because Procedure 11 would only be performed following LOSP and loss of the EDGs; i.e., following loss of all AC power. Examination of Procedure 10 reveals that troubleshooting and isolating DC battery grounds is accomplished by opening and then reclosing annunciation feeds. Since the procedure does not call for removing the battery, battery charger, circuit breakers, or fuses from their safety-related configuration, there is little chance of disabling equipment when performing Procedure 10. Thus, root cause and component group combination 8 may also be eliminated from further analysis. Table 4-15 presents the root cause and component group combinations that are to be analyzed further.

The conclusion of this screening analysis is that there are only two component common cause groups that need to be analyzed in the subsequent steps. These are: (1) station batteries and (2) battery fuse boxes.

4.2.2.2 Step 2.2 - Quantitative Screening. At this point, the number of common cause component groups and the overall logic model are small enough to not require any quantitative screening. Therefore, this step of the procedure is not taken.

Table 4-15

ROOT CAUSE AND COMPONENT GROUP COMBINATIONS IDENTIFIED IN STEP 3  
AND DESIGNATED FOR FURTHER ANALYSIS

Combination Identification Number	Equipment Description	Comments
1	Station Batteries (includes internal faults and faults associated with terminal connection detail)	These root causes of battery failure are strongly associated with the checking, testing, and maintenance program.
2	Battery Fuses	The root causes of concern are failure mechanisms that might develop during the long time period (18 months) between refueling outages.

4-15

### 4.2.3 Stage 3: Common Cause Modeling and Data Analysis

4.2.3.1 Step 3.1 - Definition of Common Cause Basic Events. The CCFs within the 125V DC power system were incorporated directly into the system fault trees of Figures 4-11 and 4-12 by simply expanding each of the components of the component-level fault tree, using a two-input OR gate as shown in Figure 4-13. One input is a basic event that represents the CCF of the batteries, and the other is the independent contributor to component unavailability. This is a conservative representation since it assumes all common cause failures are global within the three batteries modeled.

In this expansion of the fault tree, global CCF events of battery fuses are combined with the global battery CCF events for simplicity of presentation. Similarly, the independent events of batteries and fuses are lumped.

4.2.3.2 Step 3.2 - Selection of Probability Models for Common Cause Basic Events. Consistent with the logic model representation of the common cause events in the previous step, the beta factor model is selected for parametric modeling of the system. Therefore, the rate of the common cause basic events ( $\lambda_c$ ) of the extended fault tree (Figure 4-13) is quantified, using the following relation,

$$\lambda_c = 8\lambda_t \quad (4-23)$$

where  $\lambda_t$  is the total failure rate of the component.

4.2.3.3 Steps 3.3 - Data Classification and Screening. The estimation of parameters in this example problem is based on review of LERs covering the period from early 1969 through mid-1986 and a human reliability analysis. Each root cause and component group combination summarized in Table 4-15 will now be analyzed separately. In addition, selected failure events for the combinations that have been deemed unimportant will be presented for illustrative purposes.

4.2.3.3.1 Root cause and component group combination 1 - station batteries. A total of four events was identified for this category. These events are summarized in Table 4-16, which also shows their impact vectors. This impact vector application is simplified with respect to system size; i.e., the number of station batteries. The system size is assumed to comprise only three batteries because this is the minimum number of batteries involved in the scenario of interest. (The actual system size at the sample plant is eight, as indicated in Figures 4-8 and 4-9.) The impact vectors were assessed as

- Event 1. The event is a single failure of one of the two batteries at Fort St. Vrain. Therefore, the impact vector for that plant has a 1 under  $P_1$  and zero elsewhere, as shown in Table 4-16. The event is judged to be applicable to the sample system as an independent event. However, the sample system involves three

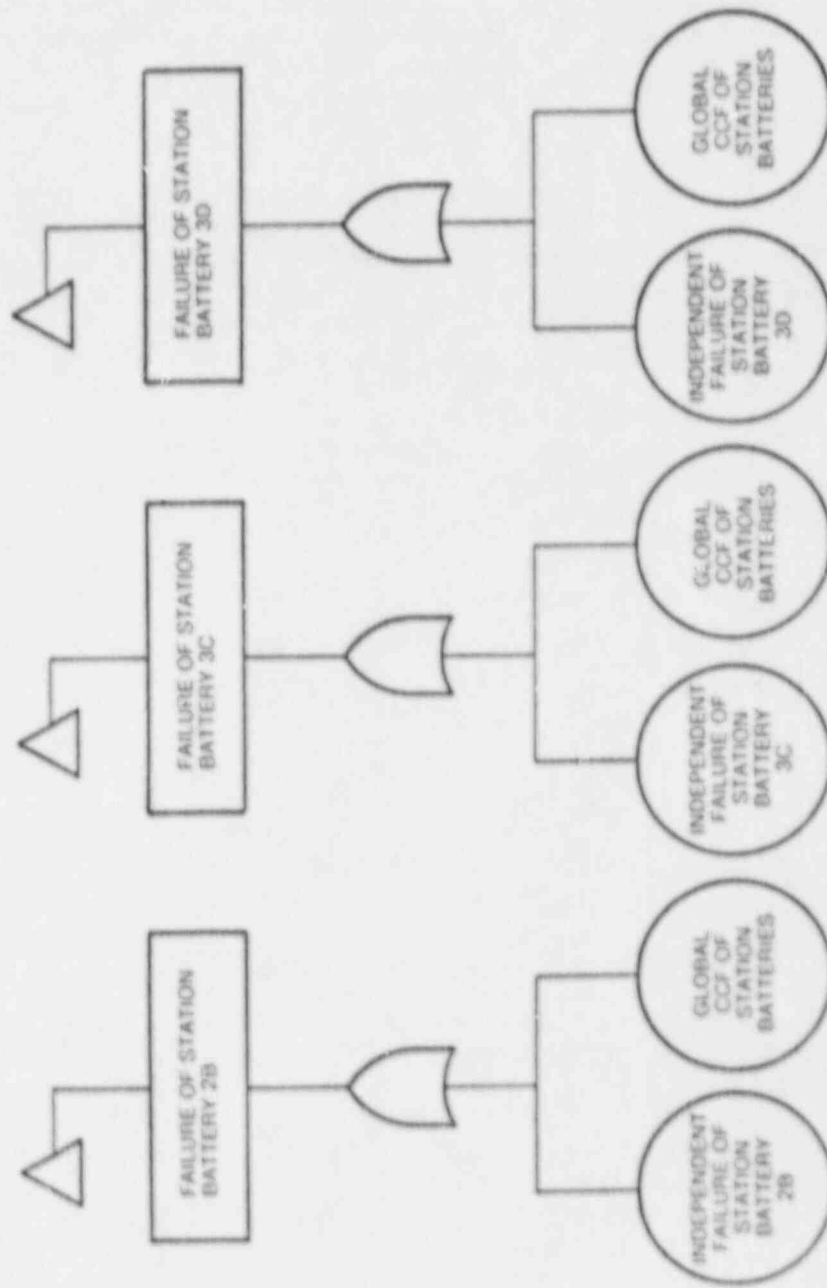


Figure 4-13. Extension of Sample DC Power System Fault Tree (Figure 4-12) To Incorporate CCF Events

batteries (system size = 3). Therefore, the original impact vector should be mapped up from system size 2 to system size 3. This is done using Eq. 3-24,

$$P_I^{(3)} = \frac{3}{2} P_I^{(2)} = 1.5$$

which is the corresponding expected number of independent events in the sample system.

Other elements of the impact vector for the sample system are zero, as shown in Table 4-16.

- Event 2. The event is a single failure of one of four batteries at Turkey Point 3. Therefore, the impact vector is  $P_I = 1$  and zero elsewhere. The cause is judged applicable to the batteries at the sample plant; however, because of the system size difference, the Turkey Point 3 impact vector should be mapped down from system size 4 to system size 3. Again, from Eq. 3-24,

$$P_I^{(3)} = \frac{3}{4} P_I^{(4)} = 0.75$$

Other elements of the sample system impact vector are zero, as shown in Table 4-16.

- Event 3. The impact vector for Brunswick 1 is assessed as follows:

Hypothesis	Probability	$P_0$	$P_1$	$P_2$	$P_3$	$P_4$
$H_1$ : Batteries did not fail.	0.9	1	0	0	0	0
$H_2$ : Batteries failed.	0.1	0	0	1	0	0
Average		0.9	0	0.1	0	0

The event that occurred at Brunswick 1 is not a failure at the sample plant in the context of the core damage scenario of interest. In this context, the batteries are only needed to start and load the EDGs, and this can be accomplished with the batteries in a degraded condition similar to the conditions at Brunswick 1. A probability of 0.1 is assigned to hypothesis  $H_2$  to account for the possibility that the condition deteriorates sufficiently to cause multiple failures at

Table 4-16

CLASSIFICATION AND IMPACT ASSESSMENT OF EVENTS INVOLVING FAILURES OF STATION BATTERIES

Event Number	Plant (Code)	Status	Event Description	Cause-Effect Diagram	Plant System Area	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	SW	SWW Type	Event Mode	Justification	
1	Earl St. Plant December 15, 1989 LSR 81-013 408 81-014	Shutdown	During the scheduled "loss of" multiple power and turbine trip" maintenance test, two diesel generators started but failed to load into the station AC bus. The station battery bank 1 was discharged and a very high voltage surge occurred in every 2' lead, resulting in tripping several units. Francis Smith II, with control loss of instrument power to both diesel generators.		Earl Plant (12)	1	0	0	0	0	0	Low Output Voltage	This event resulted in actual loss of bus of three diesel generators at this plant due to a fault in a common power source (station battery 1).	
2	Turkey Point 3 November 11, 1989 LSR 81-014	Shutdown	The 1250 RC battery 2B failed to start a charge. No cause of failure could be determined, but the entire battery was replaced due to this event.		Turkey Point (11)	0	1	0	0	0	0	Low Output Voltage	This event is assumed to have rendered the battery unavailable.	
3	Brambleton 3 November 15, 1989 LSR 81-014	Shutdown	During a 1270 battery supply test, the voltage fell below the minimum value for the first stage on 10/15/89 (0.92 V.P. below 125A and 102.1 V.P. below 125A) which was first detected. Stop occurred on both batteries. Battery terminals were found corroded and loose.		Brambleton (14)	0.9	0	0.1	0	0	0	0	Low Output Voltage	This event is assumed to have rendered both batteries unavailable under one hypothesis. (The power supply requirements are not described in the event reports.)
4	Big Rock Point March 15, 1987 LSR 81-014	MSR Event	During an inspection of a battery discharge alarm, it was found that the battery bank 1 was in a fully charged condition. However, the symptoms on all battery banks were below the minimum design specification. The issue cannot be conclusively traced to any specific component during investigation.		Sample Plant (13)	0.9	0.05	0.05	0	0	0	0	Low Output Voltage	A weight of .7 has been assumed for the hypothesis that the condition deteriorates sufficiently to cause multiple failures at the sample plant.
					Big Rock Point (14)	0	0.95	0	0	0.05	0	0	Low Output Voltage	Degraded turbine condition was observed on all battery banks. However, only one battery actually discharged.
					Sample Plant (13)	0.24	0.71	0	0.05	0	0	0	Low Output Voltage	A weight of .05 has been assumed for the hypothesis that the condition deteriorates sufficiently to cause multiple failures.
					Sample Plant Total	1.14	3.01	0.05	0.05	0.05	0.05	0.05		

LEGEND:  
Cause-Effect Diagram:  
□ = Station  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator  
○ = Diesel Generator

SWW Type:  
1 = 1st  
2 = 2nd  
3 = 3rd  
4 = 4th  
5 = 5th  
6 = 6th  
7 = 7th  
8 = 8th  
9 = 9th  
10 = 10th  
11 = 11th  
12 = 12th  
13 = 13th  
14 = 14th  
15 = 15th  
16 = 16th  
17 = 17th  
18 = 18th  
19 = 19th  
20 = 20th  
21 = 21st  
22 = 22nd  
23 = 23rd  
24 = 24th  
25 = 25th  
26 = 26th  
27 = 27th  
28 = 28th  
29 = 29th  
30 = 30th  
31 = 31st  
32 = 32nd  
33 = 33rd  
34 = 34th  
35 = 35th  
36 = 36th  
37 = 37th  
38 = 38th  
39 = 39th  
40 = 40th  
41 = 41st  
42 = 42nd  
43 = 43rd  
44 = 44th  
45 = 45th  
46 = 46th  
47 = 47th  
48 = 48th  
49 = 49th  
50 = 50th  
51 = 51st  
52 = 52nd  
53 = 53rd  
54 = 54th  
55 = 55th  
56 = 56th  
57 = 57th  
58 = 58th  
59 = 59th  
60 = 60th  
61 = 61st  
62 = 62nd  
63 = 63rd  
64 = 64th  
65 = 65th  
66 = 66th  
67 = 67th  
68 = 68th  
69 = 69th  
70 = 70th  
71 = 71st  
72 = 72nd  
73 = 73rd  
74 = 74th  
75 = 75th  
76 = 76th  
77 = 77th  
78 = 78th  
79 = 79th  
80 = 80th  
81 = 81st  
82 = 82nd  
83 = 83rd  
84 = 84th  
85 = 85th  
86 = 86th  
87 = 87th  
88 = 88th  
89 = 89th  
90 = 90th  
91 = 91st  
92 = 92nd  
93 = 93rd  
94 = 94th  
95 = 95th  
96 = 96th  
97 = 97th  
98 = 98th  
99 = 99th  
100 = 100th

the sample plant. According to this hypothesis, the cause and the coupling mechanism of the event are applicable to the sample plant. However, due to the difference in the assumed number of batteries, the impact vector should be mapped down from size 4 to size 3. Referring to the procedure of Section 3, (Table 3-2), since the cause of the event is classified as a nonlethal shock, we have

$$P_0^{(3)} = \frac{1}{4} P_1^{(4)} + P_0^{(4)} = \frac{1}{4} (0) + 0.9 = 0.9$$

$$P_1^{(3)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} = \frac{3}{4} (0) + \frac{1}{2} (0.1) = 0.05$$

$$P_2^{(3)} = \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)} = \frac{1}{2} (0.1) + \frac{3}{4} (0) = 0.05$$

$$P_3^{(3)} = \frac{1}{4} P_3^{(4)} + P_4^{(4)} = \frac{1}{4} (0) + 0 = 0$$

- Event 4. The impact vector for Big Rock Point is assessed as follows:

Hypothesis	Probability	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>
H <sub>1</sub> : Only one battery failed.	0.95	0	1	0	0	0
H <sub>2</sub> : All four batteries failed.	0.05	0	0	0	0	1
	Average	0	0.95	0	0	0.05

Although only one of four batteries actually discharged, a small probability, of 0.05 is assigned to the second hypothesis to account for the fact that a degraded condition was observed on the other three batteries.

The cause and coupling mechanism of the event is judged to be also applicable to the sample system, but because of the system size difference, the Big Rock Point impact vector should be mapped down to obtain the impact vector of the example system. Again, using the procedure applied in the case of event 3, we have



$$P_0^{(3)} = \frac{1}{4} P_1^{(4)} + P_0^{(4)} = \frac{1}{4} (0.97) + 0 = 0.24$$

$$P_1^{(3)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} = \frac{3}{4} (0.95) + \frac{1}{2} (0) = 0.71$$

$$P_2^{(3)} = \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)} = \frac{1}{2} (0) + \frac{3}{4} (0) = 0$$

$$P_3^{(3)} = \frac{1}{4} P_3^{(4)} + P_4^{(4)} = \frac{1}{4} (0) + 0.05 = 0.05$$

4.2.3.3.2 Root cause and component group combination 2 - battery fuses. The LER review revealed no failure occurrences associated with battery fuses.

4.2.3.3.3 Root cause and component group combinations 3 through 9. Although these root cause and component group combinations have been deemed unimportant and screened from further analysis, selected failure events associated with these combinations are presented in Table 4-17 for illustrative purposes. Dozens of other events associated with root cause and component group combinations 3 through 8 were screened in a similar way. The failure data review revealed no events associated with combination 9.

4.2.3.4 Step 3.4 - Parameter Estimation. The results of event screening in the previous step can now be used to estimate the parameters of the model; namely, the total failure rates and the  $\beta$ -factors for station battery and battery fuse.

4.3.2.4.1 Station batteries. In the case of station batteries, data for the number of different basic events, as summarized in Table 4-16, is

$$(n_1 = 3.01, n_2 = 0.05, n_3 = 0.05)$$

This means that the total number of failures is

$$\begin{aligned} n_t &= n_1 + 2n_2 + 3n_3 \\ &= 3.26 \end{aligned} \tag{4-24}$$

These failures occurred over a period of approximately  $T = 2,092$  battery-years. A point estimate of the total failure rate of battery due to all causes can then be estimated from

$$\lambda_{Bt} = \frac{n_t}{T} \tag{4-25}$$


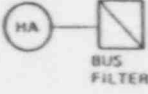
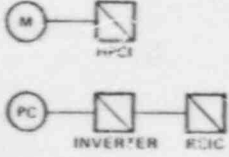

$$= \frac{3.26}{2,092} = 1.6 \times 10^{-3} \text{ per battery-year}$$

$$= 1.8 \times 10^{-7} \text{ per battery-hour} \tag{4-26}$$

Table 4-17

CLASSIFICATION AND IMPACT ASSESSMENT OF EVENTS THAT ILLUSTRATE  
ROOT CAUSE/COMPONENT GROUP COMBINATIONS 3 THROUGH 8

Sheet 1 of 2

Plant (date)	Status	Event Description	Cause-Effect Diagram	Plant	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	N/A	Shock Type	Fault Mode	Justification	
Sequoyah 1 August 29, 1985 LER 85-035	Shutdown	While troubleshooting to find the source of a DC ground, control power for a diesel generator was inadvertently lost.		Sequoyah 1	0	1	0	0	0	0	0	I	No Output Voltage	This event is included as a precursor to errors committed when performing Procedure 10 (investigating DC battery grounds).
				Sample Plant	0	0	0	0	0	1	I	No Output Voltage	See text discussion on root cause/ component group combination 8.	
Browns Ferry 1 February 5, 1985 LER 85-003	Shutdown	A voltage spike was generated when test equipment was connected to the Unit 2 generator breaker control circuit. This tripped the 161-kV lines because a breaker to the 250V DC bus filter was open. The breaker had been left open during previous activities to locate a DC ground.		Browns Ferry 1	0	1	0	0	0	0	0	I	No Output Voltage	This event is included as a precursor to errors committed when performing Procedure 10 (investigating DC battery grounds).
				Sample Plant	0	0	0	0	0	1	I	No Output Voltage	See text discussion on root cause/ component group combination 8.	
Fitzpatrick February 10, 1984 LER 84-004	100% Power	Both HPCI and RCIC systems were inoperable for about 30 minutes. While HPCI was out of service, a DC ground was being investigated on station battery A, which required a momentary interruption of DC control power to RCIC. RCIC remained inoperable, however, because the ground isolation procedure did not inform the operator that a manual reset was required to reoper an RCIC inverter following the momentary power interruption.		Fitzpatrick	0	1	0	0	0	0	0	I	No Output Voltage	This event is included as a precursor to errors committed when performing Procedure 10 (investigating DC battery grounds).
				Sample Plant	0	0	0	0	0	1	I	No Output Voltage	See text discussion on root cause/ component group combination 8.	
Grand Gulf 1 January 3, 1984 LER 84-001	Shutdown	The division 2 power supply tripped on high voltage, causing several safety-related system actuations. The equalizing potentiometer on the battery charger was set higher than its normal equalizing voltage of 140V.		Grand Gulf 1	1	0	0	0	0	0	0	I	High Output Voltage	This event is included as a precursor to battery charger-related failures that result in damage of batteries due to an overcharging condition.
				Sample Plant	1	0	0	0	0	0	0	I	High Output Voltage	See text discussion on root cause/ component group combination 3.

4-69

Table 4-17 (continued)

Plant (date)	Status	Event Description	Cause-Effect Diagram	Plant	P <sub>0</sub>	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	N/A	Shock Type	Fault Mode	Justification
Beaver Valley 1 October 27, 1983 LER 83-025	100% Power	The DC bus low voltage alarm 1 indicated a degraded voltage condition. Battery Charger 1 was functionally unavailable due to a blown output fuse.		Beaver Valley 1 Sample Plant	1	0	0	0	0	0	I	Low Output Voltage	The fuse failure was announced before substantial degradation occurred to the battery. See text discussions on root cause/component group combinations 4 and 5.
Palisades January 6, 1983 LER 83-001	99% Power	Both station batteries were temporarily removed from their DC power buses for about 1 hour. Maintenance personnel mistakenly opened the battery breakers when servicing the battery chargers, i.e., when coming the breakers associated with the chargers in service and closing the breakers for the idle chargers.		Palisades Sample Plant	0	0	1	0	0	0	N	No Output Voltage	Both station batteries were unavailable for about 1 hour. See discussion on root cause/component group combinations 6 and 7.
Brunswick 1 July 23, 1980 LER 80-004	94 Power	A surveillance test determined that station battery 105 had voltage 87% while in the float mode. Tests placed in the float mode indicated that the battery charger output voltage was 100% low while in the float mode.		Brunswick 1 Sample Plant	0	1	0	0	0	0	I	Low Output Voltage	This event is assumed to have rendered the battery unavailable. (The power supply requirements are not described in the event report.) See text discussion on root cause/component group combination 3.
Turkey Point 8 October 13, 1978 LER number not known		Two batteries were found in overcharging.		Turkey Point 1 Sample Plant	1	0	0	0	0	0	N	Low Output Voltage	This event is assumed to have rendered both batteries unavailable. See text discussion on root cause/component group combination 3.

Legend:  
Cause-Effect Diagram:  
H - Human Error  
E - Event  
D - Design Error  
U - Human Error  
N - Natural Shock  
I - Independent Event  
Shock Types:  
L - Lethal Shock  
N - Nonlethal Shock  
I - Independent Event

The  $\beta$ -factor for batteries can be estimated from the estimator of Table 3-6.

$$\begin{aligned}\beta_B &= \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \\ &= \frac{2(0.05) + 3(0.05)}{3.01 + 2(0.05) + 3(0.05)} = 0.08\end{aligned}\quad (4-27)$$

This result is clearly sensitive to the number of independent failure events. A careful search of plant-specific records and data from other utility-specific sources may turn up additional single-battery failure events. The effect of these events, if applicable to the sample plant, would be to reduce the estimated battery  $\beta$ -factor.

Since the preliminary analysis indicated that this scenario contributed substantially (51%) to the core damage frequency of the plant and since the value of  $\beta$  directly affects this contribution, the basis of the evaluation of  $\beta$  deserves closer scrutiny. Eq. 4-27 shows that the  $\beta$  value of 0.08 depends on the values of  $n_1$ ,  $n_2$ , and  $n_3$ , which are derived from Table 4-16. The values of  $n_2$  and  $n_3$ , in particular, are purely judgmental because they are based exclusively on the probabilities subjectively assigned by the analyst to hypothesis  $H_2$  for the third and fourth events in Table 4-16. This is illustrated during the evaluation of the impact vectors in the previous section. These probabilities are 0.1 and 0.05, respectively. However, events 3 and 4 in Table 4-16 did not result in actual multiple failures in the context of this accident scenario. The analyst is only postulating that they could have been actual multiple failures. Thus, it is just as defensible to assign lower numbers, say 0.01, to each of the hypotheses,  $H_2$ , as it is to assign 0.1 and 0.05. The value of  $\beta$ , however, is 0.013 in this more optimistic assignment.

The reason for the arbitrariness involved in the preceding evaluation is that Table 4-16 contains no actual CCF events. The value of  $\beta$  is much less sensitive to the analyst's judgments when the data contain at least one actual CCF event that is applicable to the plant under consideration. An alternative is to use the generic component  $\beta$ -factor given in Table 3-7. This implies that there is some average value for  $\beta$ -factors, which is an adequate assessment of common cause failure potential. The analysis of battery fuses that follows takes this approach. However, due to the significance of the CCF of the batteries at this plant, a third approach based on an examination of root causes and coupling mechanisms as a basis for the subjective assessment was used to estimate the contribution of the batteries. The basis of this approach is described in Reference 4-13.

In this alternative approach,  $\lambda_{BT}$  is redefined to represent the total frequency of events resulting in the unavailability of a

station battery. There are four such events in Table 4-16 (event 3 is assumed here to have resulted in at least one failure). Thus,

$$\begin{aligned}\lambda_{BT} &= 4 \text{ occurrences}/2,092 \text{ battery-years} \\ &= 1.9 \times 10^{-3}/\text{battery-year} \\ &= 2.2 \times 10^{-7}/\text{battery-hour}\end{aligned}$$

This generic frequency estimate was assumed applicable to the station batteries at the sample plant. It represents the total frequency of events that resulted in the unavailability of a station battery, and it has two components. One component is associated with human errors of commission (e.g., contamination of the electrolyte during maintenance), and the other is associated with human errors of omission; e.g., failure to detect severe flaking of cell plates. A human error of commission is sufficient to cause battery failure, while a human error of omission would only be relevant if a failure mechanism were already developing within the battery or its terminal connection detail. The total frequency,  $\lambda_{BT}$ , represents the frequency of battery failures due to both of these components.

$B_B$  is the conditional probability of observing multiple failures, given the occurrence of at least one failure. Since the causes of battery failure are associated with human errors,  $B_B$  was estimated by evaluating the probability of occurrence of multiple human errors, given the occurrence of at least one human error. Since human errors of omission are only relevant if a failure mechanism is also developing within the other batteries, there was some conservatism in using this approach to estimate  $B_B$ ; i.e.,  $B_B$  was not reduced to account for cases in which a failure mechanism develops within a single battery only. Nuclear power plant experience indicates that the failure mechanisms considered here do tend to affect multiple batteries. Also, this conservatism applies to errors of omission only. Therefore, the degree of conservatism was judged to be low.

Thus, the dependent failure potential associated with these causes was estimated using human reliability methodology. As pointed out previously, these causes of failure are strongly associated with the checking, testing, and maintenance program at the plant. The checking and testing procedures were determined to be clearly written and in compliance with industry standards (Reference 4-14). Therefore, errors associated with these causes are more likely to be caused by the person performing the task than by misleading or inadequate task instructions. The conditional probability of a human error for a task, given a failure on the preceding task, is provided in Reference 4-15 as a function of the level of dependence. The level of dependence can be zero, low, moderate, high, or complete and may be subjectively assessed in accordance with the general guidelines in the document. In this analysis, the level of dependence was assessed to be either low or moderate since the major factor affecting this assumption was the fact that the quarterly

checks occur at staggered intervals; the tasks are performed at least 1.6 weeks apart. The conditional probabilities of a human error for a task, given a failure on the preceding task, are then 0.05 and 0.15 (Reference 4-15) for low and moderate levels of dependence, respectively. In this analysis,  $\beta_B$  was conservatively assumed to be 0.15.

The average fault detection and restoration time was estimated from plant-specific information and from judgment based on LER descriptions of previous occurrences at other U.S. plants. It is assumed that battery internal and terminal connection detail faults would be detected during the quarterly checks at this plant. This assumption is based on the fact that, as noted earlier, the quarterly checks at this plant include measuring and recording the voltage and specific gravity of each cell; checking the general condition of the battery, racks, posts, and connectors; and conducting several other important checks; e.g., cell temperature, ambient temperature, and ventilation system operability. Therefore, the quarterly checks should reveal most potential problems with regard to the station batteries.

Figure 4-10 shows that the average detection time is either 0.8 weeks ( $1.6 \div 2$ ) whenever the fault occurs just prior to a quarterly check of a station battery (intervals 2, 3, 4, or 5 in Figure 4-10) or 3.2 weeks ( $4 \times 1.6 \text{ weeks}/2$ ) in all other cases combined (intervals 1, 6, 7, or 8 in Figure 4-10). Thus, the average detection time is

$$T_{BD} = [(4 \times 0.8)/8 + (3.2)/2] = 2 \text{ weeks (336 hours).}$$

4.2.3.4.2 Battery fuses. Since the LER review revealed no failure occurrences associated with battery fuses, this root cause and component group combination is quantified based on generic failure data and assumptions. The failure rate for low voltage (<1,000 volts) fuses in Reference 4-16 is assumed to be applicable to the battery fuses. This failure rate is  $\lambda_{ft} = 0.021 \times 10^{-6}$  per hour. If the failure mechanism of concern--a failure mechanism that might develop during the long time period (18 months) between refueling outages--is assumed to cause 5% of all fuse faults (operational experience with other fuses in 125V DC systems at nuclear power plants indicates this assumption is conservative), then the failure rate for combination 2 becomes  $1.05 \times 10^{-9}$  per hour. The average  $\beta$ -factor value of  $\beta_f = 0.1$  (see Section 3, Table 3-7) is also assumed applicable to the battery fuses.

Since any refueling outage at this plant involves testing at least one of the station batteries of interest and since testing any one of the station batteries of interest would reveal a CCF of the station battery fuses, the maximum detection time for the CCF event is the time between refueling outages. Also, it is assumed that the CCF event can occur anytime between the refueling outages. Thus, the average detection time for the CCF event is about half the time between refueling outages. Operational experience indicates that the

time between refuelings at the sample plant averages about 7,700 hours. Thus,

$$\begin{aligned}T_{FD} &\approx 7,700 \text{ hours}/2 \\ &\approx 3,900 \text{ hours}\end{aligned}$$

#### 4.2.4 Stage 4: System Quantification and Interpretation of Results

This step is accomplished using the quantitative model selected in Step 3.2 and the parameters estimated in Step 3.4. Table 4-18 summarizes this quantification, and the point estimate for the probability of a CCF of the station batteries within the scenario of interest is shown as  $4.9 \times 10^{-6}$  and  $1.1 \times 10^{-5}$ , based on the first and second quantification approaches, respectively.

These CCF contributions were calculated as

$$\lambda_{CB} = \beta_B \cdot \lambda_{Bt} \cdot T_{BD} \quad (4-28)$$

Based on the first approach, we have

$$\begin{aligned}\lambda_{CB} &= (0.08)(1.8 \times 10^{-7})(336) \\ &= 4.9 \times 10^{-6}\end{aligned}$$

and based on the second approach, we get

$$\begin{aligned}\lambda_{CB} &= (0.15)(2.2 \times 10^{-7})(336) \\ &= 1.1 \times 10^{-5}\end{aligned}$$

Also, for the fuses we have

$$\begin{aligned}\lambda_{CF} &= \beta_F \cdot \lambda_{Ft} \cdot T_{FD} \\ &= (0.1)(1.1 \times 10^{-9})(3,900) \\ &= 4.3 \times 10^{-7}\end{aligned} \quad (4-29)$$

The combined frequency of the initiating events associated with the core damage scenario discussed in this example is about 0.07 per year (Reference 4-2). Thus, the frequency of the core damage scenario of interest is about  $3.7 \times 10^{-7}$  and  $7.7 \times 10^{-7}$  per year based on the first and the second quantification approach, respectively. Both of these values are low when compared to the frequency of dominant scenarios identified in other nuclear power plant PRA studies. In addition, some conservatism involved in the quantitative analysis (e.g., the assumption that the occurrence of the initiating event and the CCF event result in

Table 4-18

## QUANTIFICATION OF CCF CONTRIBUTION

	Combination Identification Number	Root Cause Frequency (hr <sup>-1</sup> )	Root Cause-Specific Beta Factor*	Average Detection Time (hours)	Contribution to Unavailability
First Approach	1	$1.8 \times 10^{-7}$	0.08	336	$4.9 \times 10^{-6}$
	2	$1.1 \times 10^{-9}$	0.10	3,900	$4.3 \times 10^{-7}$
	Total				$5.3 \times 10^{-6}$
Second Approach	1	$2.2 \times 10^{-7}$	0.15	336	$1.1 \times 10^{-5}$
	2	$1.1 \times 10^{-9}$	0.10	3,900	$4.3 \times 10^{-7}$
	Total				$1.1 \times 10^{-5}$

\*These numbers represent the probability that at least one redundant component is unavailable due to a certain root cause, given failure of the first component due to that same root cause. Additional component failures in a sufficient number of redundant divisions are conservatively assumed to occur, given the first two failures.



enough equipment failures to cause the scenario of interest) provides further assurance that the core damage scenario analyzed in this section is not a major hazard that must be designed out of this plant. The results do indicate, however, that the core damage frequency is highly sensitive to the probability of a CCF involving the station batteries. Thus, an increase in the CCF probability will have a strong adverse effect on the risk associated with core damage accidents.

Therefore, this analysis indicates that the CCF scenario, although not requiring risk reduction measures, should be emphasized in a safety assurance program. The discussions from the qualitative screening step provide the basis for focusing safety assurance activities.

#### 4.3 REFERENCES

- 4-1. Paula, H. M., "A Probabilistic Dependent Failure Analysis of a DC Electric Power System in a Nuclear Power Plant," JBF Associates, Inc., 37932-3341, submitted for publication in Nuclear Safety, Knoxville, Tennessee, October 1987.
- 4-2. Kolaczowski, A. M., et al., "Analysis of Core Damage Frequency from Internal Events Peach Bottom, Unit 2," NUREG/CR-4550/4-10, SAND 86-2084, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, September 1986.
- 4-3. Edwards, G. T., and I. A. Watson, "A Study of Common Mode Failure," SRD-R-146, United Kingdom Atomic Energy Authority, Safety and Reliability Directorate, July 1979.
- 4-4. Paula, H. M., and D. J. Campbell, "Analysis of Dependent Failure Events and Failure Events Caused by Harsh Environmental Conditions," JBFA-LR-111-85, JBF Associates, Inc., 37932-3341, Knoxville, Tennessee, August 1985.
- 4-5. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," Pickard, Lowe and Garrick, Inc., PLG-0400, prepared for Electric Power Research Institute, February 1985.
- 4-6. Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, December 1983.
- 4-7. Atwood, C. L., "Estimators for the Binomial Failure Rate Common Cause Model," NUREG/CR-1401, prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., April 1980.
- 4-8. American Nuclear Society, and Institute of Electrical and Electronics Engineers, "PRA Procedures Guide; A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," sponsored by the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute, NUREG/CR-2300, April 1983.

- 4-9. Kolaczowski, A. M., and A. C. Payne, "Station Blackout Accident Analyses," NUREG/CR-3226, SAND82-2450, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, May 1983.
- 4-10. Baranowsky, P. W., A. M. Kalaczowski, and M. A. Fedele, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," NUREG-0666, April 1981.
- 4-11. Gunther, W. E., M. Subudhi, and J. H. Taylor, "Operating Experience and Aging--Seismic Assessment of Battery Chargers and Inverters," BNL-NUREG-51971, NUREG/CR-4564, June 1986.
- 4-12. Hellmann, E. V., and W. F. Hurley, "Qualification of Lead-Acid Batteries for Nuclear Stations," Institute of Electrical and Electronics Engineers Power Engineering Society Winter Meeting, A 80 101-6, New York, New York, February 1980.
- 4-13. Paula, H. M., "A Restructured Approach to the Partial Beta Factor Method," JBF Associates, Inc., 37932-3341, Knoxville, Tennessee, October 1986.
- 4-14. Institute of Electrical and Electronics Engineers, "Recommended Practice for Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Generating Stations and Substations," IEEE Std 450-1980, New York City, October 1980.
- 4-15. Swain, A. D., and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," U.S. Nuclear Regulatory Commission, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, New Mexico, August 1983.
- 4-16. Institute of Electrical and Electronics Engineers, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations," IEEE Std 500-1977, June 1977.

## Section 5

### AREAS FOR FUTURE ENHANCEMENT

#### 5.1 INTRODUCTION

The last few years have seen much progress in the systematic and detailed treatment of common cause failures. This report presents a consensus approach to the procedural framework that should be adopted and, also, many of the methods and techniques that can be, and have been, used to estimate the probabilities of common cause failures. Key to the development of these methods was realizing the importance of plant-specific factors that contribute to the potential for common cause failures and dependent failures in general. This realization has led to an increased emphasis on identifying root causes and causal mechanisms for multiple failures. One result of this has been the development of an event classification scheme, such as the one discussed in Section 3 and more fully described in Volume II, which provides a framework for systematic data analysis. The use of thought experiments to reinterpret historical events in the context of a particular plant has been of great value in overcoming the perennial problem of scarce data. In parallel with the improved treatment of data, there has been a development of models to translate these data into estimates of probabilities and an increased awareness of the importance of making clear the assumptions underlying these models. However, there is wide consensus that the current state of the art is more limited by the data and their analysis than it is constrained by the existing models. Although considerable progress has indeed been made in the understanding of the mechanisms of common cause failures and in the establishment of this proposed framework for the analysis, the problems that still exist in estimating common cause failure probabilities should not be underestimated. In Section 5.2, some of these problems are discussed, followed by a discussion of the areas in which improvements are most needed in Section 5.3.

#### 5.2 DIFFICULTIES IN THE ESTIMATION OF COMMON CAUSE FAILURE PROBABILITIES

The mechanisms that result in multiple failures are many and can be complex, and there can be great plant-to-plant variation in the potential for such failures. Use of information from a variety of plants, which is necessary to overcome the scarcity of data, involves interpreting event reports to identify the mechanisms and reinterpreting them for plant-specific applications and requires considerable judgment. This report has provided some methods that can be used to formalize this data analysis. The role of defenses against common cause failures that is crucial for identifying potential improvements, for example, has not been explicitly explored in detail but is, however, implicit in the event screening and reinterpretation. In Section 5.2.1, this aspect is revisited briefly from a conceptual point of view, and, in Section 5.2.2, the problems of incorporating these considerations associated with data analysis are discussed.

### 5.2.1 The Modeling of Common Cause Failures To Include Defenses

One of the problems with common cause failure analysis is accounting for the number of different mechanisms that can give rise to them and the different defensive tactics that can mitigate against them. Since the different tactics that can be employed to mitigate against common cause failures are believed to have a different impact on the different classes of common cause failure mechanisms, it is clear that any analysis that takes defenses into account must separately address the causes to some extent. The methods described in this report have addressed defenses qualitatively in the screening process or implicitly through the data analysis process; an alternative is a more explicit analysis, as discussed in the conceptual example presented in Section 5.3.5.

As discussed in Sections 2 and 3, there are various proposals for common cause failure classification. For the purpose of the following discussion, we adopt the second division (level) of the SRD R146 (Reference 5-1) scheme, which classifies events according to the shared root causes into events due to design, construction, procedural factors, and environmental factors.

Errors made or weaknesses introduced during design and construction can affect the system availability in at least two ways. First, they can be introduced at the system level so that there is an unplanned, hard-wired dependency. Such weaknesses are not flaws that would be uncovered by normal testing, but are such that they might occur only under specific conditions involving a particular sequence of events; this whole sequence might be called a trigger event. For example, the problem of undersized motor-operated valves may not be uncovered on test if the valves and pumps of a standby emergency feedwater system are tested separately. Such errors would require an actual system demand (the trigger event in this case) to occur before being revealed as a problem. Such common cause failure event probabilities could be estimated as the product of the probability of an undetected error and the probability of the trigger event.

Design and construction errors can also occur at the component level so that each of the redundant components is less reliable than assumed or intended. Unless the failure causes are investigated at a deeper level than "design error," it is not clear that any mechanism can be postulated for such a strong coupling of component failures that they occur simultaneously. These failures could still be regarded as randomly occurring but, perhaps, more bunched in time or having a particular number of cycles. These common cause failures could be modeled by modifying the unavailability of the system from  $p^n$  (assuming a redundancy level of  $n$ ) to

$$(1-\alpha)p^n + \alpha(xp)^n$$

where  $x(>1)$  is a measure of the "strength" of the design error and  $\alpha$  is the (assumed constant) probability that the design error exists. The relative probability of system failure is increased by virtue of the increase in the single-component failure probability. (This may also be an appropriate way of modeling aging effects.)

The defenses against these types of common cause failures can more easily be envisaged as affecting the probability of the occurrence of the original errors rather than, in the first case, as affecting the probability of the trigger event or, in the second case, the "strength" of the error.

There are many ways that operational practice and other factors can result in common cause failures. Operating or maintenance procedures may be in error and can lead to increased susceptibility for both system failure or unavailability or an increased susceptibility for single-component random failure. On the other hand, if the procedures are adequate, their implementation may not be adequate because of poor management control, poor operator training, incorrect interpretation, or mistakes. The factors that couple failures and result in true common cause failures are dependent on the way the plant is operated. For instance, the type of event that can cause coupling of errors made during surveillance testing may be different when testing is done on a staggered basis rather than on a nonstaggered basis. It also may depend on whether testing of redundant equipment is performed by the same or by different people. In some cases, a trigger event, such as the occurrence of a maintenance error on redundant trains that is not discovered on a post-maintenance test, can be modeled as a random event. In this case, the human error is the trigger event. In other cases, such as the existence of inadequate procedures, the human error leads to a preconditioning of the system and is more associated with establishing the coupling or the level of susceptibility to failure.

Environmental common cause failures are fairly easy to interpret. The trigger event can be modeled as a random event that leads to the environmental conditions that cause the failure results. The plant design features basically define the potential couplings; however, the possibility of design or construction errors, such as inadequate or incorrectly installed fire barriers, and nonadherence to procedures, such as propping open flood-tight doors, have to be accounted for.

The aim of the common cause analysis is to incorporate these considerations into the estimation process in as thorough a way as possible.

#### 5.2.2 Problems with Data Analysis

The methods discussed in this document rely largely on estimating the parameters of those models using generic industry data on single and multiple failure events. The source of data is typically the licensee event reports or Nuclear Power Experience (Reference 5-2). The data analysis can be thought of as an interpretation of events in the data base and a subsequent reinterpretation in the light of the defenses perceived to be in existence at the plant for which the analysis is being performed.

There are problems associated with the completeness of the data base and with the fact that, even if it were complete, an objective assessment of the efficiency of a defensive strategy is extremely difficult. For instance, almost all plants could claim, to a certain extent, to adopt most, if not all, the defensive tactics discussed earlier in

Section 5.2.1. What is really at question for many of the tactics is how effective they are rather than whether they exist. Therefore, although it may be possible because of some particular design features to screen out certain events, others should perhaps not be screened out but weighted by some factor to represent the perceived value of the defense in the plant at question, compared with the one in which the event occurred. A related question is what to do about new plants with all the right defenses to prevent the old problems observed in the industry data base, but with new, yet-to-be-observed, problems introduced. These ideas are examined more thoroughly in the two examples below.

The first is the case in which the root cause of failure has been determined to be an error in following a maintenance procedure. The tactic that would eliminate the trigger event, in this case the error and lack of its detection, is post-maintenance inspection and testing. The existence of administrative controls at the plant is a tactic that should reduce the coupling; not following plant administrative controls increases the opportunity for the trigger event to occur. It may not be clear which of these tactics was deficient: whether the post-maintenance inspection procedure was inadequate or whether it was not followed properly or both.

Furthermore, and this is perhaps the most important point from a quantification point of view, both tactics are almost certainly present at the plant at which the event occurred, but there may not be, and likely will not be, any objective way in which to measure the quality of these two tactical schemes at that plant or, in fact, at the plant being analyzed. The information at the level needed to make any sort of judgment is not readily available for the family of plants from which data are gathered. Thus, there is no clearly defensible criterion on which to include or exclude the event as being applicable to the plant in question or to modify the worth of the event by multiplying by a factor that represents the relative value of the tactics at the two plants.

As a second example, consider the case of two diesel generators failing as a result of fouling of the service water used for cooling. If the plant of interest has air-cooled diesels, it is clear that the event is not applicable and can be eliminated. In this case, the defensive tactic to provide complete redundancy in cooling, with no coupling mechanism, can be objectively assessed.

However, most of the defensive tactics mentioned earlier are the first type for which there is no well-defined procedure for measuring the quality of the defenses. Thus, the assessment has to be subjective. Recognizing this, it is important to address the uncertainty in the estimates of the parameters. A final question posed by the example is the need to assess whether potential fouling of the radiators in the air-cooled diesels is more or less likely to cause a common cause event than the corresponding problem with the water-cooled diesels. Again, the current state of the art leads us to rely on engineering judgment in data analysis to address such a problem.

In addition to the interpretation of the events and their reinterpretation in the light of conditions at the plant of interest, another problem that has been recognized in this report is the necessity to adjust the observed data to account for plant-to-plant differences in the degree of system redundancy (the mapping up and down discussed in Section 3.3.3.4). This is a process that can only be performed by making certain assumptions about the events and the mechanisms that resulted in their occurrence. Furthermore, the surveillance testing strategies at the plants from which data are obtained have an impact on the relative numbers of demands on single components and groups of components that, in turn, affect the estimates of parameter values of the common cause models. The testing strategies at all plants are not generally known.

All these factors contribute to uncertainty in the specification of the pseudo-data base for plant-specific application. One of the contributions of this report has been the explicit recognition of these sources of uncertainty and the discussion of some of the tools available for addressing this uncertainty.

### 5.3 SUGGESTED IMPROVEMENT IN COMMON CAUSE MODELING

The importance of obtaining good, detailed data and of a systematic approach to the analysis of those data has been apparent throughout this guide. It is clear that however much progress has been made recently, there is still room for improvement in collecting data and in classifying those data so that more specific guidelines can be constructed for data interpretation and screening, which should lead to a decrease in uncertainty in the results of common cause failure analyses. Although there has been progress in the development of systems for analyzing and classifying data in the form of event reports, less progress has been made in improving the event reports themselves.

#### 5.3.1 Data Collection

The previous discussion illustrates that there is an urgent need for improved reporting of event data. The particular improvements should be directed toward an increased emphasis on unambiguously identifying root causes, coupling mechanisms, and, if appropriate, defenses that were present and that failed. It is also important to have information on the spectrum of demands on components and groups of components. Improved event reporting would reduce uncertainty in parameter estimates, but such an improvement is clearly a long-term goal. The short-term needs are for designing the appropriate data collection forms and for establishing an industry commitment to perform the data collection. This commitment is unlikely to be obtained on the basis of PRA needs alone, but on the basis of realizing the value of the data for additional input into understanding the mechanisms that allow multiple failures to occur and, hence, their value in the design of hardware or operating procedures.

#### 5.3.2 Event Classification Scheme

The event classification schemes discussed in this document are based on a root cause classification, but they do not explicitly identify the coupling mechanism. This makes it difficult to interpret the event in the light of the existing defenses directly from the classification. In

addition, to get a complete picture of the effect of the defensive strategies, it is important to consider the independent failures as well as the dependent failure events. The reason for this is seen clearly in the discussion in Section 5.3.4.

A classification scheme that identifies not only the root causes of equipment failure, but the way in which the root cause arises and leads to multiple failures would be extremely valuable. It would also be of value to identify which of the defenses against common cause failures is felt to have been deficient. This, with the present data base, would of course be extremely subjective and may well be impossible in the majority of cases.

Although cause classification schemes have been addressed at great length, similar schemes for the coupling mechanisms and defensive strategies have not been so fully developed. Of course, since they are all to some extent intertwined, designing such schemes will not be trivial. However, it is necessary to improve the current framework for event interpretation to remove some of the uncertainty in the analysis. Exploring and refining these concepts will have the added benefit of providing guidelines for the analysis of data that will result in a more consistent analysis.

### 5.3.3 Qualitative Analysis

A qualitative assessment of the potential for common cause failures forms an essential part of the screening process to help concentrate resources on the most significant potential contributors. Currently, there does not exist a well-tested, consensus set of guidelines for performing such screening. Establishing such a set of guidelines requires the collection of qualitative insights obtained from engineering analyses and the analysis of event reports. This would be valuable not only for screening, but also in establishing a basis for more detailed common cause failure models.

### 5.3.4 Parameter Estimation and Representation of Uncertainty

The impact vectors discussed in Section 3 provide a useful representation of the assumptions made during the analysis of event data. These assumptions result from a subjective assessment of the data. A set of guidelines for interpreting event reports would help improve consistency in performing these assessments. Clearly, however, with the current data there would still be considerable uncertainty in applying guidelines, and this source of uncertainty may become less important but will not disappear.

An important factor that has been addressed in this report is the mapping up or down of impact vectors to reflect different degrees of redundancy at different plants. The schemes presented in this report are based on specific assumptions. The validity of these assumptions and other plausible assumptions needs to be investigated.



As discussed in Section 5.2.2, there are many sources of uncertainty. Although some of the suggestions given here are aimed at reducing this uncertainty, this will not be possible in the short term. Some simplified approximations to incorporating the different sources of uncertainty were suggested in Section 3.3.4, but it was recognized that more thorough, yet still practical, approaches are desirable.

### 5.3.5 Nondata-Based Methods - The Cause-Defense Beta Factor Model

The data-based methods for parameter estimation are currently limited by the quality and quantity of existing data. An alternative is to use engineering judgment to establish appropriate parameter values. Perhaps even more than in the case in which data are plentiful, this requires a fairly complete definition of the spectrum of the root causes and mechanisms of propagating failures and an understanding of the value and effect of the various defensive strategies. Research into defining an appropriate framework and into providing guidelines for application to different components is needed, particularly on how to get consistent quantitative, as well as qualitative, insights.

One recently developed conceptual model that explicitly accounts for the root causes, coupling mechanisms, and the efficiency of the defensive strategy is a variation of the partial beta factor model (Reference 5-3), as described in the following.

Define the spectrum of root causes. For each root cause, assess the potential for simultaneous failure of like components by identifying specific coupling mechanisms. Thus, for each component unavailability, the total unavailability is the sum of the unavailabilities from the different root causes.

$$p^{(i)} = \sum_{i \in I} p_i \quad (5-1)$$

where  $I$  is the set of all root causes.

The common cause failure frequency is therefore given by

$$p^{(c)} = \sum_i p_i \beta_i \quad (5-2)$$

where  $\beta_i$  is the partial beta factor (or the appropriate beta factor to cause  $i$ ). This model will be referred to as the cause-defense beta factor model.

Define the set of defensive tactics and, for each tactic, identify its effect on both random and dependent failures. If there are  $J$  defensive tactics, the probability of tactic  $k$  being effective against cause  $i$  is  $d_{ik}$ . Now, the effect of the defensive strategy may be different for the common failures than for the independent failures since it may prevent or mitigate the coupling mechanisms rather than the root cause.

This difference will be indicated by a c or an i, in parentheses, associated with  $d_{jk}$  (c represents common cause, and i represents independent cause). Thus, the complete expression for unavailability at the component level becomes

$$p^{(i)} = \sum_{i \in I} p_i \prod_{k \in J} (1 - d_{ik}^{(i)}) \quad (5-3)$$

and, for the common cause unavailability,

$$p^{(c)} = \sum_{i \in I} p_i R_i \prod_{k \in J} (1 - d_{ik}^{(c)}) \quad (5-4)$$

and the new  $R$  is defined as

$$R = \frac{p^{(c)}}{p^{(i)}} = \frac{\sum_{i \in I} p_i R_i \prod_{k \in J} (1 - d_{ik}^{(c)})}{\sum_{i \in I} p_i \prod_{k \in J} (1 - d_{ik}^{(i)})} \quad (5-5)$$

This is now a multiparameter model that is beyond the current capability of the data to support. However, it is a framework that can be used for a subjective assessment using the results of a common cause FMEA to define the causes, coupling mechanisms, defenses, and their relative importance at the particular plant.

A simpler version of this approach was originally developed and applied in several analyses by the Systems Reliability Directorate of the U.K. (Reference 5-3) in which the partial beta factors were subjectively estimated.

Models, such as this cause-defense beta factor model, can be valuable as a theoretical laboratory for use in investigating alternative defensive strategies and may be of particular value for plants that are in the design stage.

### 5.3.6 Improved Models of Common Cause Failures

As the physics of failures become better understood and the role of defenses and coupling mechanisms becomes clarified, it may be possible to develop different, more appropriate models for common cause failures arising from different classes of causes. It has already been recognized that it is desirable to adopt a new approach to address the effects of aging as a common cause failure mechanism for example. Whether this would have any significant effect on using the current parametric models is not at all clear, particularly as the demands on data become more stringent.

The thrust of the analysis methods in this report have been on the analysis of common cause failures from an impact point of view. An increase in detail to a cause basis raises questions about how best to define the basic events. It would appear that the basic events that represent groups of causes fall between being independent or mutually exclusive. This aspect needs to be borne in mind when developing such models.

#### 5.4 CONCLUSIONS

This section has discussed some of the problems that still exist with respect to common cause failure analysis. The need for good, quality data is paramount but is unlikely to be satisfactorily achieved in the short term. Short-term goals should focus on:

- Definition of better data collection criteria.
- Refinement of cause classification schemes.
- The establishment of qualitative screening guidelines.
- The establishment of guidelines for event interpretation and the creation of a pseudo-plant-specific data base for parameter estimation.

All of these should incorporate the concept of assessing the adequacy of defenses. In addition, there should be some focus on developing methods that are less dependent on data and based more on engineering assessments and on developing more comprehensive, yet practical, uncertainty analysis methods.

#### 5.5 REFERENCES

- 5-1. Humphreys, P., and B. D. Johnson, "SRD Dependent Failures Procedures Guide," National Centre of Systems Reliability, United Kingdom, RTS 86/1 URNT50, 1986.
- 5-2. S. M. Stoller, Nuclear Power Experience, updated monthly.
- 5-3. Johnston, B. D., "A Structured Procedure for Dependent Failure Analysis (DFA)," Reliability Engineering, Vol. 19, pp. 125-136, 1987.

NRC FORM 335 (2-84) NRCM 1102 3201, 3202 SEE INSTRUCTIONS ON THE REVERSE		U.S. NUCLEAR REGULATORY COMMISSION		1 REPORT NUMBER (Assigned by TROC add Vol. No. if any) NUREG/CR-4780 EPRI NP-5613 Vol. 1	
2 TITLE AND SUBTITLE Procedures For Treating Common Cause Failures in Safety and Reliability Studies Procedural Framework and Examples				3 LEAVE BLANK	
5 AUTHOR(S) A. Mosleh, K. Fleming, G. Parry, H. Paula, D. Worledge, and D. Rasmuson				4 DATE REPORT COMPLETED MONTH: November YEAR: 1987	
7 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Pickard, Lowe, and Garrick, Inc. 2260 University Drive Newport Beach, California 92660				6 DATE REPORT ISSUED MONTH: January YEAR: 1988	
10 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Division of Reactor and Plant Systems and Electric Power Research Institute Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, D.C. 20555				8 PROJECT/TASK WORK UNIT NUMBER  9 FIN OR GRANT NUMBER FIN A1384	
11 TYPE OF REPORT Technical				12 PERIOD COVERED (Inclusive dates)	
13 ABSTRACT (200 words or less) <p>This report presents a framework for the inclusion of the impact of common cause failures in risk and reliability evaluations. Common cause failures are defined as that subset of dependent failures for which causes are not explicitly included in the logic model as basic events. The emphasis here is on providing procedures for a practical, systematic approach that can be used to perform and clearly document the analysis.</p> <p>The framework comprises four major stages: (1) system logic model development, (2) identification of common cause component groups, (3) common cause modeling and data analysis, and (4) system quantification and interpretation of results.</p> <p>The framework and the methods discussed for performing the different stages of the analysis integrate insights obtained from engineering assessments of the system and the historical evidence from multiple failure events into a systematic, reproducible, and defensible analysis.</p>					
14 DOCUMENT ANALYSIS - KEYWORDS OR TOPICS Dependent Failures Common Cause Failures Common Mode Failures				15 AVAILABILITY STATEMENT Unlimited	
16 IDENTIFIERS OR UNCLASSIFIED TERMS				16 SECURITY CLASSIFICATION (This page) Unclassified (This report) Unclassified	
				17 NUMBER OF PAGES	
				18 PRICE	

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

OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300

SPECIAL FOURTH CLASS RATE  
POSTAGE & FEES PAID  
USNR1  
PERMIT No. G-67

120555078877 1 1A1RX  
US NRC-OARM-ADM  
DIV OF PUB SVCS  
POLICY & PUB MGT BR-PDR NUREG  
W-537  
WASHINGTON DC 20555