NUREG/CR-5485
INEEL/EXT-97-01327

Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment

Prepared by
A. Mosleh/Univ. of MD
D. M. Rasmuson/NRC
F. M. Marshall/INEEL

Idaho National Engineering and Environmental Laboratory

University of Maryland

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy,* of the *Code of Federal Regulations,* may be purchased from one of the following sources:

1. The Superintendent of Documents
   U.S. Government Printing Office
   P.O. Box 37082
   Washington, DC 20402–9328
   <http://www.access.gpo.gov/su_docs>
   202–512–1800

2. The National Technical Information Service
   Springfield, VA 22161–0002
   <http://www.ntis.gov/ordernow>
   703–487–4650

The NUREG series comprises (1) technical and administrative reports, including those prepared for international agreements, (2) brochures, (3) proceedings of conferences and workshops, (4) adjudications and other issuances of the Commission and Atomic Safety and Licensing Boards, and (5) books.

A single copy of each NRC draft report is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001
E–mail: <GRW1@NRC.GOV>
Facsimile: 301–415–2289

A portion of NRC regulatory and technical information is available at NRC's World Wide Web site:

<http://www.nrc.gov>

All NRC documents released to the public are available for inspection or copying for a fee, in paper, microfiche, or, in some cases, diskette, from the Public Document Room (PDR):

NRC Public Document Room
2121 L Street, N.W., Lower Level
Washington, DC 20555–0001
<http://www.nrc.gov/NRC/PDR/pdr1.htm>
1–800–397–4209 or locally 202–634–3273

Microfiche of most NRC documents made publicly available since January 1981 may be found in the Local Public Document Rooms (LPDRs) located in the vicinity of nuclear power plants. The locations of the LPDRs may be obtained from the PDR (see previous paragraph) or through:

<http://www.nrc.gov/NRC/NUREGS/
SR1350/V9/lpdr/html>

Publicly released documents include, to name a few, NUREG-series reports; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigation reports; licensee event reports; and Commission papers and their attachments.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852–2738. These standards are available in the library 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—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
<http://www.ansi.org>
212–642–4900

DISCLAIMER

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, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR-5485
INEEL/EXT-97-01327

Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment

Manuscript Completed: June 1998
Date Published: November 1998

Prepared by
A. Mosleh/Univ. of MD
D. M. Rasmuson/NRC
F. M. Marshall/INEEL

Idaho National Engineering and Environmental Laboratory
Lockheed Martin Idaho Technologies Company
Idaho Falls, ID 83415

Subcontractor:
Department of Materials and Nuclear Engineering
University of Maryland
College Park, MD 20742-2115

Prepared for
Safety Programs Division
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code E8247

ABSTRACT

This report provides a set of guidelines to help probabilistic risk assessment (PRA) analysts in modeling common cause failure (CCF) events in commercial nuclear power plants. The aim is to enable the analyst to identify important common cause vulnerabilities, incorporate their impact into system reliability models, perform data analysis, and quantify system unavailability in the presence of CCFs. Much of the material in this report has been presented in previous reports issued by United States Nuclear Regulatory Commission (NRC). The present document brings together the key aspects of these procedural guidelines supplemented by additional insights gained from their application, and enhanced by the capabilities of the CCF software and its data analysis capabilities, recently developed by the NRC.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission's (NRC's) Office for Analysis and Evaluation of Operational Data (AEOD) and the Idaho National Engineering and Environmental Laboratory (INEEL) staff have developed and maintain a common cause failure (CCF) database for the U. S. commercial nuclear power industry. Previous studies documented methods for identifying and quantifying CCFs. This project extends previous methods by introducing a method for identifying CCF events, a collection of CCF events from industry failure data, and a computerized system for quantifying probabilistic risk assessment (PRA) parameters and uncertainties. This report provides guidance on how to apply the CCF database information to PRA studies.

A CCF event consists of component failures that meet four criteria: (1) two or more individual components fail or are degraded, including failures during demand, in-service testing, or deficiencies that would have resulted in a failure if a demand signal had been received; (2) components fail within a selected period of time such that success of the PRA mission would be uncertain; (3) component failures result from a single shared cause and coupling mechanism; and (4) a component failure occurs within the established component boundary.

Two data sources are used to select equipment failures to be reviewed for CCF events: The Nuclear Plant Reliability Data System (NPRDS) and the Sequence Coding and Search System (SCSS). These sources served as the developmental basis for the CCF data collection and analysis system. CCF event coding guidance permits the analysts to consistently code CCF events. Sufficient information is recorded to ensure accuracy and consistency. Additionally, the CCF events are stored in a format that allows PRA analysts to review the events and develop an understanding on how the events occurred.

A software system stores CCF and independent failure data and automates the PRA parameter estimation process. The system employs two quantification models: alpha factor and multiple Greek letter. These models are used throughout the nuclear industry. Parameter estimations can be used in PRA studies throughout the industry in place of the current CCF parameter estimates, giving a more accurate treatment of common cause failures.

This report discusses the steps a PRA analyst must take to appropriately address common cause failures in PRA studies. Specifically, it is intended to be used in conjunction with the NRC CCF methods developed as part of the CCF database software, along with the data contained in the CCF database. Provided herein is direction on how to perform the qualitative and quantitative analyses to achieve the desired PRA study objective.

ACRONYMS

AEOD	Nuclear Regulatory Commission's Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
BFR	binomial failure rate
BP	basic parameter
CC	component cooling
CCBE	common cause basic event
CCCG	common cause component group
CCDAT	common cause data analysis tool (developed by EPRI)
CCF	common cause failure
CCP	centrifugal charging pump
CCW	component cooling water
CS	containment spray
CST	condensate storage tank
DP	differential pressure
EHC	electro-hydraulic control
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ESW	emergency service water
GL	generic letter
HPCI	high pressure coolant injection
HPSI	high pressure safety injection
INEEL	Idaho National Engineering and Environmental Laboratory
IRRAS	Integrated Reliability and Risk Analysis System
ISI	inservice inspection
LCO	limiting condition for operation
LER	Licensee Event Report
MDAFWP	motor driven auxiliary feedwater pump
MFP	main feedwater pump
MGL	multiple Greek letter
MLE	maximum likelihood estimators
MOV	motor operated valve
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
PRA	probabilistic risk assessment
PT	periodic test
PWR	pressurized water reactor
RBE	reliability benchmark exercise
RCIC	reactor core isolation cooling
RHR	residual heat removal
RTP	rated thermal power
SCSS	Sequence Coding and Search System
SG	steam generator
TS	technical specifications

ACKNOWLEDGMENTS

The authors would like to thank Karl Fleming, ERIN Engineering, Gareth Parry, USNRC, and Henrique Paula, JBF Associates, for their contributions to the development of this document. They have provided critical reviews of this project, and their historical work in the development of CCF analysis methods has laid a strong foundation for the present work.

Additionally, the authors want to acknowledge the efforts of Steven Novack and James Bryce of the INEEL for their reviews of several iterations of this report.

Modeling Common Cause Failures in Probabilistic Risk Assessments

1. INTRODUCTION

1.1 General Purpose and Background

This report provides a set of guidelines to help probabilistic risk assessment (PRA) analysts in modeling common cause failure (CCF) events in commercial nuclear power plants. The aim is to enable the analyst to identify important common cause vulnerabilities, incorporate their impact into system reliability models, perform data analysis, and quantify system unavailability in the presence of CCFs. Some of the material in this volume has been presented in previous reports, NUREG/CR-4780[1,2] and NUREG/CR-5801.[3] The purpose of this document is to bring together the key aspects of these procedural guidelines supplemented by additional insights gained from their application, enhanced by the capabilities of the CCF software and its data analysis capabilities, recently developed by the United States Nuclear Regulatory Commission (NRC).[4-7]

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. 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 system function compared to cases where failures are independent. In terms of system reliability modeling, incorporation of the effects of dependent failures into the model provides more realistic estimates of system unavailability.

Reactor operating experience has shown that dependent events are major elements of reactor incidents and accidents. This result, in one respect, is due to the success achieved in minimizing the frequency of potential accidents caused by the 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. The operating experience also 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.

The results of many risk studies have shown a consistent pattern that reinforces the importance of dependent events that is apparent in reactor operating experience reports. These results consistently include a finding that various types of dependent events dominate plant risk and system unavailability.

Methods for the analysis of common cause failures have evolved over the past twenty years from simple quantitative models to elaborate systematic methods for data gathering, qualitative engineering analysis, and quantification of the probabilities of CCF events and their impact on risk and reliability measures. In 1988, as the result of collaborative effort between the Electric Power Research Institute (EPRI) and the US NRC, the two volume guidebook NUREG/CR-4780[1,2] was published. NUREG/CR-4780 was a major step forward in bringing the results of earlier research and development in treatment of CCF into a coherent and comprehensive framework with extensive methodological and practical guidelines to support risk analyses. It also introduced new ideas and techniques needed to overcome problems in the areas of data analysis, reliability logic modeling, and parametric modeling of CCF probabilities. Some of these problems were identified during the international "Reliability Benchmark Exercise in Common Cause Failures," (RBE-CCF) sponsored by the Euratom Joint Research Center in Ispra, Italy.[8] Insights gained from the RBE-CCF influenced the preparation of NUREG/CR-4780.[2]

The success of NUREG/CR-4780 is evident in the impact it has had on the quality of treatment of CCF in PRA studies conducted since its publication in 1988. The guidebook, however, had its own shortcomings. Some were due to a mismatch between sophistication of the methodological requirements of the report and real application constraints in terms of resources required, and also the availability of information needed (i.e., suitable databases to support the analysis). Also the elaborate method for event analysis proposed in the guidebook did not provide adequate practical guidance for qualitative and quantitative analysis of CCF events.

Several efforts were initiated to overcome these shortcomings. To improve techniques for qualitative analysis of plant-specific vulnerabilities to CCF events and quantitative analysis of data for estimation of their probabilities, NRC-sponsored projects produced new methods and procedural guidelines for analysts.[9,10] The International Atomic Energy Agency also published a simplified common cause analysis guidebook which included some methodological improvements.[11]

In the area of data collection, EPRI issued an updated version of the CCF database[12] covering operating experience in the US commercial nuclear power plants through 1990.[13] The data were classified and analyzed using the approach in NUREG/CR-4780. In 1992 the NRC launched a major effort to collect and systematically analyze CCF events. The EPRI and NRC databases were converted into electronic format in the computer codes common cause data analysis tool (CCDAT)[14] and CCF System,[7] respectively. A new international effort known as the International Common Cause Data Exchange project, initiated in 1994, is also underway to develop a database through sharing the CCF experience of many countries and many different types of plants and operating practices.

Application of the procedures outlined in NUREG/CR-4780 and NUREG/CR-5801 usually require considerable effort and resources. To reduce this effort, it was desirable to computerize the procedure as much as practicable. CCDAT was the first step in this direction, but it was limited in functionality and scope. The CCF System is a comprehensive software system that automates many of the data analysis steps and CCF parameter estimation. The CCF System provides guidance on the screening and interpretation of data, and contains a database of relevant event data in an effort to provide a more uniform and cost-effective way of performing CCF analyses. The database contains CCF-related events that have occurred in U.S. commercial nuclear power plants from 1980 through 1995. The events were identified from failure reports in the Nuclear Plant Reliability Data System (NPRDS), which is a proprietary database maintained by the Institute of Nuclear Power Operations (INPO), and Licensee Event Reports (LERs), obtained from the Sequence Coding and Search System (SCSS) database maintained by the Oak Ridge National Laboratory for the NRC. The current data collection effort has separated the data by system as well as by component type.

The principal products of CCF System development are the method and guidelines for identifying, classifying, and coding CCF events, the CCF database containing both CCF events and an estimate of independent failure counts, and the CCF parameter estimation software.

The CCF event identification process includes reviewing failure data to identify CCF events and counting independent failure events. The process allows the analyst to consistently screen failures and identify CCF events. The CCF event coding process provides guidance for the analyst to consistently code

CCF events. Additionally, the CCF events are stored in a format that allows PRA analysts to review the events and develop an understanding of how they occurred.

The CCF analysis software uses the impact vector method demonstrated in NUREG/CR-4780. The basic information needed for understanding and coding a CCF event is based on the physical characteristics of the event, and is recorded in fields in the database. The database software allows an analyst to tailor the assessment of these parameters for plant-specific analyses.

The interpretation of the degree of impact of the CCF events on affected components is necessarily a subjective process. Impact interpretations contained in the database are clearly documented for each event. In addition, the analysis software provides the opportunity for analysts to review and modify these evaluations when performing plant-specific CCF analyses. The CCF parameters estimated by the database software are conditional on these particular interpretations. Therefore, the NRC will continue to review CCF analyses used in regulatory applications on a case-by-case basis. The use of the CCF Database should help to make the analyses easier to properly perform and more scrutable during the review process.

These advancements and improvements introduced since the publication of NUREG/CR-4780 together with lessons learned from CCF analysis applications motivated the development of the present guidebook. This guidebook incorporates the results of previous developments into an updated analysis framework and procedural guidelines which, together with tools such as the CCF system, should enable analysts to perform a more credible CCF analysis in much less time than was possible in the past. The 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. While it is not the purpose of this report to advance or promote a particular method or technique, the procedures presented here are more prescriptive than those in previous guidebooks, reflecting the lessons learned from field applications based on earlier guidance. At the same time, significant flexibility has been built into the framework and procedural steps so that the analysis can be performed to support general and specific studies.

The updated procedural framework presented in this report is designed to help the analyst make intelligent choices, while providing the structure necessary to ensure that all the issues involved are considered, to help the analyst understand 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 analyses (1) more tractable for the analyst, (2) more consistent and scrutable to peer and regulatory reviewers, (3) more realistic from a licensee perspective, and (4) more defensible by study sponsors. The framework goes further than providing procedural guidance; together with the technical appendices that explain the relationship between the various models and the associated data analysis processes, the procedure presents a conceptual, as well as practical, framework for analyzing common cause failures.

The overall objectives of this report are to

1. Provide a procedural framework for common cause analysis for use in applied risk and reliability evaluations.

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 and CCF analysis 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 to use alternative systems modeling approaches and techniques for CCF parameter estimation and data handling when alternatives exist.

1.2 PRA Treatment of Dependent Failures and Role of CCFs

The definition of CCF is closely related to the general definition of dependent failure. Therefore, a definition of dependent events is provided in a simplified presentation of the case of two events A and B. Two events, A and B, are said to be dependent if

$$P(AB) \neq P(A)P(B)$$

In the presence of dependencies, often, but not always, $P(AB) > P(A)P(B)$. Therefore, if A and B represent failure of a safety function, the actual probability of failure of both will be higher than the expected probability calculated based on the assumption of independence. In cases where a system provides multiple layers of defense against total system or functional failure, presence of dependence translates into a reduced safety margin and can result in overestimation of the level of reliability, if the dependence is ignored.

Dependencies can be classified in many different ways. A classification which is useful in relating operational data to reliability characteristics of systems is presented in the following paragraphs. In this classification dependencies are first categorized based on whether they stem from intended intrinsic functional and physical characteristics of the system, or are due to external factors and unintended characteristics. Therefore dependence is either **intrinsic** or **extrinsic** to the system. The definitions and subclassifications follow.

Intrinsic. This refers to dependencies where the functional status of one component is affected by the functional status of another. These dependencies normally stem from the way the system is designed to perform its intended function. There are several subclasses of intrinsic dependencies based on the type of influence that components have on each other. These are:

- **Functional Requirement Dependency.** This refers to the case where the functional status of component A determines the functional requirements of component B. Possible cases include

  - B is not needed when A works,
  - B is not needed when A fails,
  - B is needed when A works,
  - B is needed when A fails.

  Functional requirement dependency also includes cases where the load on B is increased upon failure of A.

- **Functional Input Dependency (or Functional Unavailability).** This is the case where the functional status of B depends on the functional status of A. An example is the case where A must work for B to work. In other words B is functionally unavailable as long as A is not working. An example is the dependence of a pump on electric power. Loss of electric power makes the pump functionally unavailable. Once electric power becomes available, the pump will also be operable.

- **Cascade Failure.** This refers to the cases where failure of A leads to failure of B. For example, failure of a valve on a pump suction line to open, may cause the pump to fail if it is started. In this case even if the valve is made operable, the pump would still remain inoperable. A cascading effect is within the design envelope and is often known to designers and operators.

Combinations of the above dependencies identifies other types of intrinsic dependencies. An example is the **Shared Equipment Dependency**, when several components are functionally dependent on the same component. For example if both B and C are functionally dependent on A, then B and C have a shared equipment dependency.

Extrinsic. This refers to dependencies where the couplings are not inherent and intended in the designed functional characteristics of the system. Such dependencies are often physically external to the system. Examples of extrinsic dependencies are:

- **Physical/Environmental.** This category includes dependencies due to common environmental factors, including harsh or abnormal environment created by a component. For example, high vibration induced by A causes failure of B.

- **Human Interactions.** Dependency due to man-machine interaction. An example is failure of multiple components due to the same maintenance error.

In risk and reliability modeling, known intrinsic dependencies should be modeled explicitly in the logic model (e.g., fault tree) of the system. In nuclear power plant risk and reliability studies, a large number of extrinsic dependencies are treated through modeling of the phenomena and the physical processes involved. Examples are fire and seismic in the category of Physical/Environmental dependencies.

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 for a first approximation are considered independent. This step is necessary to enable the analyst to construct manageable models. However, many intrinsic dependencies among component failures are not accounted for explicitly in the logic model, meaning that the basic events are not actually 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 during the mission time and due to the same shared cause. Consistent with current practice in systems modeling,[1] the reliability analysis methods presented here exclude functional dependency failures because they are assumed to modeled explicitly in the logic models. 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. Viewed in this fashion, CCFs are inseparable from the class of dependent failures and the distinction is mainly based on the level of treatment and choice of modeling approach in reliability analysis.

CCFs result from the coexistence of two main factors: a susceptibility for components to fail or become unavailable due to a particular **root cause** of failure, and a **coupling factor** (or coupling mechanism) that creates the condition for multiple components to be affected by the same cause. An example is the case where two relief valves fail to open at the required pressure due to set points being set too high, as a result of an incorrect procedure. Each of these two valves fail to fulfill their safety function due to an incorrect setpoint. What makes the two valves fail together, however, is a common calibration procedure, and perhaps a contributor is common maintenance personnel. These commonalities are the coupling factors of the failure event in this case. It is obvious that each component fails because of its susceptibility to the conditions created by the root cause, and the role of the coupling factor is to make those conditions common to several components. Defenses against root causes result in improving the overall reliability of each component but do not necessarily reduce the fraction of failures that occur due to common cause. The susceptibility of a system containing redundant components to dependent failures, as opposed to independent failures, is determined by the presence of coupling factors.

Characterization of CCF events in terms of these key elements provides an effective means of assessing the CCF phenomenon by identifying plant vulnerabilities to CCFs and evaluation of the need for, and effectiveness of, defenses against them. This characterization is equally effective in evaluation and classification of operational data and quantitative analysis of CCF probabilities.

Defining CCFs in terms of root cause and coupling factor, as well as the timing of failures, expresses (explicitly or implicitly) the main features of CCFs for most applications. The concept of a shared cause resulting in malfunction, or change in component state, is the key aspect of a CCF event. The use of the word "shared" implicitly includes the concept of coupling factor or mechanism. Also, the reference to a time interval between failures acknowledges the reliability significance of these events. For some applications, however, the time characteristic may not be the critical discrimination. Multiple component failures due to a shared cause that do not affect the mission requirements are of little or no significance from a reliability point of view. It is the correlation between component failure times and their simultaneity in reference to the specified mission time that is significant in terms of reliability. Of course, when the same cause is acting on multiple components, times of failure are often closely correlated.

Components that fail due to a shared cause normally fail in the same functional mode. The term "common mode failure," which was used in the early literature and is still used by some practitioners, is more indicative of the most common symptom of the CCF, i.e., failure of multiple components in the same mode, but it is not a precise term for communicating the important characteristics that describe a CCF event.

1.3 Structure of the Report

Section 2 of this report provides an overview of the guidelines, dividing the entire process into three phases: Screening Analysis, Detailed Qualitative Analysis, and Detailed Quantitative Analysis. These are discussed respectively in Sections 3, 4, and 5. An example application of the procedure is provided in Section 6. A series of appendices provide important technical details on the models, application of models, uncertainty of parameter estimates, and treatment of CCFs in event assessment.

2. OVERVIEW OF ANALYSIS PROCEDURE

As summarized in Figure 2-1, the procedure for CCF analysis is organized into three phases:

Phase I : **Screening Analysis,**

Phase II : **Detailed Qualitative Analysis,** and

Phase III: **Detailed Quantitative Analysis.**

'Each phase has several steps as shown in the Figure 2-1.

The objectives of the screening analysis, Phase I, are to: 1) identify in a preliminary and conservative manner all the potential vulnerabilities of the system being analyzed to CCFs, and 2) identify those groups of components within the system whose CCFs contribute significantly to the system unavailability. Phase I develops the scope and justification for the detailed analyses of Phases II and III. In addition, Phase I provides conservative, bounding system unavailabilities due to CCFs. Depending on the objectives of the study and the availability of resources, the analysis may be stopped at the end of this phase recognizing that the qualitative results may not accurately represent the actual plant vulnerabilities, and that the quantitative estimates may be very conservative.

Phase II aims at developing an understanding of the plant-specific vulnerabilities to CCFs by evaluating the susceptibility of the systems and components at a specific plant to causes and coupling factors of CCFs found throughout the industry. This involves the identification of plant-specific defenses in place and qualitative evaluation of their effectiveness. The results of the qualitative analysis form the basis to improve the defenses against CCFs and reduce the likelihood of their occurrence.

The key technique used in Phase II is the so-called Cause-Defense Matrix.[9] The procedures of this phase are summaries of the concepts and procedures provided in References 9 and 11. The steps of this phase require intensive effort in collecting and analyzing detailed information regarding the specific characteristics of the plant and systems being analyzed. As such, it is important that this phase is preceded by the preliminary screening analyses of Phase I in order to limit the scope of the detailed analysis.

Phase III uses the results of Phases I and II, and through several steps involving the detailed logic modeling, parametric representation, and data analysis, develops numerical values for system unavailabilities due to CCF events. These steps are suggested in References 1 and 3, with minor modifications to fit the scope and objectives of the present document. Given the results of the Phase I analyses, a detailed quantitative analysis can be performed even if a detailed qualitative analysis has not been performed. However, as will be seen later, some of the steps in the detailed quantification can benefit significantly from the insights and information obtained as a result of the Phase II analysis.

Depending on the overall objectives of specific studies, the analysis can stop at the end of any of these three phases. However, each successive phase builds on the results of the preceding phase(s) and should not be completed independently.

SCREENING ANALYSIS

- **Problem Definition and System Modeling**
  - Plant familiarization
  - Identification of system and analysis boundary conditions
  - Development of component level system fault tree
- **Preliminary Analysis of CCF Vulnerabilities**
  - Qualitative screening
  - Quantitative screening

DETAILED QUALITATIVE ANALYSIS

- **Review of Plant Design and Operating Practices**
- **Review of Operating Experience**
- **Development of Cause-Defense Matrices**

DETAILED QUANTITATIVE ANALYSIS

- **Common Cause Modeling**
  - Identification of common cause basic events (CCBE)
  - Incorporation of CCBEs into fault trees
  - Parametric representation of CCBEs
- **Data Analysis and Parameter Estimation**
  - Parameter estimation
  - Basic event probability development
- **System Quantification and Results Interpretation**
  - System unavailability quantification
  - Results evaluation/sensitivity analysis
  - Reporting

Figure 2-1. Procedural framework for common cause failure analysis.

3. PHASE I: SCREENING ANALYSIS

The primary objective of this phase is to perform a preliminary analysis of the CCF vulnerabilities that would identify in a conservative way, and without significant effort, all important groups of components susceptible to common cause failure. Phase I is a screening process to develop the scope of the more detailed analysis in the subsequent phases. This is done in two steps:

1. **Qualitative Screening**
2. **Quantitative Screening**

Prior to performing the CCF screening analysis the analyst should take several key steps needed in any systems analysis including

- Plant familiarization
- Identification of system and analysis boundaries
- Development of a component level system logic model (e.g., fault tree)

Since these steps are fairly standard and the related methods, procedures, and tools are widely known no further discussion will be provided on these topics. The two CCF screening steps are described next.

3.1 Qualitative Screening

At this stage, an initial qualitative analysis of the system is performed to identify the potential vulnerabilities of the system and its components to CCFs. This analysis is aimed at providing a list of components which are believed to be susceptible to CCF. At a later stage, this initial list will be modified on quantitative grounds. In this early stage, conservatism is justified and encouraged. In fact it is important not to discount any potential CCF vulnerability unless there are immediate and obvious reasons to discard it.

The most efficient approach to identifying common cause system vulnerabilities is to focus on identifying **coupling factors**, regardless of defenses that might be in place against some or all categories of CCFs. The result will be a conservative assessment of the system vulnerabilities to CCFs. This, however, is consistent with the objective of this stage of the analysis which is a preliminary, high level screening.

As described earlier, a coupling mechanism is what distinguishes CCFs from multiple independent failures. Coupling mechanisms are suspected to exist when two or more components failures exhibit similar characteristics, both in the cause and in the actual failure mechanism. The analyst, therefore, should focus on identifying those components of the system which share one or more of the following:

- Same design
- Same hardware
- Same function
- Same installation, maintenance, or operations staff
- Same procedures
- Same system/component interface
- Same location
- Same environment

This process can be enhanced by developing a checklist of key attributes, such as design, location, operation, etc., for the components of the system. An example of such a list is the following:

- **Component type (e.g., motor operated valve):** including any special design or construction characteristics, such as component size and material.

- **Component use:** system isolation, flow modulation, parameter sensing, motive force, etc.

- **Component manufacturer.**

- **Component internal conditions:** absolute or differential pressure range, temperature range, normal flow rate, chemistry parameter range, power requirements, etc.

- **Component boundaries and system interfaces:** common discharge header, interlocks, etc.

- **Component location name and/or location code:** located in the same building, or have control panels that look identical in separate rooms.

- **Component external environmental conditions:** temperature range, humidity range, barometric pressure range, atmospheric particulate content and concentration, etc.

- **Component initial conditions:** normally closed, normally open, energized, etc.; and **operating characteristics:** normally running, standby, etc.

- **Component testing procedures and characteristics:** test interval, test configuration or lineup, effect of test on system operation, etc.

- **Component maintenance procedures and characteristics:** planned, preventive maintenance frequency, maintenance configuration or lineup, effect of maintenance on system operation, etc.

The above list or a similar one is a tool to help identify the presence of identical components in the system and most commonly observed coupling factors. It may be supplemented by a plant walk-down, and review of operating experience (e.g., failure event reports). Any group of components which share similarities in one or more of these characteristics is a potential point of vulnerability to CCF. However, depending on the system design, functional requirements, and operating characteristics, a combination of commonalities may be required in order to create a realistic condition for CCF susceptibility. Such situations should be evaluated on a case by case basis before deciding on whether or not there is a vulnerability. A group of components identified in this process is called a **common cause component group** (CCCG).

In practice the following guidelines are generally adopted for the selection of CCCGs:

1. When identical, functionally non-diverse, and active components are used to provide redundancy, these components should always be assigned to a CCCG, one for each group of identical redundant components.

2. In general, as long as CCCGs in the above category are identified, the assumption of independence among diverse components is a good one and is supported by operating experience data. However, when diverse redundant components have piece parts that are identically redundant, the components should not be assumed fully independent. One approach in this case is to break down the component boundaries and identify the common piece parts as a CCCG. For example, pumps can be identical except for their drivers.

3. In system reliability analysis, it is frequently assumed that certain passive components can be omitted, based on the argument that active components dominate. In applying this

screening criteria to common cause analysis, it is important to not exclude events such as debris blockage of redundant or even diverse pump strainers.

Finally, in addition to following the above guidelines, it is important for the analyst to review the operating experience as reported in, for example, the LERs, to ensure that past failure mechanisms are included with the components selected in the screening process. Later in the detailed qualitative and quantitative analysis phases this task is performed in more detail to include the operating experience of the plant being analyzed. In the screening phase, knowledge of industry experience is sufficient.

3.2 Quantitative Screening

The qualitative screening step identifies potential vulnerabilities of the system to CCFs. By focusing on failure mechanisms and ignoring plant-specific defenses, the results of the screening are conservative. This ensures that if the analysis is stopped at this level, no major common cause vulnerabilities are neglected, and that the results of any detailed analysis are bounded by the screening results.

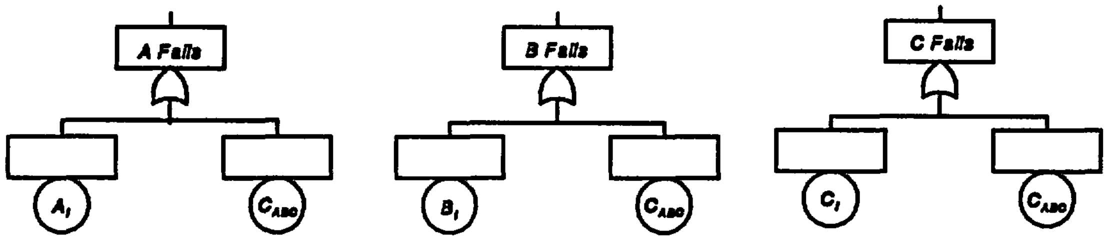
By using conservative qualitative analysis, the size of the problem is significantly reduced. However, detailed modeling and analysis of all potential common cause vulnerabilities identified in the qualitative screening may still be impractical and beyond the capabilities and resources available to the analyst. Consequently, it is desirable to reduce the size of the problem even further to enable detailed analysis of the most important common cause system vulnerabilities. Reduction is achieved by performing a **quantitative screening** analysis. This step is useful for systems reliability analysis and may be essential for accident-level analysis in which exceedingly large numbers of cutsets may be generated in solving the fault tree logic model.

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

1. The component-level fault trees are modified to explicitly include a "global" or "maximal" common cause failure event for each component in every common cause component group. A global common cause event in a group of components is one in which all members of the group fail. A maximal common cause event is one that represents two or more common cause basic events. As an example of this step of the procedure, consider a CCCG composed of three components A, B, and C. According to the procedure, the basic events of the fault tree involving these components, i.e.,

A Fails
B Fails
C Fails

are expanded to include the basic event C_{ABC}, which is defined as the concurrent failure 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 computer code [e.g., SETS[15] and Integrated Reliability and Risk Analysis System (IRRAS)[16]] to obtain the minimal cutsets for the system or accident sequence. Any resulting cutset involving the intersection $A_I B_I C_I$ will have an associated cutset involving C_{ABC}. The significance of this process is that, in large systems or accident sequences, some truncation of the 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 basic event can be estimated using a simple global parametric model:

$$P(C_{ABC}) = g\,P(A) \qquad (3.1)$$

P(A) is the total failure probability of the component. Table 3-1 lists values of the global common cause factor, g, for dependent k-out-of-n system configurations for success. The basis for these screening values is described in Section 5. Note that different g values apply depending on whether the components of the system are tested simultaneously (non-staggered) or one at a time at fixed time intervals (staggered). More details on the reasons for the difference is provided in Section 5.

The simple global or maximal parameter model (similar in form to the single parameter models discussed in Section 5) provides a conservative approximation to the CCF frequency regardless of the number of redundant components in the CCCG being considered.

Those CCCGs that are found to contribute little to system unavailability or accident sequence frequency (or which do not survive the probability-based truncation process) can be dropped from further consideration. Those that are found to contribute significantly to the system unavailability or accident sequence frequency are retained and further analyzed using the guidelines for more detailed qualitative and quantitative analysis.

The objective of the initial screening analysis is to identify potential common cause vulnerabilities and to determine those that are insignificant contributors to system unavailability and to the overall risk, to eliminate the need to analyze them in detail. The analysis can stop at this level if a conservative assessment is acceptable and meets the objectives of the study. Otherwise the component groups which survive the screening process should be analyzed in more detail, according to the Phase II and Phase III guidelines.

A complete detailed analysis should be both qualitative and quantitative. A detailed quantitative analysis, is always required to provide the most realistic estimates with minimal uncertainty. In general, a realistic quantitative analysis requires a thoroughly conducted qualitative analysis. A detailed qualitative analysis provides many valuable insights that can be of direct use in improving the reliability of the systems and safety of the plant. The next section of the report provides guidelines for performing a detailed qualitative analysis. It is then followed by guidelines for detailed quantitative analysis.

Table 3-1. Screening values of global common cause factor, g, for different system configurations.

Success Configuration	Values of g	
	Staggered Testing Scheme	Non-staggered Testing Scheme
1 of 2	0.05	0.10
2 of 2		
1 of 3	0.03	0.08
2 of 3	0.07	0.14
3 of 3		
1 of 4	0.02	0.07
2 of 4	0.04	0.11
3 of 4	0.08	0.19
4 of 4		

4. PHASE II: DETAILED QUALITATIVE ANALYSIS

The objective of the detailed qualitative analysis is to identify the potential vulnerabilities of the system being analyzed to the diverse CCFs that can occur. The difference between this and the qualitative screening analysis of Phase I is the level of detail and the number of CCF events being considered. This detailed analysis focuses on obtaining considerably more plant-specific information, and can provide the basis and justification for engineering decisions regarding system reliability improvements. In addition, the detailed evaluation of system CCF vulnerabilities provides essential information for a realistic evaluation of operating experience and plant-specific data analysis as part of the detailed quantitative analysis. It is assumed that the analyst has already conducted the screening analysis of Phase I, is armed with the basic understanding of the analysis boundary conditions, and has a preliminary list of the important CCCGs.

An effective detailed qualitative analysis involves the following activities:

- Review of operating experience (generic and plant-specific)
- Review of plant design and operating practices
- Development of root cause-defense and coupling factor-defense matrices.

The key products of this phase of analysis include a final list of common cause component groups supported by documented engineering evaluation. This evaluation may be summarized in the form of a set of Cause-Defense and Coupling Factor-Defense matrices developed for each of the CCCGs identified in Phase I. These detailed matrices explicitly account for plant-specific defenses, including design features and operational and maintenance policies, in place to reduce the likelihood of failure occurrences. The results of the detailed qualititative analysis provide insights about safety improvements that can be pursued to improve the effectiveness of these defenses and reduce the likelihood of CCF events.

4.1 Review of Operating Experience

An important step toward developing a good understanding of plant CCF vulnerabilities is a comprehensive review of operating experience at the subject plant as well as other nuclear power plants. This review enables the analyst to develop insights regarding the failure causes and mechanisms, and how they relate to the physical and operational characteristics of components, systems, and plants. For this type of detailed data review the analyst needs to consult databases that provide detailed event descriptions. Unfortunately most databases are incomplete and inconsistent, particularly with respect to the type of information required in a detailed common cause analysis. In practice, one has to consult several sources of information, including documents describing physical and functional characteristics of the systems and the plant, as well as the governing operating procedures.

For generic insights, generic compilations of CCF events such as various EPRI documents[12, 13] and the CCF System computerized database developed by the US NRC[4 - 7] provide a comprehensive source of information. For information on plant-specific experience related to common cause failures plant, records such as Maintenance Work Orders, Operator Logs, Work Request Forms, and Significant Event Reports, may be consulted.

The objective of this review is to gain qualitative insights, and not necessarily to collect statistics or perform data classification. Such data classification and statistical analyses are of course, needed as part of the subsequent detailed quantitative analysis phase. The key concepts needed for the qualitative event data review are identification of failure cause and coupling mechanism. Each of these are discussed in further detail below. (See also References 3 and 9.)

4.1.1 Failure Causes

It is recognized that the description of a failure in terms of the most obvious "cause" is often too simplistic. For example, it may be quite adequate to identify that a pump failed because of high humidity. But to understand, in a detailed way, the potential for multiple failures, it is necessary to identify further why the humidity was high and why it affected the pump (i.e., it is necessary to identify the ultimate reason for the failure). There are many different paths by which this ultimate reason for failure could be reached. Also, the sequence of events that constitute a particular failure path, or failure mechanism, is not necessarily simple. As an aid to thinking about failure mechanisms, the following concepts are useful.

A ***proximate cause*** of a failure event is the condition that is readily identifiable as leading to the failure. In the above example, humidity could be identified as the proximate cause. The proximate cause can be regarded as a symptom of the failure cause, and it does not in itself necessarily provide a full understanding of what led to that condition. As such, it may not be the most useful characterization of failure events for the purposes of identifying appropriate corrective actions.

To expand the description of the causal chain of events resulting in the failure, it is useful to introduce the concepts of ***conditioning events*** and ***trigger events***. These concepts are particularly useful in analyzing component failures from environmental causes.

A ***conditioning event*** increases component susceptibility to failure, but does not of itself cause failure. In the previous example (a pump failed because of high humidity), the conditioning event could have been failure of maintenance personnel to properly seal the pump control cabinet following maintenance. The effect of the conditioning event is latent, but the conditioning event is frequently a necessary contributor to the failure mechanism. Understanding the conditioning event can provide insights into the failure mechanism and its possible defenses. A ***trigger event*** activates a failure, or initiates the transition to the failed state, whether or not the failure is revealed at the time the trigger event occurs. The event which led to high humidity in a room, and subsequent equipment failure, would be such a trigger event. A trigger event therefore is a dynamic feature of the failure mechanism. A trigger event, particularly in the case of CCF events, is usually an event external to the components in question.

It is not always necessary, or even possible, to uniquely define a conditioning event and a trigger event for every type of failure. However, the concepts are useful in that they focus on the ideas of an immediate cause, and subsidiary causes, whose function is to increase susceptibility to failure, given the appropriate ensuing conditions. Some examples of the use of these concepts are given in Table 4-1.

The next concept of interest is that of the ***root cause***. The root cause is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence. The identification of a root cause is tied to the implementation of defenses.

As shown in Table 4-1, the root cause may be determined to be a trigger event (second event in the table) or a conditioning event (third event). It is clear from events 1 and 4 in Table 4-1 that many proximate causes (moisture and vibration) are indeed only symptoms of the root cause, and that identifying the proximate causes neither provides a full understanding of what led to that condition nor identifies how to prevent subsequent similar failure. All too often, investigations of failure occurrences (and thus the event descriptions in failure reports and in databases) do not determine the root causes of failures, even though this determination is crucial for judging the adequacy of defenses against these failures.

Table 4-1. Examples illustrating concepts useful in analyzing common cause failure.

Failure Event	Proximate Cause	Trigger Event	Conditioning Event	Root Cause
1. A pump fails to run because of moisture in the pump control cabinet	Corrosion from moisture or high humidity	Event leading to the occurrence of high humidity (e.g., steam leak in pump room)	Failure to properly seal the control cabinet following maintenance	Lack of attention during maintenance and/or deficiency in the written procedure
2. A design error is such that under real demand conditions a component fails to perform its function (Component had successfully performed its function during testing)	Equipment failure	Design error	None	Error in design realization and failure to realize that proof testing was not adequately simulating real demand conditions
3a. Following a maintenance act, a component fails. The failure is eventually attributed to an error in the maintenance crew	Maintenance error	Maintenance act	Error or ambiguity in maintenance procedure	Error or ambiguity in maintenance procedure and inadequate training
3b. Following a maintenance act, a component fails. The failure is eventually attributed to a slip on the part of the maintenance crew	Maintenance error	Maintenance act	Inadequate training and lack of attention during maintenance	Inadequate training and lack of motivation
4. A pump shaft fails because of the cumulative effect of high vibration, resulting from an installation error	Vibration	Cumulative exposure of the pump to the excessive vibration	Installation error	Inadequate training of installation crew and deficiency in installation procedures

4.1.2 Coupling Factors and Mechanisms

For failures to become multiple failures from a shared cause, the conditions have to be conducive for the trigger event and/or the conditioning events to affect all components within the group simultaneously. The meaning of simultaneity in this context is that failures lead to inability of redundant components to perform their safety function within the appropriate mission time. A coupling factor is a characteristic of a group of components or piece parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission and operational, maintenance, and test procedures. These factors, in some references, have been referred to as examples of coupling mechanisms, but because they really identify a potential for common susceptibility, it is preferable to think of these factors as characteristics of a common cause component group.

The coupling factor classification format consists of three major classes:

- Hardware Based,
- Operation Based, and
- Environment Based.

These three classes are divided into subcategories to provide more detail for important parameters and attributes. The multi-layered coding approach acknowledges that during classification it is likely that only major categories can be identified because failure event descriptions are often not detailed enough to allow fine distinction down to the subcategories. When determining the coupling factors of an event with limited data, more than one coupling factor can be assigned to a CCF event. This is not a negative point since this approach allows the analyst to evaluate a broader set of defenses when determining the applicability of the coupling factors to the plant under consideration.

4.1.2.1 Hardware Based. Hardware based coupling factors are factors that propagate a failure mechanism among several components due to identical physical characteristics. An example of hardware based coupling factors is failure of several residual heat removal (RHR) pumps because of the failure of identical pump air deflectors. There are two subcategories of hardware based coupling factors: (1) **hardware design**, and (2) **hardware quality (manufacturing and installation)**.

Hardware design coupling factors result from common characteristics among components determined at the design level. There are two groups of design-related hardware couplings: system level and component level. **System-level** coupling factors include features of the system or groups of components external to the components that can cause propagation of failures to multiple components. **Component-level** coupling factors are caused by features within the boundary of each component.

The following are coupling factors in the hardware design category.

- ***Same Physical Appearance.*** The same physical appearance refers to cases where several components have the same identifiers (e.g., same color, distinguishing number/ letter coding, and/or same size/shape). These conditions could lead to misidentification by the operating or maintenance staff.

  - An operator removed Unit 2 RHR pumps B and D for maintenance instead of Unit 3 pumps B and D. The pumps were isolated for two hours before the error was discovered. The error was due to lack of distinguishable identificati ,n codes.

- *System Layout/Configuration.* The system layout and configuration coupling factors refer to the arrangement of components to form a system.

  - Two motor-driven auxiliary feed water pumps lost suction because of air trapped in the supply header that provides condensate flow between the condensate storage tank (CST) and the hot wells. The two failed pumps took suction from the top of the header, while the turbine-driven pump (which took suction from the side of the header) was unaffected. A vent was installed on the condensate rejection line.

  - Two containment spray pumps failed to meet differential pressure requirements due to air binding at the pump suction. These failures resulted from a system piping design error.

- *Same Component Internal Parts.* The same component internal parts coupling factor refers to characteristics that could lead to several components failing because of the failure of similar internal parts or subcomponents. This coupling factor category is useful when investigating the root cause of component failures. This coupling factor is used when the investigation is limited to identifying the subcomponents or piece-part at fault, rather than the root cause of failure of the piece-part.

  - On two occasions, both the high pressure coolant injection (HPCI) and reactor core isolation cooling (RCIC) pumps tripped during tests. The cause was failed teflon rupture discs. The discs were inadequate for their intended purpose.

  - During normal operations, it was found that two auxiliary feedwater pump turbines experienced speed oscillations; in one case the turbine tripped. Both oscillation problems were researched and it was determined that the buffer springs on the governor were the wrong size. The springs were removed and replaced with the correct springs.

- *Same Maintenance/Test/Calibration Characteristics.* The same maintenance/test/calibration characteristics refer to the similarity in maintenance/test/calibration requirements, including frequency, type, tools, techniques, and personnel-required level of expertise.

  - Two diesel generators failed to load due to shutdown sequencer problems. During one diesel generator failure, the diesel could not be loaded manually or automatically due to dirty contacts on the sequencer. In the second diesel generator failure, the sequencer clutch stuck due to being dirty and needing lubrication. The cause was determined to be the lack of preventative maintenance and unsuitable maintenance and test equipment. To resolve the lack of preventative maintenance problems, a preventative maintenance procedure was developed and implemented that required cleaning and lubricating the load sequencer. The unsuitable maintenance and test equipment was resolved by selecting suitable equipment and revising test methods.

Hardware quality coupling factors refer to characteristics introduced as common elements for the quality of the hardware. These include the following:

- *Manufacturing Attributes.* The manufacturing attribute coupling factor refers to the same manufacturing staff, quality control procedure, manufacturing method, and material.

  - Two diesel generators failed due to failed roll pins on the exhaust damper linkage. The roll pins failed due to temper-embrittlement that resulted from the roll pin manufacturing process.

- *Construction/Installation Attributes (both initial and later modifications).* The construction and installation attributes coupling factor refers to the same Construction/Installation Staff, Construction/Installation Procedure, Construction/Installation Testing/ Verification Procedure, and Construction/ Installation Schedule.

- An RCIC turbine tripped, on high exhaust pressure, immediately after starting. A common reference jumper between the speed ramp generator and the electronic governor module was missing. It was also missing from the HPCI turbine.

4.1.2.2 Operational Based. The operational based coupling factors are coupling factors that propagate a failure mechanism on account of identical operational characteristics among several components. For example, failure of three redundant high pressure safety injection (HPSI) pumps to start because the circuit breakers for all three pumps were racked out due to operator error. The categories of operation based coupling factors are:

- *Same Operating Staff.* This coupling factor refers to the events that result if the same operator (team of operators) is assigned to operate all trains of a system, increasing the probability that operator errors will affect multiple components simultaneously.

  - All of the emergency service water pumps were found in the tripped condition. The trips were the result of an emergency engine shutdown device being tripped. The operations personnel did not recognize that the trip devices had to be reset following testing. The procedures were enhanced to include more detailed information and the operator training was enhanced to include more detailed instructions on operations of the trip devices.

- *Same Operating Procedure.* The same operating procedure coupling factor refers to the cases when operation of all (functionally or physically) identical components is governed by the same operating procedures. Consequently, any deficiency in the procedures could affect these components.

  - Two auxiliary feedwater pumps failed to develop the proper flow output. It was determined that the manual governor speed control knobs had been placed in the wrong position due to an error in the procedure.

Sometimes, a set of procedures or a combination of procedure and human action act as the proximate cause and coupling factor, as seen in the following example.

- The RCIC turbine tripped on high exhaust pressure during a test. The RCIC turbine exhaust stop check valve was found closed and locked. The stop check valve on the exhaust of the HPCI turbine was also found closed, but not locked. One other RCIC valve was found locked closed that should have been locked open, but this valve had no effect on RCIC operability. Mispositioning the valves was due to operator error and an incomplete procedure.

In some cases, a common procedure results in failure, or multiple failures of multiple trains, if it is applied to multiple trains at the same time.

- Due to procedure and personnel errors, the nitrogen for the air operated valves on two trains of the auxiliary feedwater system was incorrectly aligned causing a loss of the nitrogen supply. The procedures were revised to increase surveillance and clearly delineate the nitrogen bottle valve alignment requirements.

- *Same Maintenance/Test/Calibration Schedule.* This coupling factor refers to the maintenance/ test/calibration activities on multiple components being performed simultaneously or sequentially during the same maintenance/test/calibration event.

- A number of breakers in the AC power system failed to close due to dirt and foreign material accumulation in breaker relays. Existing maintenance and testing requirements allowed the relays to be inoperable and not detected as inoperable until the time that the breakers were called on to operate. The maintenance requirements or cleaning schedules had not been established or identified as being necessary.

- ***Same Maintenance/Test/Calibration Staff.*** This coupling factor refers to the same maintenance/ test/calibration team being in charge of maintaining multiple systems/components.

  - The C component cooling water (CCW) pump high bearing temperature alarm sounded. The pump bearing had rotated, blocking oil flow to the bearing. The apparent cause was pump/motor misalignment. During repairs, pumps A and B maintained CCW flow. Eleven days later, pump B sounded a high bearing temperature alarm. Again, bearing failure was due to pump/motor misalignment.

- ***Same Maintenance/Test/Calibration Procedures.*** Common procedures could also be responsible for propagation of errors through procedural errors and operator interpretation of procedural steps. It is recognized that for non-diverse equipment, it is impractical to develop and implement diverse procedures.

  - During surveillance testing, 2 of 5 electromagnetic relief valves in the automatic depressurization system failed to operate per design. A leak path around a threaded retainer prevented the valves from venting the lower chamber and subsequently opening. The maintenance procedures were revised to seal weld the retainers. Additionally the valves were bench tested to ensure operability prior to installation.

4.1.2.3 Environmental Based. The environment based coupling factors are the coupling factors that propagate a failure mechanism via identical external or internal environmental characteristics. These coupling factors are:

- ***Same Plant Location.*** The same plant location coupling factor refers to all redundant systems/components being exposed to the same environmental stresses because of the same plant location (e.g., flood, fire, high humidity, earthquake). The impact of a number of these environmental stresses is normally modeled explicitly (by analyzing the phenomena involved and incorporating their impact into the plant/system models) in current PRAs. Other environmental causes such as high humidity and temperature fluctuations are typically considered in CCF analysis and treated parametrically.

  - A service water system leak on an inlet pipe caused the auxiliary feedwater pump motors to be sprayed with water. The pumps were subsequently declared inoperable until the motors could be repaired.

- ***Same Component Location.*** The same component location coupling mechanism refers to multiple systems exposed to similar environmental stresses because of location of systems/components (e.g., vibration, failure of ventilation systems, heat generated by other components, and accidental human actions).

  - Circuit breakers for the boron injection tank inlet and outlet valves B and D were found open during a routine surveillance. The breakers were in the same area, where a ladder was found leaning against the motor control center. Presumably workmen accidentally opened the breakers.

  - One inboard containment spray valve was found with a broken motor housing. An outboard containment spray valve was found with its motor housing misaligned and when an attempt was made to operate the valve, the motor burned out. It appeared that someone stepped on the motor housings and caused the damage.

- *Internal Environment/Working Medium*. The internal environment/working medium refers to commonality of multiple components in terms of the medium of their operation such as internal fluids (water, lube oil, gas, etc.). Operating with the same dirty water, for example, could cause multiple failures due to corrosion.

  - Three of four service water pumps failed due to wear causing a high pump vibration. The pumps take a suction on ocean water, and the failures were caused by excessive quantities of abrasive particles in the ocean water. The pumps were replaced.

For ease of representation and to facilitate communication of events classified as CCFs, a coding system for coupling factors has been developed and is discussed in detail in References 5 and 6. The hierarchical structure of the coding system is particularly useful in event classification since the level of detail in available information can vary from event to event. In some cases, it may be possible to identify the coupling factor of the event at a high level of hardware-based, operational-based, or environmental-based information. In other situations a more detailed classification may be possible based on the specific information provided in the event description. In either case, the flexibility has been provided in the coding system to represent the event as closely as possible.

4.1.3 Defense Mechanisms

To understand a defense strategy against a CCF event, it is necessary to understand that defending against a CCF event is no different than defending against an independent failure that has a single root cause, except that more than one failure has occurred, and they are related through a coupling mechanism.

There are three methods of defense against a CCF: (1) defend against the failure proximate cause; (2) defend against the common cause failure coupling factor; or (3) defend against both items 1 and 2. When a defense strategy is developed using protection against a proximate cause as a basis, the number of individual failures may decrease. During a CCF analysis, defense based on the proximate cause may be difficult to assess particularly when a root cause analysis is not performed on each failure and those that are performed are not complete. However, given that a defense strategy is established based on reducing the number of failures by addressing proximate causes, it is reasonable to postulate that if fewer component failures occur, fewer CCF events would occur.

The above approach does not address the way that failures are coupled. Therefore, CCF events can occur, but at a lower frequency. If a defense strategy is developed using protection against a coupling factor as a basis, the relationship between the failures is eliminated. During a CCF analysis, defense based on the coupling factor is easier to assess because the coupling mechanism between failures is more readily apparent and therefore easier to interrupt. Given that a defense strategy is developed with protection against the coupling factor as the basis, component failures may occur that may not be related to any other failures. A defense strategy based on addressing both the proximate cause and coupling factor would be the most comprehensive.

A defense strategy against proximate causes typically includes design control, use of qualified equipment, testing and preventive maintenance programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For coupling factors, a defense strategy typically includes diversity (functional, staff, and equipment), barriers, and staggered testing and maintenance. The defense mechanisms used in the Office for Analysis and Evaluation of Operational Data (AEOD) CCF database are functional and physical barriers, monitoring and awareness, maintenance staffing and scheduling, component identification, diversity, no practical defense, and unknown. These defenses are constructed primarily based on coupling factors.

4.2 Review of Plant Design and Operating Practices

A comprehensive review should include identification of the root causes, coupling factors, and defenses in place against them. However, as discussed in Reference 9, given the rarity of common cause events, current weaknesses of event reporting and other practical limitations, approaching the problem from the point of view of defenses is, perhaps, the most effective and practical. A good defense can prevent a whole class of CCFs for many types of components, and in this way the application of a procedure based on this philosophy can provide a systematic approach to screening for potential CCF mechanisms.

The following defenses are oriented toward eliminating or reducing the coupling among failures:

- Diversity
  Functional
  Equipment
  Staff

- Physical or Functional Barriers
  Spatial separation
  Physical protection
  Interlocks
  Removal of, or administrative control on, cross-ties

- Testing and Maintenance Policy
  Staggered testing
  Staggered maintenance

- Additional Redundancy

Review guidelines for each of the above categories are provided in the following:

Diversity. Diversity means the use of a totally different approach to achieve roughly the same results (functional diversity) or the use of different types of equipment to perform the same function (equipment diversity). Equipment diversity can be considered in terms of construction, physical characteristics, manufacturing or operating principle. Diversity in staff (i.e., using different teams to install, maintain, and/or test redundant trains) is another form of applying this concept.

Diversity is perhaps the ultimate defense against CCFs, in that components of different design, operated in different ways, will be subject to different failure mechanisms, with the exception of major external environmental factors such as seismic events. However, diversity has only been used to a very limited extent in the nuclear power plants. Even in cases where the concept has been used, there are often sources of dependence that may make the components susceptible to coupling mechanisms, often in the form of similar piece-parts and common location. A good example is the auxiliary feedwater system in which the diversity of pumps (motor-driven vs. turbine-driven) is diversity of pump driving mechanisms, leaving the system vulnerable to a variety of coupling factors such as steam binding, and many environmental influences. A thorough plant CCF review, therefore, must determine the degree of diversity, and identify possible similarities and common characteristics among diverse equipment.

Physical or Functional Barriers. A barrier is any physical impediment that tends to confine and/or restrict a potentially damaging condition. Separation and physical protection are often used to reduce the coupling associated with having redundant equipment in the same location. The causes of component failures associated with these coupling factors include harsh environments such as fires, floods, moisture, high or low temperatures, and so forth.

The most complete implementation of this defense is to have redundant equipment in separate locations that are not connected in any way (e.g., the locations should not have a common heating and ventilating system). This spatial separation may also enhance defenses against human errors in realignment of redundant trains of equipment because the operator could rely on the lineup of one train, which could be incorrect, to line up the other train. A simpler implementation of this defense is to provide barriers that protect against selected harsh environments (e.g., a missile barrier between redundant pumps). The missile barrier would not, however, offer protection against other harsh environments such as a high temperature in the common location of the pumps.

Interlocks are often used as defenses in instrumentation and actuation logic of safety-related systems. This type of defense consists of providing interlocks between redundant components or channels so that only one at a time can be taken out of service for testing or maintenance. This defense reduces the coupling associated with errors such as mistakenly performing a test on one component while the redundant component is undergoing preventive maintenance.

Removal of cross-ties between redundant trains will eliminate some postulated CCFs. At one nuclear power plant, for example, the cross-ties between the air tanks in the air-start systems for diesel generators were left open, resulting in multiple unavailability of diesel generators when check valves leaked. This CCF event would not have occurred if there had been no cross-ties for the air tanks. Removal of cross-ties, however, could have a detrimental impact regarding other causes of failure. For example, if one diesel generator fails to start on demand because of a leak in the air tank and the other diesel generator is already unavailable due to a major overhaul, then not having the cross-ties precludes starting one diesel generator using the air tank of the one that is unavailable due to overhaul. Strong administrative controls on cross-ties may reduce the susceptibility to CCF events.

Barriers are effective as defenses against CCFs resulting from environmental, or external agents, if they provide one of the following:

- Separate environments for redundant components and therefore reduce the susceptibility of components to trigger events which affect the quality of the environment.

- A shield for some or all the components from potential trigger events.

Review of the barrier effectiveness should include: 1) identification of the type, location, and purpose of barriers, 2) the type of disturbance to which a barrier is impermeable, 3) the quality of its installation, and 4) the quality of administrative controls that maintain its integrity, coupled with an identification of potential sources for trigger events for the various environmental disturbances, in terms of their location and severity.

A review process for identifying potential locations of concern has been developed for dealing with internal fires and floods. It can be adopted to cover other types of environmental disturbances by following the steps below through identification of:

1. The location of the components of interest.

2. The piece parts of the components that are susceptible to each disturbance.

3. The locations of the barriers against the disturbance that divide the plant into nominally independent zones.

4. Potential sources of significant environmental disturbances.

5. Those zones which contain more than one component, or vulnerable piece parts of more than one component, and a source of hazard.

6. Potential pathways between zones containing components or vulnerable piece parts, and/or sources via penetrations/connections, or under designed barriers.

This process identifies the zones on a qualitative basis without consideration of the details of the failure mechanisms. This constitutes a coarse screening analysis. It may be refined further, following again the examples of internal fire and flood analysis.

The adequacy of a design with barriers which has allowed a zone identified in Step 5 to contain vulnerable piece parts of more than one redundant component and is a potential source of trigger events, has to be assessed against the likelihood of the occurrence of the trigger event affecting the component group. This type of analysis is done routinely in fire and flood risk analyses. The factors taken into account include the relative locations of the source(s) and the vulnerable component piece parts, the magnitude of the disturbance (as a function of frequency), the potential for propagation of the disturbance, and the possibility of early detection and mitigation of the disturbance. This analysis requires a much more detailed look at specific failure mechanisms. However, it still is not necessary to evaluate why a trigger event may occur, only if it can occur and at what location it would occur.

For the groups of zones identified in Step 6, the primary review should be directed toward establishing the adequacy of the barrier, as its existence implies that it is believed to be necessary. The barrier has to be investigated for its design adequacy, its installation, and the adequacy of, and adherence to, the administrative controls designed to maintain the integrity of the barrier.

Testing and Maintenance Policy. Staggering test and maintenance activities offers some advantages over performing these activities simultaneously or sequentially. First, it reduces the coupling associated with human-related failures that are introduced during test and maintenance activities. The probability that an operator or technician repeats an incorrect action is lower when test or maintenance activities are performed months, weeks, or even days apart, than when they are performed a few minutes or a few hours apart.

A second potential advantage of staggering test and maintenance activities relates to the exposure time for CCF events. If multiple components are indeed failed because of a CCF event and if this type of failure is detectable by testing and inspecting, then evenly staggering these activities minimizes the time that multiple components would be failed because of that CCF event, by reducing the exposure time. Staggered testing and maintenance activities is unlikely to affect errors associated with programmatic or procedural deficiencies.

Additional Redundancy. In general, redundancy cannot be regarded as a defense against CCF events in the same way as other defenses, since the definition of CCFs is that they override redundancy. In the present context, therefore, redundancy is a boundary condition which defines the size of the CCCG. However, increasing the degree of redundancy may have beneficial effects; defenses that act to create operational diversity, such as staggering of preventive maintenance and testing, may result in a reduction of the overall failure rate.

A systematic and automated method for identifying plant vulnerabilities to dependent failures is known as the generic cause approach.[17] According to this approach the generic causes are divided into two groups: shared environment such as humidity and temperature, and common links such as maintenance and manufacturer. Tables 4-2, 4-3, and 4-4 provide a list of generic environments, and Table 4-5 contains possible common links. These tables or the computerized version of the approach may be used to identify sources of dependency when reviewing the plant design and operating practices.

Another set of tables (Tables 4-6 through 4-8) are provided as an aid for documenting plant design and procedures walk-through to identify plant-specific CCF vulnerabilities. The tables are organized in a such a way to encourage the analyst to look for specific categories of causes and/or coupling mechanisms and identify possible defenses against them. Table 4-6 focuses on the environmental factors and medium of influence (air , liquid, solid). Within each category the "mechanisms" that could lead to failure are identified. The analyst then needs to identify which set of components (if any) are vulnerable, and what the possible coupling factors are. The defenses are identified in terms of alarms (local or in the control room) and physical barriers. The analyst can then evaluate the barrier effectiveness to be used in estimation of common cause failure probabilities in the quantitative phase of the analysis. Additional defenses to consider are detection systems, mitigation systems, and administrative controls.

Table 4-7 looks at vulnerabilities related to maintenance procedures. The view is limited to identification of difficulties in executing the procedures (increasing the chance of human error) and ways of detecting errors after they are made. Review of the procedures to identify possible errors in the procedures is resource intensive and may not be practical and cost-effective from a common cause analysis point of view.

The analyst will document system-level vulnerabilities in Table 4-8. System-level CCF vulnerabilities are potential system failure mechanisms that can not be attributed to individual components but rather are due to the nature of the system as it is designed and operated. The table has two parts, one dealing with existence of coupling factors due to common working medium for the system (e.g., water), and one dealing with system configuration (component interconnections, physical layout, etc.). These have been observed to be the most frequent types of system-level CCF problem. The analyst is, however, encouraged to look for other coupling mechanisms that might be unique to the plant/system being reviewed.

Table 4-2. Mechanical or thermal generic environments.

Generic Cause	Example Sources
Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuits
Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from chemical control system, organic material from raw water sources, particulate in raw systems
Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure
Vibration	Machinery motion, earthquake
Pressure	Explosion, out-of-tolerance system changes (pump overspeed, flow blockage)
Humidity	Steam pipe breaks
Moisture	Condensation, pipe rupture, rainwater
Stress	Thermal stress at welds of dissimilar metals, thermal stresses and bending moments caused by high conductivity and density of liquid sodium
Freezing	Liquid sodium solidifying, water freezing

Table 4-3. Electrical or radiation generic environments.

Generic Cause	Example Sources
Electromagnetic interference	Welding equipment, rotating electrical machinery, lightning, power supplies, transmission lines
Radiation Damage	Neutron sources, charged particle radiation, gamma radiation
Conducting Medium	Moisture, conductive gases
Out-of-tolerance	Power surge voltage, short circuit, power surge current

Table 4-4. Chemical or miscellaneous generic causes.

Generic Cause	Example Sources
Corrosion (acid)	Boric acid from neutron control system, acid used in maintenance for removing rust and cleaning
Corrosion (oxidation)	A water medium or around high temperature metals (for example, filaments)
Other chemical reactions	Galvanic corrosion; complex interactions of fuel cladding, water, oxide fuel, and fission products; leaching of carbon from stainless steel by sodium
Carbonization	Hydrocarbon (hydraulic fluid, lubricating oils, diesel fuel) in liquid sodium
Biological	Poisonous gases, explosions, missile hazards, organic material from raw water sources

Table 4-5. Common links resulting in dependencies among components.

Common Link	Example Sources
Energy Source	Common drive shaft, same power supply
Calibration	Misprinted calibration instructions
Installation	Same subcontractor or crew contractor
Maintenance	Incorrect procedure, inadequately trained personnel
Operations	Over stressed or disabled operator, faulty operating procedures
Proximity	Location of all components of a cut set in one cabinet (common location exposes all of the components to same failure causes)
Test procedure	Faulty test procedures which may affect all components normally tested together
Energy flow paths	Location in same hydraulic loop, location in same electrical circuit

Table 4-6. Documentation guide for plant walk-through to identify environmental common cause vulnerabilities.

SYSTEM:____________________
COMPONENT:________________ LOCATION:____________
SUB COMP:__________________ LOCATION:____________

CAUSE		COUPLING FACTOR		DEFENSE		
Medium	Source	Same Suscepti-bility to Source	Shared Medium	Alarm	Barrier	Barrier Quality
Air	-High Temp. -Low Temp. -Dust -Humidity -Smoke -Radiation -Other Contaminant -Electromagnetism					
Liquid	-Moisture -High Temp. -Low Temp. -Corrosion -Other Chemicals Reactions -Bio.Organism -Radioactivity					
Solid	-High Temp. -Low Temp. -Vibration -Impact -Stress -Electrical ____ ____ ____					

Source of Information:
Notes:

Table 4-7. Documentation guide for plant walk-through to identify procedural CCF vulnerabilities.

PROCEDURE NO. ____________________
TYPE: ___ PM ___ TEST___ CALIB.
SYSTEM: _________________
COMPONENT:________________
FUNCTIONAL STATE DURING PROCEDURE:_____Available_____ Unavailable

EXECUTION DIFFICULTY			
CAUSE		COUPLING FACTOR (Similarity in:)	DEFENSE (Practical only against root cause)
SOURCE	QUALITY		
Access			
Lighting			
Visibility			
Work Space			
Habitability			
Time Pressure			

DEFENSE AGAINST EXECUTION ERRORS			
DEFENSE AGAINST CAUSE		DEFENSE AGAINST COUPLING	
Full Functional Test		Staggered Testing	
Check for Normal Alignment		Crew Diversity	
Auto. Alignment on Demand		Test Equipment Diversity	
		Labeling Clarity	

Source of information:
Notes:

Table 4-8. Documentation guide for plant walk-through to identify system design CCF vulnerabilities.

SYSTEM:________________________

WORKING MEDIUM VULNERABILITIES			
MEDIUM	POTENTIAL FAILURE CAUSE	COUPLING MECHANISM	DEFENSE
-Air -Gas -Water -Oil _____ _____ _____			

COMPONENT INTERCONNECTIONS VULNERABILITIES		
CAUSE AND COUPLING FACTOR		DEFENSE
DESCRIPTION	IMPACT	

Source of Information:

Notes:

4.3 Development of Cause-Defense and Coupling Factor-Defense Matrices

An effective way to present the results of a detailed qualitative analysis is the so-called cause-defense matrix. Table 4-9 presents a hypothetical cause-defense matrix for a hypothetical component. The matrix in this table explicitly considers the influence of the various defenses on both the root causes and the coupling factors. Being a tool for qualitative analysis, the levels of influence are indicated only qualitatively. A solid square represents a strong impact; an open circle represents a weak impact; and a blank (-) means no impact. Some defenses (e.g., Defense A) tend to affect the occurrence of the root cause, while others (e.g., Defense B) tend to affect the coupling. Also some defenses may influence both the root cause and the coupling factor (e.g., Defenses C and D).

The matrix in Table 4-9 also illustrates that the matrices can be applied at different levels of detail. This flexibility is important for screening purposes. For example, the impact of specific defense alternatives (D.1 through D.4) on specific root causes (3.1 through 3.5) are shown in the matrix for a selected combination of root cause and defense tactic. This two-level approach permits concentrating analysis resources on dominant contributors to CCFs whenever it is necessary.

As discussed earlier, defenses that are typically employed to protect against the root causes of failure include design control, using environmentally qualified equipment, testing and preventive maintenance programs, review of procedures, training of personnel, quality control, and several others. Defenses that are oriented toward reducing the coupling among component failures include diversity, barriers, staggering of testing and maintenance, and additional redundancy.

In a plant-specific analysis, table entries can reflect the level of the impact or effectiveness of the specific defenses in place at the plant as determined by the analyst based on his assessment of the quality of such defenses and in reference to the effectiveness of similar defenses in other plants.

It is clear that in developing a plant-specific cause-defense matrix the analyst must be very familiar with the specific characteristics of the plant, knowledgeable about a large number of causes of failure, and familiar with the defenses which have been used to defend against them. This is why a plant walk-through and comprehensive review of failure event reports are essential first steps in this detailed qualitative analysis phase.

Tables 4-10 and 4-11 are examples of cause-defense matrices developed for selected failure mechanisms of diesel generators.[9] The entries in these tables are based on the impact of generic defenses. Such generic tables could be constructed prior to specialization of the matrices for the plant in question. The specialization can be achieved by 1) expanding or reducing the cause or defense categories to reflect plant specific features and operating history, and 2) adjusting the impact intensities to reflect the relative weaknesses or strength of the plant defenses.

Obviously one set of matrices needs to be developed for each of the component groups identified as the result of the Screening Phase, and those that may have been added to the list as the result of the plant walk-through and data review in this phase.

A comparison between the generic and plant specific matrices will help prioritize the list of CCF vulnerabilities. Armed with the detailed information gathered in the process of developing the plant specific matrices, the analyst can provide suggestions for improvements in hardware and/or operational aspects of the plant to reduce those vulnerabilities.

Table 4-9. Example of cause-defense matrix showing the impact of defensive tactics on root causes of failure and coupling factors.

		Defense Tactic													
		A		B		C		D							
								D_1		D_2		D_3		D_4	
Type of failure Mech.	Specific Failure Mech.	Root Cause	Coupling Factors	Root Cause	Coupling Factors	Root Cause	Coupling Factors	Root Cause	Coupling Factors	Root Cause	Coupling Factors	Root Cause	Coupling Factors	Root Cause	Coupling Factors
1		■	-	-	○	○	○	-	■	-	■	○	-	○	-
2		-	-	-	■	-	-	-	-	-	-	-	-	-	-
3		○	-	-	■	■	○	-	-	-	-	-	-	-	-
	3.1	-	-	-	-	-	-	-	■	-	○	○	-	■	-
	3.2	-	-	-	-	-	-	-	■	-	-	-	-	-	-
	3.3	-	-	-	-	-	-	-	■	-	○	-	-	-	-
	3.4	-	-	-	-	-	-	■	■	○	■	○	○	■	○
	3.5	-	-	-	-	-	-	-	■	-	■	-	-	■	-
4		○	-	-	■	○	○	-	-	-	-	-	-	-	-
5		■	-	-	○	○	○	-	-	-	-	-	-	-	-
6		○	-	-	-	-	-	-	-	-	-	-	-	-	-
7		○	-	-	-	-	-	-	-	-	-	-	-	-	-
8		■	-	-	○	-	-	-	-	-	-	-	-	-	-
9		○	-	-	○	○	○	-	-	-	-	-	-	-	-
10		○	-	-	○	○	○	-	-	-	-	-	-	-	-

Table 4-10. Assumed impact of selected defenses against root causes of diesel failures.

	Selected Defenses Against Root Causes											
	General Administrative/Procedural Controls				Specific Maintenance/Operation Practices				Design Features			
Selected Failure Mechanisms for Diesel Generators	Configuration Control	Maintenance Procedures	Operating Procedures	Test Procedures	Governor Overhaul	Drain Water and Sediment from Fuel Tanks	Corrosion Inhibitor in Coolant	Service Water Chemistry Control	Air Dryers or Air Start Compressors	Dust Covers with Seals on Relay Cabinets	Fuel Tank Drains	Room Coolers
Corrosion products in air start system	-	o	-	o	-	-	-	-	■	-	-	-
Dust on relay controls	-	o	-	o	-	-	-	-	-	■	-	-
Governor out of adjustment	-	o	-	o	■	-	-	-	-	-	-	-
Water/sediment in fuel	-	o	-	■	-	■	-	-	-	-	■	-
Corrosion in jacket cooling system	-	o	-	-	-	-	■	-	-	-	-	-
Improper lineup of cooing water valves	■	o	-	o	-	-	-	■	-	-	-	-
Aquatic organisms in service water	-	■	■	-	-	-	-	-	-	-	-	-
High room temperature	-	o		-	-	-	-	-	-	-	-	■
Improper lube oil pressure trip setpoint	-	o	-	o	-	-	-	-	-	-	-	-
Air start system valved out	■	o	-	o	-	-	-	-	-	-	-	-
Fuel supply valves left closed	■	o	-	o	-	-	-	-	-	-	-	-
Fuel line blockage	-	-	-	o	-	-	-	-	-	-	-	-
Air start receiver leakage	-	-	-	-	-	-	-	-	-	-	-	-
Corrective maintenance on wrong diesel generator	■	■	-	-	-	-	-	-	-	-	-	-

Table 4-11. Assumed impact of selected defenses against coupling associated with diesel generator failures.

	Selected Defenses Against Coupling						
	Diversity			Barrier		Testing and Maintenance Policy	
Selected Failure Mechanisms for Diesel Generators	Functional	Equipment	Staff	Spatial Separation	Removal of Cross-ties (or implementation of administrative controls)	Staggered Testing	Staggered Maintenance
Corrosion products in air start system	■	-	-	-	-	-	○
Dust on relay controls	-	-	-	○	-	○	○
Governor out of adjustment	-	○	○	-	-	-	○
Water/sediment in fuel	■	-	-	-	○	-	-
Corrosion in jacket cooling system	■	-	-	-	-	-	-
Improper lineup of cooling water valves	■	-	■	○	-	■	■
Aquatic organisms in service water	■	-	-	○	○	-	○
High room temperature	-	-	-	○	-	-	-
Improper lube oil pressure trip setpoint	■	■	■	○	-	■	■
Air start system valved out	■	-	■	○	-	■	■
Fuel supply valves left closed	■	-	■	○	-	■	■
Fuel line blockage	■	-	■	-	-	-	-
Air start receiver leakage	■	-		-	■	-	-
Corrective maintenance on wrong diesel generator	■	○	■	○	-	○	-

5. PHASE III: DETAILED QUANTITATIVE ANALYSIS

Given the results of the analyses in Phase I, a detailed quantitative analysis can be performed even if a detailed qualitative analysis has not been performed. However, as will be seen later, some of the steps in the detailed quantitative phase can benefit significantly from the insights and information obtained as a result of a detailed qualitative analysis.

A detailed quantitative analysis can be achieved through the following steps:

1) Identification of CCBEs
2) Incorporation of CCBEs into the system fault tree
3) Development of parametric representation of CCBEs
4) Parameter estimation
5) System unavailability quantification
6) Documentation and results evaluation

Each step is discussed in more detail in the following sections. The reader may find it necessary, however, to consult References 1, 2, and 3 for further details and examples.

5.1 Identification of CCBEs

This step provides the means for accounting for the entire spectrum of CCF impacts in an explicit manner in the logic model. It will also facilitate the fault tree quantification to obtain top event (system failure) probability.

A CCBE is an event involving failure of a specific set of components due to a common cause. For instance in a system of three redundant components A, B, and C, the CCBEs are C_{AB}, C_{AC}, C_{BC} , and C_{ABC}. The first event is the common cause event involving components A and B, and the fourth is CCF event involving all three components. Note that the CCBEs are only identified by the impact they have on specific sets of components within the CCCGs. Impact in this context is limited to "failed" or "not failed."

The complete set of basic events, including CCBEs, involving component A in the three component system is

A_I = Single independent failure of component A. (A basic event.)

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

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

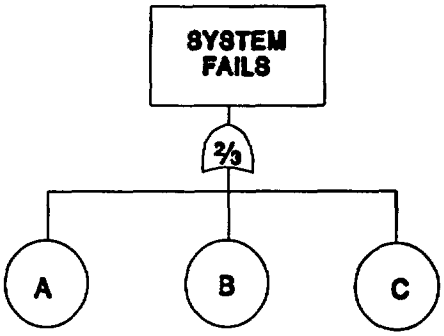
C_{ABC} = Failure of components A, B, and C from common causes.

Component A fails if any of the above events occur. The equivalent Boolean representation of total failure of component A is

$$A_T = A_I + C_{AB} + C_{AC} + C_{ABC} \tag{5.1}$$

5.2 Incorporation of CCBEs into the Component-Level Fault Tree

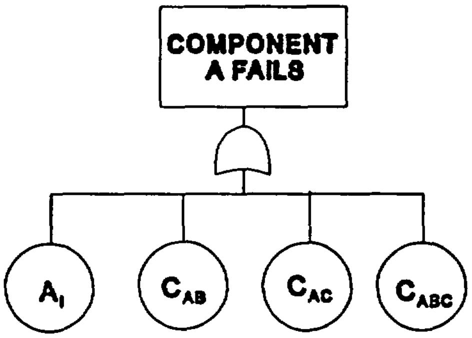
In this step the component-level fault tree is expanded in terms of the CCBEs. As an example of this expansion, consider a system of three identical components, A, B, and C, with a two-out-of-three success logic. Also assume that, based on the qualitative and quantitative screening, these three components form a single CCCG. The component-level fault tree of this system is



Note that the minimal cutsets of this fault tree are

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

The expansion of this fault tree down to the common cause impact level can be achieved by replacing each of the three component basic events by the corresponding CCBE fault tree. For instance for component A, the basic event A is replaced by



When all the components of the system are expanded similarly, the following cutsets are obtained:

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

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

$\{C_{ABC}\}$.

If the success criterion for this example had been only one out of three instead of two out of three, the expanded fault tree would produce cutsets of the type, $C_{AB}*C_{AC}$. These cutsets imply failure of the same piece of equipment due to several causes each of which is sufficient to fail the component. For example, in $C_{AB}*C_{AC}$ component A is failing due to CCF that fails AB, and also due to CCF that fails AC. These cutsets have questionable validity unless the events C_{AB} and C_{AC} are defined more precisely. Reference 1 discusses the conditions under which these cutsets are valid. However, experience shows that in general the contribution of cutsets of this type is considerably smaller than that of cutsets like C_{ABC}. These cutsets will be eliminated here.

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

$$S = A_I*B_I + A_I*C_I + B_I*C_I + C_{AB} + C_{AC} + C_{BC} + C_{ABC} \tag{5.2}$$

It can be seen immediately that this expansion results in proliferation of the cutsets, which may create practical difficulties when dealing with complex systems. The potential difficulty involving the implementation of this procedure is one of the motivations for a thorough and systematic screening in earlier steps in order to minimize the size of the expanded fault tree. Despite the potential difficulty in implementation, this procedure provides the analyst with a systematic and disciplined framework for inclusion and exclusion of common cause events with adequate assurance that the resulting model of the system is complete with respect to all possible ways that common cause events could impact the system.

Another advantage of this procedure is that once the CCBEs are included in the fault tree, standard fault tree techniques for cutset determination and probabilistic quantification can be applied without concern about dependencies due to CCFs.

If, after careful screening, the number of cutsets is still unmanageable, a practical solution 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 Equation 5.1 and the new Boolean expression would be reduced again. Other techniques include reducing the level of detail of the original component-level tree by introducing "supercomponents," and assuming that the common cause events always have a global effect. Care, however, must be exercised so that no terms in the expansion of the reduced Boolean expressions would be missed or ignored.

5.3 Parametric Representation of CCBE Probabilities

Quantification of fault trees requires transformation of system Boolean representation to an algebraic one involving probabilities of the basic events. This step is transparent to the user of most fault tree codes since such codes have built-in quantification capabilities. It is important, however, to recognize that the algorithms used for quantification of the fault tree in these codes may involve assumptions and approximations such as the rare event approximation.

Using the rare event approximation system failure probability of the two-out-of-three system is given by

$$\begin{aligned} P(S) \;=\; & P(A_I)\,P(B_I) + P(A_I)\,P(C_I) + P(B_I)\,P(C_I) + \\ & P(C_{AB}) + P(C_{AC}) + P(C_{BC}) + \\ & P(C_{ABC}) \end{aligned} \tag{5.3}$$

where

$P(x)$ = probability of event x.

It is common practice in risk and reliability analysis to assume that the probabilities of similar events involving similar 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 the above equation it is assumed that

$$\begin{aligned} P(A_1) = P(B_1) = P(C_1) = Q_1 \\ P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2 \\ P(C_{ABC}) = Q_3. \end{aligned} \tag{5.4}$$

In other words, the probability of occurrence of any basic event within a given CCCG is assumed to depend only on the number and not on the specific components in that basic event.

With the symmetry assumption and using the notation just introduced, the system failure probability can be written as

$$Q_S = 3(Q_1)^2 + 3Q_2 + Q_3 \tag{5.5}$$

For quantification of the expanded fault tree,

$Q^{(m)}{}_k$ = probability of a CCBE involving k specific components in a common cause component group of size m, ($1 \leq k \leq m$).

The model that uses $Q^{(m)}{}_k$'s to calculate system failure probability is called the **Basic Parameter (BP)** model.[1]

For several practical reasons, it is often more convenient to rewrite $Q^{(m)}{}_k$'s in terms of other more easily quantifiable parameters. For this purpose a parametric model known as the **Alpha Factor model**[18] is recommended. Reasons for this choice are that the alpha factor model, 1) is a multi-parameter model which can handle any redundancy level, 2) is based on ratios of failure rates which makes the assessment of its parameters easier when no statistical data are available, and 3) has a simpler statistical model, and produces more accurate point estimates as well as uncertainty distributions compared to other parametric models which have the above two properties.

The alpha-factor model develops CCF frequencies from a set of failure ratios and the total component failure rate. The parameters of the model are

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

α_k = fraction of the total frequency of failure events that occur in the system and involve the failure of k components due to a common cause.

Using these parameters, depending on the assumption regarding the way systems in the database are tested, the frequency of a CCBE involving failure of k components in a system of m components is given by

- For a staggered testing scheme:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \tag{5.6}$$

- For a non-staggered testing scheme:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad (5.7)$$

where the binomial coefficient is given by

$$\binom{m-1}{k-1} = \frac{(m-1)!}{(k-1)!\,(m-k)!} \qquad (5.8)$$

and

$$\alpha_t = \sum_{i=1}^{m} k\alpha_k \qquad (5.9)$$

As an example, the probabilities of the basic events of the three component system of Equation 5.5 are written as (assuming staggered testing)

$Q^{(3)}_1 = \alpha_1 Q_t$

$Q^{(3)}_2 = ½\, \alpha_2 Q_t$

$Q^{(3)}_3 = 3\, \alpha_3 Q_t$.

Therefore, the system unavailability of Equation 5.5 can now be written as

$$Q_S = 3(\alpha_1 Q_t)^2 + 3/2\alpha_2 Q_t + 3\alpha_3 Q_t \qquad (5.10)$$

Another popular multi-parameter model is known as the **Multiple Greek Letter** (MGL) model.[19] The MGL parameters consist of the total component failure frequency (which includes the effects of all independent and common cause contributions to the component failure), and a set of failure fractions which are used to quantify the conditional probabilities of the possible ways a CCF of a component can be shared with other components in the same group given a 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

Q_t = total failure frequency of the component on account of all independent and common cause events,

plus,

β = conditional probability that the common cause of a component failure will be shared by one or more additional components.

γ = 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 in addition 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.

To see how these parameters can be used in developing the probabilities of common cause basic events, consider the system of three redundant components. The total failure frequencies for this system are

$$\begin{aligned} Q^{(3)}_1 &= (1-\beta)Q_t \\ Q^{(3)}_2 &= \tfrac{1}{2}\beta(1-\gamma)Q_t \\ Q^{(3)}_3 &= \beta\gamma Q_t \end{aligned} \tag{5.11}$$

Therefore, the system unavailability of Equation 5.5 is written as

$$Q_s = 3(1-\beta)^2 Q_t^2 + \frac{3}{2}\beta(1-\gamma)Q_t + \beta\gamma Q_t \tag{5.12}$$

Note that the beta factor model is a special case of the MGL model.

The general equation that expresses the frequency of multiple component failures due to common cause, $Q^{(m)}_k$, in terms of the MGL parameter is

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) (1-\rho_{k+1})Q_t \tag{5.13}$$

$$\rho_1 = 1,\ \rho_2 = \beta,\ \rho_3 = \gamma,\ \rho_4 = \delta,\ \rho_5 = \epsilon, \ldots,\ \rho_{m+1} = 0$$

The number of parameters is always one less than system size. For example, in a system of three components ($m = 3$), those parameters which contribute are β and γ. Other parameters, i.e., δ, ε, ... will be zero. Appendix A provides a more detailed presentation of several parametric models for probability of CCF events. The appendix also includes a set of formulas for calculating parameters of the alpha factor model in terms of the MGL parameters and vice versa.

5.4 Practical Issues for Incorporating CCBEs Into Fault Trees

The CCF analysis procedure framework described in previous sections may be applied at various levels of detail. It may not always be necessary or practical to model CCF events to the level of detail discussed in Sections 5.2 and 5.3. The screening analysis, Phase I of the process, is included as an essential element in achieving a practical methodology in that it restricts the number of CCF events that have to be analyzed in detail. The purpose of this section is to discuss the practical aspects of applying the procedure presented in Sections 5.2 and 5.3, to identify where simplifying assumptions are made, and where they can be made without significant loss of accuracy.

To understand the necessity of performing simplifying assumptions on the grounds of practicality, consider the following. In system-level analyses (i.e., the analysis of common cause events within a given system), fault trees size can increase substantially as a result of identification of large CCCGs, or many CCCGs. In plant-level analyses (e.g., applied risk studies), especially those that employ the fault-tree-linking technique, the fault trees are typically large even before the inclusion of common cause events.

For example, consider the case of 1-out-of-m (for success) systems that are comprised of N components so that system failure requires failure of all m components. Suppose that all N components are assigned to the same common cause group. The systematic process described in Section 5.2 suggest the incorporation of a number of basic events into the logic model, equal to all the combinations of components that can be affected by a particular cause. This number, n_e, is defined as

$$n_e = \sum_{j=1}^{m} \binom{m}{j} = 2^m - 1 \qquad (5.14)$$

Values of n_e are listed in Table 5-1 for selected values of m, together with the number of minimal cutsets of the resulting fault trees. The highly nonlinear proliferation of cutsets with system size is evident in this table. It is necessary to either simplify the model or apply algebraic formulae to component-level logic models, as more fully described below.

In addition to the system size issue there are also cases where some of the assumptions made in developing the models presented in this document are not valid and the corresponding steps of the procedure do not apply. These cases are also discussed in this section. Further practical guidelines are provided during the example application in Section 6 of this report.

Table 5-1. Size parameters for fault tree of 1-out-of-n system including all CCF combinations.

M Number of Components in System	n Number of Basic Events in the Expanded Fault Tree[a]	n_e Number of Unique Basic Events in Expanded Fault Tree[b]	n_m Number of Minimal Cutsets in Expanded Fault Tree[c]
2	4	3	2
3	12	7	5
4	32	15	15
5	80	31	42
6	192	63	278
11	11,264	2,047	(*)
50	$2.8\text{x}10^{16}$	$1.1\text{x}10^{15}$	(*)
100	$6.3\text{x}10^{31}$	$1.3\text{x}10^{30}$	(*)

(a) Determined from

$$n = M \sum_{j=0}^{M-1} \binom{M-1}{j} = M 2^{M-1}$$

(b) Determined from Equation 5-14

(c) As determined by fault tree solution with SETS.

* Unknown. It is believed that these fault trees are well beyond existing computer software and hardware capability.

The first method discussed in this section is that of simplifying the common cause model. The second technique, truncation, is applicable to any systems analysis but is mentioned here for completeness. The third section addresses the introduction of the common cause events into the plant model. The fourth is a useful table of results that can be used to check that an analysis has been done correctly. It is called here "the pattern recognition approach." The fifth topic concerns the merits of using the global common causes terms only in the detailed modeling, and the sixth is that of refinement of common cause grouping when components are potentially a common cause group but some feature, perhaps operating characteristics, introduces some asymmetry.

5.4.1 CCF Model Simplification

In the most rigorous application of the process recommended in this procedures guide, a certain number of common cause events are added to the logic model, one for each different combination of components that could be affected by a common cause. As shown above, there are $2^m - 1$ such combinations in a group of m components. By selectively eliminating some combinations, the number of minimal cutsets in the extended fault tree can be reduced and the determination of the algebraic system model can thereby be simplified. The beta factor model,[20] for example, incorporated this technique by modeling only the purely independent events and the global common cause events; i.e., the event that fails all m components in a common cause group.

There are natural variations on this basic idea in which additional common cause events can be added to progressively allow a greater degree of detail within the model but less than the full detail provided by the more rigorous approach of Section 5.2. One such variation, for groups having five or more components, is to include the independent events, the global common cause event, and all the common cause events that fail two and three components. In this model, the global event accounts for any common cause event that fails four or more components.

The example in Section 6 of this report illustrates that neglect of all terms other than the global common cause term results in an underestimation of the system unavailability that is negligible, particularly when taking into account the uncertainties in the parameter estimates. While this is not necessarily a general rule, under a certain set of conditions the approximation is valid. The conditions are basically that the independent event unavailability is low (10^{-2} or less), and that the conditional probability of three or more components failing, given two have failed, is fairly high (on the order of 0.5), and somewhat higher than the conditional probability that two have failed, given that one has failed.

The judgment of the adequacy of the global common cause term to represent CCF effects is, therefore, a function of the probability estimates.

When the model is simplified by limiting the number of CCBEs , it is very important to analyze the data in a consistent manner. The analyst needs to ensure that any errors introduced by event deletion are controlled in a conservative manner. For example, using the above model in a system of 12 components, any event that involved failure of 4 or more components would be counted in the data analysis as failing all 12 components. As an example consider the case where the following data are obtained:

$$
\begin{aligned}
n_1 &= 100 \\
n_2 &= \ \ 4 \\
n_3 &= \ \ 2 \\
n{\geq}_4 &= \ \ 1
\end{aligned}
$$

where n_i is the number of events involving failure of I components (out of 12). Since the model has been truncated not to distinguish among any differences in impact for four or more components, to be consistent, the parameter estimators should not make the distinction. Therefore, for estimation of the α-factor, the following approach should be used to develop a point estimate:

$$\alpha_{\geq 4} = \frac{n_{\geq 4}}{n_1 + n_2 + n_3 + n_{\geq 4}} = \frac{1}{107} = 0.01$$

5.4.2 Truncation

When all common cause events are included in the logic model, or when some are omitted and others are conservatively quantified as described above, the models can be further simplified by truncating higher order cutsets. This technique is normally used in ordinary fault tree analysis and is incorporated into much of the fault tree analysis software. This technique is more powerful and more defendable if common cause events are included in the logic model. The assumption of lower probability of higher order cutsets is the basis of truncation, but is only valid if the events in a cutset are independent statistically. Explicit inclusion of common cause events preserves the validity of the assumption and the method.

In the auxiliary feedwater system example of Section 6, the numerical error associated with truncating all but first-order terms was found to be about 4%, while truncating the third-order terms yielded an error of less than 1%.

These results are rather typical and reflect an important contribution of the global common cause events. Seldom do terms of fourth order and higher make significant contributions, even collectively. It is also normally safe to truncate cutsets of an order higher than the lowest order of purely independent event cutsets of events within a common cause group. For example, if a system has minimal cutsets of order two, with single failures of components in a given component group, any cutsets of events within the same group of order three or higher can be safely truncated, provided the probabilities of the events contributing to the higher order cutsets are comparable with those of the lower order cutsets and are small.

An alternative approach is one in which cutsets or parametric model terms are truncated, based on their probability estimates. This approach is generally superior to cutset order truncation because it is not necessary to assume a direct correlation exists between cutset order and cutset probability. This comment also applies to the cutset order transaction technique.

5.4.3 Independent Subtree Simplification

In yet another approach, subtrees whose underlying basic events do not appear any other place in the system fault tree can be combined into a single "superevent" or "supercomponent." This approach is well known in fault tree analysis and is incorporated into fault tree computer programs such as IRRAS[16] and SETS.[15] This approach was used in the U. S. contribution to the Common Cause Reliability Benchmark Exercise.[8] The system analyzed consisted of four identical trains, and the success criterion was one or more trains. Each train consisted of 17 components which were grouped into 12 component groups. An ordinary fault tree of only independent events would have 20,736 minimal cutsets in a component-level fault tree. After expansion of the system fault tree to include common cause events according to the procedure of Section 5.2 the number of cutsets increased to 45,295. After making the fullest possible use of the independent subtree technique, the number of minimal cutsets was reduced to 5,739. Hence, an eight-fold reduction in the number of terms was achieved in this example. Unlike the above techniques to simplify the model, this one does not introduce any numerical errors. A minor drawback is that when independent subtrees are identified as significant contributors, they must be separately broken down so they can be used to examine causes at a level of detail consistent with the parts of the unsimplified fault tree.

5.4.4 Incorporation of Common Cause Events into the Plant Model (Basic Event Substitution)

There are basically two different approaches to plant modeling: fault tree linking and event tree linking. There is essentially no difference in the way that common cause events are introduced into these models. Perhaps the simplest approach is to introduce the common cause events directly into the support systems and frontline systems fault trees before solving for the cutsets. However, the inclusion of many additional events into fault trees can make their solution cumbersome. An alternative is to solve for the cutsets without the common cause events but substitute them into the resulting minimal cutset expressions. This approach is subject to the criticism that truncation may eliminate cutsets, based on order or probability, that might have significant common cause potential. In practice, at the system level, this is seldom a problem for an experienced analyst since he or she has identified the appropriate common cause groups and would perform a check to see why they did not appear. This may be more difficult when systems are combined together to form accident sequences. However, it is a powerful approach to providing a practical solution when used with care. It is detailed below.

As an example, consider a system of four components, X, Y, Z, and W. The first three are identical and belong to a common cause group, and the fourth, component W, is independent of the first three. All the basic events defined according to the procedure of Section 5.2 are listed as follows:

Independent Cause Events: C_X, C_Y, C_Z , C_W

Common Cause Events: C_{XY}, C_{XZ}, C_{YZ}, C_{XYZ}

Assume that the component-level minimal cutsets for the system are

$$\{X, Y\} \text{ and } \{Z, W\}$$

Therefore, the system failure Boolean equation with component level basic events is

$$T = X*Y + Z*W \tag{5.15}$$

Incorporation of the CCBEs into the fault tree is equivalent to the Boolean substitution

$$X = C_{XY} + C_{XZ} + C_{XYZ} + C_X$$

$$Y = C_{XY} + C_{YZ} + C_{XYZ} + C_Y$$

$$Z = C_{XZ} + C_{YZ} + C_{XYZ} + C_Z$$

$$W = C_W$$

Consequently Equation 5.15 becomes

$$T = [C_{XY} + C_{XZ} + C_{XYZ} + C_X]*[C_{XY} + C_{YZ} + C_{XYZ} + C_Y] + [C_{XZ} + C_{YZ} + C_{XYZ} + C_Z]*C_W$$

After Boolean reduction, the resulting equation is

$$T = C_{XY} + C_{XYZ} + C_{XZ}*C_Y + C_X*C_Y + C_{XZ}*C_{YZ} + C_{YZ}*C_W + C_{XZ}*C_W + C_Z*C_W + C_X*C_{YZ} \tag{5.16}$$

Based on the discussion in Section 5.2, cutsets containing basic events which involve the same components are disallowed. There is one such cutset: $\{C_{XZ}{*}C_{YZ}\}$. The final equation is equivalent to the following list of minimal cutsets:

Singles: $\{C_{XY}\}$; $\{C_{XYZ}\}$

Doubles: $\{C_{XZ}{*}C_Y\}$; $\{C_X{*}C_Y\}$; $\{C_X{*}C_{YZ}\}$; $\{C_{YZ}{*}C_W\}$; $\{C_{XZ}{*}C_W\}$; $\{C_Z{*}C_W\}$

The system failure probability can now be written using the rare event approximation and assuming that all the listed basic events are independent:

$$\begin{aligned} P(T) = {} & P\{C_{XY}\} + P\{C_{XYZ}\} + \\ & P\{C_{XZ}\} \bullet P\{C_Y\} + P\{C_X\} \bullet [P\{C_Y\} + P\{C_{YZ}\}] + \\ & P\{C_W\}[P\{C_{YZ}\} + P\{C_{XZ}\} + P\{C_X\}] \end{aligned} \tag{5.17}$$

Applying the assumption of symmetry, i.e.,

$$P\{C_X\} = P\{C_Y\} = P\{C_Z\} = Q_1$$

$$P\{C_{XY}\} = P\{C_{XZ}\} = P\{C_{YZ}\} = Q_2$$

$$P\{C_{XYZ}\} = Q_3$$

Equation 5.17 reduces to

$$P\{T\} = Q_2 + Q_3 + 2Q_1Q_2 + Q_1{}^2 + Q_W(Q_1 + 2Q_2) \tag{5.18}$$

5.4.5 The Pattern Recognition Approach

When the systematic procedures of Sections 5.2 and 5.3 are followed, it is not necessary to know the algebraic formulae for relating the system failure logic to the common cause model parameters. It is only necessary to know the formulae for relating each basic event to the model parameters. The effect of the system logic is systematically incorporated into the analysis using standard fault tree analysis techniques. The experience gained in applying the systematic approach to a large number of systems with different configurations has resulted in the accumulation of a "library" of formulae for different systems and situations. This library of formulae can be used to support an alternative approach (pattern recognition) to common cause analysis.

The pattern recognition approach refers to the process of developing an algebraic model for system failure frequency by recognizing the pattern or configuration of the system logic. By matching the new pattern to an existing pattern in his library, the analyst synthesizes the appropriate algebraic formulae from the library to obtain the system model. When the pattern recognition approach is used, some of the key steps of the recommended systematic procedure are bypassed. These steps include the incorporation of common cause events into the system fault tree and the systematic examination of cutsets in the development of the system algebraic model. When bypassing these steps, the analyst assumes that these steps have been properly performed and relies on the previous judgment that the patterns have been appropriately matched. Therefore, the pattern recognition approach has many pitfalls and should be followed with care. It is not difficult to inadvertently omit or double count important cutsets and key contributors. In fact, the systematic approach is recommended in favor of the pattern recognition, whenever feasible.

Unfortunately, the large fault tree problem and resource constraints on analysis projects will preclude the full implementation of the systematic approach and will maintain a continuing need for the pattern recognition approach. Moreover, it is recognized that there may be some resistance to adopting the recommended "rigorous" approach, even when it is feasible. Therefore, the following guidance is provided on the proper use of formulae for common cause analysis when the pattern recognition approach is followed.

The major limitation of the pattern recognition approach is in matching the patterns or configuration of the system being analyzed with the appropriate pattern in the "library." When the configuration and success criteria cannot be matched exactly, an attempt should be made to decompose the system into independent subsystem for pattern matching. Independence implies here that there are no shared components between two or more subsystems and that the boundaries of all the CCCGs are not crossed by the boundaries of the subsystems. If an exact match cannot be made at the system, or at the independent subsystem level, the pattern recognition approach should be abandoned since significant errors are likely to result. Seemingly minor and subtle differences in the configurations can lead to major differences in the results. A compilation of formulae for independent and common cause events in some simple, frequently encountered configurations is provided in Table 5-2. For each model, formulae are provided for the basic parameter model on the assumption that the CCBEs are mutually exclusive (see discussion in Section 5.3). Additional terms are required if independence rather than mutual exclusions is assumed. All the formulae account for all the first and second order minimal cutsets in the fault trees that include the CCBEs. In some models, the technique of omitting or disallowing some common cause events is applied.

Models 1 through 14 cover all the simple "k out of N" (for success) situations for N up to five, and "one out of N" (for success) situations for N up to six. In each of these model formulae, the only approximations made are the rare event approximation and the truncation of cutsets of order three and higher. Otherwise, all possible common cause events are accounted for. Models 15 and 16 cover selected four-component configurations that exhibit some asymmetries that have been accounted for in selecting common cause events for inclusion in the models. Cutsets for these cases are listed in Appendix B. Table 5-3 shows similar results for simple, but large parallel-series and series-parallel configurations of identical redundant components. These models do not include all the possible common cause events, but they do include the ones with significant contributions over the practical range of model parameter values.

Tables 5-4 and 5-5 provide the α-factor model formulae for probabilities of the CCFs for various system sizes(CCCG Size) under different configurations required for system success (i.e., k-out-of-N). Table 5-4 lists the formulae for systems subject to staggered testing while the formulae in Table 5-5 are valid under the non-staggered testing scheme. The screening values in Table 3-1 use these formulae and the generic estimates discussed later in Section 5.5.4.

There are pitfalls when formulae are applied to a list of minimal cutsets obtained from a component-level fault tree. To illustrate, suppose the minimal cutsets of a systems were

$$\{A, B, C\};\ \{A, B, D\};\ \{A, C, D\};\ \{B, C, D\}.$$

The correct approach is to recognize this as a "three-out-of-four" (for success) system and apply the formula for model 8 in Table 5-2. An incorrect approach is to recognize each cutset as a separate "one-out-of-three" (for success) system and compute the system formula as four times the formula for model 3. Since the cutsets share components and comprise components within the same common cause group, the separate cutsets do not correspond with independent subsystems. When this point is not recognized, the global common cause events, in which all components are affected, are multiply accounted for.

Table 5-2. Algebraic formulae for common cause events in some common system configurations.

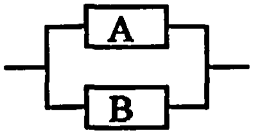
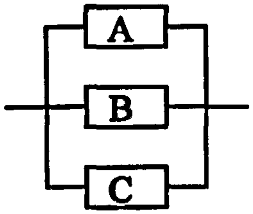
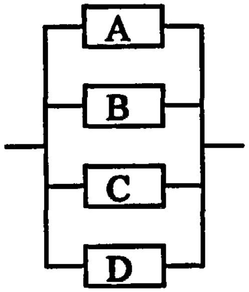
Reliability Block Diagram	Case	Model Description / Success Criteria	Approximate Formulae-Basic Parameter Model
	1	Two units in standby; one of two (1 of 2) must operate on demand.	$Q_1^2 + Q_2$
	2	Two units in standby; two of two (2 of 2) must operate on demand.	$2Q_1 + Q_2$
	3	Three units in standby; one of three (1of 3) must operate on demand.	$Q_1^3 + 3Q_1Q_2 + Q_3$
	4	Three units in standby; two of three (2 of 3) must operate on demand.	$3Q_1^2 + 3Q_2 + Q_3$
	5	Three units in standby; three of three (3 of 3) must operate on demand.	$3Q_1 + 3Q_2 + Q_3$
	6	Four units in standby; one of four (1 of 4) must operate on demand.	$Q_1^4 + 3Q_2^2 + 4Q_1Q_3 + Q_4 + 6Q_1^2Q_2$
	7	Four units in standby; two of four (2 of 4) must operate on demand.	$4Q_1^3 + 12Q_1Q_2 + 3Q_2^2 + 4Q_3 + Q_4$
	8	Four units in standby; three of four (3 of 4) must operate on demand.	$6Q_1^2 + 6Q_2 + 4Q_3 + Q_4$
	9	Four units in standby; four of four (4 of 4) must operate on demand.	$4Q_1 + 6Q_2 + 4Q_3 + Q_4$

Table 5-2. Algebraic formulae for common cause events in some common system configurations (continued).

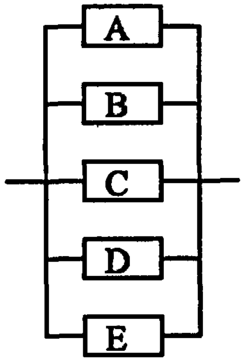
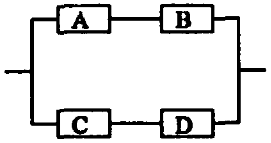
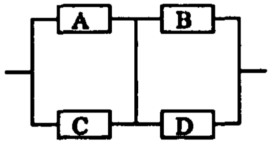
Reliability Block Diagram	Case	Model Description / Success Criteria	Approximate Formulae-Basic Parameter Model
	10	Five units in standby; one of five (1 of 5) must operate on demand.	$Q_1^5 + 10Q_1^3Q_2 + 15Q_1Q_2^2 + 10Q_1^2Q_3 +$ $10Q_2Q_3 + 5Q_1Q_4 + Q_5$
	11	Five units in standby; two of five (2 of 5) must operate on demand.	$5Q_1^4 + 30Q_1^2Q_2 + 15Q_2^2 + 20Q_1Q_3 + 10Q_2Q_3 + 5Q_4 + Q_5$
	12	Five units in standby; three of five (3 of 5) must operate on demand.	$10Q_1^3 + 30Q_1Q_2 + 15Q_2^2 + 10Q_3 + 5Q_4 + Q_5$
	13	Five units in standby; four of five (4 of 5) units must operate on demand.	$10Q_1^2 + 10Q_2 + 10Q_3 + 5Q_4 + Q_5$
	14	Five units in standby; five of five (5 of 5) must operate on demand.	$5Q_1 + 10Q_2 + 10Q_3 + 5Q_4 + Q_5$
	15	Four units in standby, one of two (1 of 2) trains must operate on demand.	$4Q_1^2 + 4Q_2 + 4Q_1Q_2 + Q_2^2 + 4Q_3 + Q_4$
	16	Four units in standby, two of four (2 of 4) must operate on demand as shown in block diagram.	$2Q_1^2 + 2Q_2 + 8Q_1Q_2 + 2Q_2^2 + 4Q_3 + Q_4$

Table 5-2. Algebraic formulae for common cause events in some common system configurations (continued).

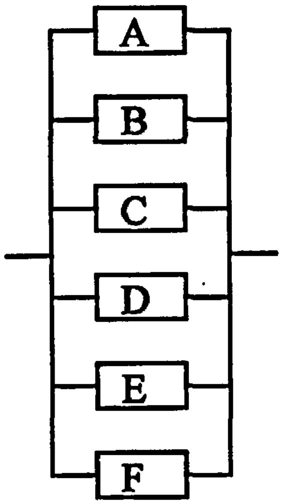
Reliability Block Diagram	Case	Model Description / Success Criteria	Approximate Formulae-Basic Parameter Model
	17	Six units in standby, one of six (1 of 6) must operate on demand as shown in the block diagram.	$Q_1^6 + 15Q_1^4Q_2 + 20Q_1^3Q_3 + 15Q_2Q_4 + 45Q_1^2Q_2^2 + Q_3^2 +$ $60Q_1Q_2Q_3 + 6Q_1Q_5 + 15Q_2^3 + 15Q_1^2Q_4 + Q_6$
	18	Six units in standby, two of six (2 os 6) must operate on demand as shown in the block diagram.	$6Q_1^5 + 60Q_1^3Q_2 + 60Q_1^2Q_3 + 90Q_1Q_2^2 + 15Q_3^2 +$ $60Q_2Q_3 + 10Q_{3_2} + 15Q_2Q_4 + 30Q_1Q_4 + 6Q_5 + Q_6$
	19	Six units in standby, three of six (3 of 6) must operate on demand as shown in the block diagram.	$15Q_1^4 + 90Q_1^2Q_2 + 60Q_1Q_3 + 45Q_2^2$ $+ 60Q_2Q_3 + 10Q_3^2 + 15Q_4 + 6Q_5 + Q_6$
	20	Six units in standby, four of six (4 of 6) must operate on demand as shown in the block diagram.	$20Q_1^3 + 60Q_1Q_2 + 45Q_2^2 + 20Q_3 + 15Q_4 + 6Q_5 + Q_6$
	21	Six units in standby, five of six (5 of 6) must operate on demand as shown in the block diagram.	$15Q_1^2 + 15Q_2 + 20Q_3 + 15Q_4 + 6Q_5 + Q_6$
	22	Six units in standby, six of six (6 of 6) must operate on demand as shown in the block diagram.	$6Q_1 + 15Q_2 + 20Q_3 + 15Q_4 + 6Q_5 + Q_6$

Table 5-3. Algebraic formulae for common cause events in some large system configurations.

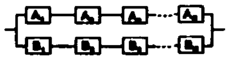
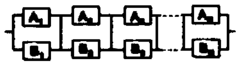
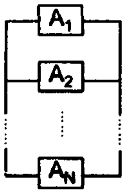
Reliability Block Diagram	Model No.	Model Description/ Success Criteria	Approximate Formulae Basic Parameter Model	Key Assumptions
	1	Two parallel trains of N identical units, all N components in one of two trains must operate on demand.	$N^2 (Q_1^2 + Q_2) + Q_{2N}$	Common cause failures either involve only two or all 2N components. Any pair of components being failed by a common cause is equally likely.
	2	Same as model (above) with cross ties; at least one of two in each of N stages most operate on demand.	$N (Q_1^2 + Q_2) + Q_{2N}$	Common cause failures either involve only two or all 2N components. Any pair of components being failed by a common cause is equally likely.
	3	N components in standby; at least k out of N components, k < N, must operate on demand.	$\sum_{i=N-k+1}^{N} \binom{N}{i} Q_1^i (1 - Q_1)^{N-i} + Q_N$	When a common cause failure occurs, all N components are assumed to fail.

Table 5-4. Common cause failure quantification using alpha factor model (staggered testing).

CCCG Size	Configuration	Common Cause Failure Probability
2	1 of 2	$\alpha_2 Q_T$
	2 of 2	
3	1 of 3	$\alpha_3 Q_T$
	2 of 3	$(3\alpha_2/2 + \alpha_3)Q_T$
	3 of 3	
4	1 of 4	$\alpha_4 Q_T$
	2 of 4	$(4\alpha_2/2 + 4\alpha_3/3 + \alpha_4)Q_T$
	3 of 4	$(4\alpha_3/3 + \alpha_4)Q_T$
	4 of 4	
5	1 of 5	$\alpha_5 Q_T$
	2 of 5	$(5\alpha_4/4 + \alpha_5)Q_T$
	3 of 5	$(5\alpha_3/3 + 5\alpha_4/4 + \alpha_5)Q_T$
	4 of 5	$(5\alpha_2/2 + 5\alpha_3/3 + 5\alpha_4/4 + \alpha_5)Q_T$
	5 of 5	
6	1 of 6	$\alpha_6 Q_T$
	2 of 6	$(6\alpha_5/5 + \alpha_6)Q_T$
	3 of 6	$(6\alpha_4/4 + 6\alpha_5/5 + \alpha_6)Q_T$
	4 of 6	$(6\alpha_3/3 + 6\alpha_4/4 + 6\alpha_5/5 + \alpha_6)Q_T$
	5 of 6	$(6\alpha_2/2 + 6\alpha_3/3 + 6\alpha_4/4 + 6\alpha_5/5 + \alpha_6)Q_T$
	6 of 6	

Note: $Q_T = Q_1/\alpha_1$ where Q_T is the total failure probability and Q_1 is the independent failure probability of the component.

Table 5-5. Common cause failure quantification using alpha factor model (nonstaggered testing).

CCCG Size	Configuration	Common Cause Failure Probability
2	1 of 2	$2\alpha_2 /\alpha_t Q_T$
	2 of 2	
3	1 of 3	$3\alpha_3/\alpha_t Q_T$
	2 of 3	$3(\alpha_2 + \alpha_3)/\alpha_t Q_T$
	3 of 3	
4	1 of 4	$4\alpha_4/\alpha_t Q_T$
	2 of 4	$4(\alpha_2 + \alpha_3 + \alpha_4)/\alpha_t Q_T$
	3 of 4	$4(\alpha_3 + \alpha_4)/\alpha_t Q_T$
	4 of 4	
5	1 of 5	$5\alpha_5/\alpha_t Q_T$
	2 of 5	$5(\alpha_4/4 + \alpha_5)/\alpha_t Q_T$
	3 of 5	$5(\alpha_3 + \alpha_4 + \alpha_5)/\alpha_t Q_T$
	4 of 5	$5(\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5)/\alpha_t Q_T$
	5 of 5	
6	1 of 6	$6\alpha_6/\alpha_t Q_T$
	2 of 6	$6(\alpha_5 + \alpha_6)/\alpha_t Q_T$
	3 of 6	$6(\alpha_4 + \alpha_5 + \alpha_6)/\alpha_t Q_T$
	4 of 6	$6(\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6)/\alpha_t Q_T$
	5 of 6	$6(\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6)/\alpha_t Q_T$
	6 of 6	

5.4.6 Modeling Asymmetrical Common Cause Failure Events

Most of the parametric models for quantification of common cause failure frequencies use an assumption regarding the symmetry of causes acting on a group of causes. The basic parameter, multiple Greek letter, alpha factor, and binomial failure rate models all assume that the frequency of a common cause event that fails a specific combination of components within a common cause group is the same for all such combinations of a given size. This was more fully discussed in Section 5.3. In a three-train system, for example, the basic parameter model assumes that

$$Q_{AB} = Q_{BC} = Q_{AC} = Q_2 \tag{5.19}$$

There are many situations in practice in which the common cause events would be expected to exhibit asymmetries. An example is the case of alternating systems (e.g., component cooling water system) where one train is normally operating, while the others are in standby. Some of these situations are described by models 1, 2, and 3 in Table 5-6. In model 1, a mix of normally operating and standby components produces asymmetry. In models 2 and 3, the location of four identical components in two different systems, and at a different reactor unit on the same site provides another example of an asymmetry. This consideration was used to justify the elimination of certain common cause events from the model; such as those affecting a pair of components, each in a different system.

The basic approach to modeling asymmetries is to incorporate the allowable CCBEs into the system logic. As an example of an asymmetrical model, consider the case of a three-train auxiliary feedwater system that includes three identical mechanical pumps, two of which are electric motor-driven and one is turbine-drive pump. A model of this system that accounts for both the symmetric and asymmetric cases is developed using the procedures of this guidebook and is presented in Section 6. A fault tree is constructed by separating the symmetric and asymmetric basic events, as shown in Figure 5-1. The asymmetry is represented by common cause event "X," which acts on components A and B only. Without the "X" event, and with the assumption of symmetry for the remaining causes (e.g., the $Q_{AB} = Q_{BC} = Q_{AC} = Q_2$), this fault tree corresponds with model 3 in Table 5-2 whose basic parameter formula for system failure probability is

$$Q_S = 3Q_1Q_2 + Q_3 + Q_1^3 \tag{5.20}$$

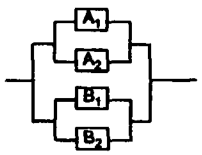
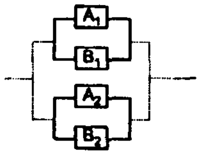
The minimal cutsets of the fault tree in Figure 5-1 (excluding cutsets containing basic events involving same components) are

First Order: $\{C_{ABC}\}$

Second Order: $\{C_{AB}, C_I\}$; $\{C_{AC}, B_I\}$; $\{C_{BC}, A_I\}$; $\{X, C_I\}$; $\{X, C_{AC}\}$; $\{X, C_{BC}\}$

Third Order: $\{A_I, B_I, C_I\}$

Table 5-6. Algebraic formulae for common cause events in some simple asymmetric configurations.

RELIABILITY BLOCK DIAGRAM	MODEL NO.	MODEL DESCRIPTION/ SUCCESS CRITERIA	APPROXIMATE FORMULAE BASIC PARAMETER MODEL*	KEY ASSUMPTIONS
	1	Two trains (A and B) of two components (1 and 2). A_1 and B_1 normally running, A_2 and B_2 in standby; at least one component must continue to operate for t hours.	$(\lambda_1 t)^4 + q_1^2(\lambda_1 t)^2$ $+ 2q_1 (\lambda_1 t)^3$ $+ (\lambda_2 t)^2 + \lambda_4 t$ $+ 2\lambda_2 t (q_1 + \lambda_1 t)(\lambda_1 t) + q_2\lambda_2 t$	Common cause failures between A_1 and A_2 or between B_1 and B_2 are accounted for in Q. No common cause events affecting exactly three components modeled.
	2	Four redundant components in standby; two in Unit 1 and two in Unit 2; one of four must operate on demand	$q_2^2 + q_4 + q_1^4$	Common cause failures involving two components can only affect A_1 and B_1 or A_2 and B_2. No common cause failures involving exactly three units modeled.
	3	Same as model 2 except components are all in operation and one must operate for t Hours.	$(\lambda_2 t)^2 + \lambda_4 t + (\lambda_1 t)^4$	Common cause failures involving two components can only affect A_1 and B_1 or A_2 and B_2. No common cause failures involving exactly three units modeled.

* Failure on demand and during operation are represented by q and λ, respectively. The mission time is t when applicable.

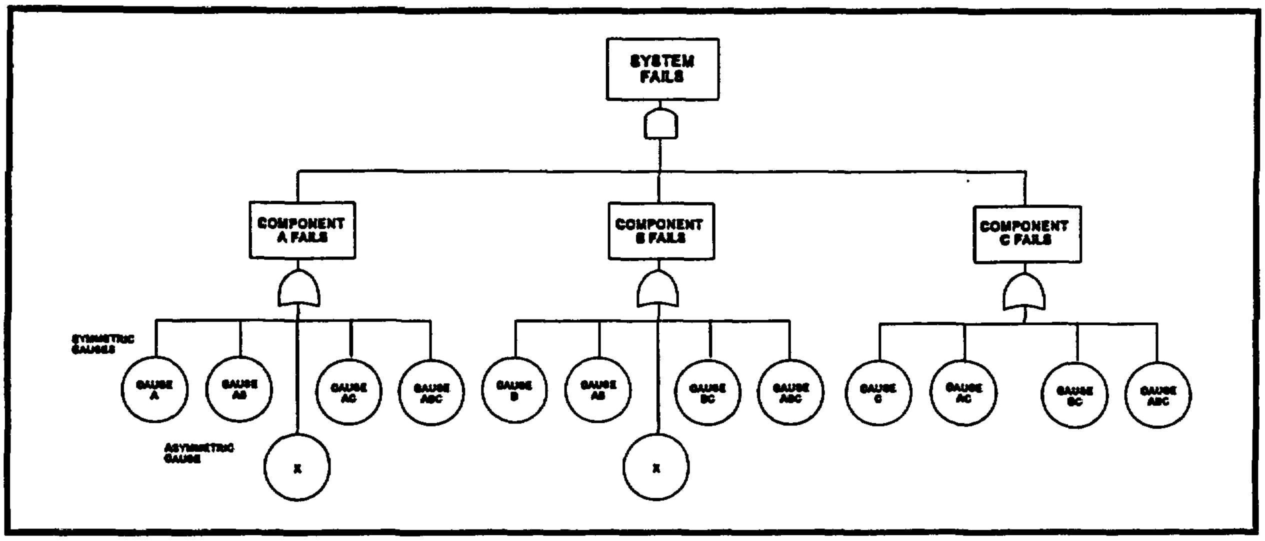


Figure 5-1. Fault tree of common cause events acting on components symmetrically and asymmetrically.

It is important to note that in data analysis and the process of setting up the impact vectors (see Section 5.5) for screening event data, events X and C_{AB} be distinguished from each other.

The above list of minimal cutsets includes all the cutsets of model 3 in Table 5-2 that include purely symmetric CCBEs, plus three second-order cutsets that include the asymmetric cause event. Using the basic parametric model, the formula for the system in Figure 5-1 is

$$Q_s \approx 3Q_1Q_2 + Q_3 + Q_1^3 + Q_X(Q_1 + 2Q_2) \tag{5.21}$$

In estimating parameters for this model, care was exercised to avoid double counting events as both symmetric and asymmetric causes.

The above example illustrates a straightforward application of the procedure of Section 5.3. The overall approach is to selectively add or delete basic events from a common cause event fault tree that initially contains all the cause events that were used to generate the symmetric models.

5.5 Parameter Estimation

The objective of this step is to estimate the CCBE probabilities or parameters of the model used to express these probabilities. Ideally, parameter values are estimated based on actual operating experience. The most relevant type of data would be the plant specific data. However, due to the rarity of plant specific common cause events a search will usually not produce statistically significant data. In almost all cases parameter estimation will have to rely mostly on experience from other plants, i.e., generic data. Unfortunately, in some cases even the generic data may be unavailable or insufficient. Therefore, it may be necessary to estimate the parameters based on the overall body of experience involving other types of components. Procedures for handling these cases are provided in the following. The first step is to review various sources of CCF data. Methods for developing statistical evidence from generic and plant-specific operating experience are presented next, followed by discussion on how to develop point estimates and uncertainty distributions for CCF model parameters. Finally, guidelines are provided for cases where no data are available.

5.5.1 Data Sources

Relevant data sources that can be used to estimate CCF model parameters include

- Industry-based generic data compilations
- Plant-specific data records
- Generically classified CCF event data and parameter estimates (reports and computerized databases).

Typical data sources within these categories are listed in Table 5-7. As mentioned earlier, due to the rarity of common cause events and the limited experience of individual plants, the amount of the plant-specific data for common cause analysis is very limited. Therefore, in most cases, data from industry experience and a variety of other sources are used to make statistical inferences about the frequency of common cause failure events. No single source of data is likely to provide a complete set of failure events for the components of interest in PRAs. The analyst should consult as many data compilations and documents as possible. Care must be exercised to recognize and take into consideration the potential biases in the databases. For instance, single independent component failures are under represented in the LERs. When such incompleteness and biases cannot be corrected by using other data sources, the impact on the parameter estimation must be assessed and considered in the uncertainty quantification. This issue will be revisited later in relation to uncertainty analysis.

Two computerized common cause failure databases have been developed in recent years, one by EPRI[14] which includes the database documented in EPRI NP-3967[12] and is proprietary to EPRI. The most comprehensive compilation of CCF data to date can be found in the CCF Data Collection and Analysis System developed by the NRC.[7] This database includes more than 2,500 common cause events involving the majority of PRA-significant components. The events are analyzed, classified, and documented in detail according to the procedures described in References 5 and 6. The CCF System database also includes more than 24,000 independent failures, also classified in terms of component type and applicable failure modes.

The CCF System performs the estimation automatically. Both point estimates and uncertainty distributions are provided for the alpha factor model. Point estimates of the MGL model are also available from the CCF System. More details on the use of the system can be found in References 4 through 7.

5.5.2. Quantitative Analysis of CCF Events

Due to the rarity of common cause events and the limited experience base for individual plants, the quantity of data for CCF analysis and plant-specific assessment of their frequencies is statistically insignificant. To overcome this difficulty, Reference 1 proposed creating plant-specific data through screening and evaluating generic data for plant-specific characteristics. This is done through a two-step process to facilitate the estimation of plant-specific CCF frequencies from generic industry experience. The first step uses an "event impact vector" to classify generic common cause events according to the level of impact of events (i.e., number of components failed) and the associated uncertainties in numerical terms. The second is impact vector specialization in which each generic event impact vector is modified to reflect the likelihood of the occurrence of the event in the plant of interest, and the degree of its potential impact. This step involves an assessment of the differences between the original plant (source plant) and the plant being analyzed (target plant) for susceptibility to various CCF events. Each technique is briefly described in the following paragraphs.

Table 5-7. Data sources for CCF analysis.

- **Generic Raw Data Compilation**
  - Licensee Event Reports
  - Nuclear Plant Reliability Data System
  - Diesel generators (NUREG/CR-1362[21])
  - Pumps (NUREG/CR-1205[22])
  - Valves (NUREG/CR-1363[23])
  - Selected instrumentation and control components (NUREG/CR-1740[24])
  - Primary containment penetrations (NUREG/CR-1730[25])
  - Control rods and drive mechanisms (NUREG/CR-1331[26])
- **Plant-specific Raw Data Records**
  - Maintenance work orders
  - Operators log
  - Work request forms
  - Significant events reports
- **Data Sources Specifically Developed for Dependent Failure Analysis.**
  - Pumps (NUREG/CR-2098[27])
  - Valves (NUREG/CR-2770[28])
  - Instrumentation and control assemblies (NUREG/CR-3289[29])
  - Diesel generators (NUREG/CR-2099[30])
  - Pumps, valves, diesel generators, and breakers (EPRI NP-3967[12])
  - Pumps, valves, diesel generators, circuit breakers, batteries, chargers (EPRI TR-100382[13])
  - CCDAT[14] (Computerized version of EPRI NP-3967[12])
  - CCF (Computerized database and data analysis tool; includes most PRA-significant components[7])

5.5.2.1 Event Impact Vector. According to Reference 1, for a component group of size m, the impact vector has m+1 elements. The (k+1) element, denoted by F_k, equals 1 if failure of exactly k components occurred, and 0 otherwise. Note that one and only one F_k equals 1; the others equal zero. For example, consider a component group of size 2. Possible impact vectors are the following:

[1, 0, 0] No components failed.

[0, 1, 0] One and only one component failed.

[0, 0, 1] Two components failed due to a shared cause.

A model, such as the impact vector described above, would be a sufficient numerical representation of the event if no sources of uncertainty existed in classifying the event as a CCF from the information available in the event report. However, many event descriptions lack sufficient detail. For example, the exact status of components is not known, and the causes and coupling factors associated with the failures are difficult to identify. Therefore, the classification of the event, including the assessment of its impact vector, may require establishing several hypotheses, each representing a different interpretation of the event.

Consider an event depicted in Figure 5-2 that affects a component group of size 3. It is not clear whether two or three components are affected by a shared cause. Thus, two hypotheses related to the number of failed components are formulated: (1) two of the three components failed, and (2) three of the three components failed. The impact vector for hypothesis one is: $I_1 = [0, 0, 1, 0]$, and the impact vector for hypothesis two is $I_2 = [0, 0, 0, 1]$. The analyst assigns a weight (or probability) to the first hypothesis equal to 0.9, and a weight of 0.1 to hypothesis two. That is, he believes that there is a 90 percent chance that hypothesis one is true and only a 10 percent chance that hypothesis two is true. To use these in a common cause failure analysis, the average or weighted impact vector is calculated. The average impact vector for this example is

$$\bar{I} = 0.9\, I_1 + 0.1\, I_2 = [0, 0, 0.9, 0.1].$$

More generally the average impact vector for a set of N hypotheses about an event is obtained by

$$\bar{I} = \sum_{i=1}^{N} w_i I_i \qquad (5.22)$$

where w_i is the weight or probability of hypothesis I with impact vector i_i and N is the number of hypotheses. The average impact vector is given by

$$\bar{I} = [\bar{F}_0, \bar{F}_1, \cdots, \bar{F}_m] \ . \qquad (5.23)$$

Some events occur where judging whether multiple failures occurred due to a shared cause or whether the failures were due to random independent causes is difficult. In such cases, the analyst again develops hypotheses and assigns probabilities to each. For example, consider a component group of size 2. Suppose that it is clear from the information that two components failed, but judging whether the failures were independent or not is difficult because of lack of information in the event report. Thus, there are two hypotheses for this case: (1) the two failures were due to a shared cause, and (2) the two failures were independent. The impact vector for hypothesis one is [0, 0, 1]. For hypothesis two, the analyst postulates independent failures of *two* components. Therefore, two impact vectors exist for this hypothesis—one for each component—since two components failed independently. Both are equal to [0, 1, 0]. If the weight for hypothesis one is 0.6 and 0.4 for hypothesis two, the average impact vector equals

$$0.6\, [0, 0, 1] + 0.4\, [0, 1, 0] + 0.4\, [0, 1, 0] = [0, 0.8, 0.6].$$

The probabilities for the hypotheses (relating to degree of impact of causes and coupling factors in the event being classified) are assessed by the analyst. However, as an aid to the analyst and to improve consistency and quality of results some guidelines for assessing the impact vectors are provided below. The proposed methods do not eliminate the need for the analyst to make subjective judgments. Rather, they provide guidance and techniques to develop the impact vectors from specific features of the events that can be characterized by numerical values more consistently.

<table>
<tr><td colspan="2"><b>Event Description:</b></td><td colspan="5">Maine Yankee, August 1977. Plant at power. Two diesel generators failed to run due to plugged radiators. The third unit radiator was also plugged.</td></tr>
<tr><td colspan="2"><b>Failure Mode:</b></td><td colspan="5">Fail to Run</td></tr>
<tr><td colspan="2"><b>Common Cause Component Group Size:</b></td><td colspan="5">3</td></tr>
<tr><td colspan="7"><b>Hypotheses for Event</b></td></tr>
<tr><td colspan="2" rowspan="2">Hypothesis</td><td rowspan="2">Probability</td><td colspan="4">Elements of Impact Vector</td></tr>
<tr><td>F_0</td><td>F_1</td><td>F_2</td><td>F_3</td></tr>
<tr><td>1.</td><td>Two of three components fail</td><td>0.9</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>2.</td><td>All three components fail</td><td>0.1</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td colspan="3" rowspan="2">Average Impact Vector ($\overline{I}$)</td><td>$\overline{F_0}$</td><td>$\overline{F_1}$</td><td>$\overline{F_2}$</td><td>$\overline{F_3}$</td></tr>
<tr><td>0</td><td>0</td><td>0.9</td><td>0.1</td></tr>
</table>

Figure 5-2. Example of the assessment of impact vectors involving multiple interpretation of event.

5.5.2.2 Generic Impact Vector Assessment. For an event to be classified as a CCF, more than one component must fail simultaneously because of a shared cause. Simultaneity and failure are defined with respect to certain performance criteria. For such events, the impact vector is uniquely and unambiguously defined as described in the previous section.

For many events, assigning a single impact category (i.e., $F_k = 1$ for some k) is not possible. This was also illustrated in the previous section. Such cases generally involve one or both of the following factors:[4-6]

1. Characteristics of the event may not match the criteria for the event to be assigned a unique impact vector. An example is an event involving two components in a *degraded* state owing to a known shared cause and coupling factor. The event does not meet the criteria of "component state" to be classified as a full CCF.

2. Critical information about individual failures involved in the CCF event (e.g.,information about the number of components affected, their functional state, and root causes of the event) may be lacking.

In general, there are three event types that require multiple hypotheses:

1. Events involving degraded component states,

2. Events involving multiple component failures closely related in time, but not simultaneously, and

3. Events involving multiple failures for which the presence of a shared cause cannot be established with certainty.

There are also events that involve combinations of these cases. The three types are discussed separately in the following paragraphs.

Case 1: Events Involving Degraded Component States

For events in this category, the analyst needs to assess the severity of degradation for each component in the event using component performance criteria as a reference (e.g., typical PRA component success criteria). In other words, given a degraded state, the analyst assesses the probability that the degree of degradation would have led to failure (e.g.,during a typical system mission as defined in PRAs). This is called the component degradation value, p_k, and has values in the range $0 \leq p_k \leq 1$.

The following scale may be used for a quantitative representation of the state of a component:

• Failed	$p = 1.00$
• Highly degraded	$p = 0.50$
• Degraded	$p = 0.10$
• Incipient	$p = 0.01$
• No Failure	$p = 0.00$

The values of the different elements of the average event impact vector can be calculated based on the possible combinations of failures expected, if the component degradation value is viewed as probability of failure. Table 5-8 shows how the various elements of the average impact vector may be calculated for components groups of size 2, 3, and 4. This technique does not require the formulation of multiple hypotheses, but it uses the information about the degraded states of the components to obtain the average impact vector.

Table 5-8. Impact vector assessment for various degrees of component degradations.

Component	Elements of the Impact Vector				
Group Size	F_0	F_1	F_2	F_3	F_4
2	$(1-p_1)(1-p_2)$	$p_1(1-p_2)+$ $p_2(1-p_1)$	p_1p_2	—	—
3	$(1-p_1)(1-p_2)$ $(1-p_3)$	$p_1(1-p_2)(1-p_3)+$ $p_2(1-p_1)(1-p_3)+$ $p_3(1-p_2)(1-p_1)$	$p_1p_2(1-p_3) +$ $p_1p_3(1-p_2) +$ $p_2p_3(1-p_1)$	$p_1p_2p_3$	—
4	$(1-p_1)(1-p_2)$ $(1-p_3)(1-p_4)$	$p_1(1-p_2)(1-p_3)(1-p_4)+$ $p_2(1-p_1)(1-p_3)(1-p_4)+$ $p_3(1-p_1)(1-p_2)(1-p_4)+$ $p_4(1-p_1)(1-p_2)(1-p_3)$	$p_1p_2(1-p_3)(1-p_4)+$ $p_1p_3(1-p_2)(1-p_4)+$ $p_1p_4(1-p_2)(1-p_3)+$ $p_2p_3(1-p_1)(1-p_4)+$ $p_2p_4(1-p_1)(1-p_3)+$ $p_3p_4(1-p_1)(1-p_2)$	$p_1p_2p_3(1-p_4)+$ $p_1p_2p_4(1-p_3)+$ $p_1p_3p_4(1-p_2)+$ $p_2p_3p_4(1-p_1)$	$p_1p_2p_3p_4$

In this case, component states (failure, degraded, etc.) do not occur, or are not detected, simultaneously. Rather they are recorded at different, but closely correlated times (or test cycles). In this case, a probability q can be assigned that reflects the degree the events (component degradations) represent a CCF event during the mission time of interest (e.g., typical PRA mission times). The following guidelines are suggested for assessing q for different operational characteristics.

Case 2: Events Involving Failures Distributed in Time.

Operating Components. For operating components, the values of the timing factor probability q are based on comparing the minimum difference in the time of the failures to the PRA mission time. There is no assumption about the time of failure or whether the multiple failures, or degraded states, occurred at the same time. The following guidelines are used to assign values of q:

- For component failures that occur within one PRA mission time, the event is interpreted as a CCF event and q = 1.00.
- For k components that fail more than one (PRA) mission time apart, but within 1 month of each other, q = 0.50.
- For component failures that occur more than one month apart, q = 0.10.
- For component failures that occur more than one test interval apart, events are considered as independent, thus q = 0.00.

Standby Components. For standby components, the situation is more complex. If redundant components fail from a shared cause and at consecutive tests separated in time, there is evidence that the same mechanism is at work (some "randomizing" effect is also taking place, which on other occasions may not be so effective at decoupling failure time). If failures occur more than one test apart, then the randomizing effect is stronger. To account for the randomizing effect, consideration is given to the strategies and frequency. However, since test strategies are usually not known to the analyst for generic events, conservative assumptions may be made based on the following reasoning. There are two approaches to this problem: the standby failure rate concept and a failure probability on demand.

Approach Using the Standby Failure Rate Model. If non-staggered testing is adopted, it is possible for the components to fail immediately following the test, in which case, the latent CCF state could exist for the test interval, T_I. The average time a latent CCF state could exist is half the test interval. Therefore using the same rules should be conservative. Based on this, q will be assigned as follows:

- If components fail, or are reported failed, within half the test interval, the event is interpreted as CCF with q = 1.00,
- If component failures are separated by a time interval longer than $T_I/2$, but shorter than T_I, the event is interpreted as a CCF with q = 0.50,
- If component failures are separated by a time interval longer than T_I, but shorter than $3/2\ T_I$, the event is interpreted as a CCF with q = 0.10, and
- If the component failures are separated by a time interval longer than $3/2\ T_I$, the event is interpreted as two (or m) independent failures.

For staggered testing, the situation is more complex. While the tests will be conducted on individual components, at intervals corresponding to the same interval T_I as discussed above (usually determined by technical specifications), there will be a test on some component at intervals of T_I/m where m is the redundancy level of the system. Thus, even if there is no immediate testing of redundant components following a revealed failure, there would be evidence of a CCF within an interval T_I/m. Thus the average exposure time to an unrevealed CCF should be less in staggered testing cases.

Since test intervals vary between plants and systems for like components, some average values may have to be assumed. A month is appropriate for diesel generators in U. S. plants, but is too short for most other components. Test intervals must be determined for each individual system/component combination as part of the initial system familiarization process, discussed in Section 2 of this report.

Approach Using the Probability of Failure on Demand Model. For standby systems where a CCF is considered for failure on demand, the value chosen for q depends on the number of tests (challenges) of the second component between its failure and the failure of the first component (assuming a two component system to illustrate the point). To clarify terminology, it is instructive to discuss test strategies. With a non-staggered testing regime, components are usually tested sequentially but within a short time. If the first component works, there may be no CCF. However, if the first fails, the subsequent test performed on the second will reveal if there is a CCF. In the case of staggered testing, there are two extremes; the redundant component is tested immediately upon failure of the component being tested, or it is tested on the next scheduled test. In the following discussion, the first challenge refers to the first test on the second component, following the failure of the first component, whether it immediately follows the first failure or is separated in time. Failure on the second challenge implies one successful challenge of the second component following failure of the first component; this also holds for CCCG > 2. The following guidelines are suggested for assigning the value of q:

- If the second component fails on the first challenge after failure of the first component, the event is interpreted as CCF with q = 1.00.

- If the failures are separated by one successful challenge, then using the binomial concept, a point estimate for the probability of failure of the second component given the failure of the first one is ½ (one failure in two challenges). In this case, the event is interpreted as a CCF with q = 0.50.

- If the failures are separated by two successful challenges, then following the same line of reasoning, a point estimate for q would be 1/3. However, it is felt that this value is conservative. A more realistic value is q = 0.10.

- Failures separated by more than two successful challenges can be assumed to be independent.

Average Impact Vector Calculation. Regardless of how q is determined, the impact vector for these situations is obtained from two sets of impact vectors, one representing the common cause hypothesis with probability q, and another representing the hypothesis of independent events. The probability q is the probability that on a real demand, the mechanisms would have led to a CCF.

As an example, if two of three components fail because of a shared cause but at different times, then the set of impact vectors will be the following:

For common cause failure,

$$I_{CCF} = q\,[0,0,1,0] = [0,0,q,0]$$

For independent failure of component 1,

$$I_{e_1} = (1\text{-}q)\,[0,1,0,0]$$

$$= [0, 1\text{-}q, 0, 0] \text{ for component 1}$$

and for independent failure of component 2,

$$\begin{aligned} I_{e_2} &= (1\text{-}q)\,[0,1,0,0] \\ &= [0, 1\text{-}q, 0, 0] \text{ for component 2.} \end{aligned}$$

The average impact vector for this specific case is

$$\bar{I} = [0,2\,(1\text{-}q), ..., q, ..., 0].$$

Generally, for an event involving a time delay failure of k components in a system of m redundant components, there are k+1 impact vectors as follows:

$$\begin{aligned} I_{CCF} &= [0, 0,..., q, ..., 0], \text{ where q is the k+1 element of the vector,} \\ I_{e_1} &= [0, 1\text{-}q, 0, ..., 0] \text{ for component 1} \\ &\vdots \\ I_{e_k} &= [0, 1\text{-}q, 0, ..., 0] \text{ for component k.} \end{aligned} \qquad (5.24)$$

The average impact vector in this case is

$$\bar{I} = [0, k(1\text{-}q), ..., q, ..., 0\,],$$

where q is the k+1 element of the vector.

Case 3: Events Involving Uncertainty about Shared Cause

Uncertainty because of insufficient information regarding component states and failure times can be folded in the component degradation parameters p_i's, and timing factor, q, respectively. Uncertainty stemming from inability to determine whether the multiple failures were due to a shared cause or are independent deserves a parameter of its own since it relates to an important and distinct element of CCF events, i.e., the amount of coupling between the multiple events. For this reason a parameter, "shared cause factor," c, ($0 \le c \le 1$) is introduced as the analyst's degree of confidence about the presence of a shared cause in the event. The following scale may be used for a quantitative representation of the analyst's confidence that the failures are coupled and share the same cause:

• Very High	c = 1.0,
• High	c = 0.50,
• Moderate	c = 0.10,
• Low	c = 0.01,
• No coupling	c = 0.00.

The effect of this factor on the event impact vector can be obtained similarly to the timing factor q. More specifically, the set of Equations 5.24 can be used after replacing q with c.

$$
\begin{aligned}
I_{CCF} &= [0, 0, ..., c, ..., 0], \text{ where c is the k+1 element of the vector,} \\
I_{c_1} &= [0, (1\text{-}c), 0, ..., 0] \text{ for component 1,} \\
&\vdots \\
I_{c_k} &= [0, (1\text{-}c), 0, ..., 0] \text{ for component k.}
\end{aligned}
\qquad (5.25)
$$

The average impact vector in this case is

$$
\bar{I} = [0, k(1\text{-}c), ..., c, ..., 0],
$$

where c is the k+1 element of the vector.

Case 4: Events Involving Degraded States, Time Delay, and Uncertain Shared Cause

In cases where the event involves degraded states, time delay, and uncertainty about presence of a shared cause, the impact vector can be obtained by first developing the impact vector as if the events did not involve any time delay or uncertainty about shared cause, and then modifying the resulting impact vector to reflect separation of failures or degraded states in time and or cause. The resulting set of impact vectors is given by

$$
\begin{aligned}
I_{CCF} &= [cqF_0, cqF_1, ..., cqF_m], \\
I_{c_1} &= [(1\text{-}cq)(1\text{-}p_1), (1\text{-}cq)\, p_1, 0, ..., 0], \text{ for component 1,} \\
&\vdots \\
I_{c_k} &= [(1\text{-}cq)(1\text{-}p_m), (1\text{-}cq)\, p_m, 0, ..., 0], \text{ for component k.}
\end{aligned}
\qquad (5.26)
$$

In these impact vectors, the p_i's represent the degree of degradation of the I-th component, and the F_i's are calculated from p_i's according to the relations in Table 5-8 for m = 2, 3, and 4, or similar ones for m > 4. Finally, the average impact vector is obtained by adding I_{CCF} and the I_c's.

Note that the product of cq represents an overall measure of coupling strength. The decomposition of this measure, in terms of c and q, is merely an aid to the analyst's subjective assessment of the strength based on different manifestations of the degree of coupling presence. As can be seen from Equation 5.26, the quantity modifying the impact vectors for shared cause strength is cq, which could be replaced by a single parameter.

5.5.2.3 Specializing Impact Vectors for Plant Specific Analyses. The discussions to this point have addressed the use of industry data to perform generic analyses. According to Reference 1, modification to the original impact vector for application to plant specific analyses requires a two-step adjustment of the original impact vector to account for qualitative and quantitative differences between the original and target systems. These modifications are discussed separately.

Adjustment Based on Qualitative Differences. In this step, the following question is addressed. Considering design, environmental, and operational characteristics of the original and target systems, could the same event occur in a target system? In other words, is the system that is being analyzed vulnerable to the cause(s) and coupling factor(s) of historic events?

In answering, the analyst must rely on knowledge of the target plant system design, specific component design, operational activities, and the characteristics of the system in which the components operate. In addition, the analyst uses information contained in the event reports to decide which characteristics of the target system are similar to those of the original systems, and which are different. This information helps the analyst determine the applicability of an event. Since there are many possibilities, no specific guidelines are provided here.

Generally, if the cause or coupling mechanism of an event cannot exist in the system being analyzed, the event is screened out; otherwise, it is retained for further consideration in the data specialization step. Here it is recognized that the analyst may be uncertain whether the event is applicable, based on the available information. According to Reference 1, in this situation, the analyst can multiply the original impact vector by an **event applicability factor r**, ($0 \leq r \leq 1$) which is subjectively assessed and is a measure of applicability of the cause and coupling factor of the event to the target system. The r number is a measure of the physical, operational, and environmental differences between the original and the target system, as well as the analyst's uncertainty as to whether such differences exist.

The modified application-specific impact vector is then written as

$$I_r = r * I. \qquad (5.27)$$

The r factor may be written as the product of two factors r_1 and r_2, which are measures of applicability of the root cause and coupling factor of the event, respectively.[5] The "strength" of a root cause manifests itself in the degree to which each of the components is affected. Therefore, on the arbitrary scale of zero to one, a root cause of zero strength results in no failure. The likelihood of a failure increases as the root cause strength moves towards one. In contrast, the coupling factor strength represents the degree to which multiple failures share a common-cause. Coupling strength of zero means failures are independent, while CCFs are characterized by coupling strength of one. The role of these two factors in creating various types of events is shown schematically in the diagram of Figure 5-3.

Estimates of r_1 and r_2 are the analyst's assessment of the quality of target system defenses against the root cause and coupling factor of the event as compared with the original system. Again this requires subjective judgment, which is often a difficult task because of lack of sufficient information, particularly, concerning the original system. In such cases, it is recommended that the analyst compare the target system against an "average" system. The values listed in Table 5-9 are suggested values for r_1 and r_2.

Another issue which impacts the applicability factor, and which is often encountered in data analysis, is what to do with events which have led to modifications and improvements to the system. It is frequently argued that given a modification to correct a root cause of an event, the event should be screened from the database since it is not expected to occur. In contrast, some argue that the events observed in the past are merely realizations of a class of failures, and that the evidence for the frequency of occurrence of that class should not be removed. It is also argued that modifications do not always lead to improvements, at least not immediately, on account of the potential for introduction of new problems and failure mechanisms.

Both sides of this debate have valid points. The key issue is how much credit can be given to a design improvement. As an approach, the success rate of past design changes (to remove failure causes) can be considered. This can be done by reviewing the operating experience for a specific class of components and systems, over several years, to ascertain the change in the ratio of design-related failure numbers to the total number of failures. The slope of change can be used as an effective measure of design improvements and as a weight for database events which have led to design changes. This weighting can be used as an estimator for the values of r_1 and r_2. Data need to be collected and classified with this in mind, since the level of detail in current data compilations do not support this type of estimation.

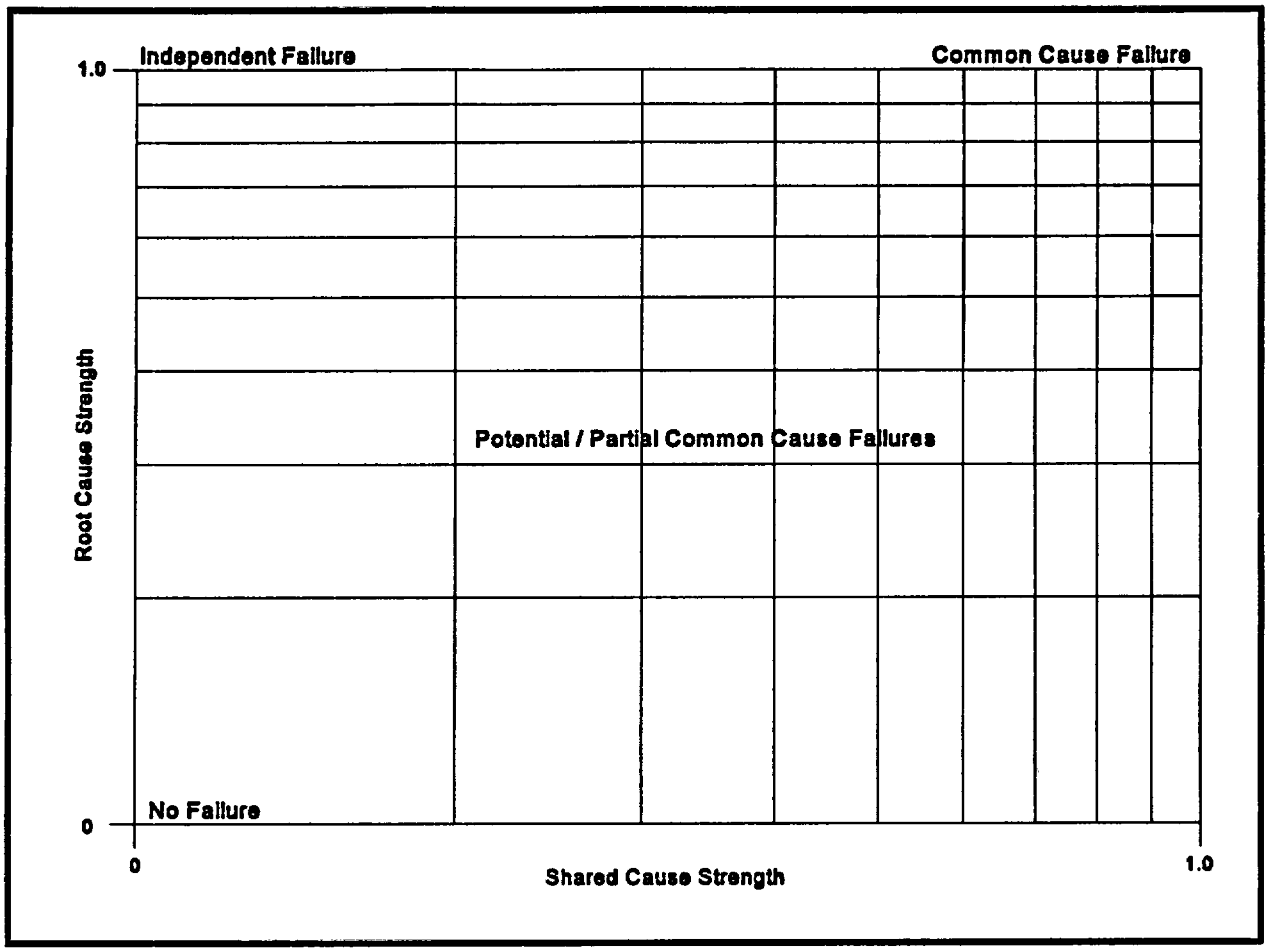


Figure 5-3. Schematic representation of the role of coupling factor and root cause strength information of different classes of events (the density of vertical and horizontal lines represents the degree of strength for illustrative purposes).

Table 5-9. Suggested values for r_1 and r_2.

Strength of Target Plant Defenses Compared with Original/Average Plant	Applicability Factor Root Cause (r_1)	Applicability Factor Coupling (r_2)
Complete Defense	0.0	0.0
Superior Defense	0.1	0.1
Moderately Better Defense	0.5	0.5
Weaker or No Defense	1.0	1.0

Adjustment for Quantitative Difference. In the next step, the level impact of the event on the target system is analyzed because of the difference that may exist between the level of exposed population of the target and original systems. Depending on whether the target system size (i.e., the number of similar components in the system, typically the level of exposed population), is larger, equal, or smaller than the original system, the impact vector must be "mapped up," "kept unchanged," or "mapped down." Reference 1 provides mapping rules for the following cases:

1. **Mapping Down.** Mapping down is done when the component group size in the original system is larger than in the system being analyzed (target system).

2. **Mapping Up.** Mapping up is done when the component group size in the original system is smaller than in the system being analyzed (target system).

Reference 1 does not, however, provide an estimator for a critical parameter in the formulae for mapping up. Mapping rules and corresponding algorithms for typical situations are summarized in Appendix C of this report. The following estimator is suggested for the mapping up parameter (see Appendix C):

$$\rho = \sum_{l=1}^{m} \frac{l}{m} \bar{F}_l \qquad (5.28)$$

where F_l is the I-th element of the impact vector and m is the size of the original system. This estimator is consistent with the binomial assumption which forms the basis of the formulae for mapping up. The mapping up assumption, in turn, is the basis for the binomial failure rate model.

The end result of the two-step process of impact vector adjustment is an adjusted impact vector that represents the number of components that would fail if the event occurred in the target system.

5.5.3 Estimation of CCF Event Frequencies from Impact Vectors

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

$$n_k = \sum_{l=1}^{m} \bar{F}_k(l) \ , \qquad (5.29)$$

where

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

$\bar{F}_k(l)$ = the k-th element of the average impact vector for event I.

Event statistics are used to develop estimates of CCF model parameters. For example, the parameters of the alpha-factor model (see Appendix A for a description of several parametric models) can be estimated using the following maximum likelihood estimator (MLE):

$$\hat{\alpha}_k = \frac{n_k}{\sum_{j=1}^{m} n_j} . \qquad (5.30)$$

Table 5-10 provides a set of estimators for various parametric models. More details on estimators are provided in Appendix A. Except for the MGL model, the estimators presented in Table 5-10 are the maximum likelihood estimators and are presented here for their simplicity. The mean values obtained from probability distribution characterizing uncertainty in the estimated values are more appropriate for point value quantification of system unavailability. These mean values are presented in the context of developing statistical uncertainty distributions for the various parameters in Appendix D. Due to lack of a clear

Table 5-10. Simple point estimators for various parametric models.

Method	Non-Staggered Testing[a]	Staggered Testing	Remarks
Basic Parameter	$Q_k^m = \dfrac{n_k}{\binom{m}{k} N_D}$ $k = 1, ..., m$	$Q_k^m = \dfrac{n_k}{m \binom{m}{k} N_D}$ $k = 1, ..., m$	For time-based failure rates replace system demands (N_D) with total system exposure time T.
Alpha Factor	$\alpha_k^m = \dfrac{n_k}{\sum_{j=1}^{m} n_j}$ $k = 1, ..., m$	Same as Non-staggered case	
MGL[b]	$\rho_j^m = \dfrac{\sum_{k=j}^{m} k n_k}{\sum_{k=j-1}^{m} k n_k}$ $k = 1, ..., m$ $(j \geq 2)$ $\rho_2 \equiv \beta$ $\rho_3 \equiv \gamma$ *etc.* $\rho_4 \equiv \delta$	$\rho_j^m = \dfrac{\sum_{k=j}^{m} n_k}{\sum_{k=j-1}^{m} n_k}$ $k = 1, ..., m$ $(j \geq 2)$ $\rho_2 \equiv \beta$ $\rho_3 \equiv \gamma$ *etc.* $\rho_4 \equiv \delta$	Estimators are based on approximate method described in Appendix A, and Appendix D.

(a) N_D is the total number of tests or demands on a system of m components.

(b) Except for MGL, formulae provided are maximum likelihood estimators. The basis for the MGL estimators is explained in Appendix D.

sampling model for the MGL method, the MLEs cannot be rigorously obtained. Estimators listed in Table 5-10 for MGL parameters are obtained from MLE estimates of the basic parameter model.

Table 5-10 displays two sets of estimators developed based on assuming different testing schemes. Depending on how a set of redundant components in a system are tested (demanded) in staggered or non-staggered fashion, the total number of challenges that various combinations of components are subjected to is different. This needs to be taken into account in the exposure (or success) part of the statistics used, affecting the form of the estimators. The details of why and how the estimators are affected by testing schedule are provided in Appendix A.

5.5.4 Treatment of Uncertainties

Estimation of model parameters involve uncertainties that need to be identified and quantified. A broad classification of the types and sources of uncertainty and potential variabilities in the parameter estimates is as follows:

1. Uncertainty in statistical inference based on limited sample size.

2. Uncertainty due to estimation model assumptions. Some the most important assumptions are

   (a) Assumption about applicable testing scheme (i.e., staggered vs. non-staggered testing methods).

   (b) Assumption of homogeneity of the data generated through specializing generic data to a specific plant. An alternative assumption is that even after mapping generic impact vectors to a specific plant application, the resulting statistical data still exhibit plant-to-plant variability and should be treated as a non-homogeneous population.

   (c) Reduction of multiple impact vectors (associated with multiple hypotheses about a given event) to an average impact vector. An alternative method (exact method) uses individual impact vectors and creates multiple statistical databases which are then used in parameter estimation (Appendix D).

3. Uncertainty in data gathering, and database development. These include

   (a) Uncertainty because of lack of sufficient information in the event reports, including incompleteness of data sources with respect to number of failure events, number of system demands, and operating hours.

   (b) Uncertainty in translating event characteristics to numerical parameters for impact vector assessment (creation of generic database).

   (c) Uncertainty in determining the applicability of an event to a specific plant design and operational characteristics (specializing generic database for plant-specific application).

The role of uncertainty analysis is to produce a probability distribution of the common cause failure frequency of interest in a particular application, covering all relevant sources of uncertainty from the above list. Clearly, some of the sources or types of uncertainty may be inapplicable, depending on the intended use of the CCF parameter and the form and content of the available database. Also, methods for handling various types of uncertainty vary in complexity and accuracy. The choice depends on the resources available to the analyst and the importance of an accurate account of uncertainties. The following discussion summarizes the steps that can be taken by the analyst and corresponding methods and tools at the analyst's disposal to develop uncertainty distributions of CCF model parameters. Some of the mathematical details are described in Appendix D.

It is easier to formulate and describe methods for analyzing uncertainties in categories 2 and 3 within the framework and methods for treating uncertainties in category 1. Thus the discussion of uncertainty treatment will start with a description of how the statistical uncertainties for category 1 are treated.

5.5.4.1 Statistical Uncertainty. This type of uncertainty is usually quantified through the statistical distributions or confidence bounds produced in process of converting the sample data into estimates of the parameters of interest. For example, consider the case where the applicable statistical sample is produced by combining various impact vectors according to Equation 5.29. In this case the sample data are

$$Data = [n_1, \dots, n_m], \tag{5.31}$$

Appendix D uses a particular statistical method known as the Bayesian approach to develop the uncertainty distributions or CCF model parameters (e.g., $\alpha_1, \alpha_2, \dots, \alpha_m$). Alternatively, classical statistical methods could be used to develop confidence bounds for each parameter. The CCF software[7] can be used to perform the Bayesian computations for the α-factor model.

5.5.4.2 Model Uncertainty. Each of the three key model-related uncertainties is discussed separately in the following.

(a) When data are collected, it is often difficult to determine the testing scheme applied. Even if the testing scheme can be identified, it can vary from plant to plant and can change within each plant over time. In other words, the exact testing scheme is uncertain and non-uniform in a database. As discussed in Appendix A, the testing method impacts the number of challenges on the common cause component group, and thus the statistical sample size used explicitly or implicitly in developing CCF parameter estimators and associated statistical uncertainty distributions.

Two approaches can be taken to account for this source of uncertainty. The first approach is to select the assumption that results in the more conservative estimates of the CCF model parameters, if such conservatism does not distort critical conclusions of the PRA analysis.

A second approach is to formally account for this source of uncertainty by a mixture of two distributions developed based on the two testing schemes. The uncertainty distribution of α_2 is shown as

$$\pi(\alpha_2) = w_s \pi_s(\alpha_2) + w_{ns} \pi_{ns}(\alpha_2) \tag{5.32}$$

where $\pi_s(\alpha_2)$ and $\pi_{ns}(\alpha_2)$ are the statistical uncertainty distributions based on staggered and nonstaggered testing schemes, respectively, and w_s and $w_{ns} = 1 - w_s$ are the corresponding weights or degrees of confidence given to each testing hypothesis. The assessment of such weights is the responsibility of the analyst based on his/her assessment of the percentage of plants that follow one testing strategy versus another. Currently most plants employ the staggered testing scheme.

(b) The assumption leading to generation of the statistical data of Equation 5.31 is that once the CCF events are re-interpreted for plant-specific application and impact vectors are mapped for applicability, a homogeneous population of events is created. That is, after the specialization of the CCF event impact vectors, the events are considered to belong to the same population and coming from the plant being analyzed.

An alternative assumption is that the data from various plants are kept separate assuming that even after mapping the generic impact vectors to a specific plant the resulting statistical data still carry a residual plant-to-plant variability. The form of the statistical data generated under this assumption is

$$D^{(i)} = [n_1^{(i)}, n_2^{(i)}, \ldots, n_m^{(i)}], \quad i = 1, \ldots, N \tag{5.33}$$

where $D^{(i)}$ is the statistical data for the I-th plant, and N is the number of plants in the database.

Appendix D outlines the Bayesian approach for using the data of Equation 5.33 in developing the uncertainty distributions of CCF model parameters under the assumption of plant-to-plant variability of CCF frequencies. The resulting distributions are normally broader than those obtained based on the homogeneous data of Equation 5.31.

Both the homogeneous and nonhomogeneous models are available in the CCF software.[7] The non-homogeneous option can be used to develop generic and global assessment of the ranges of CCF parameters across the industry. It can also be used as a prior distribution in plant-specific estimations. For this use the data from the plant being analyzed should be excluded from the non-homogeneous database, Equation 5.33, to be used as plant-specific data in the Bayesian updating process.,

(c) The method described in Section 5.5.4 develops statistical evidence needed for parameter estimation, i.e., Equation 5.33 by averaging event impact vectors over multiple hypotheses and corresponding probabilities. The averaging procedure leads, as described in Reference 1, to an underestimation of uncertainties, while producing nearly exact mean values. Reference 1 proposed a formal uncertainty analysis method to account for the impact of the multiple-hypothesis approach to data classification. This is discussed in more detail in Appendix D of this report.

5.5.4.3 Data Uncertainty. From earlier discussions it is evident that there are potentially significant uncertainties in the development of a statistical database from CCF event reports. Analysts are likely to have different interpretations of the events, and make different assumptions about what might be missing from both the event reports and physical and operational descriptions of the plants involved. This is true even though specific guidelines have been provided in this report to ensure, as a minimum, a reasonable level of accuracy and consistency and to reduce analyst-to-analyst variabilities.

Certain formal and rigorous methods for handling uncertainties in CCF frequencies, as a function of analyst uncertainty in the impact vector assessment, have been suggested and applied to a small data sample. These methods, however, tend to be tedious for large databases. A rough approximation of the range of uncertainty in CCF frequency estimates can be developed through ad-hoc techniques, such as bounding of the uncertainties. For example, an analyst assesses the impact vectors "optimistically" (tends to judge events "independent" when in doubt) and, then, assesses the impact vectors "pessimistically" (tends to judge events as common cause). Distributions of CCF frequency are then developed from statistics obtained from each of the two sets of impact vectors, according to the methods described in Appendix D. These distributions are combined to obtain the overall uncertainty range in the CCF frequency estimate, similar to Equation 5.32.

One disadvantage of the Hierarchical Bayes method for assessing the spread of the α-factor distribution due to plant-to-plant variability (non-homogeneous assumption), is its computational complexity. In contrast, uncertainty estimation based on homogeneous data model is relatively simple. It is worth noting that even with the homogeneous assumption, the final CCF probability distribution may not be narrow. This is because common cause failure frequencies, Q_k's, are calculated by multiplying α-factors and total component failure frequency, Q_t:

$$Q_k \propto \alpha_k Q_t \tag{5.34}$$

The spread of the distribution of Q_k is, therefore, also influenced by the spread of the distribution of Q_t, which often includes uncertainties due to plant-to-plant variability. Also for skewed distributions with fixed mean value, the tail behavior (e.g., value of the 95-th percentile) is not very sensitive to the spread of the distribution. In other words, since the distribution of an α factor obtained by both homogeneous and nonhomogeneous methods have practically the same mean values but different spreads, at least the upper bound of the distributions are numerically very close.

A relatively simple and practical approach for developing uncertainty distribution of common cause failure parameters for a component of interest is as follows: Develop a pseudo plant-specific database by specializing (mapping) the generic event data for that component to the plant being analyzed. Assume that this database is homogeneous, i.e., all non-homogeneities have been removed through the process of modification of the generic impact vectors to match the conditions at the plant being analyzed. Finally use the Bayesian estimation procedure for homogeneous data (e.g., Equation 5.33) to estimate the parameter distribution.

A critical element of the above procedure is the choice of prior distribution for the parameters (α's). This distribution could be the analyst's subjective judgement, or based on observed ranges of variation of the parameters. One option is to develop a plant-to-plant variability distribution of various α-factors (or other CCF model parameters) across all components and failure modes using the Hierarchical Bayes method.

A second approach that can be used to estimate prior distributions is to obtain the MLE for a given α_k, and then use a constrained noninformative prior[31] as its uncertainty distribution. This distribution maximizes the uncertainty given a constraint on the mean value. This distribution is usually much broader than the corresponding hierarchical Bayes distribution. For a CCCG of size m, it is assumed that the constrained noninformative prior distributions are statistically independent. Care must be used when updating these distributions to make sure that the means of the updated distributions sum to 1.0. It is usually best to estimate the mean of the distributions for $\alpha_2, \ldots, \alpha_m$, and subtract their sum from 1.0 to obtain the mean for α_1.

A third approach uses information from the constrained noninformative prior distributions to obtain an estimate of the parameter A_T of a Dirichlet distribution described in Appendix D. For a CCCG of size m, there are m estimates of A_T. These estimates can be combined to obtain an effective estimate for A_T. The arithmetic mean, geometric mean, or a weighted mean of these estimates can be used to combine them.

This last approach was used to develop prior distributions for the α-factors for each CCCG size. All CCF events in the CCF database[7] were used to estimate the prior distributions. First, events were mapped to a given CCCG size. The MLE for each alpha factor was obtained and fit with constrained noninformative distribution. The estimate of A_T for each alpha was then calculated, and the results combined using the geometric mean. The results are displayed in Table 5-11.

5.5.5 Use of the CCF Data Collection and Analysis System

Much of the difficulty in performing data analysis in support of CCF analysis has been removed with the development of the CCF Data Collection and Analysis System.[4-7] This system is designed to perform data classification and parameter estimation for a large number of components usually modeled in PRAs. This analysis can be done on a generic basis or for a plant-specific study. To obtain estimates of the CCF parameters, the analyst needs to have identified all important CCCG using the guidelines provided earlier in this report. Knowing the component type and analysis boundaries and armed with the qualitative information collected in the qualitative phase of the analysis (Section 4) the analyst can select the events

Table 5-11. Generic prior distributions for various system sizes.

CCCG Size m	α-Factor	Distributions Parameters		Percentiles			Mean
		a	b	P_{05}	P_{50}	P_{95}	
2	α_1	9.5300	0.470	8.20E-01	9.78E-01	1.00E-00	0.95300
	α_2	0.4700	9.530	1.42E-04	2.16E-02	1.81E-01	0.04700
3	α_1	15.2000	0.800	8.42E-01	9.67E-01	9.99E-01	0.95000
	α_2	0.3872	15.613	2.10E-05	8.79E-03	1.01E-01	0.02420
	α_3	0.4128	15.587	3.45E-05	1.01E-02	1.05E-01	0.02580
4	α_1	24.7000	1.300	8.67E-01	9.61E-01	9.95E-01	0.95000
	α_2	0.5538	25.446	1.44E-04	1.08E-02	7.81E-02	0.02130
	α_3	0.2626	25.737	2.98E-07	1.99E-03	4.82E-02	0.01010
	α_4	0.4836	25.516	6.29E-05	8.42E-03	7.17E-02	0.01860
5	α_1	38.042	1.958	8.86E-01	9.58E-01	9.91E-01	0.95106
	α_2	0.7280	39.272	3.72E-04	1.10E-02	6.05E-02	0.01820
	α_3	0.4120	39.588	1.32E-05	3.93E-03	4.22E-02	0.01030
	α_4	0.2336	39.766	4.57E-08	8.97E-04	2.89E-02	0.00584
	α_5	0.5840	39.416	1.24E-04	7.66E-03	5.27E-02	0.01460
6	α_1	50.4724	2.528	8.97E-01	9.58E-01	9.89E-01	0.95231
	α_2	0.7791	52.221	3.76E-04	9.20E-03	4.78E-02	0.01470
	α_3	0.5406	52.459	6.04E-05	5.02E-03	3.79E-02	0.01020
	α_4	0.3127	52.687	9.28E-07	1.56E-03	2.66E-02	0.00590
	α_5	0.2433	52.757	5.77E-08	7.67E-04	2.24E-02	0.00459
	α_6	0.6519	52.348	1.66E-04	6.93E-03	4.27E-02	0.01230
7	α_1	74.5360	3.464	9.12E-01	9.59E-01	9.86E-01	0.95559
	α_2	0.9906	77.009	6.44E-04	8.84E-03	3.79E-02	0.01270
	α_3	0.6817	77.318	1.39E-04	5.05E-03	2.99E-02	0.00874
	α_4	0.4891	77.511	2.21E-05	2.82E-03	2.42E-02	0.00627
	α_5	0.2941	77.706	3.39E-07	8.97E-04	1.74E-02	0.00377
	α_6	0.2051	77.795	3.84E-09	2.94E-04	1.35E-02	0.00263
	α_7	0.8034	77.197	2.89E-04	6.52E-03	3.32E-02	0.01030
8	α_1	97.6507	4.349	9.20E-01	9.60E-01	9.84E-01	0.95736
	α_2	1.1118	100.888	7.25E-04	7.91E-03	3.13E-02	0.01090
	α_3	0.7915	101.209	2.07E-04	4.87E-03	2.52E-02	0.00776
	α_4	0.6253	101.375	6.92E-05	3.34E-03	2.17E-02	0.00613
	α_5	0.4417	101.558	8.51E-06	1.76E-03	1.74E-02	0.00433
	α_6	0.2581	101.742	6.09E-08	4.74E-04	1.21E-02	0.00253
	α_7	0.1969	101.803	1.59E-09	1.93E-04	1.00E-02	0.00193
	α_8	0.9241	101.076	3.82E-04	6.12E-03	2.78E-02	0.00906

from the CCF database to be used in parameter estimation. The CCF Data Collection and Analysis System has two main features allowing users to:

1. Perform generic analysis of CCF events in the database. Generic analysis includes a qualitative analysis of causes and severity of CCF events and an estimation of generic values for the alpha factor and the MGL models.

2. Perform plant-specific (or application-specific) analysis of CCF events in the database. This allows the user to specialize (modify) events for application to a specific plant by considering design and operational differences between that plant and the plants in which the events have occurred. As a result of this mapping of events and creation of a "plant-specific" database, the user will be able to develop plant specific estimates for the CCF model parameters. The mapping process requires an event by event assessment of the three applicability factors:

   r_1 = Cause Applicability Factor
   r_2 = Coupling Applicability Factor
   r_3 = Failure Model Applicability Factor

All three factors are numbers in the range [0,1] and represent the degree of similarity of the original plant and the plant being analyzed with respect to the given characteristic of the CCF event, i.e., its cause, its coupling factor, and the failure mode of the components involved. To provide meaningful assessment of these factors, the analyst must be familiar with the events stored in the CCF System and be armed with the qualitative information collected during Phase II, or at least Phase I of CCF analysis as outlined in Sections 3 and 4 of this report. More detailed guidelines regarding the numerical values of these parameters are provided in Reference 2. Examples are provided in Section 6 of this report.

5.5.6 Parameter Estimation with No Operating Data

Despite recent advances in CCF database development, it still not possible to determine parameters by analyzing operating data for all the components of interest in risk and reliability studies of nuclear power plants. There is, therefore, a practical need for estimating parameter values based on engineering judgement.

Depending on the significance of the particular CCBE being considered, the process of subjective estimation of common cause parameters can range from simple bounding value assessments, to more sophisticated, structured, engineering evaluations aided with techniques such as the Cause-Defense Matrix[9] and partial parameterization.[5,6] Regardless of the procedure applied, the estimation is essentially a subjective quantification of event frequencies entailing significant uncertainties which must be quantified and represented in the results.

Table 5-11 provides a set of "generic" alpha factor values which may be used when a more detailed evaluation is not feasible. A similar set of values for the parameters of the MGL model can be developed by using the α-factor values of Table 5-11 in the α-MGL conversion formulae provided in Appendix A. A piece of evidence in support of the suggested generic values is Figure 5-4, which shows the distribution of α_2 parameters across different components and failure modes. The figure shows both the frequency distribution of the estimated α_2's, as well as a beta distribution fitted to the data. The mean of this beta distribution is $\alpha_2 = 0.04$.

It is generally believed that the values of parameters for failure during operation mode are lower than those for failure on demand. It is recommended that the values of α_2, α_3, and α_4 in Table 5-11 be reduced by a factor of 2 when applied to frequency of failure during operation.

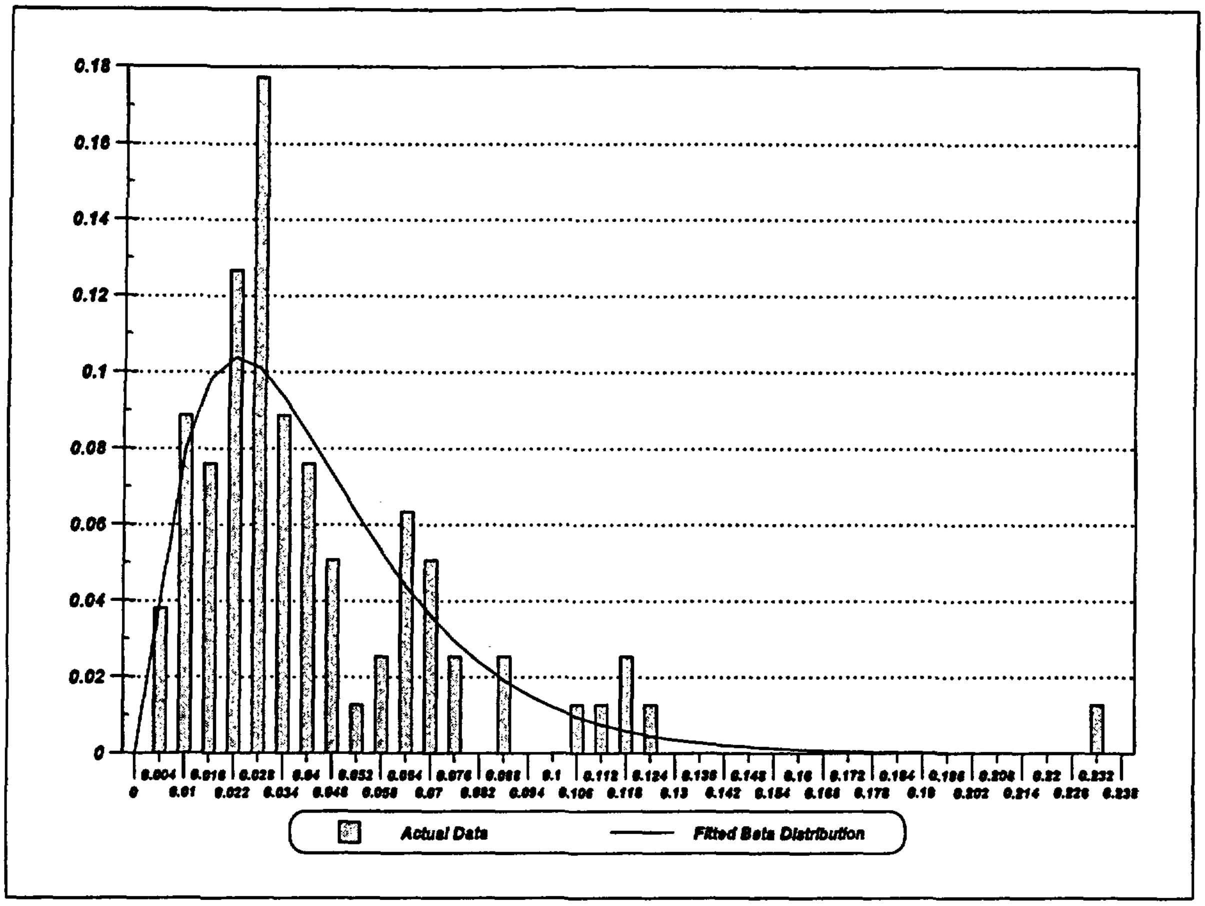


Figure 5-4. Component-to-component variability distribution of α_2 (CCCG=2).

5.6 System Unavailability Quantification

In this step, the parameter estimates obtained in Section 5.5 are used along with the algebraic (probability) equations developed in Section 5.4 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. Many programs, such as IRRAS and SETS series, 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.

It is important to remember that most appropriate point estimate of the parameters for point calculation of the system unavailability is the mean value of their uncertainty distribution.

The final step of system analysis prior to documentation is the interpretation 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 CCFs. 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 identifying possible 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.

5.7 Results Evaluation and Sensitivity Analysis

As was discussed in Section 5.5.4, 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 are by using sensitivity analyses to illustrate the direct relationship between the input values for the CCBEs 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 common cause failure analysis is briefly addressed in Reference 2.

5.8 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 plant-specific data because this area of the analysis is the source of greatest uncertainty. The impact vectors assessment process serves as a vehicle for consistent documentation of the assumptions made, but needs 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.

6. EXAMPLE APPLICATION OF COMMON CAUSE ANALYSIS PROCESS

This section of the report provides an example of the common cause failure analysis process. This process includes understanding the plant system, identifying common cause component groups, integrating component groups into the logic model of the system, data analysis, parameter and basic event probability estimation. The relative significance of various common cause failure basic events is also investigated. The system selected for this application is a three-train auxiliary feedwater (AFW) system at an existing U.S. nuclear power plant. The example analysis presentation is organized according to the procedural steps of the three phases of the analysis, as presented in Sections 3, 4, and 5 of this report.

6.1 Phase I: Boundary Definition and Preliminary Screening

6.1.1 Problem Definition and System Modeling

This section presents the steps for the problem definition and system modeling phase ϲf the common cause analysis process. These steps include system familiarization, identification of system boundary conditions, and development of component level system logic models.

6.1.1.1 System Familiarization. A simplified piping diagram of the example auxiliary feedwater system is shown in Figure 6-1. Pressurized water reactor (PWR) auxiliary feedwater systems in the U.S. are not standard in configuration, but the one shown in Figure 6-1 is similar to many plants and consists of three pump trains, which take suction from a common condensate storage tank and supply header to 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 (MOV) at the pump discharge that are normally closed. Each motor-driven pump can supply flow through the MOVs, assuming

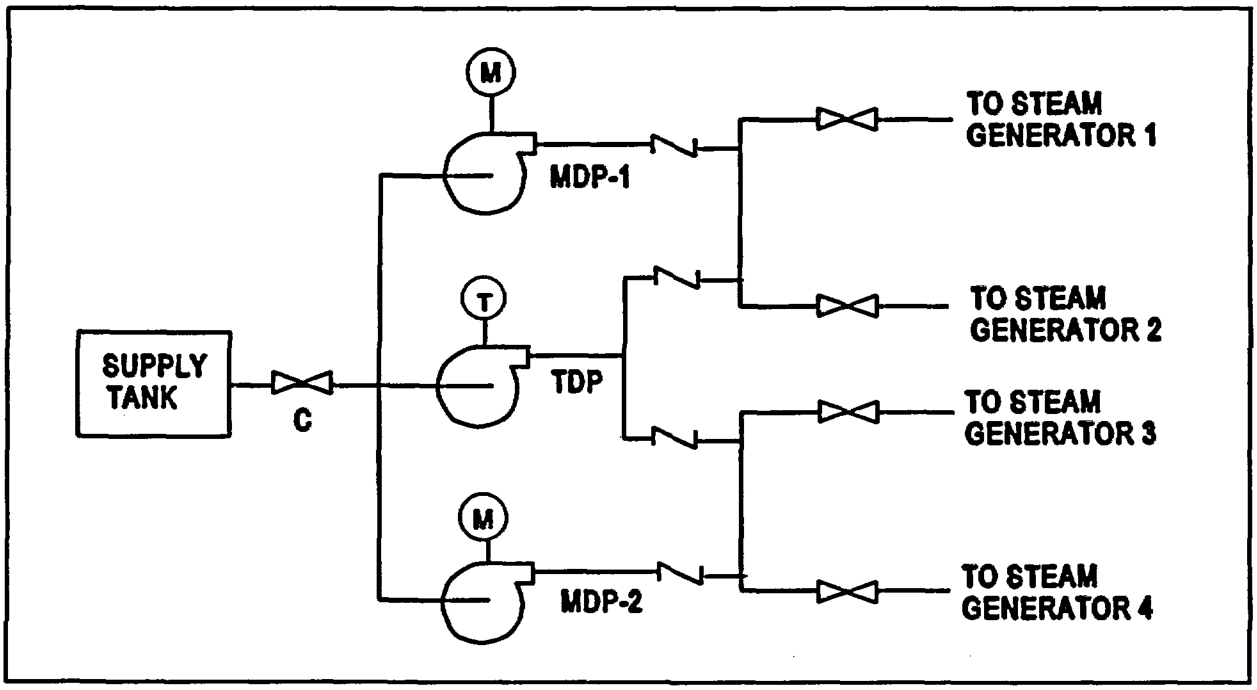


Figure 6-1. Simplified diagram of major components in the example auxiliary feedwater system.

that the valves successfully open on demand, 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 are open. An important characteristic of this system is that, although diversity is employed in pump drivers, all three pumps are mechanically identical. System success is defined as CST flow through two motor-driven pumps or one turbine-driven pump to two of four steam generators. This also requires that the valves function to allow or regulate flow to the steam generators. Some plant designs employ two turbine driven pumps and only one motor driven pump, but it is a less common design than the system shown here.

Table 6-1 presents a simplified list of the major maintenance, test, and emergency procedures that are applicable to this system. For an actual plant analysis, the list of procedures considered would be expanded to include all the procedures that involve any operation or work on the AFW components. Each pump is tested quarterly (Procedure 1 in Table 6-1) to ensure proper flow is available, by opening a minimum recirculation valve (not shown in Figure 6-1) and pumping water back to the CST in a recirculation loop (also not shown in Figure 6-1). If a system actuation signal is received during a pump test, the minimum recirculation line should isolate automatically but does not need to be isolated to meet the system success criteria. Each isolation valve undergoes a monthly stroke test (Procedure 2 in Table 6-1) 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 6-1) that includes adjustment of torque and limit switch settings and lubrication. Technical Specifications (TS) require the licensee to perform a stroke test immediately following maintenance.

Table 6-1. 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 Pump Emergency Operating Procedure

The AFW pumps are located in a common building, but with physical barriers between the pumps. The pumps are maintained according to Procedure 4 listed in Table 6-1. Although pump maintenance can be a complex activity, the TS for the AFW pumps do not require a complete flow test (Procedure 1 in Table 6-1) to be performed immediately following every maintenance activity. Following any test and maintenance activity, however, there are restoration steps to be performed along with the required retesting to ensure full operability. Activities that involve dismantling the pump or that modify the flow components (e.g., impeller) usually require the licensee to perform a full flow test to ensure that the pump operational requirements can be met. If the maintenance activity involves only the motor or turbine, the post-maintenance test will typically only require verification of a successful pump start. Additionally, operators must verify that the system has been restored to the proper configuration following automatic initiation. If the AFW control system fails to actuate properly on an automatic signal, the operator must manually control proper flow to the steam generator (Procedure 5 in Table 6-1).

6.1.1.2 Identification of System and Analysis Boundary Condition. This step in the common cause analysis procedure involves the definition of analysis objectives, boundary conditions, mission time, potential system alignments, environmental hazards (including such external events as earthquakes), basic events (e.g., component failures) and the relevant component failure modes, potential operator actions, and any other assumptions for analysis.

The objectives of this example analysis are to determine AFW system unavailability 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 will 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 for this example. Component boundaries are defined as follows. The MOVs include:

- Motor/operator (including limit switches and torque switches)
- Operator circuit breaker
- Indication circuit
- Control circuit, and switch
- Torque limit bypass switch
- Valve hardware (body, disc, stem, etc.)
-

Pumps include:

- Driver (motor and turbine)
- Circuit breaker or turbine control valve
- Control circuit, and switch
- Pump hardware (body, impeller, flow vanes, etc.)

Electric power supply and other support systems (e.g., cooling water) are outside the scope of this analysis, and are assumed to be available. Basic events are to be considered at the component level. External events, such as seismic, fire, and flood, are also assumed to be outside the scope of this analysis. There is no credit given in the analysis for operator intervention or recovery actions, except as noted in the qualitative analysis. It is assumed that the system must operate for 6 hours following its demand.

Various possible system alignments are normally considered in typical PRA system analysis. However, to simplify this example, the AFW system presented here will be analyzed only for the normal alignment in which no testing or maintenance is performed.

6.1.1.3 Development of Component-Level System Logic Model. The reliability block diagram and component-level fault tree for the system are presented in Figures 6-2 and 6-3, respectively.

6.1.2 Preliminary Analysis of CCF Vulnerabilities, Identification of Common Cause Component Groups

The next step is to identify the common cause important vulnerabilities and the corresponding component groups, using both quantitative and qualitative methods.

6.1.2.1 Qualitative Screening. The purpose of this step is to determine which common cause failure events in the database may contribute to system vulnerabilities at the example plant and therefore should be included in the subsequent steps of the analysis. Identification of these events relies on assumptions, based on judgment and feedback from operating experience, to ensure that all applicable events are included and that events that are not applicable are excluded. For presentation of this example, another consideration is to keep the number of events at a manageable level.

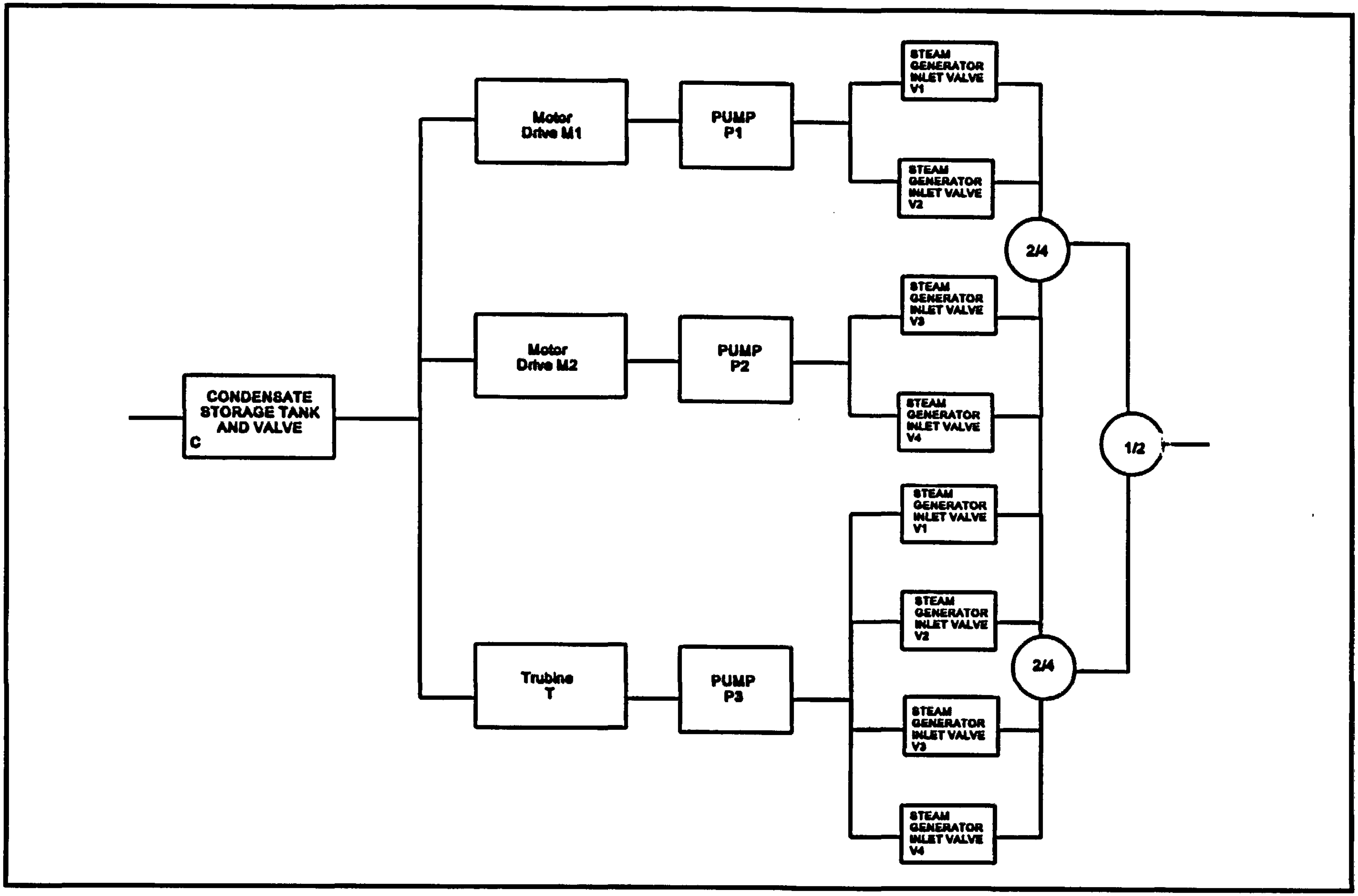

CONDENSATE STORAGE TANK AND VALVE
C
Motor Drive M1
Motor Drive M2
Trubine T
PUMP P1
PUMP P2
PUMP P3
STEAM GENERATOR INLET VALVE V1
STEAM GENERATOR INLET VALVE V2
STEAM GENERATOR INLET VALVE V3
STEAM GENERATOR INLET VALVE V4
STEAM GENERATOR INLET VALVE V1
STEAM GENERATOR INLET VALVE V2
STEAM GENERATOR INLET VALVE V3
STEAM GENERATOR INLET VALVE V4
2/4
2/4
1/2

Figure 6-2. Reliability block diagram of auxiliary feedwater system (normal alignment).

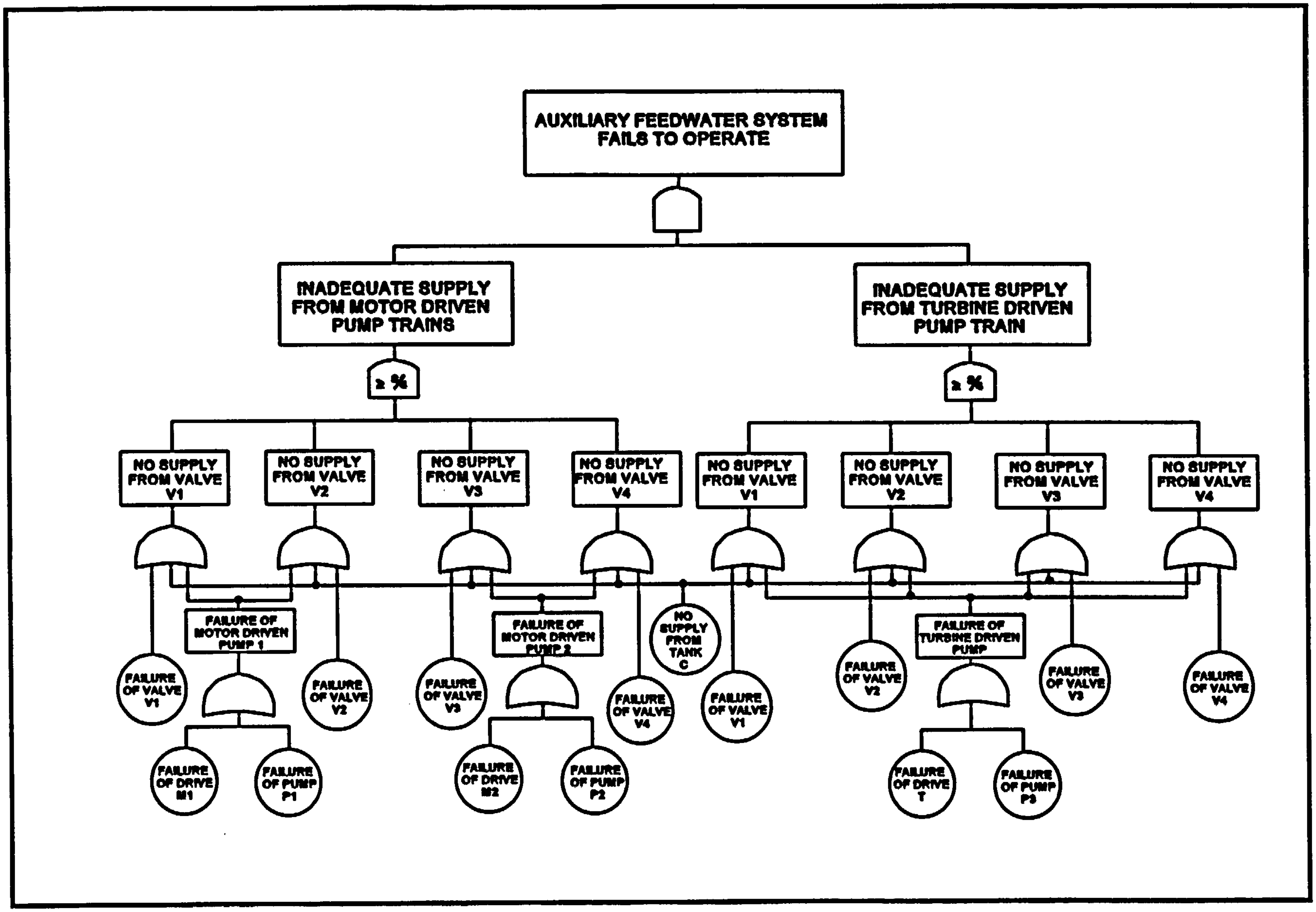


Figure 6-3. Component-level fault tree of example system.

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 system analysis, it is necessary to understand the factors that affect independence, or lack thereof, among the components in the system. Such factors include whether groups of identical components are used, 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 important consideration is the potential for human errors in the design, manufacturing, 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 this 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 more complete analysis, they should be included as a group. Components not within the selected groups are assumed to fail independently, i.e., no common cause failures will be considered for these components. Operating experience indicates that common cause events often affect sets of identical (redundant) components but very few, if any, affect diverse components. Keeping the number of possibilities allowed for in the models at a manageable level requires qualitative and quantitative judgment guided by feedback from operating and PRA analysis experience. Such judgments, however, are not unlike the numerous judgments that need to be made by a systems analyst during the independent failure analysis and to account for system configuration differences.

The three candidate common cause component groups of this example problem are (see Figure 6-2):

Pump Group, Mechanical	**Motor Group**	**MOV Group**
Motor-Driven Pump - P1	M1	V1
Motor-Driven Pump - P2	M2	V2
Turbine-Driven Pump - P3		V3
		V4

6.1.2.2 Quantitative Screening. The objective of this step is to remove from further consideration those common cause component groups which are not likely to have a significant impact on the total system unavailability. This is achieved by expanding the component level fault tree of Figure 6-3 to include a global common cause basic event for every common cause component group, according to the procedure described in Section 3.2. Next, the cutsets of the expanded fault tree are obtained. The cutsets are listed below using the following notation: the first letter indicates component type (e.g., P for pump, V for valve, M for motor, T for Turbine, and C for condensate storage tank), the number following the first letter identifies the specific component in the group (e.g., P1 means pump 1), the letter G stands for global CCF (failure of all in the group), and I stands for independent failure:

First Order Cutset (a total of 3)
{C}, {VG}, {PG}

Second Order Cutsets (a total of 2)
{MG*P3I}, {MG*T}

Third Order Cutsets (a total of 28)
{V1I *V2I *V3I}, {V1I *V2I *VS4 }, {V1I *V3I *V4I}, {V2I *V3I *V4I},
{P1I *P2I *P3I}, {M1I *P2I *P3I}, {M2I *P1I *P3I}, {M1I *M2I *P3I},
{P1I *P2I *T}, {M1I *P2I *T}, {M2I *P1I *T}, {M1I *M2I *T},
{V1I *P2I *P3I}, {V2I *P2I *P3I}, {V3I *P1I *P3I}, {V4I *P1I *P3I},

{V1I *P2I *T}, {V2I *P2I *T}, {V3I *P1I *T}, {V4I *P1I *T},
{V1I *M2I *P3I}, {V2I *M2I *P3I}, {V3I *M1I *P3I}, {V4I *M1I *P3I},
{V1I *M2I *T}, {V2I *M2I *T}, {V3I *M1I *T}, {V4I *M1I *T}.

The algebraic equation for system unavailability, Q_S, in terms of basic parameter model parameters is:

$$Q_S = Q_C + Q_{VG} + Q_{PG} + Q_{MG} (Q_P + Q_T) + 4(Q_V)^3 + (Q_P)^3 + [2Q_M + Q_T + 4Q_V](Q_P)^2 + 2\, Q_M\, Q_P\, Q_T \\ + (Q_M)^2 (Q_P + Q_T) + 4\, Q_V\, Q_P\, Q_T + 4\, Q_V\, Q_M\, Q_P + 4\, Q_V\, Q_M\, Q_T$$

where Q_x is the probability of basic event (x).

Using the global CCF factors listed in Table 3-1, and generic estimates for total component failure probabilities from Table 6-2, the various terms in the above equation for Q_S can be quantified. For example,

$$\begin{aligned} Q_{VG} &= g_w^{(4)}\, q_v \\ &= (0.11)(4.3E\text{-}3) \\ &= 4.7E\text{-}3. \end{aligned}$$

Table 6-2. Generic parameter estimates for screening analysis.

Component	Failure Mode	Q_t	Global CCF Parameter (g)*
MOV	FO	$q_v = 4.30E\text{-}3$	0.11
PUMP	FS	$q_p = 1.65E\text{-}3$	0.08
	FR	$\lambda_p = 1.71E\text{-}5$	0.08
MOTOR	FS	$g_M = 1.65E\text{-}3$	0.10
	FR	$\lambda_M = 1.71E\text{-}5$	0.10
TURBINE	FS	$g_T = 3.15E\text{-}2$	
	FR	$\lambda_T = 1.01E\text{-}3$	
TANK	RVP	$\lambda_C = 2.70E\text{-}8$	

* Based on Table 3.1.

For the time based component failure probabilities, the failure rate (λ) is multiplied by a mission time (t=6 hrs). For example, for pump motors:

$$Q_M = q_M + \lambda_M t$$

and for the corresponding global CCF probabilities:

$$Q_{MG} = g^{(2)}\, q_M + g^{(2)}\, \lambda_M t$$

From this exercise it is evident that the terms involving global CCF events dominate and that all three groups are important.

Now that the analysis boundaries have been established and the analyst has determined which common cause component groups must be analyzed, a detailed qualitative evaluation of CCF vulnerabilities (Section

6.2) can provide the basis for data analysis in support of the quantification of system unavailability and engineering insights for reliability improvements that might be needed.

6.2 Phase II: Detailed Qualitative Analysis

This section presents a detailed analysis of the root causes and coupling mechanisms of equipment failures in the example AFW system, in conjunction with evaluation of the events in the CCF database, to ensure that all the applicable failure mechanisms are identified. The process detailed here is the application of the analysis described in Section 4 of the report. This step has two objectives: (1) to provide the basis and justification for engineering decisions regarding system reliability improvements, and (2) to provide engineering evaluation of potential CCF events to determine their applicability to the target example AFW system (shown in Figure 6-1), to be used in the quantitative analysis step. An effective detailed qualitative analysis involves the following activities:

- Review of plant design and operating practices, and
- Review of operating experience (generic and plant-specific)

The purpose of the plant design review is to identify the specific design and operating features of the system of interest, in this case the AFW system, and to apply that knowledge to the CCF event review to eliminate the events that are not applicable to the system. Additionally, the review includes evaluation of the plant operating and maintenance procedures to determine what specific activities are performed on the AFW system. The list of procedures in Table 6-1 is a product of the plant design review. Other plants could have different maintenance practices or retest requirements; it is important for the analyst to be familiar with the requirements for the specific plant of interest, in order to accurately apply the applicability factors during the operating experience review.

The review of operating experience is performed by first identifying an initial set of coupling factors for the equipment in the AFW system. The specific coupling factors to be applied against different component groups are then based mostly on engineering judgements to assess how they could impact the example AFW. Some coupling factors may be "not applicable" to the example AFW due to the specific plant features. This conclusion allows the analyst to eliminate related failure events from the quantitative data analysis in Phase III. Other combinations may be judged applicable to AFW and the analyst must ensure that events with those coupling factors are included in the analysis.

Three types of coupling factors must be addressed:[4]

- Hardware Based: primarily affect similar equipment.

- Operation Based: affect equipment operated or maintained according to the same procedures (with emphasis on maintenance errors, particularly misalignment).

- Environment Based: affect equipment in the same location, or with the same internal environment.

Initial analysis of root causes of failure for the equipment of interest consists of a detailed review of

1. Plant failure reports (e.g., LERs, NPRDS, plant logs).

2. Other system reliability analyses.

3. Previous studies on similar systems.

This initial effort identifies the fault categories to 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. For working this relatively simplistic example, analysts have relied primarily on LERs and NPRDS data. In an actual application, a more exhaustive data review should be performed to ensure that as many as possible root causes of failure are considered. Nevertheless, the following discussion covers the most commonly observed root causes of failure for the equipment of interest.

Table 6-3 summarizes mapping of coupling factor categories to the relevant component groups, and defines combinations of the coupling factors and component groups to be evaluated for the example AFW system. In the Hardware Based category, most causes of AFW pump (excluding driver) failure are potential CCFs of interest because of the similarity between the three pumps in the example system. Additionally, most causes of pump drive motor and AFW isolation valve faults will also be considered due to hardware similarity in each group. Since all three pumps are located in the same building, although not in the same room, harsh environments (e.g., pipe ruptures, missiles, extreme temperatures, etc.) are potential causes of multiple failures within the AFW system. Therefore all the equipment in the building are also identified as susceptible to environmental causes.

The potential impact of various procedures are recognized under the Operations Based coupling factors. This permits a closer scrutiny of the plant testing and operational activities.

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. Each coupling factor and component group combination identified in the initial effort and summarized in Table 6-3 will now be analyzed, based mostly on a combination of operating experience reports and engineering judgment.

Table 6-3. Coupling factors and equipment mapping.

Coupling Factor Categories	Affected Equipment	Combination Number
Hardware Based	AFW pumps	1
	AFW pump motors	2
	AFW isolation MOVs	3
Operation Based	Procedure 1: AFW pumps	4
	Procedure 2: AFW isolation MOVs	5
	Procedure 3: AFW isolation MOVs	6
	Procedure 4: AFW pumps	7
	Procedure 5: All AFW pumps, motors, valves	8
Environment Based	AFW pumps	9

Coupling Factor and Component Group Combination 1: AFW Pumps. Design deficiencies are often associated with control circuitry, but some events have been observed involving the fluid system modifications that 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. Material defects (e.g., cracked shafts, or impellers) also cause pump failures and these events are very strongly coupled since most licensees procure major equipment in groups from the same supplier.

Since a number of credible root causes and coupling factors that affect the three auxiliary feedwater pumps have been identified, combination 1 from Table 6-3 is judged credible at this plant.

Coupling Factor and Component Group Combination 2: Pump Motor. The review of operational experience revealed that fewer events occurred involving AFW pump motors than involving pumps. 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).

This combination is judged less likely than combinations 1 or 3 (discussed below), but it is still a credible group.

Coupling Factor 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, poor maintenance practices, 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 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).

Combination 3 from Table 6-3 is judged credible at this plant since several root causes and coupling factors with high CCF potential have been identified.

Coupling Factor 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 minimum recirculation valve in a recirculation loop and starting the pump. Realignment errors following the test are not important in a risk analysis because the minimum recirculation lines need not be isolated to meet the system success criteria. Thus, combination 4 is discarded from further analysis.

Coupling Factor and Component Group Combination 5: Equipment Addressed in Procedure 2. The auxiliary feedwater isolation valve monthly stoke 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. Starting these pumps with the injection valves open may cause the pumps to trip on high starting current, or may damage the pumps by placing them in a run-out condition. Thus, combination 5 is judged credible and is used in the analysis.

Coupling Factor 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 recreating human errors is significant.

- Failures due to these root causes may not occur the first time the valve is cycled. This is because of corrosion or hardening of lubrication that may occur in a standby valve, creating friction on the valve stem that may cause a valve to fail a stroke test. 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 AFW system.) 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. Inadvertent operator actions resulting in valve unavailability(ies). This possibility is not directly associated with Procedure 3 but with erroneously misaligning equipment in other systems.

Procedure 3 requires that the maintenance is to be performed on only one valve at a time. The valve must be locked open during maintenance, and both the control signal and the power supply must be disconnected before starting maintenance activities. A human error to fail to open a valve before starting maintenance is judged unimportant because it would result in a single valve unavailability only. A potential CCF error of interest is failure to open one valve, subsequent removal of control signal and power supply to that valve, then starting maintenance activities on a different valve (note that this scenario involves two human errors). This scenario is judged to be unlikely. 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 the section on 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 most of 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 inadvertent actions can credibly occur at this plant. Sufficient evidence of worse-than-average administrative controls was found, and item 3 above is judged credible at this plant.

Coupling Factor and Component Group Combination 7: Equipment Addressed in Procedure 4. For this simplified example, maintenance is performed on the three auxiliary feedwater pumps once per year. All three pumps are serviced sequentially by a single maintenance crew, so the potential for repeating an error (e.g., installing the seal improperly) on all three pumps does exist. The faulted condition of the pumps may 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 three months. 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 requiring 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 indicated that a reduced flow condition is often observed before sufficient plugging causes pump failure). Another cause of loss of suction is personnel error when the suction valves are left closed following operational or test activities. Typically, these events are modeled as valve unavailabilities, but they can result in subsequent pump damage, so they need to be considered in this analysis.

Procedure 4 was also 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). One identified cause of multiple failures is an inadvertent operator action resulting in removal of the AFW pumps from service when attempting to remove pumps in a different system from service. Other causes of multiple failures that are identified in operational histories are incorrect maintenance activities resulting in incorrect material installed in the pumps, material installed incorrectly, or failure to properly align the pumps for operation following the maintenance. While administrative requirements (retesting) are in place at this plant, and should be sufficient to prevent these errors from disabling the pumps, these types of events have occurred at other plants that also had retesting programs. Thus, this combination is determined to be credible.

Coupling Factor and Component Group Combination 8: Equipment Addressed in Procedure 5. The AFW is normally actuated by an automatic control system, but Procedure 5 (Emergency Operating Procedure) 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 system, but problems have occurred during manual actuation. At this plant, the control system uses time delays for starting the pumps, and the emergency operating procedure (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 combination is judged unimportant in this analysis.

Coupling Factor and Component Group Combination 9: Harsh Environments Affecting Equipment in the Pump Room. The review of operational experience indicates harsh environments such as moisture and low temperature as possible causes of equipment failure. These harsh environments should not be a problem at this plant because the AFW equipment is environmentally qualified, and the plant maintains an appropriate winter provisions program to ensure adequate room temperatures for all safety-related equipment. A complete search for credible sources of energetic harsh environments (e.g., pipe ruptures, missile impacts, etc.) that could disable the AFW system revealed only one scenario of potential interest. Since all three pumps are indeed located in the same building, 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 to withstand high temperature and humidity environments. This includes 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 the turbine-driven pump and turbine are in a different room in the building from the motor-driven pumps, separated from the motor-driven pumps by doors that are supposed to be closed. Thus, it is expected that the motor-driven pumps can only fail due to the steam supply line break if a sustained steam release fills the entire building with high temperature steam. Even in this case, failure of both pumps is unlikely because they are 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 inservice inspection (ISI) program for the steam supply line. An augmented ISI program is judged to greatly reduce the probability of a line rupture.

- 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, such as failure to properly seal the equipment following maintenance. These types of failures are addressed for the applicable equipment when analyzing under the hardware based category combinations in Table 6-3. Thus, no additional environment based combination has been identified for further analysis, and combination 9 is judged unimportant in the CCF analysis.

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.

The conclusion of the preceding discussion is that, from a qualitative standpoint, all three common cause component groups (pumps, motors, and MOVs) 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. Table 6-4 summarizes the results of the root cause analysis for the AFW system.

6.3 Phase III: Detailed Quantitative Analysis

6.3.1 Identification of Common Cause Basic Events

Based on the results of Phase I and Phase II of the analysis, the common cause basic events for this example include all CCF event categories for MOVs, pumps and motors. The notation used to encode these 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) is similar to the notation used to discuss the cutsets in Section 6.1 of this report and is as follows: the first letter of the CCBE name denotes the common cause group (e.g., V for valve, P for pump, or M for motor); the second letter denotes the impact of the cause (i.e., S for single component, D for double component, T for triple component, and G for global) of all components or the specific combinations of components affected by that cause; the numeral indicates the specific component

Table 6-4. Summary of root cause analysis for the example AFW system.

Combination Identifier Number	Affected Equipment	Comments
1	AFW pumps	Important for CCF analysis several root causes identified with significant CCF potential.
2	AFW pump motors	Important for CCF analysis; judged less likely that combinations 1 or 3.
3	AFW isolation valves	Important for CCF analysis; several root causes identified with significant CCF potential.
4	Equipment addressed in procedure 1: AFW pumps	Unimportant for CCF analysis; no root causes identified with significant potential.
5	Equipment addressed in procedure 2: AFW isolation valves	Important for CCF analysis; several root causes identified with significant CCF potential.
6	Equipment addressed in procedure 3: AFW isolation valves	Important for CCF analysis; inadvertent operator actions could disable AFW system. Also, maintenance related causes were identified.
7	Equipment addressed in procedure 4: AFW pumps	Important for CCF analysis; inadvertent operator actions could disable AFW system. Also, maintenance related causes were identified.
8	Equipment addressed in procedure 5: All AFW pumps, pump motors, and isolation valves	Unimportant for CCF analysis, due to equipment configuration and EOP provisions at this plant.
9	All equipment in pump building	Unimportant for CCF analysis; this plant is well protected against the identified harsh environment due to the system configuration.

of interest. Using this notation, PS1 is interpreted to mean a single failure of pump #1. This notation will be helpful in developing the algebraic equations after the Boolean reduction is completed. In the next step, the common cause basic events are incorporated into the fault tree, based on the methodology presented in Section 5.

6.3.2 Incorporation of Common Cause Basic Events Into Fault Tree

The incorporation of common cause events into the component-level logic model of Figure 6-3 is illustrated in Figures 6-4 and 6-5 for the fault tree logic form. Specification of the events, facilitated by the 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 only the events that affect that particular component (i.e., all the ways that a particular component can fail). Therefore, for the pump group, the following events would first be specified as part of the logic model:

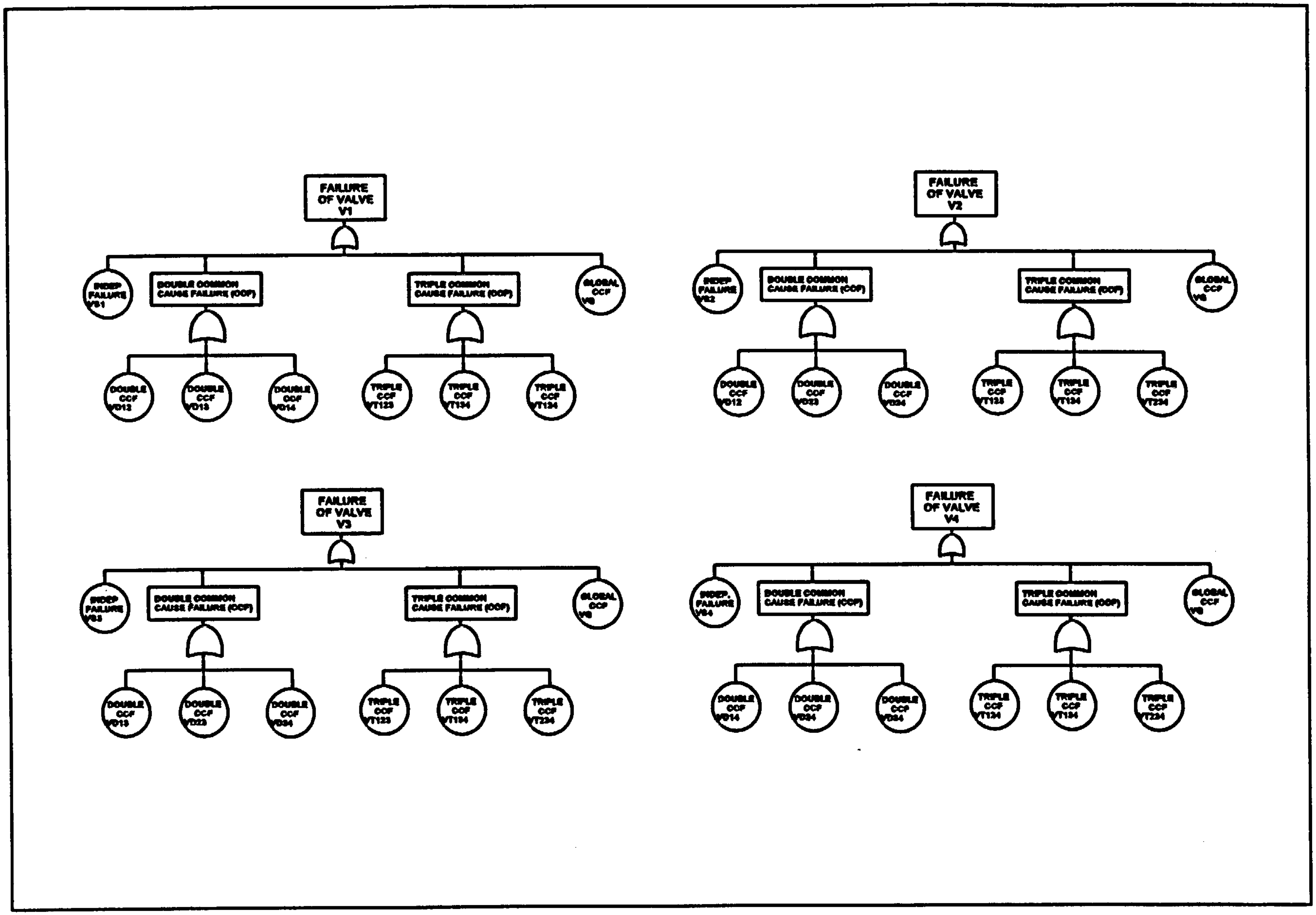


Figure 6-4. Extensions to the component-level fault tree of Figure 6-3 to incorporate common cause basic events for the MOV group.

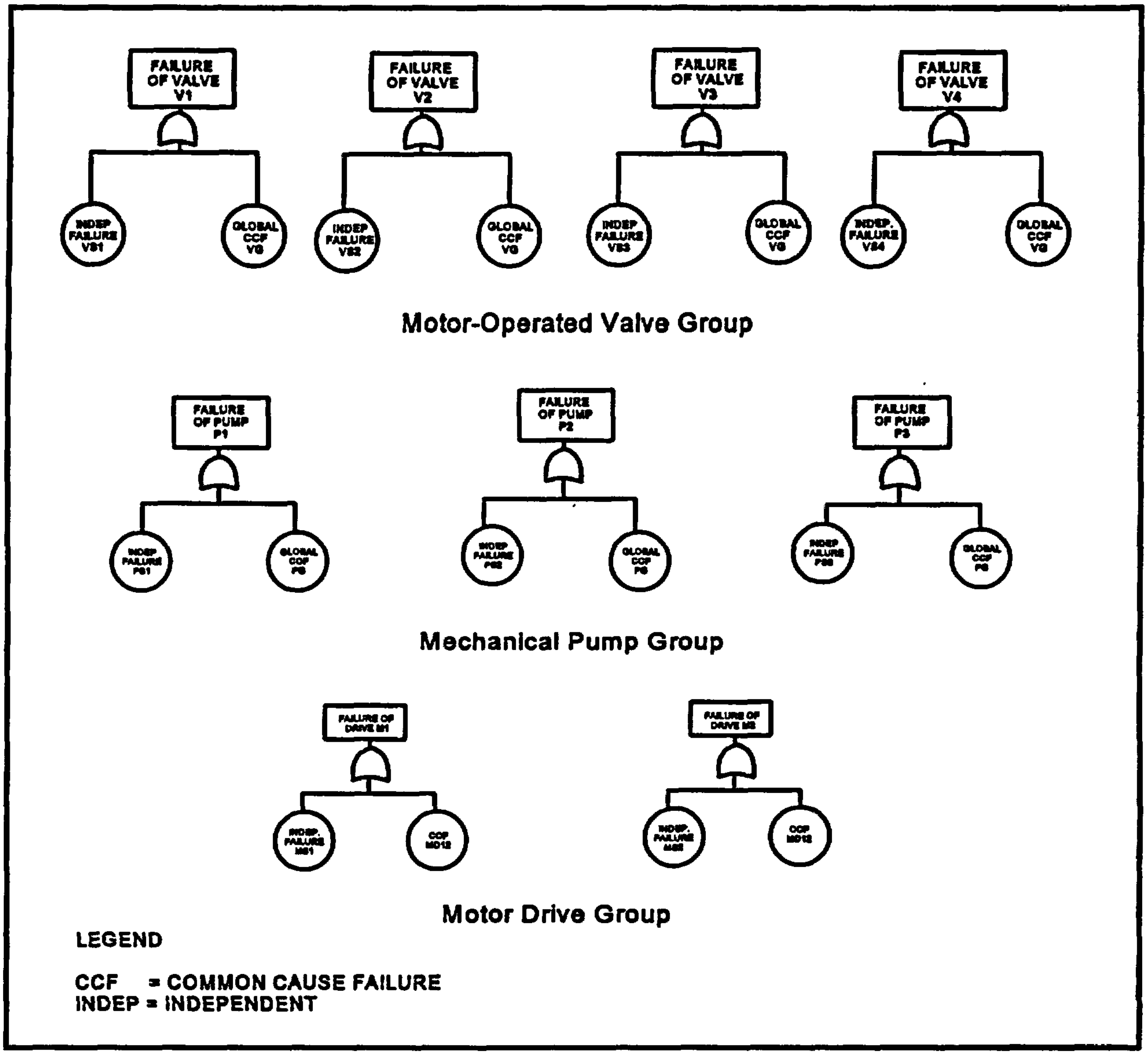


Figure 6-5. Extensions to the component level fault tree of Figure 6-3 to incorporate common cause basic events for the pump and pump drive groups.

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 one (1) and the global event: PS1, PD12, PD13, and PG.

The minimal cutsets of the fault tree, expanded to include the common cause events, are presented in Figure 6-6. Any fault tree software can be used to do this once the common cause events are properly incorporated. Note that the cutsets including basic events which involve similar components are not included in the figure. For a discussion of this type of cutset, refer to Section 5.2 and Reference 1. These are:

VD12 * VD13, 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.

Table 6-5 shows the algebraic terms corresponding to the fault tree evaluation. Note that the assumption of symmetry of basic common cause events discussed in Section 5 has been used in developing the algebraic equations of Table 6-5. 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 , these are all assumed to have the same probability. For basic events associated with a common cause group, the notation X_j is used, where j represents the number of type X components 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 only necessary in the fault tree basic event notation to properly identify minimal cutsets.

A very important result noted earlier and shown in Table 6-6 is the proliferation of cutsets associated with the introduction of common cause events into the fault tree. For this example, the impact is more than a four-fold increase in the number of cutsets. Of the total of 114 cutsets shown in Figure 6-6, only the 29 that are underlined appear without the common cause events. 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 some cutsets may be excluded and some may be overlooked if this important step is buried in the algebraic formulae.

6.3.3 Parametric Representation of CCBEs

After finding the minimal cutsets for each alignment, the analyst makes the transition from Boolean algebra to normal algebra. This transition is necessary to quantify the frequencies of the top event and all its contributors. Consider the term $4V_1^3$ in Table 6-6 that represents the four minimal cutsets in the fault tree involving combinations of three independent valve failures. (The actual cutsets shown in Figure 6-6 are VS1*VS2*VS3, VS1*VS2*VS4, etc.) The common cause terms, V_4 (VG), $4V_3$ (VT123, VT124, VT134 VT234), $12V_2V_1$ (VD12*VS3, VD12*VS4, etc.), $3V_2^2$ (VD12*VD34, VD13*VD24, VD14*VD23), all represent additional 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.

First Order Cutsets (a total of 7)[a]

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

Second Order Cutsets (a total of 39)

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

Third Order Cutsets (a total of 68)

VS1*VS2*VS3, VS1*VS2*VS4, VS1*VS3*VS4, VS2*VS3*VS4, PS1*PS2*PS3

MS1*PS2*PS3, MS2*PS1*PS3, MS1*MS2*PS3, PS1*PS2*T, MS1*PS2*T,
MS2*PS1*T, MS1*MS2*T

VS1*PS2*PS3, VS2*PS2*PS3, VS3*PS1*PS3, VS4*PS1*PS3
VS1*PS2*T, VS2*PS2*T, VS3*PS1*T, VS4*PS1*T
VS1*MS2*PS3, VS2*MS2*PS3, VS3*MS1*PS3, VS4*MS1*PS3
VS1*MS2*T, VS2*MS2*T, VS3*MS1*T, VS4*MS1*T

PS2*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*VD13

MS2*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*VD34

MS2*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*VD34

PS2*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

a. Cutsets underlined are the only ones that would appear without adding common cause events to the system fault tree.

Figure 6-6. Minimal cutsets of the expanded fault tree of the auxiliary feedwater system.

Table 6-5. Quantification formulae for CCF models for the example system.

	Probability Equations for Parametric Common Cause Models	
Algebraic Term	Basic Parameter Model	Alpha-Factor Model**
$^*V_1$	q_{1V}	$\alpha_{1V} q_V$
$^*V_2$	q_{2V}	$⅓\, \alpha_{2V} q_V$
$^*V_3$	q_{3V}	$⅓\, \alpha_{3V} q_V$
$^*V_4$	q_{4V}	$\alpha_{V4} q_V$
P_1	$q_{1P} + \lambda_{1P} t$	$\alpha_{1P} q_P + \alpha'_{1P} \lambda_P t$
P_2	$q_{2P} + \lambda_{2P} t$	$½\, \alpha_{2P} q_P + ½\, \alpha'_{2P} \lambda_P t$
P_3	$q_{3P} + \lambda_{3P} t$	$\alpha_{3P} q_P + \alpha'_{3P} \lambda_P t$
M_1	$q_{1M} + \lambda_{1M} t$	$\alpha_{1M} q_M + \alpha'_{1M} \lambda_M t$
M_2	$q_{2M} + \lambda_{2M} t$	$\alpha_{2M} q_M + \alpha'_{2M} \lambda_M t$
T	$q_T + \lambda_T t$	$q_T + \lambda_T t$
C	$q_C + (T_C/2 + t)$	$\lambda_C (T_C/2 + t)$

* Time-based failure rate for these terms are assumed to be negligible.

** Assumed staggered testing.

Table 6-6. Terms of the algebraic model for the example system in 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	$+ 12V_2V_1 + 3\overset{2}{V_2} + 10V_2P_2 + 3P_1P_2$ $+ 2P_2M_1 + 2P_2M_2 + 4P_2V_1 + P_2T + M_2P_1 + M_2T$
Third Order Cutsets	$4\overset{3}{V_1} + \overset{3}{P_1} + 2M_1\overset{2}{P_1} + P_1\overset{2}{M_1}$ $+ TP^2 + 2M_1TP_1 + T\overset{2}{M_1} + 4V_1\overset{2}{P_1}$ $+ 4V_1TP_1 + 4V_1M_1P_1 + 4M_1V_1T$	$+ 10\overset{2}{P_1} V_2 + 10P_1V_2T + 10P_1V_2M_1 + 10V_2M_1T$

It is important to note 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 probabilities than most of the cutsets containing purely independent events.

To complete development of algebraic models to a form that is suitable for quantification, there are, as discussed in Section 5.5, alternative paths to follow depending on the type of parametric model selected. The following parametric models are used in Table 6-5 for various algebraic terms:

- Basic Parameter Model
- Alpha - Factor Model

6.3.4 Parameter Estimation Data Classification and Screening

All of the parametric common cause analysis approaches discussed in this guidebook (e.g., basic parameter, Alpha Factor, MGL) require event data to be classified and categorized prior to parameter estimation. The analysis is identical for all such models.

For the quantification of the parameters for this example, only the Alpha-Factor Model will be used. The process involves the use of the CCF computer code and database[4-7] to specialize the data for the various common cause component groups to the example plant. This specialization requires the analyst's input regarding the applicability of the events in the database to the example plant in terms of the causes and coupling mechanisms involved. In this process the analyst makes use of the information gathered during the detailed qualitative analysis in which the specific characteristics of the plant and potential common cause failure vulnerabilities are identified.

As part of working this example, all AFW events for pumps, motors, and MOVs in the CCF database were reviewed for applicability to the example system. Some of the events used in this example are detailed below and in Table 6-7. The descriptions of the events are the event descriptions from the CCF database, and the codes in Table 6-7 are taken directly from the database. The applicability factors listed as the last three rows of Table 6-7 (cause, coupling, and failure mode) were assigned based on similarity between the plant where the event actually occurred and the example target plant. Additional information about the event coding and the codes may be found in Reference 6.

An applicability factor of 1.0 indicates that the analyst determined the cause, coupling, or failure mode of the event would be very likely to occur at the target plant, given the same event conditions. An applicability factor of 0.5 indicates that the analyst knows that the event in the database has approximately a 50% chance of occurring at the target plant. Some reasons why the event might not occur are administrative controls at the target plant that decrease the susceptibility to the same failure mechanisms. If the analyst believes that the event probably would not occur at the target plant, but has a small chance of occurring, the applicability is 0.1. If there is no chance of the event occurring at the target plant (e.g., a turbine pump event from the database is not applicable to a plant with no turbine pump) , the event is dropped from the analysis.

Example Event 1: Following a plant trip, it was discovered that the auxiliary feedwater pumps had internal damage. Some channel ring vanes had chips missing, and several parts were found in the SG auxiliary feedwater piping. The pumps were repaired and strainers have been installed to prevent foreign material from entering the venturis. The following paragraph is the actual event description from LER 28188010:

On May 16, 1988, at 0324 hours, with Unit 2 at 100% power, a reactor trip occurred as a result of steam generator (S/G) low low level. At 49 seconds after the trip, safety injection was manually initiated in accordance with Emergency Procedure 1.0 due to pressurizer level decreasing to 13%. The cause of the reactor trip was rapid closure of the turbine governor valves which resulted in shrink of the S/G levels to the reactor trip setpoint. Extensive testing was conducted on the turbine control circuitry and the electro-

Table 6-7. Event codes and applicability factors for the example CCF events from the CCF database.

CCF Database Codes	Event 1	Event 2	Event 3	Event 4	Event 5	Event 6
LER #	28188010	29592016	30292004	31190042	34880014	41388015
Power Level	100%	0%	0%	100%	0%	97%
Event Date	5/16/1988	9/26/1992	5/1/1992	12/20/1990	2/1/1980	3/9/1988
System	AFW	AFW	AFW	AFW	AFW	AFW
Component	PMP	PMP	MOV	PMP	MOT	PMP
Shock Type	NL	L	NL	NL	L	NL
CCCG Size	3	3	4	3	2	3
Failure Mode	FR	FS	OO	FS	FS	FR
Failure Mode Applicability	1.00	1.00	1.00	1.00	1.00	1.00
Cause	IC	DE	IC	QP	DC	IC
Coupling Factor	HQMM	HDSC	OMTC	EE	HQIC	EI
Shared Cause Factor	1.00	1.00	1.00	1.00	1.00	1.00
Timing Factor	1.00	1.00	1.00	1.00	1.00	1.00
Operational Mode	BO	BO	BO	BO	SD	OP
Detection Mode	O	D	D	O	D	O
Event Type	CCF	CCF	CCF	CCF	CCF	CCF
Event Level	SYS	SYS	COM	SYS	COM	SYS
Defense Mechanism	MON	FSB	MAI	PBR	FSB	NON
p_1	0.50	1.00	0.50	0.50	1.00	0.50
p_2	0.50	1.00	0.50	0.50	1.00	0.50
p_3	0.50	1.00	0.50	0.00	-	0.00
p_4	-	-	0.00	-	-	-
Cause Applicability	1.0	0.5	1.0	1.0	1.0	0.0
Coupling Applicability	1.0	1.0	0.5	1.0	1.0	0.5
Failure Mode Applicability	1.0	1.0	1.0	1.0	1.0	1.0

hydraulic control (EHC) system. No deficiencies were detected. The turbine impulse pressure transmitter was calibrated. Further monitoring of the EHC system will be performed during the unit startup.

All three applicability factors were assigned a value of 1.0. This is an indication that the analyst determined that the cause of internal equipment failure (specifically internal pump material degradation), the coupling factor of hardware quality in the manufacturing process, and the failure mode of fail to run (due to internal pump damage) could all occur at the target plant.

Example Event 2: A modification design error (in 1983-1984) removed a start permissive interlock contact. At cold shutdown this deenergized the auxiliary lube oil pump, consequently, when the 1B AFW pump was started it ran for 2.5 seconds and tripped on low oil pressure. Further investigation showed all the Unit 1 and Unit 2 motor driven AFW pumps (MDAFWP) would be affected in the same way. The design error combined with insufficient post modification testing led to this CCF event. The following paragraph is the actual event description from LER 29592016:

On September 26, 1992, at 1445, with Unit 1 in Mode 5, cold shutdown, a manual start of the 1B AFW pump was attempted per Periodic Test (PT)-7B-ST. The pump ran for approximately 2.5 seconds and then tripped on low oil pressure. Immediate investigation found the auxiliary lube oil pump deenergized due to the existing plant conditions. The auxiliary lube oil pump was energized and the 1B AFW pump was started. Subsequent investigation culminated in a common mode failure determination on all Unit 1 and Unit 2 motor driven AFW pumps. This determination was made at 0801 hours on September 30, 1992, at which time Unit 2 being in Mode 1, power operation, was declared in limiting condition of operation (LCO) 3.7.2.B. Temporary alterations were prepared and installed to remove the time-delayed oil pressure trip feature from the control circuitry and the Unit 2 motor driven pumps were declared operable at 0943 on September 30, 1992. The cause was a design error and insufficient post modification testing. A modification design error removed a start permissive interlock contact (in 1983-1984) but failed to consider the effect of the time delayed trip on low oil pressure during pump start. Corrective actions included investigating a modification to permanently remove reliance on the lube oil system for pump start, and reviewing the event with the technical staff and nuclear engineering site groups with design responsibilities.

The cause applicability factor was assigned a value of 0.5, due to the analyst's determination that the target plant does not have the same interlock on the control system. The target plant does, however, perform design modifications, so the root cause of design change control problems is still somewhat applicable to the target plant. Both the coupling factor (system design) and failure mode (failure to start) applicability factors were determined to be 1.0, indicating that the target plant is susceptible to the same factors that resulted in this CCF event.

Example Event 3: The licensee determined that the AFW flow control valves would not close under the differential pressure of full power operating conditions. The following paragraph is the actual event desccription from LER 30292004:

On April 24, 1992, the plant was in Mode 1 (power operation) at 65.5% of rated thermal power (RTP). During April 1992, engineering personnel were revising a test procedure associated with differential pressure (DP) testing AFW block valve EFV-14 in accordance with NRC Generic Letter (GL) 89-10. The maximum DP previously used in earlier testing and evaluation was determined to not represent worst case conditions. At that time, it was decided to close EFV-14 and a similar valve EFV-11 as an interim corrective action. On May 1, with the plant in Mode 5 (cold shutdown at 0% RTP), further testing revealed that none of the AFW block valves would fully close against the calculated worst case DP. The root cause of the inability of the valves to close is attributed to valve condition due to normal wear. The affected AFW block valve/motor operator/cable combinations will be modified to enable the valves to meet DP test requirements.

The coupling applicability factor was assigned a value of 0.5, because the target plant has a more aggressive testing program that should detect independent valve failures before all the valves fail. Both the cause (internal equipment failure) and failure mode (fail to close) applicability factors were determined to be 1.0, indicating that the analyst determined the target plant to be susceptible to the same conditions that caused this CCF event.

Example Event 4: Both motor driven AFW pumps were sprayed when a service water pipe developed a through wall leak. The following paragraph is the actual event description from LER 3190042:

On December 20, 1990, an emergency service water (ESW) system through wall leak on the inlet pipe to the No. 21 component cooling (CC) pump room cooler (upstream of the 21SW128 CC pump room cooler SW inlet valve) occurred. Subsequently, No. 21 SW header was isolated to stop the leak. With No. 21 SW header inoperable, two (2) groups of containment fan coil units (i.e., Nos. 21 and 22 CFCUS) and the No. 21 containment spray (CS) pump room cooler are made inoperable. Since Technical Specification 3.6.2.3 Action B could not be met, with two (2) groups of CFCUS and one CS pump inoperable, Technical Specification Action Statement 3.0.3 was entered. Also, with both high head safety injection pumps inoperable, the Technical Specification 3.5.2 Action Statements do not apply. One of the trains had been declared inoperable solely due to an inoperable generator; therefore, Technical Specification Action Statement 3.0.5 applied. No. 22 centrifugal charging pump (CCP) was inoperable due to inoperability of No. 21 SW header and No. 21 CCP was declared inoperable due to inoperability of the 2B diesel generator. Per the Technical Specification Action Statements, a unit shutdown was initiated. The root cause of this event is attributed to equipment failure of another component .

All three applicability factors were assigned a value of 1.0. This is an indication that the analyst determined that the cause of equipment failure of another component, the coupling factor of external environment, and the failure mode of fail to start could all occur at the target plant.

Example Event 5: During surveillance testing, neither motor-driven AFP would start. The pump control circuit was found with autostart defeat switches labeled backwards, causing all autostarts except the low-low steam generator level to be defeated. The labels were corrected. The original installation error was the result of an inadequate design change process that did not require sufficient verification and testing of the modification. The turbine pump was out of service. The following paragraphh is the actual event description from LER 34880014:

Power level - 0%. On September 5, 1978, a design change was implemented which installed an auto-defeat selector switch to allow bypass of the control grade auto start signal of the motor driven AFW pumps upon trip of both main feedwater pumps (MFP) when MFPs are intentionally removed from service. On February 14, 1980, while testing the control grade auto start feature, A and B motor driven AFW pumps failed to auto start on the loss of MFP test signal. This event is attributable to inadequate design change control. The pre-implementation engineering review of design changes has been strengthened and includes a review to identify design errors, a review to identify procedures affected by the design change, a review to verify compliance of the design with Technical Specifications, and other licensing requirements, and a more comprehensive determination of post implementation testing requirements.

All three applicability factors were assigned a value of 1.0. This is an indication that the analyst determined that the cause of installation error (from original installation), the coupling factor of hardware quality from initial installation, and the failure mode of fail to start could all occur at the target plant.

Example Event 6: All AFW pumps were declared inoperable because of Asiatic clam debris in the pumps, decreasing the flow below the required flowrate. The following paragraph is the actual event description from LER 41388015:

Power Level - 097%. On March 9, 1988, at approximately 1825 hours, Unit 2 tripped from approximately 20% full power. During the transient following the trip, three AFW pumps started automatically as designed. However, motor driven AFW pump (MDAFWP) 2A swapped suction automatically to the nuclear service water system (ESW) when a sustained low suction pressure condition was sensed, and raw water from Lake Wylie entered two SGs. After the initial trip recovery, it was noted that AFW flow to S/Gs 2A and 2B had degraded following the suction swap. Two work requests were written to inspect the internals of the AFW pump 2A to S/G 2A and 2B flow control valves. The inspections revealed that the cavitrol cages for these valves were clogged with shredded Asiatic clam shells. Following discovery, all AFW pumps for both units were declared inoperable. This resulted in both units being taken to Mode 4, hot shutdown. Unit 1 was operating in Mode 1, power operation, at 97% power and Unit 2 was in Mode 3, hot standby. This incident has been attributed to Asiatic clam larvae from Lake Wylie entering the ESW system and growing to maturity in normally stagnant or low flow lines which provide assured water supplies to various safety related systems.

The cause appplicability was assigned a value of 0.0, because the raw water source used at the target plant is not the correct environment for Asiatic clam growth. The coupling factor was assigned a value of 0.5, because even though they are not susceptible to Asiatic clam infestation, they are susceptible to other environmental contamination through the raw water source. The failure mode applicability factor was assigned a value of 1.0, indicating that the target plant would be likely to experience the same failure mode (failure to start) given the same conditions as in the CCF event.

Subsequent to assigning of the event aplicability factors, the actual quantitative analyses are performed using the CCF software.[7] The resulting parameter estimations for the α-factor model for this AFW example system are displayed in Table 6-8. Also shown in the table are the total failure frequencies for each of the components in the model.

6.3.5 System Quantification

The next step in the analysis quantification is to obtain a point estimate using the mean values of the uncertainty distributions for the parameters. The results are used to identify significant contributors and to reduce the amount of effort and computation required to propagate the uncertainty distributions in the final results. In this computation of a mission on time of t=6 hours and test interval of Tc=720 hours are assumed. First, point estimate results are obtained and then the uncertainty distribution for the system unavailability is calculated.

The role of event data screening through impact vector analysis and assessment of plant-specific applicability factors, can be seen by comparing the results of generic α-factor estimates for MOVs and corresponding plant-specific results. This is shown in Table 6-9 where the mean values of the two analyses are compared.

Point Estimate Results

The point estimate results are presented in Table 6-10 in a "source" format. This format permits the analyst to determine which component combinations are 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.

Uncertainty Analysis

The distributions listed in Table 6-8 were used to compute the uncertainty distribution for the total system unavailability. The resulting cumulative probability density function and probability distribution function are shown in Figures 6-7 and 6-8, respectively. The main characteristics of the distribution are:

mean	= 2.05E-4
5th percentile	= 4.41E-5
50th percentile	= 1.44E-4
95th percentile	= 5.37E-4.

Table 6-8. Parameter estimates obtained from CCF software for the example AFW system.

Component	Mode	Q_t	Parameter	Mean	5th Percentile	95th Percentile
MOV	FO	$q_v = 4.30E-3$	α_{1V} α_{2V} α_{3V} α_{4V}	0.9668498 1.47E-02 1.16E-02 6.86E-03	0.945792 4.55E-03 2.93E-03 9.13E-04	0.9834864 2.94E-02 2.49E-02 1.74E-02
PUMP	FS	$q_p = 1.65E-3$	α_{1P} α_{2P} α_{3P}	0.8912187 6.09E-02 4.79E-02	0.8379498 2.81E-02 1.95E-02	0.9361154 1.03E-01 8.60E-02
	FR	$\lambda_p = 1.71E-5$	α'_{1P} α'_{2P} α'_{3P}	0.9864337 1.06E-02 3.01E-03	0.9758982 3.82E-03 2.47E-04	0.9942943 2.00E-02 8.36E-03
MOTOR	FS	$q_M = 1.65E-3$	α_{1M} α_{2M}	0.9534516 4.66E-02	0.9146396 1.80E-02	0.9820435 8.54E-02
	FR	$\lambda_M = 1.71E-5$	α'_{1M} α'_{2M}	0.9911947 8.81E-03	0.9645303 1.55E-05	0.9999829 3.55E-02
TURBINE	FS	$q_T = 3.15E-2$				
	FR	$\lambda_T = 1.01E-3$				
TANK	RUPTURE	$\lambda_C = 2.70E-8$				

Table 6-9. Comparison of generic and plant specific α-factor estimates for MOVs (failure to open).

Parameter	Generic Estimate	Plant-Specific Estimate
α_{1v}	0.9624707	0.9668498
α_{2v}	1.74E-02	1.47E-02
α_{3v}	1.30E-02	1.16E-02
α_{4v}	7.08E-03	6.86E-03

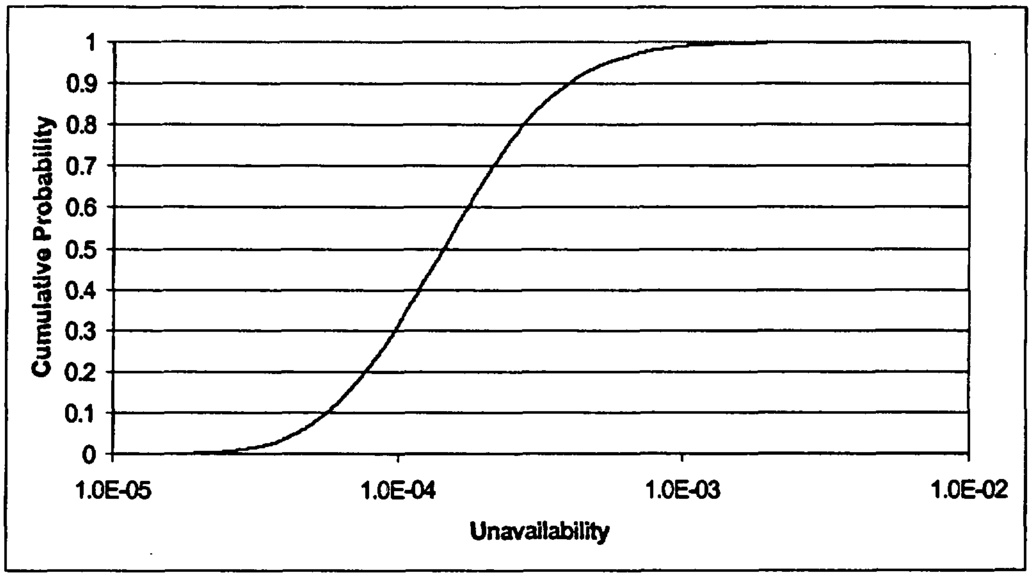


Figure 6-7. Cumulative probability distribution of the total system unavailability.

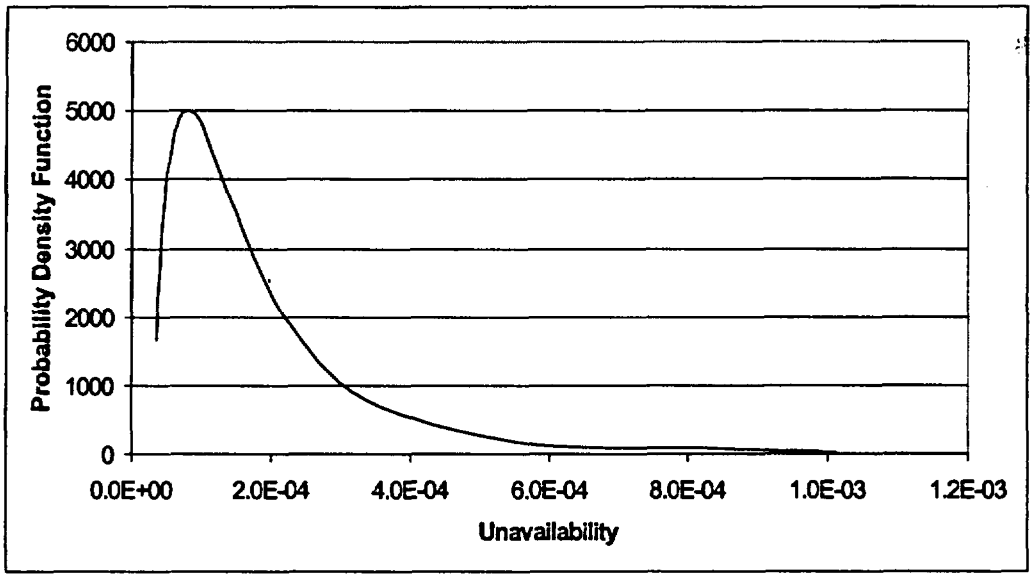


Figure 6-8. Probability distribution of the total system unavailability.

6.4 Results Evaluation

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, only 6.5% of the point estimate result is due to purely independent terms. The fact that more than 93% of the system unavailability is due to cutsets involving common cause events fully justifies the added complexity of incorporating these events into the logic models. Hence, failure to include common cause events in this systems analysis would have resulted in a system point estimate result that is non-conservative by two orders of magnitude.

It is instructive to examine the results in light of the complexity that was added through the direct incorporation of the common cause events into the system fault tree. It is obvious from a comparison of Tables 6-10 and 6-11 that only a small number of terms in the system algebraic model are significant in the overall results.

Table 6-10. System quantification point estimate results.

Algebraic Term	Probability
P_3	7.9E-5
$4V_3$	6.6E-5
V_4	2.9E-5
C	9.9E-6
M_2T	2.9E-6
P_2T	1.9E-6
$12V_2V_1$	1.1E-6
$4M_1V_1T$	1.1E-6
$4V_1P_1T$	9.8E-7
$4P_2V_1$	8.4E-7
$4V_1^3$	2.9E-7
$3P_1P_2$	2.4E-7
$2M_1TP_1$	2.0E-7
$2P_2M_1$	1.7E-7
M_2P_1	1.2E-7
Others	3.5E-7
Total	1.9E-4

To get a picture of which terms contributed to the final results, an examination was made of each term in Figure 6-6. Table 6-5 displays these results and includes 29 algebraic terms that cover the 114 minimal cutsets in the system fault tree.

The point estimates of the frequencies of all 29 terms in Table 6-5 were separately quantified. The terms are first segregated by cutset order, then by type. Six groups of terms are identified:

1. First Order - Independent Event (e.g., C)
2. First Order - Common Cause Event (e.g.,V_4)
3. Second Order - Mixed Events (e.g., P_1 P_2)
4. Second Order - Common Cause Events (e.g., P_2 M_2)
5. Third Order - Independent Events [e.g., $(V_1)^3$]
6. Third Order - Mixed Events (e.g., $V_2 M_1 T$)

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 distribution of failure frequency contribution (percent) was obtained and is displayed in Table 6-11. From this table it is shown that about 95% of the contribution comes from first-order cutsets, most of which come 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:

Table 6-11. Distribution of contributions to system unavailability by cutset category.

Terms	Percent Contribution to Total Unavailability	
First-Order Terms	94.83	
1. Independent Events		5.06
2. Common Cause Events		89.77
Second-Order Terms	3.72	
3. Mixed Events		3.71
4. Common Cause Events		0.01
Third-Order Terms	1.45	
5. Independent Events		1.44
6. Mixed Events		0.01
Total	100.0	100.0

- System unavailability is dominated by first-order common cause events (these are the global CCF events). The first-order common cause events are about 10 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 93% of the total frequency is contained within two groups of terms from the table: number 2, first-order common cause events, and number 3, second-order mixed events.

- With the exception of the first-order result, there is a tendency for the terms of orders 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.

7. REFERENCES

1. U. S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failure in Safety and Reliability Studies: Procedural Framework an Examples, Volume 1,* NUREG/CR-4780, EPRI NP-5613, January 1988.

2. U. S. Nuclear Regulatory Commission, *Procedures for Testing Common Cause Failure in Safety and Reliability Studies: Analytical Background and Techniques, Volume 2,* NUREG/CR-4780, EPRI NP-5613, January 1989.

3. U. S. Nuclear Regulatory Commission, *Procedures for Analysis of Common Cause Failure in Safety Analysis,* NUREG/CR-5801, SAND91-7087, April 1993.

4. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 1--Overview,* NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

5. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System, Volume 2-- Event Definition and Classification,* NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

6. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 3-- Data Collection and Event Coding,* NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

7. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 4--CCF Software Reference Manual,* NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

8. 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.

9. U. S. Nuclear Regulatory Commission, *A Cause-Defense Approach to the Understanding and Analysis of Common-Cause Failures,* NUREG/CR-5460, SAND89-2368, March 1990.

10. Mosleh, A., and A. Afzali; *Consideration of Plant-Specific Characteristics in Estimation of Common-Cause Failure Probabilities,* NRC Grant Report, University of Maryland, 1991.

11. Parry, G., et al., *Guidelines for Conducting Common-Cause Failure Analysis in Probabilistic Safety Assessment,* IAEA, 1990.

12. Fleming, K. N., and A. Mosleh, *Classification and Analysis of Reactor Operating Experience Involving Dependent Events,* EPRI NP-3967, June 1985.

13. Fleming, K. N., et al., *A Database of CCF Events for Risk and Reliability Applications,* EPRI TR-100382, 1992.

14. Electric Power Research Institute, *Common-Cause Data Analysis Tool (CCDAT) User's Manual,* EPRI TR-102747, August 1993.

15. U. S. Nuclear Regulatory Commission, *A SETS User's Manual for Accident Sequence Analysis,* NUREG/ER-3547, SAND83-2238, January 1985.

16. U. S. Nuclear Regulatory Commission, *Integrated Reliability and Risk Analysis System Version 5.0 Reference Manual, NUREG/CR-6116, December, 1993.*

17. Rasmuson, D. M., et al., *Use of COMCAN III in System Design and Reliability*, EGG 2187, EG&G Idaho, March 1982.

18. 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.

19. 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.

20. Fleming K. N., *A Reliability Model for Common Model Failure on Redundant Safety Systems*, Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A13284, April 23-25, 1975.

21. U. S. Nuclear Regulatory Commission, *Data Summaries of License Event Reports of Diesel Generators at U. S. Commercial Nuclear Power Plants, January 1, 1976 to December 31, 1978*, NUREG/CR-1362, EGG-EA-5092, March 1980.

22. U. S. Nuclear Regulatory Commission *Data Summaries of Licensee Event Reports of Pumps at U. S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978*, NUREG/CR-1205, EGG-EA-5044, January 1982.

23. U. S. Nuclear Regulatory Commission *Data Summaries of Licensee Event Reports of Valves at U. S. Commercial Nuclear Power Plants, January 1, 1976 to December 31, 1978*, NUREG/CR-1363, EGG-EA-5125, October 1982.

24. U. S. Nuclear Regulatory Commission, *Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U. S. Commercial Nuclear Power Plants*, NUREG/CR-1740, EGG-EA-5816, Rev. 1, October 1982.

25. U. S. Nuclear Regulatory Commission, *Data Summaries of Licensee Event Reports of Primary Containment Penetrations at U. S. Commercial Nuclear Power Plants, January 1, 1972 to December 31, 1978*, NUREG/CR-1730.

26. U. S. Nuclear Regulatory Commission, *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*, NUREG/CR-1331.

27. U. S. Nuclear Regulatory Commission, *Common-Cause Fault Rates for Pumps*, NUREG/CR-2098, February 1983.

28. U. S. Nuclear Regulatory Commission, *Common-Cause Fault Rates for Valves*, NUREG/CR-2770, February 1983.

29. U. S. Nuclear Regulatory Commission, *Common-Cause Fault Rates for Instrumentation*, NUREG/CR-3289, May 1983.

30. U. S. Nuclear Regulatory Commission, *Common-Cause Fault Rates for Diesel Generators*, NUREG/CR-2099, June 1982.

31. Atwood, C. L., *Constrained noninformative Priors in Risk Assessment, Reliability Engineering and System Safety*, 53 (1996), 37-46.

GLOSSARY

Application—A particular set of CCF events selected from the common cause failure database for use in a specific study.

Average Impact Vector—An average over the impact vectors for different hypotheses regarding the number of components failed in an event.

Basic Event—An event in a reliability logic model that represents the state in which a component or group of components is unavailable and does not require further development in terms of contributing causes.

Common Cause Event—A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.

Common Cause Basic Event—In system modeling, a basic event that represents the unavailability of a specific set of components because of shared causes that are not explicitly represented in the system logic model as other basic events.

Common Cause Component Group—A group of (usually similar [in mission, manufacturer, maintenance, environment, etc.]) components that are considered to have a high potential for failure due to the same cause or causes.

Common Cause Failure Model—The basis for quantifying the frequency of common cause events. Examples include the beta factor, alpha factor, and basic parameter, and the binomial failure rate models.

Complete Common Cause Failure—A common cause failure in which all redundant components are failed simultaneously as a direct result of a shared cause; i.e., the component degradation value equals 1.0 for all components, and both the timing factor and the shared cause factor are equal to 1.0.

Component—An element of plant hardware designed to provide a particular function.

Component Boundary—The component boundary encompasses the set of piece parts that are considered to form the component.

Component Degradation Value (*p*)—The assessed probability ($0.0 \leq p \leq 1.0$) that a functionally or physically degraded component would fail to complete the mission.

Component State—Component state defines the component status in regard to its intended function. Two general categories of component states are defined, *available* and *unavailable.*

- *Available*—The component is available if it is capable of performing its function according to a specified success criterion. (N.B., available is not the same as availability.)

- *Unavailable*—The component is unavailable if the component is unable to perform its intended function according to a stated success criterion. Two subsets of unavailable states are *failure* and *functionally unavailable.*

  - *Failure*—The component is not capable of performing its specified operation according to a success criterion.

- *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, etc.

- *Potentially unavailable*—The component is capable of performing its function according to a success criterion, but an incipient or degraded condition exists. (N.B., potentially unavailable is not synonymous with hypothetical.)

  - *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.

  - *Incipient*—The component is in a condition that, if left unremedied, could ultimately lead to a degraded or unavailable state.

Coupling Factor/Mechanism—A set of causes and factors characterizing why and how a failure is systematically induced in several components.

Date—The date of the failure event, or date the failure was discovered.

Defense—Any operational, maintenance, and design measures taken to diminish the frequency and/or consequences of common cause failures.

Dependent Basic Events—Two or more basic events, A and B, are statistically dependent if, and only if,

$$P[A \cap B] = P[B|A]P[A] = P[A|B]P[B] \neq P[A]P[B],$$

where P[X] denotes the probability of event X.

Event—An event is the occurrence of a component state or a group of component states.

Exposed Population—The set of components within the plant that are potentially affected by the common cause failure event under consideration.

Failure Mechanism—The history describing the events and influences leading to a given failure.

Failure Mode—A description of component failure in terms of the component function that was actually or potentially unavailable.

Failure Mode Applicability—The analyst's probability that the specified component failure mode for a given event is appropriate to the particular application.

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.

Independent Basic Events—Two basic events, A and B, are statistically independent if, and only if,

$$P[A \cap B] = P[A]P[B],$$

where P[X] denotes the probability of event X.

Mapping—The impact vector of an event must be "mapped up" or "mapped down" when the exposed population of the target plant is higher or lower than that of the original plant that experienced the common cause failure. The end result of mapping an impact vector is an adjusted impact vector applicable to the target plant.

Mapping Up Factor—A factor used to adjust the impact vector of an event when the exposed population of the target plan is higher than that of the original plant that experienced the common cause failure.

Potential Common Cause Failure—Any common cause event in which at least one component degradation value is less than 1.0.

Proximate Cause—A characterization of the condition that is readily identified as leading to failure of the component. It might alternatively be characterized as a symptom.

Reliability Logic Model—A logical representation of the combinations of component states that could lead to system failure. A fault tree is an example of a system logic model.

Root Cause—The most basic reason for a component failure which, if corrected, could prevent recurrence. The identified root cause may vary depending on the particular defensive strategy adopted against the failure mechanism.

Shared-Cause Factor (c)—A number that reflects the analyst's uncertainty ($0.0 \leq c \leq 1.0$) about the existence of coupling among the failures of two or more components, i.e., whether a shared cause of failure can be clearly identified.

Shock—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, i.e., *lethal* and *nonlethal.*

System—The entity that encompasses an interacting collection of components to provide a particular function or functions.

Timing Factor (q) —The probability ($0.0 \leq q \leq 1.0$) that two or more component failures (or degraded states) separated in time represent a common cause failure. This can be viewed as an indication of the strength-of-coupling in synchronizing failure times.

APPENDIX A

PARAMETRIC MODELS AND THEIR ESTIMATES

APPENDIX A

Parametric Models and Their Estimates

A.1 INTRODUCTION

This appendix provides a more detailed description of the various parametric models presented in Section 5 of this report, develops a set of estimators for their parameters, and describes the implication of the assumptions made in developing the estimators. The estimators presented here are point estimators. Appendix D discusses the representation of the statistical uncertainty in the values of these estimates. The models are described by showing how each model is used to calculate the probability of occurrence of the various common cause basic events (CCBEs). It is therefore helpful to review the definition of common cause basic events and other key concepts prior to the discussion of the models.

As described in Section 5.1, a common cause basic event is defined as "an event representing multiple failures of (usually similar) components due to a shared cause."

Thus, in modeling a system of three components A, B, and C as in Section 5.2, in addition to the basic events A_I, B_I, and C_I representing unavailability or failure of one and only one component, it is necessary to consider the common cause basic events C_{AB}, C_{BC} and C_{AC}, C_{ABC}. When defined in this way, events are clearly interpreted as specifying the impact of the underlying causes of failure. In the same way that the single component basic events represent the sum of contributions from many causes, so do the common cause basic events.

When constructing system models, not taking common cause failures into account, the basic events representing unavailability of different component are regarded as independent. The question arises whether, since the common cause basic events form a partition of the failure space of the components, these basic events can be defined as being independent. To investigate this further it is necessary to decompose the events into the contributions from root causes.

Define

$$A_I = \sum_{I} A_I^{(I)} + \sum_{J} A_{C_1}^{(J)} \tag{A.1}$$

where $A_I^{(I)}$ is a truly independent failure of component A as a result of cause I, and $A_{C_1}^{(J)}$ is a failure of component A and only A as a result of the occurrence of a common cause trigger j. In this context, the common cause trigger implies the occurrence of some root cause of failure and also the existence of a coupling mechanism.

Similarly, define

$$C_{AB} = \sum_{I} C_{AB(C_2)}^{(I)} \tag{A.2}$$

where $C_{AB(C_2)}^{(I)}$ is a failure of components A and B from the occurrence of a common cause, I, which resulted in the two failures only. In the notation used, (C_2) indicates that the common cause event involved two components only. Similar expansions can be developed for B_I and C_{BC}.

If these events are regarded as being independent, the following (cause level) cutset expansions of the system cutsets result:

$$A_I \cdot B_I = \sum_i A_I^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_I^{(i)} \cdot \sum_j B_{C_1}^{(j)} + \sum_i A_{C_1}^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_{C_1}^{(i)} \cdot \sum_j B_{C_1}^{(j)} \tag{A.3}$$

$$C_{AB} \cdot C_{BC} = \sum_i C_{AB(C_2)}^{(i)} \cdot \sum_j C_{BC(C_2)}^{(j)} \tag{A.4}$$

Looking at the causal cutsets more closely it can be seen that among them there exist cutsets of the type:

$$A_I^{(k)} \cdot B_I^{(k)}$$

$$A_{C_1}^{(k)} \cdot B_{C_1}^{(k)}$$

$$C_{AB(C_2)}^{(k)} \cdot C_{BC(C_2)}^{(k)}$$

The first of these is logically correct given that the causes indicated by a subscript I are independent. Then the two failures may by chance occur simultaneously. However, when the failures results from a common cause, cutsets such as $A_{C_1}^{(k)} \cdot B_{C_1}^{(k)}$ would be indistinguishable from $C_{AB(C_2)}^{(k)}$, and should be classified as the latter. Similarly, $C_{AB(C_2)}^{(k)} \cdot C_{BC(C_2)}^{(k)}$ would be indistinguishable from $C_{ABC(C_3)}^{(k)}$. Thus, when the common cause failures are introduced into the model at the impact level (i.e., by evaluating the functional state of components involved and not the specific causes), the basic events can no longer be regarded as truly independent since this may cause logical inconsistencies with the system model.

A convenient approach to properly model common cause failure events is to define the events A_I, C_{AB}, C_{AC} and C_{ABC} to be mutually exclusive, since they partition the failures space of A according to the explicit impact on other components in the common cause group.

Such a definition implies that cutsets of the type $C_{AB} \cdot C_{AC}$ are identically zero. This definition has particular implications for the analysis of event data in that events in which three components fail, must be identified as one or another of the combinations $A_I C_{BC}$, $A_I B_I C_I$, C_{ABC}, and other permutations, but excluding $C_{AB} \cdot C_{BC}$. This, and the observation made earlier about indistinguishability, guarantees mutual exclusivity of the partition of the failure space of each components. It should be noted that in this report the A_I, B_I, and C_I are still regarded as independent events even though the common cause contribution to these events, the $A_{C_I}^{(j)}$ in Equation A.1, can lead to some cutsets at the cause level, which have the same problem concerning indistinguishability as the multiple component cutsets discussed previously. The contribution of the latter is considered to be insignificant.

Once the basic events are defined, a simplifying assumption is made to reduce the number of probabilities that need to be estimated. According to this assumption, the probabilities of similar basic events involving similar types of components are the same (symmetry assumption). For example, if A, B, and C are identical components, then

$$\begin{aligned} P\left(A_I\right) &= P\left(B_I\right) = P\left(C_I\right) = Q_1 \\ P\left(C_{AB}\right) &= P\left(C_{AC}\right) = P\left(C_{BC}\right) = Q_2 \\ P\left(C_{ABC}\right) &= Q_3 \end{aligned} \tag{A.5}$$

Note that, with the symmetry assumption, the probability of failure of any given common cause basic event involving similar components depends only on the number and not on the specific components in that basic event. This number is indicated as a subscript to the letter Q used to represent the probabilities of basic events. Therefore, Q_2, for example, is the probability of basic events involving failure of two and only two components due to a shared cause.

It should be mentioned at this point that, as will be seen shortly, the probability of the basic event Q_k changes with "m", the total number of components in the common cause component group.[1]

Therefore, the general representation of the probabilities of basic events is the following:

$$Q_k^{(m)} \equiv \text{probability of a basic event involving k specific components } (1 \leq k \leq m) \text{ in a common cause component group of size m} \quad \text{(A.6)}$$

and, the general,

$$Q_k^{(m)} \neq Q_k^{(l)} \quad l \neq m \quad \text{(A.7)}$$

The above discussion provides the necessary background for the following presentation of the various parametric models for calculating the probabilities of common cause basic events.

A.2 PARAMETRIC MODELS

Parametric models refer to different ways in which the probabilities of the basic events in terms of a set of parameters are calculated. Numerous parametric models have been proposed over the past two decades, and some have been widely used in risk and reliability analyses. The models presented in this appendix and also in Section 5, cover a wide range of such models. The main characteristics of these models are summarized in Table A-1.

Table A-1 also provides a categorization of these models based on how each of the basic event probabilities is estimated.

The two major categories are:
- Shock Models
- Nonshock Models

A "shock model" recognizes two failure mechanisms: (1) failures due to random independent causes of single component failures and (2) failures of one or more components due to common cause "shocks" that impact the systems at a certain frequency. The shock models, therefore, develop the frequency of the second type of failure as the product of the frequency of shocks and the conditional probability of failure of components, given the occurrence of shocks.

The nonshock models estimate basic event probabilities without postulating a model for the underlying failure process. The Basic Parameter model is used to estimate the basic event probabilities directly. The other models discussed here, namely, the Beta Factor, MGL, and Alpha Factor models, are reparameterizations of the basic parameter model. They are used whenever common cause failure probabilities are estimated by using estimates of the ratios or probabilities from one source of data, and independently a total failure rate or probability from another source. For example, plant-specific data may

[1] A common cause component group (CCCG) is a set of (usually identical) components considered to be susceptible to common cause failure (See also Sections 3, and 4).

Table A-1. Key characteristics of some popular parametric models.

<table>
<tr><th colspan="3">Estimation Approach</th><th>Model</th><th>Model Parameters*</th><th>General Form for Multiple Component Failure Frequency**</th></tr>
<tr><td rowspan="4">NONSHOCK MODELS</td><td colspan="2">Direct</td><td>Basic Parameter</td><td>$Q_1^{(m)}, Q_2^{(m)}, \ldots, Q_m^{(m)}$</td><td>$Q_k^{(m)} = Q_k^{(m)} \qquad k = 1, 2, \ldots, m$</td></tr>
<tr><td rowspan="3">INDIRECT</td><td>SINGLE PARAMETER</td><td>Beta Factor</td><td>Q_t, β</td><td>$Q_k^{(m)} = \begin{cases} (1-\beta)Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$</td></tr>
<tr><td rowspan="2">MULTIPARAMETER</td><td>Multiple Greek Letters</td><td>$Q_t, \beta, \gamma, \delta, \ldots$</td><td>$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) \left(1 - \rho_{k+1}\right) Q_t$
$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$</td></tr>
<tr><td>Alpha Factor</td><td>$Q_t, \alpha_1, \alpha_2, \ldots, \alpha_m$</td><td>Non-staggered testing
$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad k = 1, \ldots, m$
$\alpha_t \equiv \sum_{k=1}^{m} k \alpha_k$</td></tr>
<tr><td colspan="3">SHOCK MODELS</td><td>Binomial Failure Rate</td><td>Q_1, μ, ρ, ω</td><td>$Q_k^{(m)} = \begin{cases} Q_1 + \mu\rho(1-\rho)^{m-1} & k = 1 \\ \mu\rho^k(1-\rho)^{m-k} & 2 \le k < m \\ \mu\rho^m + \omega & k = m \end{cases}$</td></tr>
</table>

* Refer to the text for definition of various parameters

** Formulae are presented for the basic events in a common cause component group of size m.
For the Alpha Factor Model equations are shown for the non-staggered test scheme (see discussion in section A-3).

be used to estimate a total failure probability but, as there is insufficient data to estimate multiple failure probabilities, a generic source like Nuclear Power Experience[A-1] may be used to estimate ratios of multiple to single components failure events.

Basic Parameter Model

The basic parameter model[A-2] refers to the straightforward definition of the probabilities of the basic events as given by Equation A.6. Depending on the system modeling requirements, $Q_k^{(m)}$'s can be defined as demand-based (frequency of failures per demand) or time-based (rate of failures per unit time). The latter can be defined both for the standby failure rates as well as for the rate of failures during operation.

In terms of the basic specific parameters defined in Equation A.6, the total failure probability, Q_t, of a component in a common cause group of m components is

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \tag{A.8}$$

where the binomial term

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(m-k)!\,(k-1)!} \tag{A.9}$$

represents the number of different ways that a specified component can fail with (k-1) other components in a group of m similar components. In this formulation, the events $Q_k^{(m)}$, $Q_j^{(m)}$ are mutually exclusive for all k, j. If the events $Q_k^{(m)}$ were not defined as being mutually exclusive, but independent, Equation A.8 is still valid under the rare event approximation.

Beta Factor Model

The beta factor model[A-3] is a single parameter model; that is, it uses one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. It was the first model to be applied to common cause events in risk and reliability studies. The model assumes that a constant fraction (β) of the component failure probability can be associated with common cause events shared by other components in that group. Another assumption is that whenever a common cause event occurs, all components within the common cause component group fail. Therefore, for a group of m components, all $Q_k^{(m)}$'s defined in Equation A.6 are zero except $Q_1^{(m)}$ and $Q_m^{(m)}$. The last two quantities are written as (dropping the superscript m)

$$\begin{aligned} Q_1^{(m)} &= (1-\beta)\,Q_t \\ Q_m^{(m)} &= \beta\,Q_t \end{aligned} \tag{A.10}$$

This implies that

$$\beta = \frac{Q_m^{(m)}}{Q_1^{(m)} + Q_m^{(m)}} \tag{A.11}$$

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

$$Q_t = Q_1^{(m)} + Q_m^{(m)} \tag{A.12}$$

which is the special case of Equation A.8 when $Q_2^{(m)} = Q_3^{(m)} = \cdots = Q_{m-1}^{(m)} = 0$.

Therefore, using the beta factor model, the frequencies of various basic events in a common cause group of m components are

$$Q_k^{(m)} = \begin{cases} (1-\beta)\,Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta\, Q_t & k = m \end{cases} \tag{A.13}$$

As can be seen, the beta factor model requires an estimate of the total failure rate of the components, which is generally available from generic data sources, and a corresponding estimate for the beta factor. As will be shown later in this appendix, the estimators of beta do not explicitly depend on system or component success data, which are not generally available. Also, estimates of the beta parameter for widely different types of components do not appear to vary appreciably. These two observations and the simplicity of the model are the main reasons for its wide use in risk and reliability studies.

It should be noted that relaxing the requirement for data on demands or time in operation (success data) requires making specific assumptions concerning the interpretation of data. This and several related issues regarding the assumptions behind the various models and the implications of the assumptions are discussed later in this appendix. The questions about interpretation of data and its impact on the form of estimators led to the development of a single parameter model known as the C-factor model[A-4] which is different from the beta factor model only in the way the data are used to estimate the single parameter of the model.

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 reveals that, in some cases, it gives reasonably accurate (only slightly conservative) results for redundancy levels up to about three or four. 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.

Multiple Greek Letter Model

The MGL model[A-5] 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.[A-6] In this model, other parameters in addition to the beta factor are introduced to account more explicitly for higher order redundancies and to allow for different probabilities of failures of subgroups of the common cause component group.

The MGL parameters consist of the total component failure probability, Q_t, 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 group 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 probability of each component due to all independent and common cause events.

plus

β = conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.

γ = conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or some additional components, given that two specific components have failed.

δ = conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components given that three specific components have failed.

The general equation that expresses the probability of k specific component failures due to common cause, Q_k, in terms of the MGL parameters, is consistent with the above definitions. The MGL parameters are defined in terms of the basic parameter model parameters for a group of three similar components as

$$Q_t = Q_1^{(3)} + 2\,Q_2^{(3)} + Q_3^{(3)} \tag{A.14}$$

$$\beta^{(3)} = \frac{2\,Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2\,Q_2^{(3)} + Q_3^{(3)}}$$

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2\,Q_2^{(3)} + Q_3^{(3)}} \tag{A.15}$$

δ and higher order terms are identically zero.

For a group of four similar components, the MGL parameters are

$$Q_t = Q_1^{(4)} + 3\,Q_2^{(4)} + 3\,Q_3^{(4)} + Q_4^{(4)} \tag{A.16}$$

$$\delta^{(4)} = \frac{Q_4^{(4)}}{3\,Q_3^{(4)} + Q_4^{(4)}} \tag{A.17}$$

It is important to note that the integer coefficients in the above definitions are a function of m, the number of components in the common cause group. Therefore, it is generally inappropriate to use MGL parameters that were quantified for an m unit group in an ℓ unit group, $m \neq \ell$. The same comment applies to the other similar multi-parameter methods.

The following equations express the probability of multiple component failures due to common cause, Q_k, in terms of the MGL parameters for a three-component common cause group:

$$\begin{aligned} Q_1^{(3)} &= (1 - \beta)\,Q_t \\ Q_2^{(3)} &= \frac{1}{2}\,\beta\,(1 - \gamma)\,Q_t \\ Q_3^{(3)} &= \gamma\,\beta\,Q_t \end{aligned} \tag{A.18}$$

For a four-component group, the equations are

$$\beta^{(4)} = \frac{3\,Q_2^{(4)} + 3\,Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3\,Q_2^{(4)} + 3\,Q_3^{(4)} + Q_4^{(4)}}$$

$$\gamma^{(4)} = \frac{3\,Q_3^{(4)} + Q_4^{(4)}}{3\,Q_2^{(4)} + 3\,Q_3^{(4)} + Q_4^{(4)}} \qquad \text{(A.19)}$$

$$Q_1^{(4)} = (1 - \beta)\,Q_t$$

$$Q_2^{(4)} = \frac{1}{3}\,\beta\,(1 - \gamma)\,Q_t$$

$$Q_3^{(4)} = \frac{1}{3}\,\beta\,\gamma\,(1 - \delta)\,Q_t$$

$$Q_4^{(4)} = \beta\,\gamma\,\delta\,Q_t$$

The generalization of this is given by

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{l=1}^{k} \rho_l \left(1 - \rho_{k+1}\right) Q_t \qquad \left(k = 1, \ldots, \rho_{m+1} = 0\right) \qquad \text{(A.20)}$$

where

$$\rho_1 = 1,\ \rho_2 = \beta,\ \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$$

Alpha-Factor Model

As explained in Appendix D, rigorous estimators for the beta factor and the MGL model parameters are fairly difficult to obtain, although approximate methods have been developed and used in practice.[A-7] A rigorous approach to estimating beta factors is presented in Reference A-8 by introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference A-9 uses the multi-parameter generalizations of event-based parameters directly to estimate the common cause basic event probabilities. This multi-parameter common cause model is called the alpha factor model.

Alpha factor parameters are estimated from observable data from a sampling scheme. The MGL parameters cannot be directly related to any known sampling scheme and observable data. This difference and its implications are described more fully in Appendix D.

The alpha factor model defines common cause failure probabilities from a set of failure frequency ratios and the total component failure frequency, Q_T. In terms of the basic event probabilities, the alpha factor parameters for non-staggered testing are defined as

$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}} \tag{A.21}$$

where $\binom{m}{k} Q_k^{(m)}$ is the frequency of events involving k component failures in a common cause group of m components, and the denominator is the sum of such frequencies. In other words,

$\alpha_k^{(m)}$ = probability that when a common cause basic event occurs in a common cause group of size m, it involves failure of k components.

For example, for a group of three similar components we have

$$\begin{aligned}
\alpha_1^{(3)} &= \frac{3\,Q_1^{(3)}}{3\,Q_1^{(3)} + 3\,Q_2^{(3)} + Q_3^{(3)}} \\
\alpha_2^{(3)} &= \frac{3\,Q_2^{(3)}}{3\,Q_1^{(3)} + 3\,Q_2^{(3)} + Q_3^{(3)}} \\
\alpha_3^{(3)} &= \frac{Q_3^{(3)}}{3\,Q_1^{(3)} + 3\,Q_2^{(3)} + Q_3^{(3)}}
\end{aligned} \tag{A.22}$$

and $\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1$ as expected.

Using Equations A.21 and A.8, we can see that the basic event probabilities can be written as a function of Q_t and the alpha factors as follows:

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} Q_t \tag{A.23}$$

where

$$\alpha_t \equiv \sum_{k=1}^{m} k\,\alpha_k^{(m)} \tag{A.24}$$

To see how Equation A.23 is obtained from Equations A.8 and A.21, note that Equation A.21 can also be written as

$$\frac{k}{m} \left\{ \sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)} \right\} \alpha_t^{(m)} = \binom{m-1}{k-1} Q_k^{(m)}$$

By summing both sides over k we get

$$\frac{1}{m} \left\{ \sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)} \right\} \sum_{k=1}^{m} k\,\alpha_t^{(m)} = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)}$$

or

$$\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)} = \frac{m}{\alpha_t} Q_t$$

where we have used Equations A.8 and A.24. By using the above equation in Equation A.21 and solving for $Q_k^{(m)}$ we get Equation A.23.

The parameters of the α-factor and the MGL models are related through a set of simple relations. For example, for a common cause component group of size three, the MGL parameters are

$$\beta^{(3)} = \frac{2\,\alpha_2 + 3\,\alpha_3}{\alpha_1 + 2\,\alpha_2 + 3\,\alpha_3} \qquad \text{(A.25)}$$

$$\gamma^{(3)} = \frac{3\,\alpha_3}{2\,\alpha_2 + 3\,\alpha_3}$$

Similarly, the alpha factor model parameters for the same group are written as

$$\alpha_1^{(3)} = 3\,(1 - \beta)$$

$$\alpha_2^{(3)} = \frac{3}{2}\,\beta\,(1 - \gamma) \qquad \text{(A.26)}$$

$$\alpha_3^{(3)} = \beta\,\gamma$$

The form of these relations depends on assumptions regarding the particular testing scheme (staggered vs. non-staggered) applied to the system as described in Section A.3. Tables A-2, A-3, and A-4 list such conversion equations for common cause component groups of up to size m = 8, under both staggered and non-staggered testing schemes.

Binomial Failure Rate Model

The Binomial Failure Rate (BFR) model[A-10] 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. For a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution, hence the name Binomial Failure Model. When originally presented and applied, the model only included the 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.

μ ≡ frequency of occurrence of nonlethal shocks.

Table A-2. MGL to alpha factor conversion formulae for staggered testing.

m	MGL to Alpha Factor	Alpha Factor to MGL
2	$\alpha_1 = 1 - \beta$ $\alpha_2 = \beta$	$\beta = 1 - \alpha_1 = \alpha_2$
3	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = \beta\gamma$	$\beta = \alpha_2 + \alpha_3$ $\gamma = \frac{\alpha_3}{\alpha_2 + \alpha_3}$
4	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = (1 - \delta)\beta\gamma$ $\alpha_4 = \beta\gamma\delta$	$\beta = \alpha_2 + \alpha_3 + \alpha_4$ $\gamma = \frac{\alpha_3 + \alpha_4}{\alpha_2 + \alpha_3 + \alpha_4}$ $\delta = \frac{\alpha_4}{\alpha_3 + \alpha_4}$
5	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = (1 - \delta)\beta\gamma$ $\alpha_4 = (1 - \epsilon)\beta\gamma\delta$ $\alpha_5 = \beta\gamma\delta\epsilon$	$\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5$ $\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5}$ $\delta = \frac{\alpha_4 + \alpha_5}{\alpha_3 + \alpha_4 + \alpha_5}$ $\epsilon = \frac{\alpha_5}{\alpha_4 + \alpha_5}$
6	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = (1 - \delta)\beta\gamma$ $\alpha_4 = (1 - \epsilon)\beta\gamma\delta$ $\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$ $\alpha_6 = \beta\gamma\delta\epsilon\mu$	$\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6$ $\gamma = \frac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}$ $\delta = \frac{\alpha_4 + \alpha_5 + \alpha_6}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6}$ $\epsilon = \frac{\alpha_5 + \alpha_6}{\alpha_4 + \alpha_5 + \alpha_6}$ $\mu = \frac{\alpha_6}{\alpha_5 + \alpha_6}$

Table A-2. MGL to alpha factor conversion formulae for staggered testing (continued).

m	MGL to Alpha Factor	Alpha Factor to MGL
7	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = (1 - \delta)\beta\gamma$ $\alpha_4 = (1 - \epsilon)\beta\gamma\delta$ $\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$ $\alpha_6 = (1 - \nu)\beta\gamma\delta\epsilon\mu$ $\alpha_7 = \beta\gamma\delta\epsilon\mu\nu$	$\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7$ $\gamma = \dfrac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$ $\delta = \dfrac{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$ $\epsilon = \dfrac{\alpha_5 + \alpha_6 + \alpha_7}{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7}$ $\mu = \dfrac{\alpha_6 + \alpha_7}{\alpha_5 + \alpha_6 + \alpha_7}$ $\nu = \dfrac{\alpha_7}{\alpha_6 + \alpha_7}$
8	$\alpha_1 = 1 - \beta$ $\alpha_2 = (1 - \gamma)\beta$ $\alpha_3 = (1 - \delta)\beta\gamma$ $\alpha_4 = (1 - \epsilon)\beta\gamma\delta$ $\alpha_5 = (1 - \mu)\beta\gamma\delta\epsilon$ $\alpha_6 = (1 - \nu)\beta\gamma\delta\epsilon\mu$ $\alpha_7 = (1 - \kappa)\beta\gamma\delta\epsilon\mu\nu$ $\alpha_8 = \beta\gamma\delta\epsilon\mu\nu\kappa$	$\beta = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8$ $\gamma = \dfrac{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$ $\delta = \dfrac{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$ $\epsilon = \dfrac{\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}{\alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$ $\mu = \dfrac{\alpha_6 + \alpha_7 + \alpha_8}{\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8}$ $\nu = \dfrac{\alpha_7 + \alpha_8}{\alpha_6 + \alpha_7 + \alpha_8}$ $\kappa = \dfrac{\alpha_8}{\alpha_7 + \alpha_8}$

Table A-3. Alpha factor to MGL conversion formulae for non-staggered testing.

m	Alpha Factor to MGL
2	$\beta = 1 - \alpha_1 = \alpha_2$
3	$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$ $\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3}$
4	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4}{2\alpha_2 + 3\alpha_3 + 4\alpha_4}$ $\delta = \frac{4\alpha_4}{3\alpha_3 + 4\alpha_4}$
5	$\beta = \frac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\gamma = \frac{3\alpha_3 + 4\alpha_4 + 5\alpha_5}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\delta = \frac{4\alpha_4 + 5\alpha_5}{3\alpha_3 + 4\alpha_4 + 5\alpha_5}$ $\epsilon = \frac{5\alpha_5}{4\alpha_4 + 5\alpha_5}$

Table A-3. Alpha factor to MGL conversion formulae for non-staggered testing (continued).

m	Alpha Factor to MGL
6	$\beta = \dfrac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\gamma = \dfrac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\delta = \dfrac{4\alpha_4 + 5\alpha_5 + 6\alpha_6}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\epsilon = \dfrac{5\alpha_5 + 6\alpha_6}{4\alpha_4 + 5\alpha_5 + 6\alpha_6}$ $\mu = \dfrac{6\alpha_6}{5\alpha_5 + 6\alpha_6}$
7	$\beta = \dfrac{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\gamma = \dfrac{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\delta = \dfrac{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}{3\alpha_3 + 4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\epsilon = \dfrac{5\alpha_5 + 6\alpha_6 + 7\alpha_7}{4\alpha_4 + 5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\mu = \dfrac{6\alpha_6 + 7\alpha_7}{5\alpha_5 + 6\alpha_6 + 7\alpha_7}$ $\nu = \dfrac{7\alpha_7}{6\alpha_6 + 7\alpha_7}$

Table A-3. Alpha factor to MGL conversion formulae for non-staggered testing (continued).

m	Alpha Factor to MGL
8	$\beta = \dfrac{2\alpha_2+3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}{\alpha_1+2\alpha_2+3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}$ $\gamma = \dfrac{3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}{2\alpha_2+3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}$ $\delta = \dfrac{4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}{3\alpha_3+4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}$ $\epsilon = \dfrac{5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}{4\alpha_4+5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}$ $\mu = \dfrac{6\alpha_6+7\alpha_7+8\alpha_8}{5\alpha_5+6\alpha_6+7\alpha_7+8\alpha_8}$ $\nu = \dfrac{7\alpha_7+8\alpha_8}{6\alpha_6+7\alpha_7+8\alpha_8}$ $\kappa = \dfrac{8\alpha_8}{7\alpha_7+8\alpha_8}$

Table A-4. MGL to alpha factor conversion formulae for non-staggered testing.

m	MGL to Alpha Factor
2	$\alpha_1 = \frac{2(1-\beta)}{2-\beta}$ $\alpha_2 = \frac{\beta}{2-\beta}$
3	$\alpha_1 = \frac{6(1-\beta)}{6-\beta(3+\gamma)}$ $\alpha_2 = \frac{3\beta(1-\gamma)}{6-\beta(3+\gamma)}$ $\alpha_3 = \frac{2\beta\gamma}{6-\beta(3+\gamma)}$
4	$\alpha_1 = \frac{12(-1+\beta)}{-12+\beta(6+(2+\delta)\gamma)}$ $\alpha_2 = \frac{6\beta(-1+\gamma)}{-12+\beta(6+(2+\delta)\gamma)}$ $\alpha_3 = \frac{4\beta(-1+\delta)\gamma}{-12+\beta(6+(2+\delta)\gamma)}$ $\alpha_4 = \frac{3\beta\gamma\delta}{-12+\beta(6+(2+\delta)\gamma)}$
5	$\alpha_1 = \frac{12(-1+\beta)(5+4\epsilon)}{\boldsymbol{D}}$ $\alpha_2 = \frac{6\beta(5+4\epsilon)(-1+\gamma)}{\boldsymbol{D}}$ $\alpha_3 = \frac{4\beta(-1+\delta)(5+4\epsilon)\gamma}{\boldsymbol{D}}$ $\alpha_4 = \frac{3\beta\gamma\delta(-5+\epsilon)}{\boldsymbol{D}}$ $\alpha_5 = \frac{12\beta\gamma\delta\epsilon}{\boldsymbol{D}}$ where $\boldsymbol{D} = -60+30\beta-48\epsilon+24\beta\epsilon+10\beta\gamma+5\beta\gamma\delta+8\beta\epsilon\gamma+7\beta\delta\epsilon\gamma$

Table A-4. MGL to alpha factor conversion formulae for non-staggered testing (continued).

m	MGL to Alpha Factor
6	$\alpha_1 = \frac{12(-1+\beta)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_2 = \frac{6\beta(-1+\gamma)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_3 = \frac{4\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$ $\alpha_4 = \frac{3\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$ $\alpha_5 = \frac{12\beta\gamma\delta\epsilon(-1+\mu)}{D}$ $\alpha_6 = \frac{10\beta\gamma\delta\epsilon\mu}{D}$ where $D = 60 - 30\beta + 48\epsilon - 24\beta\epsilon - 10\beta\gamma - 5\beta\gamma\delta - 8\beta\epsilon\gamma - 7\beta\delta\epsilon\gamma$ $-48\epsilon\mu + 24\beta\epsilon\mu + 8\beta\epsilon\gamma\mu + 2\beta\delta\gamma\epsilon\mu$
7	$\alpha_1 = \frac{84(-1+\beta)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_2 = \frac{42\beta(-1+\gamma)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_3 = \frac{28\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$ $\alpha_4 = \frac{21\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$ $\alpha_5 = \frac{84\beta\gamma\delta\epsilon(-1+\mu)}{D}$ $\alpha_6 = \frac{70\beta\gamma\delta\epsilon\mu(-1+\nu)}{D}$ $\alpha_7 = \frac{60\beta\gamma\delta\epsilon\mu\nu}{D}$ here $D = -420 + 210\beta - 336\epsilon + 168\beta\epsilon + 70\beta\gamma + 35\beta\gamma\delta + 56\beta\epsilon\gamma + 49\beta\delta\epsilon$ $+336\epsilon\mu - 168\beta\epsilon\mu - 56\beta\epsilon\gamma\mu - 14\beta\delta\gamma\epsilon\mu + 10\beta\gamma\delta\epsilon\mu\nu$

Table A-4. MGL to alpha factor conversion formulae for non-staggered testing (continued).

m	MGL to Alpha Factor
8	$\alpha_1 = \frac{84(-1+\beta)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_2 = \frac{42\beta(-1+\gamma)(-5+4\epsilon(-1+\mu))}{D}$ $\alpha_3 = \frac{28\beta(-1+\delta)\gamma(-5+4\epsilon\mu)}{D}$ $\alpha_4 = \frac{21\beta\gamma\delta(-5+\epsilon+4\epsilon\mu)}{D}$ $\alpha_5 = \frac{84\beta\gamma\delta\epsilon(-1+\mu)}{D}$ $\alpha_6 = \frac{70\beta\gamma\delta\epsilon\mu(-1+\nu)}{D}$ $\alpha_7 = \frac{60\beta\gamma\delta\epsilon\mu\nu(-1+\kappa)}{D}$ $\alpha_8 = \frac{105\beta\gamma\delta\epsilon\mu\nu\kappa}{2D}$ where $D = -420+210\beta-336\epsilon+168\beta\epsilon+70\beta\gamma+35\beta\gamma\delta+56\beta\epsilon\gamma+49\beta\delta\epsilon\gamma$ $+336\epsilon\mu-168\beta\epsilon\mu-56\beta\epsilon\gamma\mu-14\beta\delta\gamma\epsilon\mu+10\beta\gamma\delta\epsilon\mu\nu+60\beta\gamma\delta\epsilon\mu\nu\kappa$

ρ ≡ conditional probability of failure of each component, given a nonlethal shock.

ω ≡ frequency of occurrence of lethal shocks.

Thus, the frequency of basic events involving k specific components is given as

$$Q_k^{(m)} = \begin{cases} Q_I + \mu\rho(1-\rho)^{m-1} & k = 1 \\ \mu(\rho)^k(1-\rho)^{m-k} & 2 \leq k < m \\ \mu\rho^m + \omega & k = m \end{cases} \tag{A.27}$$

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.

A.2.1 Some Estimators for Parameters of the Common Cause Models

In order to estimate a parameter value, it is necessary to find an expression that relates the parameters to measurable quantities. This expression is called an estimator.

There are several possible estimators that can be used for a given parameter. Estimators presented in this section are the maximum likelihood estimators and are presented here for their simplicity. However, the mean values obtained from probability distribution characterizing uncertainty in the estimated values are more appropriate for point value quantification of system unavailability. These mean values are presented in the context of developing uncertainty distributions for the various parameters in Appendix D.

The estimators of this section are also based on assuming a particular component and system testing scheme. More specifically, it is assumed that, for the plants in the data base, in each test or actual demand, the entire system (or common cause component group) and all possible combinations of multiple components are challenged. This corresponds to the nonstaggered testing scheme. However, if this assumption is changed (e.g., if a staggered testing scheme is assumed), the form of the estimators will also change, resulting in numerically different values for the parameters. The estimators presented in this section are the more conservative, given a fixed Q_T. A more detailed discussion the effects of various assumptions including alternative strategies is given in Section A.3.

Estimators for Basic Parameters

The maximum likelihood estimator for Q_k is given as

$$\hat{Q}_k = \frac{n_k}{N_k} \tag{A.28}$$

where

n_k ≡ number of events involving k components in a failed state,

and

N_k ≡ number of demands on any k component in the common cause group.

If it is assumed that each time the system is operated, all of the m components in the group are demanded, and this number of demands is N_D, then

$$N_k = \binom{m}{k} N_D \tag{A.29}$$

The binomial term $\binom{m}{k}$ represents the number of groups of k components that can be formed from m components. We, therefore, have

$$\hat{Q}_k^{(m)} = \frac{n_k}{\binom{m}{k} N_D} \tag{A.30}$$

Thus, Equation A.30 assumes that the data are collected from a set of N_D system demands for which the state of all m components in the common cause group is checked. It is simply the ratio of the number of basic events involving k components, divided by the total number of times that various combinations of k components are challenged in N_D system demands. This is represented by the binomial term in the denominator of Equation A.30. Similar estimators can be developed for rate of failure per unit time by replacing N_D with T, the total system operating time.

Replacing Q_k in Equation A.8 with the corresponding estimator yields the following estimator for the total failure probability for a specific component:

$$\hat{Q}_t = \frac{1}{m N_D} \sum_{k=1}^{m} k n_k \tag{A.31}$$

Estimator for the β-Factor Model Parameter

Although the β-factor was originally developed for a system of two redundant components and the estimators that are often presented in the literature also assume that the data are collected from two-unit systems, a generalized β-factor estimator can be defined for a system of m redundant components.

Such an estimator is based on the following general definition of the β-factor (identical to the way it is defined in the more general MGL model).

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!\,(k-1)!} Q_k \tag{A.32}$$

Using the estimator of $Q_k^{(m)}$, given by Equation A.30, and Q_t, given by Equation A.31, in the above equation results in the following estimator for β.

$$\beta = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{A.33}$$

For a two-unit system (m = 2), the above estimator reduces to the familiar estimator of the β-factor.

$$\beta = \frac{2n_2}{n_1 + 2n_2} \tag{A.34}$$

Note that the estimator β is developed from maximum likelihood estimators of Q_k's. An alternative estimator can be developed directly from the distribution of the beta factor based on its definition in Equation A.32. Additional discussion of this is in Appendix D of this report.

Estimators for the MGL Parameters

In the following we develop estimators for the first three parameters of the MGL model for a system of m components. Estimators for the higher order parameters can be developed in a similar fashion. Based on the definition of the MGL parameters,

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!\,(k-1)!} Q_k^{(m)} \tag{A.35}$$

$$\gamma = \frac{1}{\beta Q_t} \sum_{k=3}^{m} \frac{(m-1)!}{(m-k)!\,(k-1)!} Q_k^{(m)} \tag{A.36}$$

$$\delta = \frac{1}{\beta \gamma Q_t} \sum_{k=4}^{m} \frac{(m-1)!}{(m-k)!\,(k-1)!} Q_k^{(m)} \tag{A.37}$$

Therefore, by using Equations A.30 and A.31 in the above expressions, the following estimators are obtained:

$$\hat{\beta} = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{A.38}$$

$$\hat{\gamma} = \frac{\sum_{k=3}^{m} k n_k}{\sum_{k=2}^{m} k n_k} \tag{A.39}$$

$$\hat{\delta} = \frac{\sum_{k=4}^{m} k n_k}{\sum_{k=3}^{m} k n_k} \tag{A.40}$$

For instance, for a three-unit system (m=3), we have

$$\hat{\beta} = \frac{2 n_2 + 3 n_3}{n_1 + 2 n_2 + 3 n_3} \tag{A.41}$$

Similarly,

$$\hat{\gamma} = \frac{3 n_3}{2 n_2 + 3 n_3} \tag{A.42}$$

As can be seen from the above estimators, the MGL parameters are essentially the ratios of the number of component failures in various basic events. For instance in Equation A.42, the numerator ($3n_3$) is the total number of components failed in common cause basic events that fail three components (n_3). This is in contrast with estimates of the α-factor model, which are in terms of the ratios of events rather than component states, and is demonstrated in the following section.

Estimators for the α-factor Model Parameters

An estimator for each of the α-factor parameters (α_k) can be based on its definition as the fraction of total failure events that involve k component failures due to common cause. Therefore, for a system of m redundant components,

$$\hat{\alpha}_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{A.43}$$

It is shown in Appendix D that $\hat{\alpha}_k$'s correspond to the maximum likelihood estimate of the distribution of α_k's.

Estimators for the BFR Model

The main parameters of the model are Q_I, μ, ω, and ρ. To develop estimators for these parameters, several other quantities are defined as:

λ_t ≡ rate of nonlethal shocks that cause at least one component failure
n_t ≡ total number of common cause failure events

$$n_t \equiv \sum_{k=1}^{m} n_k \tag{A.44}$$

where, as before, n_k is the number of basic events involving k components, and

n_L = the number of occurrences of lethal shocks.
n_I = the number of individual component failures, not counting failures due to lethal and nonlethal shocks.

The maximum likelihood estimators for the four parameters Q_I, λ_t, ω, and ρ, as presented in Appendix D, are

$$\hat{Q}_I = \frac{n_I}{m N_D} \tag{A.45}$$

$$\hat{\lambda}_t = \frac{n_t}{N_D} \tag{A.46}$$

$$\hat{\omega} = \frac{n_L}{N_D} \tag{A.47}$$

and $\hat{\rho}$ is the solution of the following equation:

$$\hat{s} = \hat{\rho}\,\frac{m\,n_t}{1-(1-\rho)^m} \tag{A.48}$$

where

$$\hat{s} = \sum_{k=1}^{m} k\,n_k \tag{A.49}$$

Based on the above estimators, an estimator for μ can be obtained from the following equation:

$$\lambda_t = \mu\left[1-(1-\rho)^m\right] \tag{A.50}$$

which is based on the definition of λ_t at the rate of nonlethal shocks that cause at least one component failure. Therefore,

$$\hat{\mu} = \frac{\hat{\lambda}_t}{1-(1-\hat{\rho})^m} \tag{A.51}$$

A.3 THE EFFECT OF TESTING SCHEMES ON ESTIMATORS

The testing scheme to which the system (or common cause component group) is subjected has an impact on the form of the statistical estimator of some model parameters. It also affects the conversion relations between various parametric models such as those shown in Tables A-2 through A-4.

For example, in the estimator for Q_k in the basic parameter model, the number of times a group of k components is challenged (N_k) is derived from the number of test episodes, N_D, using the following relation:

$$N_k = \binom{m}{k} N_D \tag{A.52}$$

This means that all such combinations are assumed to be challenged in each episode.

Note that N_D in this case is the same as N_{TS}, the number of tests of each of the redundant trains (components) as specified by plant technical specifications:

$$N_D = N_{TS}$$

However, assuming a staggered testing scheme results in different values of N_k; the value depends on the response to the failure observed. Suppose, that a given failure is observed in the single component tested in a particular test episode, all the other components are tested immediately, then N_k can be evaluated in terms of the number of test episodesN_D^* as follows. (Note that in this case the number of test episodes is denoted as N_D^*. This is done to avoid an equivalence being made with the number of test episodes of the non-staggered testing case. In fact, for the same technical specifications or frequency of testing of a component, the value of N_D^* in any given calendar time period would be related to N_{TS} by $N_D^* = m\, N_{TS}$, since in each of the test episodes for non-staggered testing all components in the group are tested at a test episode whereas unless there is a failure, in the staggered case only one is tested in a test episode.)

Each successful test results in demonstrating that for $\binom{m-1}{k-1}$ groups of k components there was no common cause failure. In addition, each time the component failed the test, all other components are tested and this leads to $\binom{m-1}{k-1}$ tests on any group of k components.[2]

Neglecting the second order effects arising from the complication that if k+1 components are failed this modifies the number of feasible tests on k components; the number of demands on a group of k components can be expressed as

$$\begin{aligned} N_k &= \left(N_D^* - \sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1} + \left(\sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1} \\ &= N_D^*\binom{m-1}{k-1} = m\,N_{TS}\binom{m-1}{k-1} \end{aligned} \tag{A.53}$$

[2] In this example, it is assumed that we are estimating Q_k, and not specifically a common cause failure probability. If we were identifying combinations of multiple and independent failures such as $Q_1 \bullet Q_k$ at each testing episode, this term would be $\binom{m}{k}$. However, since the n_j's are collectively usually much smaller than N_D^*, this subtle distinction will make little difference.

The number of single component demands is given by

$$N_D^* + \sum_{j=1}^{m} n_j \cdot (m-1) \tag{A.54}$$

with the above estimates of N$_k$ for different testing schemes, the following estimators for the probability of basic events involving k components are derived:

For a nonstaggered testing scheme, using Equation A.52,

$$Q_k^{NS} = \frac{n_k}{\binom{m}{k} N_{TS}} \tag{A.55}$$

For a staggered testing scheme, using Equation A.53,

$$Q_k^{S} = \frac{n_k}{m\binom{m-1}{k-1} N_{TS}} \tag{A.56}$$

Therefore $Q_k^S \leq Q_k^{NS}$ because

$$\frac{Q_k^S}{Q_k^{NS}} = \frac{1}{k} \tag{A.57}$$

In light of the above difference, we can now see that estimates of beta-factor, for example, are different depending on what testing scheme is assumed. To show this we recall that, for a two component system,

$$\beta = \frac{Q_2}{Q_1 + Q_2} \tag{A.58}$$

Therefore,

$$\beta^S = \frac{Q_2^S}{Q_1^S + Q_2^S} \tag{A.59}$$

and,

$$\beta^{NS} = \frac{Q_2^{NS}}{Q_1^{NS} + Q_2^{NS}} \tag{A.60}$$

thus,

$$\beta^{NS} = \frac{2Q_2^S}{Q_1^S + 2Q_2^S} \cong 2\frac{Q_2^S}{Q_1^S + Q_2^S} = 2\beta^S \tag{A.61}$$

where we assumed, as it is true in most cases, that $Q_2 << Q$. The staggered-based estimator is approximately a factor of 2 smaller.

The estimator presented by Equation A.59 is similar in form to the estimator of a single parameter model called the C-factor model.[A-4] In this respect, C-factor is another estimator of the β-factor under the assumptions leading to Equation A.59. It should be mentioned, however, that the C-factor method was developed to try to use the LER summary data to provide estimates of common cause failure probabilities. It essentially involved an interpretation of data on historical events based on an assessment of root cause. The potential of each observed root cause for being a cause of multiple failures at the plant in question was judged on engineering grounds, taking into account such aspect as plant design, maintenance, philosophy, etc. The estimator (the C-factor) was the fraction of observed root causes of failure that either did, or were judged to have the potential to, result in multiple failure. The spectrum of root causes used comes from both single and multiple failure events. Since it is the occurrence of the root cause that is important and the common cause root causes are assumed to result in this model in totally coupled failures, the multiple failure events, if applicable, are only counted once (not multiplied by the number of components failed).

A.4 REFERENCES

A-1. Nuclear Power Experience, S. M. Stoller Corporation, updated monthly.

A-2. Fleming, K. N., and A. Mosleh, *Classification and Analysis of Reactor Operation Experience Involving Dependent Events*, Pickard Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

A-3. 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-A13284, April 23-25, 1975.

A-4. Parry, G. W., *Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty*, 1984 Annual Meeting of the Society for Risk Analysis.

A-5. 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.

A-6. Poucet, A., A. Amendola, and P. C. Carriabue, *Summary of the Common Cause Failure Reliability Benchmark Exercise*, Joint Research Center Report, EUR-11054 EN, Ispra Italy,1987.

A-7. Mosleh, A., *Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data*, Nuclear Engineering and Design, August 1985.

A-8. Paula, H. M., *Comments on the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation*, Nuclear Safety, Vol. 27, No. 2, April/June 1986.

A-9. 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, 1987.

A-10. 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.

A-11. American Nuclear Society and Institute of Electrical and Electronic 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.

APPENDIX B

MINIMAL CUTSETS FOR COMMON CAUSE GROUPS FOR VARIOUS CONFIGURATIONS

APPENDIX B

Minimal Cutsets for Common Cause Groups for Various Configurations

The minimal cutsets associated with the various configurations listed in Table 5-2 of this report are presented in Table B-1.

Table B-1. Minimal cutsets for common cause groups for various configurations.

CASE	NUMBER OF CUTSETS	MINIMAL CUTSETS
1	2	[A, B], [C_{AB}]
2	3	[A], [B], [C_{AB}]
3	5	[A, B, C], [A, C_{BC}], [B, C_{AC}], [C, C_{AB}], [C_{ABC}]
4	7	[A, B], [A, C], [B, C], [C_{AB}], [C_{AC}], [C_{BC}], [C_{ABC}]
5	7	[A], [B], [C], [C_{AB}], [C_{AC}], [C_{BC}], [C_{ABC}]
6	15	[A, B, C, D], [C_{AB}, C_{CD}], [C_{AC}, C_{BD}], [C_{AD}, C_{BC}], [A, C_{BCD}], [B, C_{ACD}], [C, C_{ABD}], [D, C_{ABC}], [C_{ABCD}], [A, B, C_{CD}], [A, C, C_{BD}], [A, D, C_{BC}], [B, C, C_{AD}], [B, D, C_{AC}], [C, D, C_{AB}]
7	24	[A, B, C], [A, B, D], [A, C, D], [B, C, D], [A, C_{BC}], [A, C_{BD}], [A, C_{CD}], [B, C_{AC}], [B, C_{AD}], [B, C_{CD}], [C, C_{AB}], [C, C_{AD}], [C, C_{BD}], [D, C_{AB}], [D, C_{AC}], [D, C_{BC}], [C_{AB}, C_{CD}], [C_{AC}, C_{BD}], [C_{AD}, C_{BC}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABCD}]
8	17	[A, B], [A, C], [A, D], [B, C], [B, D], [C, D], [C_{AB}], [C_{AC}], [C_{AD}], [C_{BC}], [C_{BD}], [C_{CD}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABCD}]
9	15	[A], [B], [C], [D], [C_{AB}], [C_{AC}], [C_{AD}], [C_{BC}], [C_{BD}], [C_{CD}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABCD}]
10	52	[C_{ABCDE}], [A, C_{BCDE}], [B, C_{ACDE}], [C_{ABDE}, C], [C_{ABCE}, D], [C_{ABCD}, E], [C_{AB}, C_{CDE}], [C_{ABC}, C_{DE}], [C_{ABD}, C_{CE}], [C_{ABE}, C_{CD}], [C_{AC}, C_{BDE}], [C_{ACD}, C_{BE}], [C_{ACE}, C_{BD}], [C_{ADE}, C_{BC}], [C_{AE}, C_{BCD}], [C_{AD}, C_{BCE}], [A, B, C_{CDE}], [A, C_{BDE}, C], [A, C_{BCD}, E], [A, C_{BCE}, D], [B, C_{ACD}, E], [B, C_{ACE}, D], [C_{ABC}, D, E], [C_{ABD}, C, E], [C_{ABE}, C, D], [B, C, C_{ADE}], [A, C_{BC}, C_{DE}], [A, C_{BD}, C_{CE}], [A, C_{BE}, C_{CD}], [B, C_{AC}, C_{DE}], [B, C_{AD}, C_{CE}], [B, C_{AE}, C_{CD}], [C_{AB}, C_{CD}, E], [C_{AB}, C_{CE}, D], [C_{AB}, C_{DE}, C], [C_{AC}, C_{BD}, E], [C_{AC}, C_{BE}, D], [C_{AD}, C_{BC}, E], [C_{AD}, C_{BE}, C], [C_{AE}, C_{BC}, D], [C_{AE}, C_{BD}, C], [A, B, C_{CD}, E], [A, B, C_{CE}, D], [A, B, C_{DE}, C], [A, C_{BC}, D, E], [A, C_{BD}, C, E], [A, C_{BE}, C, D], [B, C_{AC}, D, E], [B, C_{AD}, C, E], [C_{AB}, C, D, E], [C_{AE}, B, C, D], [A, B, C, D, E]
11	86	[A, B, C, D], [A, B, C, E], [A, B, D, E], [A, C, D, E], [B, C, D, E], [A, C_{BCD}], [A, C_{BCE}], [A, C_{BDE}], [A, C_{CDE}], [B, C_{ACD}], [B, C_{ACE}], [B, C_{ADE}], [B, C_{CDE}], [C_{ABC}, D], [C_{ABC}, E], [C_{ABD}, C], [C_{ABD}, E], [C_{ABE}, C], [C_{ABE}, D], [C_{ACD}, E], [C_{ACE}, D], [C_{ADE}, C], [C_{BCD}, E], [C_{BCE}, D], [C_{BDE}, C], [C_{AB}, C_{CD}], [C_{AB}, C_{CE}], [C_{AB}, C_{DE}], [C_{AC}, C_{BD}], [C_{AC}, C_{BE}], [C_{AC}, C_{DE}], [C_{AD}, C_{BC}], [C_{AD}, C_{BE}], [C_{AD}, C_{CE}], [C_{AE}, C_{BC}], [C_{AE}, C_{BD}], [C_{AE}, C_{CD}], [C_{BC}, C_{DE}], [C_{BD}, C_{CE}], [C_{BE}, C_{CD}], [A, B, C_{CD}], [A, B, C_{CE}], [A, B, C_{DE}], [A, C_{BC}, D], [A, C_{BC}, E], [A, C_{BD}, C], [A, C_{BD}, E], [A, C_{BE}, C], [A, C_{BE}, D], [A, C_{CD}, E], [A, C_{CE}, D], [A, C_{DE}, C], [B, C_{AC}, D], [B, C_{AC}, E], [B, C_{AD}, C], [B, C_{AD}, E], [B, C_{AE}, C], [B, C_{AE}, D], [B, C_{CD}, E], [B, C_{CE}, D], [B, C_{DE}, C], [C_{AB}, C, D], [C_{AB}, C, E], [C_{AB}, D, E], [C_{AC}, D, E], [C_{AD}, C, E], [C_{AE}, C, D], [C_{BC}, D, E], [C_{BD}, C, E], [C_{BE}, C, D], [C_{ABC}, C_{DE}], [C_{AD}, C_{BCE}], [C_{AC}, C_{BDE}], [C_{ABD}, C_{CE}], [C_{ABE}, C_{CD}], [C_{ADE}, C_{BC}], [C_{ACD}, C_{BE}], [C_{ACE}, C_{BD}], [C_{AB}, C_{CDE}], [C_{AE}, C_{BCD}], [C_{ABCE}], [C_{ABDE}], [C_{ACDE}], [C_{BCDE}], [C_{ABCD}], [C_{ABCDE}]

Table B-1. Minimal cutsets for common cause groups for various configurations (continued).

CASE	NUMBER OF CUTSETS	MINIMAL CUTSETS
12	71	[A, B, C], [A, B, D], [A, B, E], [A, C, D], [A, C, E], [A, D, E], [B, C, D], [B, C, E], [B, D, E], [C, D, E], [A, C_{BC}], [A, C_{BD}], [A, C_{BE}], [A, C_{CD}], [A, C_{CE}], [A, C_{DE}], [B, C_{AC}], [B, C_{AD}], [B, C_{AE}], [B, C_{CD}], [B, C_{CE}], [B, C_{DE}], [C_{AB}, C], [C_{AB}, D], [C_{AB}, E], [C_{AC}, D], [C_{AC}, E], [C_{AD}, C], [C_{AD}, E], [C_{AE}, C], [C_{AE}, D], [C_{BC}, D], [C_{BC}, E], [C_{BD}, C], [C_{BD}, E], [C_{BE}, C], [C_{BE}, D], [C_{CD}, E], [C_{CE}, D], [C_{DE}, C], [C_{AB}, C_{CD}], [C_{AB}, C_{CE}], [C_{AB}, C_{DE}], [C_{AC}, C_{BD}], [C_{AC}, C_{BE}], [C_{AC}, C_{DE}], [C_{AD}, C_{BC}], [C_{AD}, C_{BE}], [C_{AD}, C_{CE}], [C_{AE}, C_{BC}], [C_{AE}, C_{BD}], [C_{AE}, C_{CD}], [C_{BC}, C_{DE}], [C_{BD}, C_{CE}], [C_{BE}, C_{CD}], [C_{ABC}], [C_{ABD}], [C_{ABE}], [C_{ACD}], [C_{ACE}], [C_{ADE}], [C_{BCD}], [C_{BCE}], [C_{BDE}], [C_{CDE}], [C_{ABCD}], [C_{ABCE}], [C_{ABDE}], [C_{ACDE}], [C_{BCDE}], [C_{ABCDE}]
13	36	[A, B], [A, C], [A, D], [A, E], [B, C], [B, D], [B, E], [C, D], [C, E], [D, E], [C_{AB}], [C_{AC}], [C_{AD}], [C_{AE}], [C_{BC}], [C_{BD}], [C_{BE}], [C_{CD}], [C_{CE}], [C_{DE}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABE}], [C_{ACE}], [C_{ADE}], [C_{BCE}],[C_{BDE}], [C_{CDE}], [C_{ABCD}], [C_{ABCE}], [CA_{BDE}], [C_{ACDE}], [C_{BCDE}], [C_{ABCDE}]
14	31	[A], [B], [C], [D], [E], [C_{AB}], [C_{AC}], [C_{AD}], [C_{AE}], [C_{BC}], [C_{BD}], [C_{BE}], [C_{CD}], [C_{CE}], [C_{DE}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABE}], [C_{ACE}], [C_{ADE}], [C_{BCE}],[C_{BDE}], [C_{CDE}], [C_{ABCD}], [C_{ABCE}], [C_{ABDE}], [C_{ACDE}], [C_{BCDE}], [C_{ABCDE}]
15	18	[A, C], [A, D], [B, C], [B, D], [C_{AC}], [C_{AD}], [C_{BC}], [C_{BD}], [C, C_{AB}], [D, C_{AB}], [A, C_{CD}], [B, C_{CD}], [C_{BCD}], [C_{ACD}], [C_{AB}, C_{CD}], [C_{ABD}], [C_{ABC}], [C_{ABCD}]
16	19	[A, C], [B, D], [C_{AC}], [C_{BD}], [A, C_{BC}], [D, C_{BC}], [B, C_{CD}], [A, C_{CD}], [C, C_{AB}], [D, C_{AB}], [B, C_{AD}], [C, C_{AD}], [C_{AB}, C_{CD}], [C_{BC}, C_{AD}], [C_{BCD}], [C_{ACD}], [C_{ABD}], [C_{ABC}], [C_{ABCD}]

Table B-1. Minimal cutsets for common cause groups for various configurations (continued).

Case	Number of Cutsets	Minimal Cutsets
17	203	[A, B, C, D, E, F], [A, B, C, D, C_{EF}], [C_{AB}, C, D, E, F], [A, B, C_{CF}, D, E], [A, B, C, C_{DF}, E], [C_{AC}, B, D, E, F], [A, B, C_{CD}, E, F], [A, C_{BD}, C, E, F], [A, C_{BC}, D, E, F], [C_{AD}, B, C, E, F], [A, B, C, C_{DE}, F], [C_{AE}, B, C, D, F], [A, C_{BE}, C, D, F], [C_{AF}, B, C, D, E], [A, B, C_{CE}, D, F], [A, C_{BF}, C, D, E], [A, C_{BCF}, D, E], [C_{ACF}, B, D, E], [A, C_{BDF}, C, E], [A, B, C_{CDE}, F], [C_{ACD}, B, E, F], [C_{AEF}, B, C, D], [C_{ABF}, C, D, E], [A, B, C, C_{DEF}], [A, C_{BEF}, C, D], [C_{ABD}, C, E, F], [C_{ABE}, C, D, F], [A, B, C_{CEF}, D], [A, C_{BCD}, E, F], [A, B, C_{CDF}, E], [C_{ACE}, B, D, F], [A, C_{BDE}, C, F], [C_{ADE}, B, C, F], [C_{ADF}, B, C, E], [C_{ABC}, D, E, F], [A, C_{BCE}, D, F], [C_{AF}, B, C_{CE}, D], [C_{AE}, B, C, C_{DF}], [A, B, C_{CF}, C_{DE}], [A, C_{BC}, D, C_{EF}], [A, C_{BD}, C_{CF}, E], [A, C_{BF}, C, C_{DE}], [A, C_{BD}, C, C_{EF}], [C_{AD}, B, C, C_{EF}], [C_{AE}, B, C_{CF}, D], [C_{AD}, C_{BF}, C, E], [C_{AF}, C_{BC}, D, E], [C_{AF}, B, C, C_{DE}], [C_{AB}, C, D, C_{EF}], [A, B, C_{CD}, C_{EF}], [C_{AB}, C, C_{DE}, F], [A, C_{BF}, C_{CE}, D], [C_{AD}, B, C_{CF}, E], [A, C_{BC}, C_{DE}, F], [C_{AF}, C_{BE}, C, D], [C_{AD}, C_{BE}, C, F], [C_{AF}, C_{BD}, C, E], [A, C_{BC}, C_{DF}, E], [A, C_{BE}, C_{CD}, F], [C_{AF}, B, C_{CD}, E], [A, C_{BE}, C, C_{DF}], [C_{AE}, C_{BF}, C, D], [C_{AC}, C_{BF}, D, E], [C_{AB}, C_{CE}, D, F], [C_{AC}, B, C_{DE}, F], [C_{AD}, B, C_{CE}, F], [C_{AB}, C_{CF}, D, E], [C_{AC}, B, D, C_{EF}], [C_{AC}, B, C_{DF}, E], [A, C_{BD}, C_{CE}, F], [C_{AB}, C_{CD}, E, F], [C_{AC}, C_{BD}, E, F], [C_{AD}, C_{BC}, E, F], [A, B, C_{CE}, C_{DF}], [C_{AE}, B, C_{CD}, F], [C_{AB}, C, C_{DF}, E], [C_{AE}, C_{BC}, D, F], [A, C_{BF}, C_{CD}, E], [C_{AC}, C_{BE}, D, F], [A, C_{BE}, C_{CF}, D], [C_{AE}, C_{BD}, C, F], [C_{ABDF}, C_{CE}], [C_{ACEF}, C_{BD}], [C_{ABCF}, C_{DE}], [C_{AC}, C_{BDEF}], [C_{ABDE}, C_{CF}], [C_{ABEF}, C_{CD}], [C_{AE}, C_{BCDF}], [C_{AF}, C_{BCDE}], [C_{ADEF}, C_{BC}], [C_{ACDE}, C_{BF}], [C_{AD}, C_{BCEF}], [C_{AB}, C_{CDEF}], [C_{ACDF}, C_{BE}], [C_{ABCE}, C_{DF}], [C_{ABCD}, C_{EF}], [C_{ACD}, C_{BEF}], [C_{ABF}, C_{CDE}], [C_{ABD}, C_{CEF}], [C_{ACE}, C_{BDF}], [C_{ADE}, C_{BCF}], [C_{ADF}, C_{BCE}], [C_{ACF}, C_{BDE}], [C_{ABE}, C_{CDF}], [C_{ABC}, C_{DEF}], [C_{AEF}, C_{BCD}], [A, C_{BCDEF}], [C_{ABDEF}, C], [C_{ABCEF}, D], [C_{ACDEF}, B], [C_{ABCDF}, E], [C_{ABCDE}, F], [C_{AB}, C_{CE}, C_{DF}], [C_{AE}, C_{BC}, C_{DF}], [C_{AC}, C_{BE}, C_{DF}], [C_{AD}, C_{BE}, C_{CF}], [C_{AE}, C_{BF}, C_{CD}], [C_{AD}, C_{BF}, C_{CE}], [C_{AE}, C_{BD}, C_{CF}], [C_{AB}, C_{CD}, C_{EF}], [C_{AC}, C_{BD}, C_{EF}], [C_{AF}, C_{BD}, C_{CE}], [C_{AF}, C_{BC}, C_{DE}], [C_{AB}, C_{CF}, C_{DE}], [C_{AD}, C_{BC}, C_{EF}], [C_{AF}, C_{BE}, C_{CD}], [C_{AC}, C_{BF}, C_{DE}], [C_{ACDE}, B, F], [A, C_{BCDE}, F], [A, C_{BDEF}, C], [C_{ACDF}, B, E], [A, B, C_{CDEF}], [C_{ADEF}, B, C], [C_{ABCF}, D, E], [C_{ABEF}, C, D], [C_{ACEF}, B, D], [C_{ABDF}, C, E], [C_{ABDE}, C, F], [C_{ABCE}, D, F], [C_{ABCD}, E, F], [A, C_{BCEF}, D], [A, C_{BCDF}, E], [A, C_{BCF}, C_{DE}], [C_{ADE}, C_{BF}, C], [C_{ACE}, C_{BF}, D], [C_{ABD}, C_{CE}, F], [C_{ABE}, C_{CD}, F], [C_{ADE}, B, C_{CF}], [C_{AF}, C_{BCE}, D], [C_{AEF}, B, C_{CD}], [C_{ABD}, C_{CF}, E], [A, C_{BDE}, C_{CF}], [C_{ACF}, C_{BE}, D], [C_{ACF}, B, C_{DE}], [C_{ADF}, C_{BC}, E], [C_{AEF}, C_{BD}, C], [C_{ABC}, C_{DF}, E], [C_{ABF}, C_{CE}, D], [C_{AD}, B, C_{CEF}], [C_{AE}, C_{BDF}, C], [C_{ADE}, C_{BC}, F], [C_{AF}, C_{BCD}, E], [C_{AE}, C_{BCD}, F], [C_{ABF}, C, C_{DE}], [A, C_{BE}, C_{CDF}], [A, C_{BF}, C_{CDE}], [C_{ABC}, D, C_{EF}], [C_{ADF}, B, C_{CE}], [C_{AEF}, C_{BC}, D], [C_{ACD}, B, C_{EF}], [A, C_{BC}, C_{DEF}], [C_{AD}, C_{BEF}, C], [C_{AF}, B, C_{CDE}], [C_{AC}, B, C_{DEF}], [C_{ADF}, C_{BE}, C], [C_{AB}, C_{CDE}, F], [A, C_{BCE}, C_{DF}], [C_{ACE}, B, C_{DF}], [C_{AC}, C_{BEF}, D], [A, C_{BCD}, C_{EF}], [C_{ABD}, C, C_{EF}], [C_{ABE}, C_{CF}, D], [A, C_{BD}, C_{CEF}], [C_{AB}, C_{CDF}, E], [C_{AD}, C_{BCF}, E], [C_{ACD}, C_{BE}, F], [C_{AC}, C_{BDE}, F], [C_{AB}, C, C_{DEF}], [C_{AE}, C_{BCF}, D], [C_{AC}, C_{BDF}, E], [C_{AF}, C_{BDE}, C], [A, C_{BDF}, C_{CE}], [C_{ABC}, C_{DE}, F], [C_{ACD}, C_{BF}, E], [C_{ACF}, C_{BD}, E], [C_{ABF}, C_{CD}, E], [C_{ACE}, C_{BD}, F], [C_{AD}, C_{BCE}, F], [A, C_{BEF}, C_{CD}], [C_{ABE}, C, CDF], [C_{AE}, B, C_{CDF}], [C_{AB}, C_{CEF}, D], [C_{ABCDEF}]

Table B-1. Minimal cutsets for common cause groups for various configurations (continued).

CASE	NUMBER OF CUTSETS	MINIMAL CUTSETS
18	353	[B, C, D, E, F], [A, C, D, E, F], [A, B, D, E, F], [A, B, C, E, F], [A, B, C, D, F], [A, B, C, D, E], [C_{BC}, D, E, F], [C_{AC}, D, E, F], [C_{AB}, D, E, F], [B, C_{CD}, E, F], [A, C_{CD}, E, F], [C_{BD}, C, E, F], [C_{AD}, C, E, F], [C_{AB}, C, E, F], [A, C_{BD}, E, F], [A, C_{BC}, E, F], [C_{AD}, B, E, F], [C_{AC}, B, E, F], [B, C, C_{DE}, F], [A, C, C_{DE}, F], [A, B, C_{DE}, F], [B, C_{CE}, D, F], [A, C_{CE}, D, F], [C_{BE}, C, D, F], [C_{AE}, C, D, F], [C_{AB}, C, D, F], [A, C_{BE}, D, F], [A, C_{BC}, D, F], [C_{AE}, B, D, F], [C_{AC}, B, D, F], [A, B, C_{CE}, F], [A, B, C_{CD}, F], [A, C_{BE}, C, F], [A, C_{BD}, C, F], [C_{AE}, B, C, F], [C_{AD}, B, C, F], [B, C, D, C_{EF}], [A, C, D, C_{EF}], [A, B, D, C_{EF}], [A, B, C, C_{EF}], [A, B, C_{DF}, E], [B, C, C_{DF}, E], [A, C, C_{DF}, E], [B, C_{CF}, D, E], [A, C_{CF}, D, E], [C_{BF}, C, D, E], [C_{AF}, C, D, E], [C_{AB}, C, D, E], [A, C_{BF}, D, E], [A, C_{BC}, D, E], [C_{AF}, B, D, E], [C_{AC}, B, D, E], [A, B, C_{CF}, E], [A, B, C_{CD}, E], [A, C_{BF}, C, E], [A, C_{BD}, C, E], [C_{AF}, B, C, E], [C_{AD}, B, C, E], [A, B, C, C_{DF}], [A, B, C, C_{DE}], [A, B, C_{CF}, D], [A, B, C_{CE}, D], [A, C_{BF}, C, D], [A, C_{BE}, C, D], [C_{AF}, B, C, D], [C_{AE}, B, C, D], [C_{BCD}, E, F], [C_{ACD}, E, F], [C_{ABD}, E, F], [C_{ABC}, E, F], [C_{BCE}, D, F], [C_{ACE}, D, F], [C_{ABE}, D, F], [C_{ABC}, D, F], [C_{BDE}, C, F], [B, C_{CDE}, F], [A, C_{CDE}, F], [C_{ADE}, C, F], [C_{ABE}, C, F], [C_{ABD}, C, F], [A, C_{BDE}, F], [A, C_{BCE}, F], [A, C_{BCD}, F], [C_{ADE}, B, F], [C_{ACE}, B, F], [C_{ACD}, B, F], [C_{BCF}, D, E], [C_{ACF}, D, E], [C_{ABF}, D, E], [C_{ABC}, D, E], [B, C_{CEF}, D], [A, C_{CEF}, D], [B, C_{CDF}, E], [C_{BDF}, C, E], [C_{ADF}, C, E], [C_{ABF}, C, E], [B, C, C_{DEF}], [A, C, C_{DEF}], [A, B, C_{DEF}], [C_{ABD}, C, E], [C_{BEF}, C, D], [C_{AEF}, C, D], [C_{ABF}, C, D], [A, C_{BEF}, D], [C_{ABE}, C, D], [A, C_{CDF}, E], [A, C_{BDF}, E], [C_{ADF}, B, E], [A, C_{BCF}, E], [A, C_{BDF}, C], [A, C_{BEF}, C], [A, C_{BDE}, C], [C_{AEF}, B, D], [C_{ACF}, B, D], [C_{ACE}, B, D], [C_{AEF}, B, C], [C_{ADF}, B, C], [C_{ADE}, B, C], [A, C_{BCD}, E], [A, B, C_{CEF}], [A, C_{BCF}, D], [A, C_{BCE}, D], [C_{ACF}, B, E], [C_{ACD}, B, E], [A, B, C_{CDF}], [A, B, C_{CDE}], [C_{BC}, C_{DE}, F], [C_{AC}, C_{DE}, F], [C_{AB}, C_{DE}, F], [C_{BD}, C_{CE}, F], [C_{AD}, C_{CE}, F], [C_{AB}, C_{CE}, F], [C_{BE}, C_{CD}, F], [C_{AE}, C_{CD}, F], [C_{AB}, C_{CD}, F], [C_{AD}, C_{BE}, F], [C_{AC}, C_{BE}, F], [C_{AE}, C_{BD}, F], [C_{AC}, C_{BD}, F], [C_{AE}, C_{BC}, F], [C_{AD}, C_{BC}, F], [C_{BC}, D, C_{EF}], [C_{AC}, D, C_{EF}], [C_{AB}, D, C_{EF}], [B, C_{CD}, C_{EF}], [A, C_{CD}, C_{EF}], [C_{BD}, C, C_{EF}], [C_{AD}, C, C_{EF}], [C_{AB}, C, C_{EF}], [A, C_{BD}, C_{EF}], [A, C_{BC}, C_{EF}], [C_{AD}, B, C_{EF}], [C_{AC}, B, C_{EF}], [C_{BC}, C_{DF}, E], [C_{AC}, C_{DF}, E], [C_{AB}, C_{DF}, E], [C_{BD}, C_{CF}, E], [C_{AD}, C_{CF}, E], [C_{AB}, C_{CF}, E], [C_{BF}, C_{CD}, E], [C_{AF}, C_{CD}, E], [C_{AB}, C_{CD}, E], [C_{AD}, C_{BF}, E], [C_{AC}, C_{BF}, E], [C_{AF}, C_{BD}, E], [C_{AC}, C_{BD}, E], [C_{AF}, C_{BC}, E], [C_{AD}, C_{BC}, E], [B, C_{CE}, C_{DF}], [A, C_{CE}, C_{DF}], [C_{BE}, C, C_{DF}], [C_{AE}, C, C_{DF}], [C_{AB}, C, C_{DF}], [A, C_{BE}, C_{DF}], [A, C_{BC}, C_{DF}], [C_{AE}, B, C_{DF}], [C_{AC}, B, C_{DF}], [B, C_{CF}, C_{DE}], [A, C_{CF}, C_{DE}], [C_{BF}, C, C_{DE}], [C_{AF}, C, C_{DE}], [C_{AB}, C, C_{DE}], [A, C_{BF}, C_{DE}], [A, C_{BC}, C_{DE}], [C_{AF}, B, C_{DE}], [C_{AC}, B, C_{DE}], [C_{BE}, C_{CF}, D], [C_{AE}, C_{CF}, D], [C_{AB}, C_{CF}, D], [C_{BF}, C_{CE}, D], [C_{AF}, C_{CE}, D], [C_{AB}, C_{CE}, D], [C_{AE}, C_{BF}, D], [C_{AC}, C_{BF}, D], [C_{AF}, C_{BE}, D], [C_{AC}, C_{BE}, D], [C_{AF}, C_{BC}, D], [C_{AE}, C_{BC}, D], [A, C_{BE}, C_{CF}], [A, C_{BD}, C_{CF}], [C_{AE}, B, C_{CF}], [C_{AD}, B, C_{CF}], [A, C_{BF}, C_{CE}], [A, C_{BD}, C_{CE}], [C_{AF}, B, C_{CE}], [C_{AD}, B, C_{CE}], [A, C_{BF}, C_{CD}], [A, C_{BE}, C_{CD}], [C_{AF}, B, C_{CD}], [C_{AE}, B, C_{CD}], [C_{AE}, C_{BF}, C], [C_{AD}, C_{BF}, C], [C_{AF}, C_{BE}, C], [C_{AD}, C_{BE}, C], [C_{AF}, C_{BD}, C], [C_{AE}, C_{BD}, C], [C_{AB}, C_{CD}, C_{EF}], [C_{AB}, C_{CE}, C_{DF}], [C_{AB}, C_{CF}, C_{DE}], [C_{AC}, C_{BD}, C_{EF}], [C_{AC}, C_{BE}, C_{DF}], [C_{AC}, C_{BF}, C_{DE}], [C_{AD}, C_{BC}, C_{EF}], [C_{AD}, C_{BE}, C_{CF}], [C_{AD}, C_{BF}, C_{CE}], [C_{AE}, C_{BC}, C_{DF}], [C_{AE}, C_{BD}, C_{CF}], [C_{AE}, C_{BF}, C_{CD}], [C_{AF}, C_{BC}, C_{DE}], [C_{AF}, C_{BD}, C_{CE}], [C_{AF}, C_{BE}, C_{CD}], [C_{BCD}, C_{EF}], [C_{ACD}, C_{EF}], [C_{ABD}, C_{EF}], [C_{ABC}, C_{EF}], [C_{BCE}, C_{DF}], [C_{ACE}, C_{DF}], [C_{ABE}, C_{DF}], [C_{ABC}, C_{DF}], [C_{BC}, C_{DEF}], [C_{AC}, C_{DEF}], [C_{AB}, C_{DEF}], [C_{BCF}, C_{DE}], [C_{ACF}, C_{DE}], [C_{ABF}, C_{DE}], [C_{ABC}, C_{DE}], [C_{BDE}, C_{CF}], [C_{ADE}, C_{CF}], [C_{ABE}, C_{CF}], [C_{ABD}, C_{CF}], [C_{BD}, C_{CEF}], [C_{AD}, C_{CEF}], [C_{AB}, C_{CEF}], [C_{BDF}, C_{CE}], [C_{ADF}, C_{CE}], [C_{ABF}, C_{CE}], [C_{ABD}, C_{CE}], [C_{BE}, C_{CDF}], [C_{AE}, C_{CDF}], [C_{AB}, C_{CDF}], [C_{BF}, C_{CDE}], [C_{AF}, C_{CDE}], [C_{AB}, C_{CDE}], [C_{BEF}, C_{CD}], [C_{AEF}, C_{CD}], [C_{ABF}, C_{CD}], [C_{ABE}, C_{CD}], [C_{ADE}, C_{BF}], [C_{ACE}, C_{BF}], [C_{ACD}, C_{BF}], [C_{AD}, C_{BEF}], [C_{AC}, C_{BEF}], [C_{ADF}, C_{BE}], [C_{ACF}, C_{BE}], [C_{ACD}, C_{BE}], [C_{AE}, C_{BDF}], [C_{AC}, C_{BDF}], [C_{AF}, C_{BDE}], [C_{AC}, C_{BDE}], [C_{AEF}, C_{BD}], [C_{ACF}, C_{BD}], [C_{ACE}, C_{BD}], [C_{AE}, C_{BCF}], [C_{AD}, C_{BCF}], [C_{AF}, C_{BCE}], [C_{AD}, C_{BCE}], [C_{AF}, C_{BCD}], [C_{AE}, C_{BCD}], [C_{AEF}, C_{BC}], [C_{ADF}, C_{BC}], [C_{ADE}, C_{BC}], [C_{ABC}, C_{DEF}], [C_{ABD}, C_{CEF}], [C_{ABE}, C_{CDF}], [C_{ABF}, C_{CDE}], [C_{ACD}, C_{BEF}], [C_{ACE}, C_{BDF}], [C_{ACF}, C_{BDE}], [C_{ADE}, C_{BCF}], [C_{ADF}, C_{BCE}], [C_{AEF}, C_{BCD}], [C_{AD}, C_{BCEF}], [C_{AC}, C_{BDEF}], [C_{AB}, C_{CDEF}], [C_{ABEF}, C_{CD}], [C_{ACDE}, C_{BF}], [C_{ABDF}, C_{CE}], [C_{ABDE}, C_{CF}], [C_{ABCE}, C_{DF}], [C_{ABCD}, C_{EF}], [C_{ACDF}, C_{BE}], [C_{ACEF}, C_{BD}], [C_{AE}, C_{BCDF}], [C_{AF}, C_{BCDE}], [C_{ADE}F, C_{CD}], [C_{ADEF}, C_{BC}], [A, C_{BCEF}], [A, C_{BCDF}], [A, C_{BDEF}], [A, C_{CDEF}], [A, C_{BCDE}], [C_{BCDE}, F], [C_{ACDE}, F], [C_{ABDE}, F], [C_{ABCE}, F], [C_{ABCD}, F], [C_{BCDF}, E], [C_{ACDF}, E], [C_{ABDF}, E], [C_{ABCF}, E], [C_{ABCD}, E], [C_{BCEF}, D], [C_{ACEF}, D], [C_{ABEF}, D], [C_{ABCF}, D], [C_{ABCE}, D], [C_{BDEF}, C], [C_{ADEF}, C], [C_{ABEF}, C], [C_{ABDF}, C], [C_{ABDE}, C], [C_{ADEF}, B], [C_{ACEF}, B], [C_{ACDF}, B], [C_{ACDE}, B], [B, C_{CDEF}], [C_{BCDEF}], [C_{ACDEF}], [C_{ABDEF}], [C_{ABCEF}], [C_{ABCDF}], [C_{ABCDE}], [C_{ABCDEF}]

Table B-1. Minimal cutsets for common cause groups for various configurations (continued).

Case	Number of Cutsets	Minimal Cutsets
19	302	[A, B, C, D], [A, B, C, E], [A, B, C, F], [A, B, D, E], [A, B, D, F], [A, B, E, F], [A, C, D, E], [A, , D, F], [A, C, E, F], [A, D, E, F], [B, C, D, E], [B, C, D, F], [B, C, E, F], [B, D, E, F], [C, D, E, F], [A, B, C_{CD}], [A, B, C_{CE}], [A, B, C_{CF}], [A, B, C_{DE}], [A, B, C_{DF}], [A, B, C_{EF}], [A, C, C_{BD}], [A, C, C_{BE}], [A, C, C_{BF}], [A, C, C_{DE}], [A, C, C_{DF}], [A, C, C_{EF}], [A, D, C_{BC}], [A, D, C_{BE}], [A, D, C_{BF}], [A, D, C_{CE}], [A, D, C_{CF}], [A, D, C_{EF}], [A, E, C_{BC}], [A, E, C_{BD}], [A, E, C_{BF}], [A, E, C_{CD}], [A, E, C_{CF}], [A, E, C_{DF}], [A, F, C_{BC}], [A, F, C_{BD}], [A, F, C_{BE}], [A, F, C_{CD}], [A, F, C_{CE}], [A, F, C_{DE}], [B, C, C_{AD}], [B, C, C_{AE}], [B, C, C_{AF}], [B, C, C_{DE}], [B, C, C_{DF}], [B, C, C_{EF}], [B, D, C_{AC}], [B, D, C_{AE}], [B, D, C_{AF}], [B, D, C_{CE}], [B, D, C_{CF}], [B, D, C_{EF}], [B, E, C_{AC}], [B, E, C_{AD}], [B, E, C_{AF}], [B, E, C_{CD}], [B, E, C_{CF}], [B, E,C_{DF}], [B, F, C_{AC}], [B, F, C_{AD}], [B, F, C_{AE}], [B, F, C_{CD}], [B, F, C_{CE}], [B, F, C_{DE}], [C, D, C_{AB}], [C, D, C_{AE}], [C, D, C_{AF}], [C, D, C_{BE}], [C, D, C_{BF}], [C, D, C_{EF}], [C, E, C_{AB}], [C, E, C_{AD}], [C, E, C_{AF}], [C, E, C_{BD}], [C, E, C_{BF}], [C, E, C_{DF}], [C, F, C_{AB}], [C, F, C_{AD}], [C, F, C_{AE}], [C, F, C_{BD}], [C, F, C_{BE}], [C, F, C_{DE}], [D, E, C_{AB}], [D, E, C_{AC}], [D, E, C_{AF}], [D, E, C_{BF}], [D, E, C_{CF}], [D, F, C_{AB}], [D, F, C_{AC}], [D, F, C_{AE}], [D, F, C_{BC}], [D, F, C_{BC}], [D, F, C_{BE}], [D, F, C_{CE}], [E, F, C_{AB}], [E, F, C_{AC}], [E, F, C_{AD}], [E, F, C_{BC}], [E, F, C_{BD}], [E, F, C_{CD}], [A, C_{BCD}], [A, C_{BCE}], [A, C_{BCF}], [A, C_{BDE}], [A, C_{BDF}], [A, C_{BEF}], [A, C_{CDE}], [A, C_{CDF}], [A, C_{CEF}], [A, C_{DEF}], [B, C_{ACD}], [B, C_{ACE}], [B, C_{ACF}], [B, C_{ADE}], [B, C_{ADF}], [B, C_{AEF}], [B, C_{CDE}], [B, C_{CDF}], [B, C_{CEF}], [B, C_{DEF}], [C, C_{ABD}], [C, C_{ABE}], [C, C_{ABF}], [C, C_{ADE}], [C, C_{ADF}], [C, C_{AEF}], [C, C_{BDE}], [C, C_{BDF}], [C, C_{BEF}], [C, C_{DEF}], [D, C_{ABC}], [D, C_{ABE}], [D, C_{ABF}], [D, C_{ACE}], [D, C_{ACF}], [D, C_{AEF}], [D, C_{BCE}], [D, C_{BCF}], [D, C_{BEF}], [D, C_{CEF}], [E, C_{ABC}], [E, C_{ABD}], [E, C_{ABF}], [E, C_{ACD}], [E, C_{ACF}], [E, C_{ADF}], [E, C_{BCD}], [E, C_{BCF}], [E, C_{BDF}], [E, C_{CDF}], [F, C_{ABC}], [F, C_{ABD}], [F, C_{ABE}], [F, C_{ACD}], [F, C_{ACE}], [F, C_{ADE}], [F, C_{BCD}], [F, C_{BCE}], [F, C_{BDE}], [F, C_{CDE}], [C_{AB}, C_{CD}], [C_{AB}, C_{CE}], [C_{AB}, C_{CF}], [C_{AB}, C_{DE}], [C_{AB}, C_{DF}], [C_{AB}, C_{EF}], [C_{AC}, C_{BD}], [C_{AC}, C_{BE}], [C_{AC}, C_{BF}], [C_{AC}, C_{DE}], [C_{AC}, C_{DF}], [C_{AC}, C_{EF}], [C_{AD}, C_{BC}], [C_{AD}, C_{BE}], [C_{AD}, C_{BF}], [C_{AD}, C_{CE}], [C_{AD}, C_{CF}], [C_{AD}, C_{EF}], [C_{AE}, C_{BC}], [C_{AE}, C_{BD}], [C_{AE}, C_{BF}], [C_{AE}, C_{CD}], [C_{AE}, C_{CF}], [C_{AE}, C_{DF}], [C_{AF}, C_{BC}], [C_{AF}, C_{BD}], [C_{AF}, C_{BE}], [C_{AF}, C_{CD}], [C_{AF}, C_{CE}], [C_{AF}, C_{DE}], [C_{BC}, C_{DE}], [C_{BC}, C_{DF}], [C_{BC}, C_{EF}], [C_{BD}, C_{CE}], [C_{BD}, C_{CF}], [C_{BD}, C_{EF}], [C_{BE}, C_{CD}], [C_{BE}, C_{CF}], [C_{BE}, C_{DF}], [C_{BF}, C_{CD}], [C_{BF}, C_{CE}], [C_{BF}, C_{DE}], [C_{CD}, C_{EF}], [C_{CE}, C_{DF}], [C_{CF}, C_{DE}], [C_{AB}, C_{CDE}], [C_{AB}, C_{CDF}], [C_{AB}, C_{CEF}], [C_{AB}, C_{DEF}], [C_{AC}, C_{BDE}], [C_{AC}, C_{BDF}], [C_{AC}, C_{BEF}], [C_{AC}, C_{DEF}], [C_{AD}, C_{BCE}], [C_{AD}, C_{BCF}], [C_{AD}, C_{BEF}], [C_{AD}, C_{CEF}], [C_{AE}, C_{BCD}], [C_{AE}, C_{BCF}], [C_{AE}, C_{BDF}], [C_{AE}, C_{CDF}], [C_{AF}, C_{BCD}], [C_{AF}, C_{BCE}], [C_{AF}, C_{BDE}], [C_{AF}, C_{CDE}], [C_{BC}, C_{ADE}], [C_{BC}, C_{ADF}], [C_{BC}, C_{AEF}], [C_{BC}, C_{DEF}], [C_{BD}, C_{ACE}], [C_{BD}, C_{ACF}], [C_{BD}, C_{AEF}], [C_{BD}, C_{CEF}], [C_{BE}, C_{ACD}], [C_{BE}, C_{ACF}], [C_{BE}, C_{ADF}], [C_{BE}, C_{CDF}], [C_{BF}, C_{ACD}], [C_{BF}, C_{ACE}], [C_{BF}, C_{ADE}], [C_{BF}, C_{CDE}], [C_{CD}, C_{ABE}], [C_{CD}, C_{ABF}], [C_{CD}, C_{AEF}], [C_{CD}, C_{BEF}], [C_{CE}, C_{ABD}], [C_{CE}, C_{ABF}], [C_{CE}, C_{ADF}], [C_{CE}, C_{BDF}], [C_{CF}, C_{ABD}], [C_{CF}, C_{ABE}], [C_{CF}, C_{ADE}], [C_{CF}, C_{BDE}], [C_{DE}, C_{ABC}], [C_{DE}, C_{ABF}], [C_{DE}, C_{ACF}], [C_{DE}, C_{BCF}], [C_{DF}, C_{ABC}], [C_{DF}, C_{ABE}], [C_{DF}, C_{ACE}], [C_{DF}, C_{BCE}], [C_{EF}, C_{ABC}], [C_{EF}, C_{ABD}], [C_{EF}, C_{ACD}], [C_{EF}, C_{BCD}], [C_{ABC}, C_{DEF}], [C_{ABD}, C_{CEF}], [C_{ABE}, C_{CDF}], [C_{ABF}, C_{CDE}], [C_{ACD}, C_{BEF}], [C_{ACE}, C_{BDF}], [C_{ACF}, C_{BDE}], [C_{ADE}, C_{BCF}], [C_{ADF}, C_{BCE}], [C_{AEF}, C_{BCD}], [C_{ABCD}], [C_{ABCE}], [C_{ABCF}], [C_{ABDE}], [C_{ABDF}], [C_{ABEF}], [C_{ACDE}], [C_{ACDF}], [C_{ACEF}], [C_{ADEF}], [C_{BCDE}], [C_{BCDF}], [C_{BCEF}], [C_{BDEF}], [C_{CDEF}], [C_{ABCDE}], [C_{ABCDF}], [C_{ABCEF}], [C_{ABDEF}], [C_{ACDEF}], [C_{BCDEF}], [C_{ABCDEF}]]

Table B-1. Minimal cutsets for common cause groups for various configurations (continued).

CASE	NUMBER OF CUTSETS	MINIMAL CUTSETS
20	167	[A, B, C], [A, B, D], [A, B, E], [A, B, F], [A, C, D], [A, C, E], [A, C, F], [A, D, E], [A, D, F], [A, E, F], [B, C, D], [B, C, E], [B, C, F], [B, D, E], [B, D, F], [B, E, F], [C, D, E], [C, D, F], [C, E, F], [D, E, F], [A, C_{BC}], [A, C_{BD}], [A, C_{BE}], [A, C_{BF}], [A, C_{CD}], [A, C_{CE}], [A, C_{CF}], [A, C_{DE}], [A, C_{DF}], [A, C_{EF}], [B, C_{AC}], [B, C_{AD}], [B, C_{AE}], [B, C_{AF}], [B, C_{CD}], [B, C_{CE}], [B, C_{CF}], [B, C_{DE}], [B, C_{DF}], [B, C_{EF}], [C, C_{AB}], [C, C_{AD}],[C, C_{AE}], [C, C_{AF}], [C, C_{BD}], [C, C_{BE}], [C, C_{BF}], [C, C_{DE}], [C, C_{DF}], [C, C_{EF}], [D, C_{AB}], [D, C_{AC}], [D, C_{AE}], [D, C_{AF}], [D, C_{BC}], [D, C_{BE}], [D, C_{BF}], [D, C_{CE}], [D, C_{CF}], [D, C_{EF}], [E, C_{AB}], [E, C_{AC}], [E, C_{AD}], [E, C_{AF}], [E, C_{BC}], [E, C_{BD}], [E, C_{BF}], [E, C_{CD}], [E, C_{CF}], [E, C_{DF}], [F, C_{AB}], [F, C_{AC}], [F, C_{AD}], [F, C_{AE}], [F, C_{BC}], [F, C_{BD}], [F, C_{BE}], [F, C_{CD}], [F, C_{CE}], [F, C_{DE}], [C_{AB}, C_{CD}], [C_{AB}, C_{CE}], [C_{AB}, C_{CF}], [C_{AB}, C_{DE}], [C_{AB}, C_{DF}], [C_{AB}, C_{EF}], [C_{AC}, C_{BD}], [C_{AC}, C_{BE}], [C_{AC}, C_{BF}], [C_{AC}, C_{DE}], [C_{AC}, C_{DF}], [C_{AC}, C_{EF}], [C_{AD}, C_{BC}], [C_{AD}, C_{BE}], [C_{AD}, C_{BF}], [C_{AD}, C_{CE}], [C_{AD}, C_{CF}], [C_{AD}, C_{EF}], [C_{AE}, C_{BC}], [C_{AE}, C_{BD}], [C_{AE}, C_{BF}], [C_{AE}, C_{CD}], [C_{AE}, C_{CF}], [C_{AE}, C_{DF}], [C_{AF}, C_{BC}], [C_{AF}, C_{BD}], [C_{AF}, C_{BE}], [C_{AF}, C_{CD}], [C_{AF}, C_{CE}], [C_{AF}, C_{DE}],[C_{BC}, C_{DE}], [C_{BC}, C_{DF}], [C_{BC}, C_{EF}], [C_{BD}, C_{CE}], [C_{BD}, C_{CF}], [C_{BD}, C_{EF}], [C_{BE}, C_{CD}], [C_{BE}, C_{CF}], [C_{BE}, C_{DF}], [C_{BF}, C_{CD}], [C_{BF}, C_{CE}], [C_{BF}, C_{DE}], [C_{CD}, C_{EF}], [C_{CE}, C_{DF}], [C_{CF}, C_{DE}], [C_{ABC}], [C_{ABD}], [C_{ABE}], [C_{ABF}], [C_{ACD}], [C_{ACE}], [C_{ACF}], [C_{ADE}], [C_{ADF}], [C_{AEF}], [C_{BCD}], [C_{BCE}], [C_{BCF}], [C_{BDE}], [C_{BDF}], [C_{BEF}], [C_{CDE}], [C_{CDF}], [C_{CEF}], [C_{DEF}], [C_{ABCD}], [C_{ABCE}], [C_{ABCF}], [C_{ABDE}], [C_{ABDF}], [C_{ABEF}], [C_{ACDE}], [C_{ACDF}], [C_{ACEF}], [C_{ADEF}], [C_{BCDE}], [C_{BCDF}], [C_{BCEF}], [C_{BDEF}], [C_{CDEF}], [C_{ABCDE}], [C_{ABCDF}], [C_{ABCEF}], [C_{ABDEF}], [C_{ACDEF}], [C_{BCDEF}], [C_{ABCDEF}]
21	72	[A, B], [A, C], [A, D], [A, E], [A, F], [B, C], [B, D], [B, E], [B, F], [C, D], [C, E], [C, F], [D, E], [D, F], [E, F], [C_{AB}], [C_{AC}], [C_{AD}], [C_{AE}], [CAF], [C_{BC}], [C_{BD}], [C_{BE}], [C_{BF}], [C_{CD}], [C_{CE}], [C_{CF}], [C_{DE}], [C_{DF}], [C_{EF}], [C_{ABC}], [C_{ABD}], [C_{ABE}], [C_{ABF}], [C_{ACD}], [C_{ACE}], [C_{ACF}], [C_{ADE}], [C_{ADF}], [C_{AEF}], [C_{BCD}], [C_{BCE}], [C_{BCF}], [C_{BDE}], [C_{BDF}], [C_{BEF}], [C_{CDE}], [C_{CDF}], [C_{CEF}], [C_{DEF}], [C_{ABCD}], [C_{ABCF}], [C_{ABDE}], [C_{ABCE}], [C_{ABDF}], [C_{ABEF}], [C_{ACDE}], [C_{ACDF}], [C_{ACEF}], [C_{ADEF}], [C_{BCDE}], [C_{BCDF}], [C_{BCEF}], [C_{BDEF}], [C_{CDEF}], [C_{ABCDE}], [C_{ABCDF}], [C_{ABCEF}], [C_{ABDEF}], [C_{ACDEF}], [C_{BCDEF}], [C_{ABCDEF}]
22	63	[A], [B], [C], [D], [E], [F], [C_{AB}], [C_{AC}], [C_{AD}], [C_{AE}], [C_{AF}], [C_{BC}], [C_{BD}], [C_{BE}], [C_{BF}], [C_{CD}], [C_{CE}], [C_{CF}], [C_{DE}], [C_{DF}], [C_{EF}], [C_{ABC}], [C_{ABD}], [C_{ABE}], [C_{ABF}], [C_{ACD}], [C_{ACE}], [C_{ACF}], [C_{ADE}], [C_{ADF}], [C_{AEF}], [C_{BCD}], [C_{BCE}], [C_{BCF}], [C_{BDE}], [C_{BDF}], [C_{BEF}], [C_{CDE}], [C_{CDF}], [C_{CEF}], [C_{DEF}], [C_{ABCD}], [C_{ABCE}], [C_{ABCF}], [C_{ABDE}], [C_{ABDF}], [C_{ABEF}], [C_{ACDE}], [C_{ACDF}], [C_{ACEF}], [C_{ADEF}], [C_{BCDE}], [C_{BCDF}], [C_{BCEF}], [C_{BDEF}], [C_{CDEF}], [C_{ABCDE}], [C_{ABCDF}], [C_{ABCEF}], [C_{ABDEF}], [C_{ACDEF}], [C_{BCDEF}], [C_{ABCDEF}]

APPENDIX C

ACCOUNTING FOR COMMON CAUSE GROUP SIZE DIFFERENCE IN COMMON CAUSE PARAMETER ESTIMATION (HOW TO MAP IMPACT VECTORS)

APPENDIX C

Accounting for Common Cause Group Size Differences in Common Cause Parameter Estimation (How to Map Impact Vectors)

C.1 INTRODUCTION

One of the key elements of the procedures presented in this report is the recognition of the necessity, when reviewing data from several plants, to take account of the differences between those plants and the particular plant to be modeled in order to produce a plant-specific evaluation of common cause potential.

There are two types of differences between systems of interest in data classification: qualitative and quantitative. The former refers to physical differences in characteristics, component type operating conditions, environments, etc. The latter deals with the sizes of the common cause component group in terms of the different number of components present. The purpose of this appendix is to establish relationships among the databases associated with groups having different numbers of components; i.e., different levels of redundancy. These relationships are intended to help combine the databases in support of parameter estimation. In particular, the insights derived should provide useful guidance on how to account in parameter estimation for differences in size between the system being analyzed and those that generated the data.

The objectives of this appendix are to:

- Establish relationships between databases of systems[3] of identical components having different levels of redundancy.

- Provide guidance for interpretation of data from systems of different size from the one for which the analysis is being performed and for the assignment of impact vectors for the system of interest; in this report this is referred to as mapping up and mapping down impact vectors.

C.2 DEFINITION OF BASIC EVENTS

As an example, consider a system[1] (common cause component group) of four identical redundant components. In this four-train system, a number of different types of events can be defined in terms of a particular combination of components that fail. The total number of different basic events of this type that can be defined for a system of four components is given as

$$\sum_{j=1}^{4}\binom{4}{j} = 2^4 - 1 = 15$$

These 15 different basic events include 4 events in which 1 and only 1 component is impacted, 6 that impact 2, 4 that impact 3, and 1 that impacts all 4 components. In this scheme, each event is uniquely defined by a particular combination of components that fail. Note that all the causes that impact one specific combination of components are counted as one basic event. The specific causes are not identified a priori.

Note also that when data are collected (e.g., reports are filed to note problems identified during a system test) there is usually at most one "event" identified in each event report. On rare occasions, there may be two or more concurrent independent events covered in the report. The event classification system used

[3] In this context, system can thought of as meaning "common cause component group."

in Reference C-1 accounts for this by drawing two or more separate cause-effect logic diagrams to cover the separate events. One of the problems facing the data analyst is the need to distinguish between a single event impacting a set of components and the coincidence of multiple independent events impacting the same set of components. However, experience has shown the latter category to be much less frequent than the former.

The first question we address is: given a set of data from a four-train redundant system (common cause component group consisting of four identical components), what would the data look like for an otherwise identical system having either three, two, or one identical components; i.e., how does the level of redundancy or population of components impact the characteristics of the data in the limit of a very large number of demands in operating experience when the same set of causes are "acting" on the system?

Models of common cause events, such as the beta factor, BFR, MGL, and basic parameter models, all recognize the potential for two broad categories of event causes: independent events resulting in single component failures, and common cause events resulting in multiple component failures. In view of this general distinction, when one assumes that the occurrences of the causes of the common cause events are independent of the number of components present, it follows that the same cause may have different impacts depending on the number of components present. As a trivial example, any of the causes impacting two or more specific components in a system with two or more components could only impact one component when only one component is challenged.

The above point is illustrated quite visibly in Table C-1. In the left column are listed the 15 different basic events that could occur in a system of 4 components denoted as A, B, C, and D. Each basic event characterizes the occurrence of any cause that fails a specific set of components. Any event that could occur in a four-train system is covered by these possibilities. In the next three columns in Table C-1, each of the four-train basic events is evaluated in terms of the impact each event would have if only three, two, or one specific components were present. As the transition is made between any two adjacent columns, it is seen that any basic event in a j train system would either fail the same number of components or one less component if the same basic event were postulated to occur in a j - 1 train system. In the case of the independent events, which are covered by the basic events A_I, B_I, C_I, and D_I, the above observation is simply a reflection of the fact that the frequency of independent failures is the sum of the independent component failures rates. However, for common cause events, the situation is more complicated. Some of the common cause events take on a characteristic of the independent events in mapping downward--they impact a single component. Such events, which might be termed "latent common cause events," may appear to be independent events, but if more components were present, they could reveal their true character as common cause events. This may help to explain the observation that was made in Reference C-1 that more than 50% of the data that was collected on events involving single component effects were due to external causes (e.g., design errors, operator errors, etc.), that on other occasions produced multiple component effects. It is generally believed that most of the data in Reference C-1 came from low redundancy systems; i.e., two redundant components per system.

At this point we introduce the symmetry assumption that is incorporated into all the CCF models (β, MGL, BFR, and basic parameter). This assumption states that the probability of each basic event is independent of the specific combination of components affected; it is only dependent on the number of components failed.

Table C-1. Impact of four-train "independent" and common cause events on three, two, and one-train systems.

Event Type	Basic Events in Four-Train System (A, B, C, D)	Basic Event Probability	Impact on Three-Train System (A, B, C)*	Impact on Two-Train System (A, B)*	Impact on One-Train System (A)*
Independent	A B C D	$Q_1^{(4)}$**	A B C None	A B None None	A None None None
Common Cause Impacting Two Components	AB AC AD BC BD CD	$Q_2^{(4)}$**	AB AC A BC B C	AB A A B B None	A A A None None None
Common Cause Impacting Three Components	ABC ABD ACD BCD	$Q_3^{(4)}$**	ABC AB AC BC	AB AB A B	A A A None
Common Cause Impacting Four Components	ABCD	$Q_4^{(4)}$	ABC	AB	A

*Impact expressed in terms of the specific set of components failed by each basic event.
**Applies to each basic event within the braces.

These probabilities are the parameters of the basic parameter model that, for the four-train system, include the following:

Parameter*	Applicable Basic Events
$Q_1^{(4)}$	A_I, B_I, C_I, D_I
$Q_2^{(4)}$	C_{AB}, C_{AC}, C_{AD}, C_{BC}, C_{BD}, C_{CD}
$Q_3^{(4)}$	C_{ABC}, C_{ABD}, C_{ACD}, C_{BCD}
$Q_4^{(4)}$	C_{ABCD}

*The parameter defines the probability of each (not the total) of the indicated applicable events.

If a four-train system is challenged N times and it is assumed that a challenge results in all four trains being challenged, and if N is large, the average number of events involving a cause impacting j components, M_j, is given by

$$M_j^{(4)} = \binom{4}{j} Q_j^{(4)} N \qquad \text{(C.1)}$$

In other words, in N system challenges there are $\binom{4}{j}$ N challenges of combinations of j components and $Q_j^{(4)}$ is the probability that each of those challenges results in j-specific component failures. Evaluating Equation (C.1) for the parameters in a four-train model yields

$$M_1^{(4)} = 4Q_1^{(4)N}; \quad M_2^{(4)} = 6Q_2^{(4)N}; \quad M_3^{(4)} = 4Q_3^{(4)N}; \quad M_4^{(4)} = Q_4^{(4)N} \qquad \text{(C.2)}$$

The total database generated by N demands on the four-train system is given by

$$\text{Event Data Vector} = \left\{ M_1^{(4)}, M_2^{(4)}, M_3^{(4)}, M_4^{(4)} \right\} \qquad \text{(C.3)}$$

To simplify the subsequent development, we introduce a set of system or component group failure rates that correspond with each of the components of the event data vector

$$q_j(4) = \frac{M_j^{(4)}}{N}, \quad j = 1, 2, 3, 4 \qquad \text{(C.4)}$$

where q_j = frequency of events that occur within the four-train system resulting in j component failures (events per system demand).

The $q_j^{(4)}$ can be regarded as system failure rates and should not be confused with component failure rates. These rates provide a means of describing a database that is normalized against the number of system demands.

Returning to Table C-1 we can establish what the four-train data would look like in three, two, and one-train systems in terms of the basic event probabilities for the four-train system that on the assumption that these probabilities are in fact independent of system size, and that the system demand is equivalent to a demand on all components. On comparison of the first two columns of Table C-1, the following relationships are easily established:

$$\begin{aligned}
q_0^{(3)} &= Q_1^{(4)} = \frac{1}{4} q_1^{(4)} \\
q_1^{(3)} &= 3Q_1^{(4)} + 3Q_2^{(4)} = \frac{3}{4} q_1^{(4)} + \frac{1}{2} q_2^{(4)} \\
q_2^{(3)} &= 3Q_2^{(4)} + 3Q_3^{(4)} = \frac{1}{2} q_2^{(4)} + \frac{3}{4} q_3^{(4)} \\
q_3^{(3)} &= Q_3^{(4)} + Q_4^{(4)} = \frac{1}{4} q_3^{(4)} + q_4^{(4)}
\end{aligned} \qquad \text{(C.5)}$$

These and the remaining relationships among the databases are summarized in Table C-2. Each column of Table C-2 shows how the four-train events are distributed in smaller sized systems. The total number of basic events is conserved in each column; however, the number of events having no impact grows, moving from left to right. These latter events are essentially unobservable since data are only available when failures occur--the available data on cause events that do not produce at least one component failure are sketchy, at best.

C.3 MAPPING DOWN IMPACT VECTORS

The relationship in Table C-2 can be used to calculate impact vectors of classified events in a system of three, two, or one component, given an impact vector in any system with more components up to four. This is true because of the specific properties of the databases indicated in Table C-2. The key property is that, when moving form left to right to simulate downward mapping of data, the events are distributed in a predictable way. Take, for instance, the data, the events are distributed in a predictable way. Take, for instance, the term $n_1^{(4)}$which represents the system failure rate of single component failures in four-train systems. Now we ask the question: if one of these same events were postulated to occur in a three-train system, what is the probability that a single component failure would occur? Using the information in Table C-2:

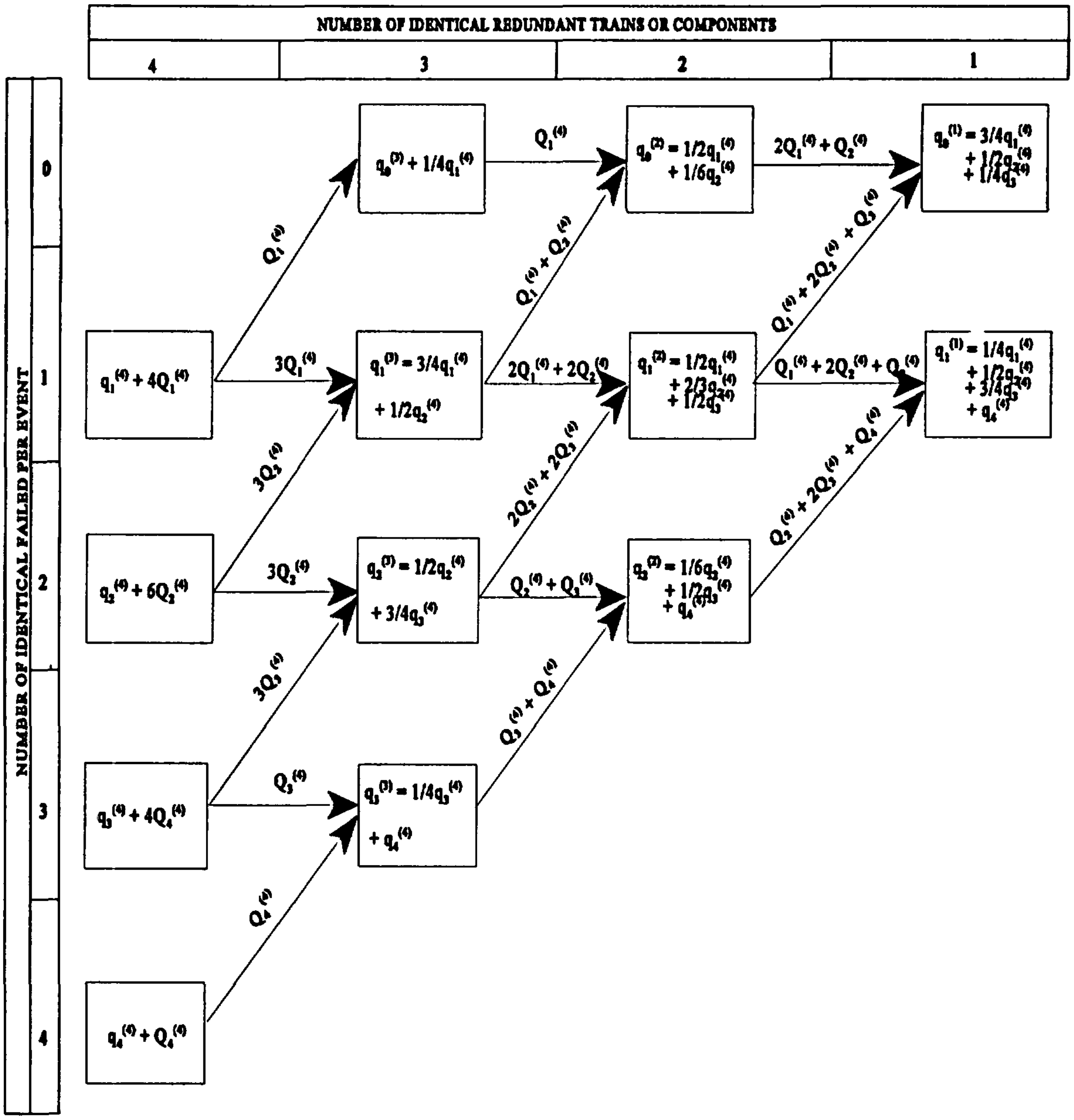
$$Pr\left\{1^{(4)} \rightarrow 1^{(3)}\right\} = \frac{3\,Q_1^{(4)}}{4\,Q_1^{(4)}} = 0.75 \qquad \text{(C.6)}$$

This probability and all the other downward mapping probabilities are independent of the underlying failure rate parameters; they are only dependent on the sizes of the systems being mapped! A complete set of formulae for mapping down data from systems having four, three, or two components to any identical system having fewer components is presented in Table C-3.

The application of these formulae to binary impact vectors (i.e., impact vectors whose entries are either zero or one) is illustrated in Table C-4 for mapping down data from four or three-train systems. This provides the basis for the formulae presented in Section C.3 for downward mapping of impact vectors. Note that, because these formulae depend on Equation C.2, they are dependent on the assumption made about the sampling scheme that produced the data.

The probability of impact of zero components is carried through these tables (C-2, C-3, and C-4) for bookkeeping purposes--to show how the event impact probability is conserved. Also, the accounting of the P_O term of the impact vector reveals important factors that must be taken into account in parameter estimation. In combining data from systems having different sizes, only the impact vector terms associated with one or more component failures are "observable;" i.e., have the potential for showing up in an event report. However, in the process of synthesizing statistics from the generic database, a picture of what the database would look like if it came from a collection of systems with the same size, conserving the probability of impacting zero components is extremely important. Take, for example, mapping set No. 4 in Table C-4, which covers the case of mapping single component failures in P_O terms shows in this case how the frequency of single component failures in the system is proportional to the number of components present. Hence, half of the $P_1^{(4)}$events would not occur in a two-train system. This factor must be reflected in parameter estimation to account for differences in system size among the systems in the database in relation to the size of the system being analyzed. To illustrate this point numerically suppose that data from systems having four, three, and two components were being used to assess a two-component system. Further, suppose that the number of single component failures observed in these systems was 40, 30, and 20, respectively. Without consideration of the zero impact effect, the data analyst would be led to interpret this data as 40 + 30 + 20 = 90 instances of component failures for use in parameter estimation. However, if

Table C-2. Average rate of occurrence* of basic events in systems as a function of system size and the number of trains failed per event.


NUMBER OF IDENTICAL REDUNDANT TRAINS OR COMPONENTS
4
3
2
1
NUMBER OF IDENTICAL FAILED PER EVENT
0
1
2
3
4
$q_0^{(3)} + 1/4q_1^{(4)}$
$Q_1^{(4)}$
$q_0^{(2)} = 1/2q_1^{(4)} + 1/6q_2^{(4)}$
$2Q_1^{(4)} + Q_2^{(4)}$
$q_0^{(1)} = 3/4q_1^{(4)} + 1/2q_2^{(4)} + 1/4q_3^{(4)}$
$Q_1^{(4)}$
$Q_1^{(4)} + Q_2^{(4)}$
$Q_1^{(4)} + 2Q_2^{(4)} + Q_3^{(4)}$
$q_1^{(4)} + 4Q_1^{(4)}$
$3Q_1^{(4)}$
$q_1^{(3)} = 3/4q_1^{(4)} + 1/2q_2^{(4)}$
$2Q_1^{(4)} + 2Q_2^{(4)}$
$q_1^{(2)} = 1/2q_1^{(4)} + 2/3q_2^{(4)} + 1/2q_3^{(4)}$
$Q_1^{(4)} + 2Q_2^{(4)} + Q_3^{(4)}$
$q_1^{(1)} = 1/4q_1^{(4)} + 1/2q_2^{(4)} + 3/4q_3^{(4)} + q_4^{(4)}$
$3Q_2^{(4)}$
$2Q_2^{(4)} + 2Q_3^{(4)}$
$Q_2^{(4)} + 2Q_3^{(4)} + Q_4^{(4)}$
$q_2^{(4)} + 6Q_2^{(4)}$
$3Q_2^{(4)}$
$q_2^{(3)} = 1/2q_2^{(4)} + 3/4q_3^{(4)}$
$Q_2^{(4)} + Q_3^{(4)}$
$q_2^{(2)} = 1/6q_2^{(4)} + 1/2q_3^{(4)} + q_4^{(4)}$
$3Q_3^{(4)}$
$Q_3^{(4)} + Q_4^{(4)}$
$q_3^{(4)} + 4Q_4^{(4)}$
$Q_3^{(4)}$
$q_3^{(3)} = 1/4q_3^{(4)} + q_4^{(4)}$
$Q_4^{(4)}$
$q_4^{(4)} + Q_4^{(4)}$

* Rates are given in units of events per system demand.

Table C-3. Formulae for mapping down event impact vectors.

		SIZE OF SYSTEM MAPPING TO (NUMBER OF IDENTICAL TRAINS)		
		3	2	1
SIZE OF SYSTEM MAPPING FROM	4	$p_0^{(3)} = p_0^{(4)*} + \frac{1}{4}p_1^{(4)}$ $p_1^{(3)} = \frac{3}{4}p_1^{(4)} + \frac{1}{2}p_2^{(4)}$ $p_2^{(3)} = \frac{1}{2}p_2^{(4)} + \frac{3}{4}p_3^{(4)}$ $p_3^{(3)} = \frac{1}{4}p_3^{(4)} + p_4^{(4)}$	$p_0^{(2)} = \frac{1}{2}p_1^{(4)} + \frac{1}{6}p_2^{(4)}$ $p_1^{(2)} = \frac{1}{2}p_1^{(4)} + \frac{2}{3}p_2^{(4)} + \frac{1}{2}p_3^{(4)}$ $p_2^{(2)} = \frac{1}{6}p_2^{(4)} + \frac{1}{2}p_3^{(4)} + p_4^{(4)}$	$p_0^{(1)} = \frac{3}{4}p_1^{(4)} + \frac{1}{2}p_2^{(4)} + \frac{1}{4}p_3^{(4)}$ $p_1^{(1)} = \frac{1}{4}p_1^{(4)} + \frac{1}{2}p_2^{(4)} + \frac{3}{4}p_3^{(4)} + p_4^{(4)}$
	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 C-4. Mapping down binary impact vectors from four-train and three-train system data.

System	Impact Vector*				
	P_0	P_1	P_2	P_3	P_4
Mapping of Event 1					
Original Four-Train System	0	0	0	0	1
Identical Three-Train System	0	0	0	1	-**
Identical Two-Train System	0	0	1	-	-
Identical One-Train System	0	1	-	-	-
Mapping of Event 2					
Original Four-Train System	0	0	0	1	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	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	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	0	0	0	0
Identical Three-Train System	1	0	0	0	-
Identical Two-Train System	1	0	0	-	-
Identical One-Train System	1	0	-	-	-

System	Impact Vector*			
	P_0	P_1	P_2	P_3
Mapping of Event 6				
Original Three-Train System	0	0	0	1
Identical Two-Train System	0	0	1	-
Identical One-Train System	0	1	-	-
Mapping of Event 7				
Original Three-Train System	0	0	1	0
Identical Two-Train System	0	.67	.33	-
Identical One-Train System	.33	.67	-	-
Mapping of Event 8				
Original Three-Train System	0	1	0	0
Identical Two-Train System	.33	.67	0	-
Identical One-Train System	.67	.33	-	-
Mapping of Event 9				
Original Three-Train System	1	0	0	0
Identical Two-Train System	1	0	0	-
Identical One-Train System	1	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 system of a smaller size than (but otherwise identical to) the "original" system are given.

**(-) means the impact category is inapplicable consideration is given to what this data would have looked like had it come from all two-component systems, the equivalent data would be interpreted (based on mapping sets 4 and 8 in Table C-4) as 40(.5) + 30(.67) + 20 = 60 occurrences of single component failure events. The numerical importance of system size mapping in the estimation of common cause parameters was first explained by Peter Doerre of Reliability Benchmark Exercise.[C-2, C-3]

C.4 MAPPING UP IMPACT VECTORS

The above discussion demonstrates 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 additional uncertainties, given that the basic assumptions on which the mapping formulae are based are accepted. Mapping up, however, is a different story. To understand this point, let us return to Table C-2. Suppose an $n_1^{(3)}$ event occurred and the system being analyzed consisted of four units. As can be seen from the table, there is some chance that, if the same event were postulated to occur in a four-train system, either one or two component failures would result. Based on the information provided in Table C-2, the following statements can be made about the probability that this event would result in one or two component failures, respectively:

$$Pr\left\{1^{(3)} \rightarrow 1^{(4)}\right\} = \frac{3Q_1^{(4)}}{3Q_1^{(4)} + 3Q_2^{(4)}} \tag{C.7}$$

$$Pr\left\{1^{(3)} \rightarrow 2^{(4)}\right\} = \frac{3Q_2^{(4)}}{3Q_1^{(4)} + 3Q_2^{(4)}} \tag{C.8}$$

Therefore, the upward mapping probabilities, unlike the downward mapping probabilities, are dependent on the underlying basic event probabilities. (Recall that the downward mapping probabilities were shown to be independent of the underlying basic event probabilities.) Therefore, it is necessary to either bring in more information about the events, or accept a greater degree of uncertainty in the case of upward mapping. In reference to the above relationships, this uncertainty corresponds with not knowing, a priori, what the underlying basic event probabilities are.

There are some aspects of the downward mapping relationships presented in Tables C-2, C-3, and C-4 that help to reduce uncertainties in upward mapping. One useful property derived from these tables is that any event involving k components in a k train system would result in either k or k + 1 component failures in a k + 1 train system, and either k, k + 1 or k + 2 in a k + 2 train system. Therefore, the possibilities for upward mapping are well defined, but the probabilities are not.

The concept that is used in the definition of the BFR common cause model can be used to try to limit the problem. 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.

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 (category 1) are 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 described below. It is only in the case of nonlethal shocks that an added element of uncertainty is introduced upon mapping upward. How each event is handled is separately described below.

C.4.1 Mapping Up Independent Events

As noted at the beginning of this appendix, the purpose of mapping impact vectors is to estimate or infer what the database of applicable events would look like if it all was generated by system of the same size (i.e., the number of components in each common cause group) as the system being analyzed. In the case of the independent events, the number of such events observed in the database is simply proportional to the number of components in the system. Therefore, if we collected data from systems of two components having some level of system experience and observed, say $M_i^{(2)}$ instances of independent events involving a single component, we should expect to see twice as many independent events, $M_i^{(4)} = 2M_i^{(2)}$, if the same amount of system experience were accumulated with identical four-component systems.

The above result is compatible with the notion that independent events are due to internal causes. If we add more components and fix the level of system experience, we add a like amount of opportunities for the occurrence of independent events. The following set of relationships directly follows from the simple assumption that the number of independent events observed in a system of size k, $M_I^{(k)}$, where k = 1, 2, or 3, is proportional to the underlying independent failure rate. What we seek to determine is the equivalent number of independent events, $M_I^{(j)}$, that we would expect to observe if the same amount of system experience were accumulated with identical systems of size j, j = 1 through 4.

$$M_i^{(j)} = \frac{j}{k} M_I^{(k)} \tag{C.9}$$

From the above relationship, the following formula is derived to estimate the equivalent number of independent events that would be observed from systems of size ℓ, given data on independent events in different size systems:

$$M_i^{(l)} = \sum_{k=1} \frac{l M_I^{(k)}}{k} \tag{C.10}$$

For the purpose of mapping impact vectors of each independent event, Equation C.9 translates into

$$p_i^{(l)} = \frac{l p_I^{(k)}}{k} \tag{C.11}$$

Because this approach adds events that were not actually observed, it artificially strengthens the database and reduces the statistical uncertainty associated with estimates of P_I. However, the impact on the uncertainty is generally negligible compared with other sources of uncertainty.

C.4.2 Mapping Up Lethal Shocks

Once an event is classified as a lethal shock, the upward mapping of its impact vector is straightforward. 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 of the system is constant and independent of system size. This is a reasonable assumption. From it the following simple relationship is derived:

$$p_l^{(l)} = p_j^{(j)}, \text{ for all l and j} \qquad \text{(C.12)}$$

Therefore, 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 ℓ component system without modification.

C.4.3 Mapping Up Nonlethal Shocks

In order to uniquely map up the effect of nonlethal shocks, it is essential to use a model that can relate the probability of failure of k or more component in terms of parameters that can be determined from measurements of numbers of failure events involving I = 0, ..., k-1 components. The only one of the models discussed which is capable of supporting this is the BFR model.

According to the BFR model, nonlethal shock failures are viewed as the result of a nonlethal shock that acts on the system at a constant rate that is independent of the system size. For each shock, there is a constant probability, ρ is the conditional probability of each component failure given a shock. The mapping up of an event is based on a subjective assessment of ρ. This assessment is performed for each event and may be different for different events. When mapping up an event from a system of size "I" to a system of size "j", j > I, the parameters of the BFR model are assumed not to change. In other words, the shock rate and the probability ρ that a component fails, given the shock occurrence, are conserved. While, as shown in Section 4.1, the BFR model is somewhat lacking in its generality (because all nonlethal events in the data are assumed to have the same shock rate and binomial parameter ρ), allowing a different assessment of the ρ parameter for each event restores the generality. The BFR model in this context is used as a way of extrapolating events, but not as an integral common cause failure model to parametize all possible events.

The BFR model is used to perform upward mapping of impact vectors according to the following procedure:

1. Write BFR equations for the system size "I" from which the data comes. For example, in mapping up from a system size I = 2,

$$\begin{aligned} n_0^{(2)} &= \mu(1-\rho)^2 \\ n_1^{(2)} &= 2\mu(1-\rho)\rho \qquad \text{(C.13)} \\ n_2^{(2)} &= \mu\rho^2 \end{aligned}$$

where $n_\ell^{(I)}$ is used in this section to represent the frequency of events that occur within an I-train system resulting in ℓ train failures due to nonlethal shocks. These equations postulate that the observed values of $n_1^{(2)}$ and $n_2^{(2)}$ were generated in a BFR process with parameters μ and ρ.

2. Write BFR equations for system size j to which the data are to be applied. For mapping up from a system size I = 2 to a system size j = 4 for example, these equations are

$$\begin{aligned} n_0^{(4)} &= \mu(1-\rho)^4 \\ n_1^{(4)} &= 4\mu(1-\rho)^3\rho \\ n_2^{(4)} &= 6\mu(1-\rho)^2\rho^2 \\ n_3^{(4)} &= 4\mu(1-\rho)\rho^3 \\ n_4^{(4)} &= \mu\rho^4 \end{aligned} \tag{C.14}$$

These equations postulate (if the μ and ρ are used from step 1) that we would have observed the values of $n_1^{(4)}$, $n_2^{(4)}$, $n_3^{(4)}$, $n_4^{(4)}$ from the same BFR process that generated the values of $n_1^{(2)}$, $n_2^{(2)}$ if the data had been collected from a four-train system.

3. Use the equations in steps 1 and 2 to derive $n^{(j)}$'s as a function of $n^{(I)}$'s. For example,

$$\begin{aligned} n_1^{(4)} &= 4\mu(1-\rho)^3\rho = \left[2\mu(1-\rho)\rho\right]\left[2(1-\rho)^2\right] \\ &= 2(1-\rho)^2 n_1^{(2)} \end{aligned} \tag{C.15}$$

In some cases, it is not clear which $n^{(I)}$'s contribute to a specific $n^{(j)}$. For example, do $n_1^{(2)}$ and $n_2^{(2)}$ contribute to $n_3^{(4)}$? How much? In these cases, use Table C-1. Table C-1 shows that half of $n_3^{(4)}$ is "observed" as $n_2^{(2)}$ in a two-train system. The other half is "observed" as $n_1^{(2)}$. Thus,

$$\begin{aligned} n_3^{(4)} &= 4\mu(1-\rho)\rho^3 = 2\mu(1-\rho)\rho^3 + 2\mu(1-\rho)\rho^3 \\ &= \rho^2\left[2\mu(1-\rho)\rho\right] + 2(1-\rho)\rho\,(\mu\rho^2) \\ &= \rho^2 n_1^{(2)} + 2(1-\rho)\rho\, n_2^{(2)} \end{aligned} \tag{C.16}$$

Table C-5 includes formulae to cover all the upward mapping possibilities with system sizes up to four. By making use of the concepts of the BFR model, the uncertainty inherent in mapping up impact vectors is reduced to the uncertainty in estimating the parameter ρ; that is, the probability that the nonlethal shock or cause would have failed a single hypothetical component added to the system. While this may seem obvious, it should reduce the overall uncertainty in mapping up the impact vector since the formulae in Table C-5 take care of all the bookkeeping problems of enumerating the possibilities and factoring in the system size effects.

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.

Table C-5. Formulae for upward mapping of events classified as nonlethal shocks.

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

C.5 SUMMARY OF IMPACT VECTOR MAPPING

The impact vector mapping concepts of this appendix are summarized in the form of a decision tree for the data analyst in Figure C-1. 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 database, as well as for the system being analyzed, and the use of the appropriate mapping formulae derived in this appendix. Examples of impact vector mapping are presented in Tables C-4 and C-6 for downward and upward mapping, respectively. It should be stressed that the particular formulae given in those tables are dependent on the assumptions made, particularly with regard to data collection and, in the case of upward mapping, the BFR assumptions.

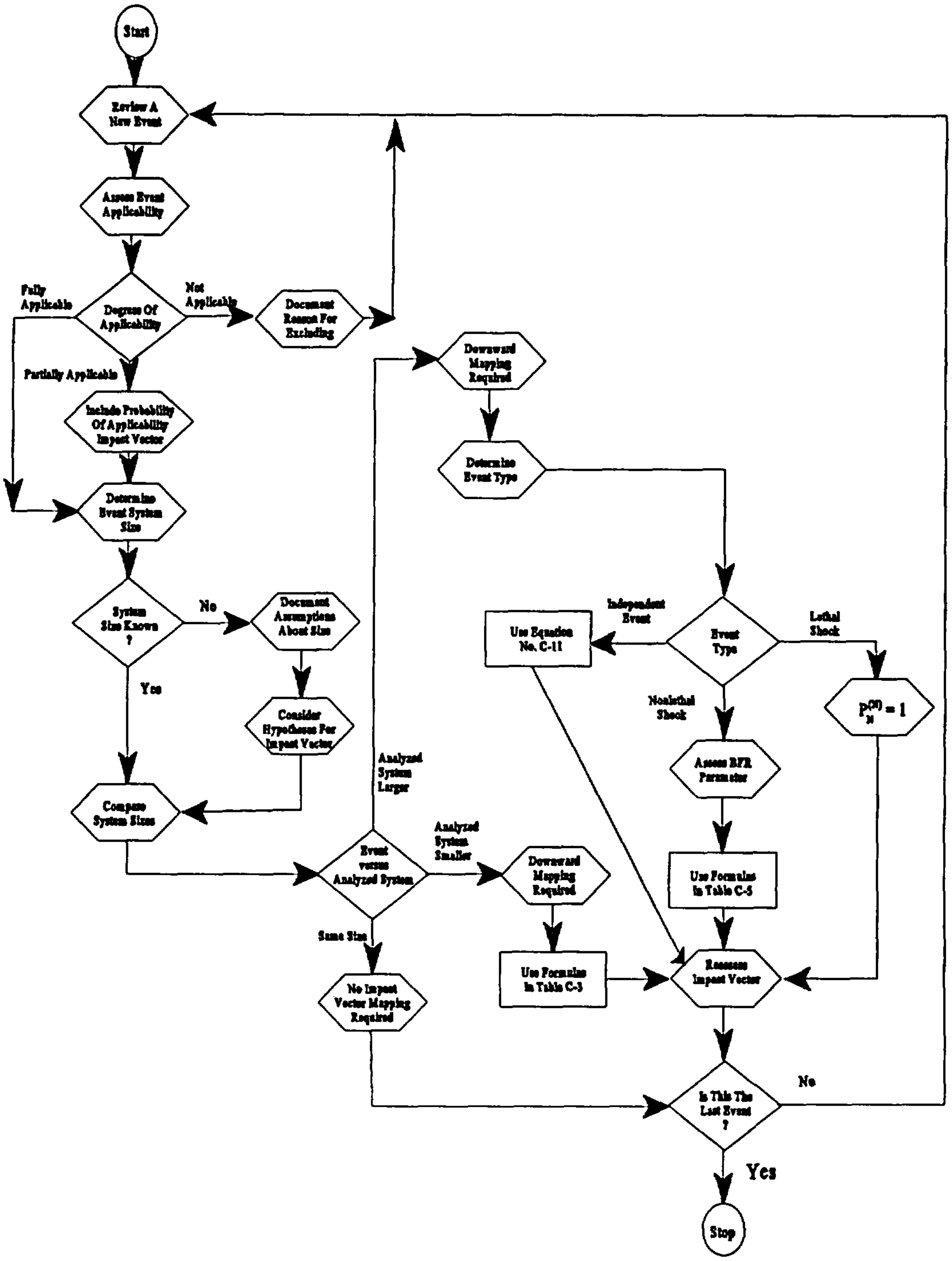


Figure C-1. Decision tree for assessing and mapping event impact vectors.

Table C-6. Example of upward mapping of impact vectors.

Event No.	System Size	Impact Vector*			
		P_1	P_2	P_3	P_4
	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	-	-	-
	Identical Three-Train	1.5	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 (ρ = 0.10)				
4-	Original - One Train	1	-	-	-
	Identical Two-Train	1.8	.1	-	-
	Identical Three-Train	2.43	.27	.01	-
	Identical Four-Train	2.916	.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 One-Train	.5	.5	-	-
	Identical Two-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 Cases				
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 (ρ = 0.9)				
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 (ρ = 0.5)				
10-	Original One-Train	1	-	-	-
	Identical Two-Train	1	.5	-	-
	Identical Three-Train	.75	.75	.25	-
	Identical Four-Train	.5	.75	.5	.25
11-	Original One-Train	0	1	-	-
	Identical Two-Train	0	.5	.5	-
	Identical Three-Train	0	.25	.5	.25
12-	Original One-Train	.5	.5	-	-
	Identical Two-Train	.375	.5	.25	-
	Identical Three-Train	.25	.4375	.375	.125
13-	Original One-Train	.25	.5	.25	-
	Identical Two-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

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

- If an event is classified as a nonlethal shock and it fails only one component, it is reasonable to expect that ρ is small ($\rho < 0.5$).
- If a nonlethal shock fails a number of components intermediate to the number present, it is unreasonable to expect that ρ is either very small ($\rho \rightarrow 0$) or very large ($\rho \rightarrow 1$).
- If a nonlethal shock fails all the components present in a system, it is reasonable to expect that ρ is large ($\rho > 0.5$).

C.6 REFERENCES

C-1. Fleming, K. N., et al., *Classification and Analysis of Reactor Operator Experience Involving Dependent Events,* prepared for Electric Power Research Institute by Pickard, Lowe and Garrick, Inc., EPRI NP-3967, June 1985.

C-2. Poucet, A., A. Amendolam, and P. C. Cacciabus, *Summary of the Common Cause Failure Reliability Benchmark Exercise*, Joint Research Center Report, PER 1133/86, Ispra, Italy, April 1986.

C-3. Doerre, P., *Possible Pitfalls in the Process of CCF Event Data Evaluation*, Proceedings of PSA 87 International Topical Conference on Probabilstic Safety Assessment and Risk Management, Zurich, Switzerland, August 30-September 4, 1987.

APPENDIX D

STATISTICAL UNCERTAINTY DISTRIBUTION FOR MODEL PARAMETERS

APPENDIX D

Statistical Uncertainty Distribution for Model Parameters

D.1 INTRODUCTION

The major sources of uncertainty in the CCF parameters were identified in Section 5.5.4. It also presented an overview of the statistical methods used to quantify the uncertainties. This appendix details the statistical models that can be used to represent uncertainty in the estimates of the parameters of various parametric models. The uncertainties addressed by the statistical models of Sections D.1 through D.4 are those associated with statistical inference based on limited sample size (the standard statistical uncertainty). However, simple extensions of the general structure of these models provide the vehicle for incorporating other sources of uncertainty, as discussed in Section 5.5.4 of this report. Examples of these sources are uncertainty in impact vector assessment, incompleteness of data bases with respect to the number of failures and success data.

The assumption in the models presented here, therefore, is that the statistical information necessary to estimate the parameters of a model is available without any uncertainty concerning the various pieces of that information. The approach adopted for the analysis of the uncertainty that is due to data set size is the Bayesian approach, in which the distribution of a parameter, θ, in light of evidence E, is obtained from

$$\pi(\theta|E) = \frac{L(E|\theta)\,\pi_o(\theta)}{\int L(E|\theta)\,\pi_o(\theta)\,d\theta} \tag{D.1}$$

where

$\pi(\theta|E)$ ≡ posterior distribution of θ given evidence E.
$\pi_o(\theta)$ ≡ distribution of θ prior to the evidence.
$L(E|\theta)$ ≡ likelihood function or the probability of the evidence E, given θ.

The following sections describe how the above concept can be used to develop the uncertainty distributions of various parameter models. For all models except BFR[D-1], the presentation is limited to the demand-based failure frequencies. The time-based failure rate models can be developed by a simple change in selected statistical distribution.

D.2 DISTRIBUTION OF THE BASIC PARAMETER MODEL

The demand based parameters of the basic parameter model are defined as Q_k ≡probability of failure of k-specific components on demand due to a common cause.

The statistical evidence needed to estimate Q_k is of the form:

$$E = \{n_k, k = 1, ..., m; N_D\} \tag{D.2}$$

where n_k ≡ number of failure of events involving failure of k components in a common cause group of size m, and N_D ≡ number of system demands.

Assuming non-staggered testing, the number of times a group of k components is challenged in each test of a system of m components can calculated from

$$N_k = \binom{m}{k} N_D \tag{D.3}$$

where the binomial term $\binom{m}{k}$ is the number of groups of k components that can be formed from m components. Bayes' theorem, in this case, is written as

$$\pi\left(Q_k \mid n_k, N_k\right) = \frac{1}{C} L\left(n_k \mid Q_k, N_k\right) \pi_o\left(Q_k\right) \tag{D.4}$$

where

$$C \equiv \int_o^1 L\left(n_k \mid Q_k, N_k\right) \pi_o\left(Q_k\right) dQ_k$$

The binomial distribution

$$L\left(n_k \mid Q_k, N_k\right) = \binom{N_k}{n_k} Q_k^{n_k} \left(1 - q_k\right)^{N_k - n_k} \tag{D.5}$$

for the likelihood and its conjugate distribution, beta

$$\pi_o\left(Q_k\right) = \frac{\Gamma\left(A_k + B_k\right)}{\Gamma\left(A_k\right) + \Gamma\left(B_k\right)} Q_k^{A_k - 1} \left(1 - Q_k\right)^{B_k - 1} \tag{D.6}$$

for the prior distribution, are logical and convenient choices. Here A_k and B_k are the two parameters of the beta distribution and the gamma function $\Gamma(x)$ is defined as

$$\Gamma(x) = \int_0^\infty z^{x-1} e^{-z} dz \tag{D.7}$$

The parameters of the posterior distribution that will also be a member of the beta family of distributions are

$$\begin{aligned} A_k' &= A_k + n_k \\ B_k' &= B_k + N_k - n_k \end{aligned} \tag{D.8}$$

The mean of the posterior distribution is given by

$$\bar{Q}_k = \frac{A_k'}{A_k' + B_k'} \tag{D.9}$$

Therefore,

$$\bar{Q}_k = \frac{n_k + A_k}{N_k + B_k + A_k} \qquad k = 1, \cdots, m \tag{D.10}$$

For a uniform prior with $A_k = B_k = 1$,

$$\bar{Q}_k = \frac{n_k + 1}{N_k + 2} \tag{D.11}$$

Since, for higher values of k (k > 2), the n_k are generally small, the assumption of the particular prior can have a significant effect on common cause failure probability estimates. This is true of the other models also. Therefore, these results should not be used without an understanding of what drives them.

The mode of the posterior distribution is given by

$$Q_k = \frac{A'_k - 1}{A'_k + B'_k - 2} \tag{D.12}$$

which, in terms of the prior distribution parameters and the data, is written as

$$Q_k = \frac{n_k + A_k - 1}{N_k + B_k + A_k - 2} \tag{D.13}$$

For a uniform prior ($A_k = B_k = 1$), the above estimator reduces to a form commonly known as the maximum likelihood estimators (MLE):

$$Q_k = \frac{n_k}{N_k} \tag{D.14}$$

In application to the uncertainty analysis of a system unavailability, or sequence frequency, the distributions on the Q_k are regarded as statistically independent. So for example, in a Monte Carlo analysis, the distributions on the Q_k are sampled independently. This, of course, results in underestimation of the overall uncertainty.

D.3 DISTRIBUTION OF THE ALPHA-FACTOR MODEL PARAMETERS

D.3.1 Homogeneous Population

The following discussion applies to cases where the data from various plants or systems are pooled, based on an assumption of homogeneity.

In this case, the data needed to estimate α_k's are of the following form:

$$E = \{n_k: k = 1,...,m\} \tag{D.15}$$

where n_k is the number of events involving exactly k component failures in a common cause component group of size m.

The likelihood of observing this evidence, given a set of values for α_k's, is

$$L\left(n_1, n_2, \cdots, n_m \,|\, \alpha_1, \alpha_2, \cdots, \alpha_m\right) = \frac{\Gamma\left(n_1 + n_2 + \cdots + n_m\right)}{\Gamma\left(n_1\right) \cdots \Gamma\left(n_m\right)} \prod_{k=1}^{m} \alpha_k^{n_k} \tag{D.16}$$

where

$$\sum_{k=1}^{m} \alpha_k = 1 \tag{D.17}$$

This is a multi-nominal distribution.

This distribution is based on the assumption that n_k's are generated independently with probabilities given by α_k's subject to the constraint that the sum of α's is one. By using equation D.16 as the likelihood function in Bayes theorem and choosing a Dirichlet distribution function as the prior for α's, a posterior distribution function, which is also Dirichlet in form, is obtained:

$$\pi(\alpha_1, \ldots, \alpha_m) = \frac{\Gamma(A_1 + A_2 + \cdots + A_m)}{\Gamma(A_1) \cdots \Gamma(A_m)} \alpha_1^{A_1 - 1} \alpha_2^{A_2 - 1} \cdots \alpha_m^{A_m - 1} \, , \qquad \text{(D.18)}$$

where A_k's (k = 1,...,m) are the parameters of the posterior distribution and are related to a similar set of prior distribution parameters $[A_{o1}, \ldots, A_{om}]$ through the following relationship:

$$A_k = A_{ok} + n_k . \qquad \text{(D.19)}$$

Note that $0 \leq A_k < \infty$ for all k.

The general form of marginal distribution of each α_k is a beta distribution of the form

$$\pi_j(\alpha_j) = \frac{\Gamma(A_T)}{\Gamma(A_j)\Gamma(A_T - A_j)} \alpha_j^{A_j - 1} (1 - \alpha_j)^{(A_T - A_j) - 1} . \qquad \text{(D.20)}$$

where

$$A_T = \sum_{j=1}^{m} A_j \qquad \text{(D.21)}$$

The marginal distribution of α_k is a beta distribution with mean and mode given by

$$mean: \quad \bar{\alpha}_k = \frac{A_{0k} + n_k}{\sum_{i=1}^{m} (A_{0i} + n_i)} = \frac{A_k}{A_T} \qquad k = 1, \cdots, m \qquad \text{(D.22)}$$

$$mode: \quad \alpha_{k,mode} = \frac{A_k + n_{0k} - 1}{\sum_{i=1}^{m} \left(A_{0i} + n_i\right) - 1} = \frac{A_k - 1}{A_T - 1} \qquad k = 1, \cdots, m \qquad \text{(D.23)}$$

For a uniform prior $A_k = 1$ $k = 1, \ldots, m$, the maximum likelihood estimator of α_k is

$$\alpha_k = \frac{n_k}{\sum_{i=1}^{m} n_k} \qquad k = 1, \cdots, m \qquad \text{(D.24)}$$

which is the maximum likelihood estimator of α_k.

D.3.2 Non-homogeneous Population

The above treatment assumes that once the CCF events are reinterpreted and impact vectors mapped for a particular application, a homogeneous population of events is created. That is, after the specialization of the CCF event impact vectors, the events are considered as belonging in the same population and coming from the plant under consideration. If on the other hand, the potential population variability (plant-to-plant variability) of CCF events are considered, a different statistical model, one based on non-homogenous population, applies.

In this approach average impact vector elements are summed for each impact category for each plant. A data set is thus generated for each of the N plants in the database. That is,

$$D^{(l)} = [n_1^{(l)}, n_2^{(l)}, \ldots, n_m^{(l)}], \quad l = 1, \ldots, N \tag{D.25}$$

Note that the data set of Equation D.15 is formed by summing the $D^{(l)}$ for all plants.

The plant-to-plant variability distribution of each α_j can be obtained through the following steps. First, assume that the distribution can be represented by a beta distribution:

$$\pi_j(\alpha_j) = \frac{\Gamma(a_j + b_j)}{\Gamma(a_j)\Gamma(b_j)} \alpha_j^{a_j}(1 - \alpha_j)^{b_j} \tag{D.26}$$

where a_j and b_j are two (unknown) parameters. The distribution of ${}_j$a and${}_j$ b can be obtained using the following data set developed from Equation D.25:

$$D_j = [n_j^{(l)}, n_t^{(l)}; \; l = 1, \ldots, N] \tag{D.27}$$

where

$$n_t^{(l)} = \sum_{j=1}^{m} n_j^{(l)} \tag{D.28}$$

The distribution is developed by Bayes Theorem:

$$f(a_j,b_j|D_j) = \frac{L(D_j|a_j,b_j)f_0(a_j,b_j)}{\int\int L(D_j|a_j,b_j)f_0(a_j,b_j)da_jdb_j} \tag{D.29}$$

where the likelihood function is

$$L(D_j|a_j,b_j) = \prod_{l=1}^{N}[\int B(n_j^{(l)},n_t^{(l)}|\alpha_j)\,\pi_j(\alpha_j)d\alpha_j] \tag{D.30}$$

In Equation D.30, $B(n_j^{(l)},n_t^{(l)}|\alpha_j)$ is a binomial distribution corresponding to the data from plant I. The final step is to use the posterior distribution of Equation D.29 to find various estimates of the desired distribution of α_j, including a mean density function:

$$\bar{\pi}_j(\alpha_j) = \int\int \pi_j(\alpha_j|a_j,b_j)f(a_j,b_j|D_j)da_jdb_j \tag{D.31}$$

Clearly, development of the mean probability density function and the steps leading to it require numerical methods and can only be done by computer. Both the homogeneous and nonhomogeneous models are available in the CCF software.[7] The non-homogeneous option can be used to develop generic and global assessment of the ranges of CCF parameters across the industry. It can also be used as a prior distribution in plant-specific estimations. For this use the data from the plant being analyzed should be excluded from the non-homogeneous database, Equation 5.38, to be used as plant-specific data in the Bayesian updating process. The resulting distribution from this procedure is expected to be wider than the distribution obtained based on the homogeneous assumption (Equation D.15).

D.4 DISTRIBUTION OF THE MGL MODEL PARAMETERS

The distribution of the MGL parameters is first developed in its exact form. However, since the exact form as it will be seen is complicated and for some practical applications difficult to use, an approximate method is also described along with a discussion of its limitations and constraints. In both cases, the presentation is limited to the MGL parameters for a three-component system. The results can be easily generalized for systems of higher redundancy.

D.4.1 Exact Method

Since the available statistical data are in the form of the number of events involving different common cause basic events, an event-based parameter such as the α-factor can be estimated directly from the data. However, the MGL parameters are, by definition, component based and as such, cannot be directly related to the observables (n_k's). Therefore, the distribution of MGL parameters must be obtained indirectly through the distribution of an event-based parameter. The event-based model selected for this purpose is the α-factor model.

Note that, based on the definition of the α-factors and the MGL parameters, the following relations can be established:

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \qquad \text{(D.32)}$$

$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3} \qquad \text{(D.33)}$$

Using the standard approach for change of variables, the distributions of the MGL and a α-factor model parameters are related through the following equation:

$$\pi_{\gamma,\beta}(\beta, \gamma) = \frac{\pi(\alpha_1, \alpha_2, \alpha_3)}{\left|J(\alpha_1, \alpha_2, \alpha_3)\right|} \qquad \text{(D.34)}$$

where, defining a dummy parameter X = α_2, the Jacobian is written as

$$J(\alpha_1, \alpha_2, \alpha_3) = \begin{vmatrix} \dfrac{\partial\beta}{\partial\alpha_1} & \dfrac{\partial\beta}{\partial\alpha_2} & \dfrac{\partial\beta}{\partial\alpha_3} \\[2ex] \dfrac{\partial\gamma}{\partial\alpha_1} & \dfrac{\partial\gamma}{\partial\alpha_2} & \dfrac{\partial\gamma}{\partial\alpha_3} \\[2ex] \dfrac{\partial\chi}{\partial\alpha_1} & \dfrac{\partial\chi}{\partial\alpha_2} & \dfrac{\partial\chi}{\partial\alpha_3} \end{vmatrix} \qquad \text{(D.35)}$$

Since,

$$\frac{\partial \beta}{\partial \alpha_2} = \frac{\partial \beta}{\partial \alpha_2} = \frac{\partial \chi}{\partial \alpha_1} = \frac{\partial \chi}{\partial \alpha_3} = 0 \tag{D.36}$$

then,

$$J\left(\alpha_1, \alpha_2, \alpha_3\right) = -\left(\frac{\partial \beta}{\partial \alpha_1}\right)\left(\frac{\partial \gamma}{\partial \alpha_3}\right) - \left(\frac{\partial \beta}{\partial \alpha_3}\right)\left(\frac{\partial \gamma}{\partial \alpha_1}\right) \tag{D.37}$$

From Equations D.32 and D.33, eliminating α_2, we have

$$\frac{\partial \beta}{\partial \alpha_2} = \frac{-\frac{9}{2} - \frac{9}{4}\alpha_3}{\left(3 - \frac{3}{2}\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{D.38}$$

$$\frac{\partial \beta}{\partial \alpha_3} = \frac{\frac{9}{4}\alpha_1}{\left(3 - \frac{3}{2}\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{D.39}$$

$$\frac{\partial \gamma}{\partial \alpha_1} = \frac{\frac{27}{2}\alpha_3}{\left(3 - 3\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{D.40}$$

$$\frac{\partial \gamma}{\partial \alpha_3} = \frac{\frac{27}{2} - \frac{27}{2}\alpha_1}{\left(3 - 3\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{D.41}$$

Using the above equations in Equation D.37 and replacing α_1 and α_3 with the following equalities:

$$\alpha_1 = \frac{3(1 - \beta)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{D.42}$$

$$\alpha_3 = \frac{\beta\gamma}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{D.43}$$

$$J = \frac{2}{9\beta}\left(3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma\right)^3 \tag{D.44}$$

Therefore,

$$\pi_{\gamma,\beta}(\beta, \gamma) = \frac{9\beta}{2\left(3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma\right)^3}\,\pi_{\alpha_1,\alpha_2,\alpha_3}\left(\alpha_1, \alpha_2, \alpha_3\right) \tag{D.45}$$

Based on the discussion in Section D.3, for a uniform prior distribution, the distribution of α_1, α_2, and α_3 is given by

$$\pi_{\alpha_1,\alpha_2,\alpha_3}\left(\alpha_1, \alpha_2, \alpha_3\right) = \frac{\Gamma\left(n_1 + n_2 + n_3\right)}{\Gamma\left(n_1\right)\Gamma\left(n_2\right)\Gamma\left(n_3\right)}\,\alpha_1^{n_1 - 1}\,\alpha_2^{n_2 - 1}\,\alpha_3^{n_3 - 1} \tag{D.46}$$

Equations D.42 and D.43 give the relation between α_1 and α_3 and β and γ. The corresponding equation for α_2 is

$$\alpha_2 = \frac{\frac{3}{2}\beta(1 - \gamma)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{D.47}$$

Now α_1, α_2, and $\alpha_3$can be replaced in Equation D.46 by Equations D.42, D.43, and D.47. The resulting distribution can then be used in Equation D.46 to obtain the distribution of β and γ.

$$\pi_{\gamma,\beta}(\beta, \gamma) = C\,\frac{\beta^{n_2 + n_3 - 1}\,(1 - \beta)^{n_1 - 1}\,\gamma^{n_3 - 1}\,(1 - \gamma)^{n_2 - 1}}{\left(3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma\right)^{n_1 + n_2 + n_3}} \tag{D.48}$$

where

$$C = \frac{3^{n_1 + n_2}}{3^{n_2}}\,\frac{\Gamma\left(n_1 + n_2 + n_3\right)}{\Gamma\left(n_1\right)\Gamma\left(n_2\right)\Gamma\left(n_3\right)} \tag{D.49}$$

From Equation D.48, it can be seen that mean values of β and γ can only be obtained numerically, which is not a desirable property for most practical applications where the mean value may be needed for an initial quantitative screening of the common cause component. In such cases, the approximate method described in the following section may be used.

D.4.2 Approximate Method

The uncertainty distribution of the MGL parameters can be approximated with simpler parametric distributions if the observed events are assumed to be independent component failures within different categories of common cause events. In other words, the set $\{n_k\ k=1, ..., m\}$ where n_k is the number of <u>events</u> involving failure of k components due to common cause will be interpreted as $\{kn_k;\ k=1, ..., m\}$ where kn_k is the number of <u>components</u> failed in common cause events involving k component failures, and kn_k events will be assumed to have occurred independently.

With the above assumption, let us define the following conditional probabilities (for a system of these components).

$Z_1 \equiv 1 - \beta$ = conditional probability of component failure being a single failure.
$Z_2 \equiv \beta(1 - \gamma)$ = conditional probability of component being involved in a double failure.
$Z_3 \equiv \beta\gamma$ = conditional probability of component being involved in a triple failure.

Note that

$$Z_1 + Z_2 + Z_3 = 1$$

The likelihood of observing n_1 single failures, $2n_2$ component failures due to double failures, and $3n_3$ component failures due to triple failures can be modeled by a multinomial distribution for Z_i's, as follows:

$$P\left(n_1, 2n_2, 3n_3 \mid Z_1, Z_2, Z_3\right) = \frac{\left(n_1 + 2n_2 + 3n_3\right)!}{\left(n_1\right)!\left(2n_2\right)!\left(3n_3\right)!}\ Z_1^{n_1}\ Z_2^{2n_2}\ Z_3^{3n_3} \qquad \text{(D.50)}$$

Rewriting Equation D.42 in terms of β and γ results in

$$P\left(n_1, 2n_2, 3n_3 \mid \beta, \gamma\right) = M\beta^{2n_2 + 3n_3}\,(1 - \beta)^{n_1}\,\gamma^{3n_3}\,(1 - \gamma)^{2n_2} \qquad \text{(D.51)}$$

where M is the multinomial multiplier as in Equation D.50.

Now Bayes' theorem is written as

$$\pi\left(\beta, \gamma \mid n_1, 2n_2, 3n_3\right) = \frac{1}{C}\,P\left(n_1, 2n_2, 3n_3 \mid \beta, \gamma\right)\,\pi_0(\beta, \gamma) \qquad \text{(D.52)}$$

where π_0 and π are the prior and posterior distribution of β and γ and C is a normalizing factor defined as

$$C = \int_0^1\int_0^1 P\left(n_1, 2n_2, 3n_3 \mid \beta, \gamma\right)\,\pi_0(\beta, \gamma)\,d\beta\,d\gamma \qquad \text{(D.53)}$$

As the prior, one can use a multinomial distribution:

$$\pi_0(\beta, \gamma) = h\,\beta^{A_0 - 1}\,(1 - \beta)^{B_0 - 1}\,\gamma^{C_0 - 1}\,(1 - \gamma)^{D_0 - 1} \qquad \text{(D.54)}$$

where h is given by

$$h = \frac{\Gamma(A_0 + B_0 + C_0 + D_0)}{\Gamma(A_0)\Gamma(B_0)\Gamma(C_0)\Gamma(D_0)} \tag{D.55}$$

A flat prior distribution is obtained by setting $A_0 = B_0 = C_0 = D_0 = 1$.

Using Equation D.54 in Equation D.52 results in a posterior for distribution for β and γ that is also multinomial, with parameters:

$$\begin{aligned} A &= A_0 + 2n_2 + 3n_3 \\ B &= B_0 + n_1 \\ C &= C_0 + 3n_3 \\ D &= D_0 + 2n_2 \end{aligned} \tag{D.56}$$

The mode of the posterior distribution occurs at

$$\beta = \frac{A - 1}{A + B - 2} \tag{D.57}$$

$$\gamma = \frac{C - 1}{C + D - 2} \tag{D.58}$$

The mean values are calculated from

$$\bar{\beta} = \frac{A}{A + B} \tag{D.59}$$

$$\bar{\gamma} = \frac{C}{C + D} \tag{D.60}$$

Note that for the flat prior the mode of the posterior distribution is

$$\beta = \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \tag{D.61}$$

$$\gamma = \frac{3n_3}{2n_2 + 3n_3} \tag{D.62}$$

which correspond to the point estimates developed in Section 5 of this report, for a component common cause group of size m = 3. As we can see, the approximate method results in estimators that are similar to the commonly used estimators for the MGL parameters. The commonly used estimators, therefore, are not exact and should only be used if the magnitude of error introduced is judged to be insignificant compared with other sources of error and uncertainty. The most important difference between the exact and the approximate methods described here is that the spread of the distributions based on the approximate method is smaller, a consequence of assuming that the component statistics (kn_k) are the result of independent observations.[D-2, D-3] The difference may not be significant, however, if other sources of uncertainty are accounted for in the development of these distributions.

D.5 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 (see discussion in Section 5 of this report), for the system being analyzed. Formally, this type of uncertain data can be represented as

$$E = \left\{ \left\langle P_{ij}, I_{ij} \right\rangle \ i = 1, \ldots, N; \ j = 1, \ldots, M_i \right\} \qquad (D.63)$$

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

$$\sum_{j=1}^{M_i} P_{ij} = 1 \qquad (D.64)$$

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

Event	Hypothesis	Probability	Impact Vector			
			F_0	F_1	F_2	F_3
Event 1	I_{11} I_{12}	P_{11} P_{12}	0 0	0 0	1 0	0 1
Event 2	I_{21} I_{22} I_{23}	P_{21} P_{22} P_{23}	1 0 0	0 1 0	0 0 1	0 0 0

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

Data Set	Probability	Event Statistics			
		n_0	n_1	n_2	n_3
D_1	$w_1 = P_{11}P_{21}$	1	0	1	0
D_2	$w_2 = P_{11}P_{22}$	0	1	1	0
D_3	$w_3 = P_{11}P_{23}$	0	0	2	0
D_4	$w_4 = P_{12}P_{21}$	1	0	0	1
D_5	$w_5 = P_{12}P_{22}$	0	1	0	1
D_6	$w_6 = P_{12}P_{23}$	0	0	1	1

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

$$\pi(\alpha) = \sum_{i=1}^{6} w_i \, \pi_i\left(\alpha \,|\, D_i\right) \tag{D.65}$$

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 5 of this report, before combining them to obtain the total number of events in each impact category. Formally,

$$\bar{D} = \left\{\bar{I}_i ; \quad i = 1,\ldots,N\right\} \tag{D.66}$$

where

$$\bar{I}_i = \sum_{j=1}^{M_i} P_{ij} \, I_{ij} \tag{D.67}$$

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

Event	F_0	F_1	F_2	F_3
Event 1	0	0	P_{11}	P_{12}
Event 2	P_{21}	P_{22}	P_{23}	0

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

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

The implications of this approximation and comparison with the rigorous treatment according to Equation D.65 are discussed in Section 5.5.4 of this report.

D.6 REFERENCES

D-1. 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.

D-2. Paula, H. M., *Comments on the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation*, Nuclear Safety, Vol. 27, No. 2, April-June 1986.

D-3. Apostolakis, G., and P. Moieni, *The Foundations of Models of Dependence in Probabilistic Safety Assessment*, Reliability Engineering, Vol. 18, pp. 177-195, 1987.

APPENDIX E

TREATMENT OF COMMON CAUSE FAILURES IN EVENT ASSESSMENT

APPENDIX E

Treatment of Common Cause Failures in Event Assessment

E.1 INTRODUCTION

The treatment of CCF in PRAs and reliability studies is well established in the literature and in practice.[E-1, E-3] The USNRC has recently developed a CCF database that uses the principles presented in References E-1 through E-3. The technical reports[E-4 - E-8] associated with the database address the collection of CCF data, estimation of CCF parameters, and the incorporation of CCFs in PRAs and reliability studies. However, no guidance has been provided for the treatment of CCFs in event assessment. Common cause failures have been treated in the Accident Sequence Precursor Program analyses, but no formal guidance exists. This appendix provides that guidance. It is assumed that the reader is familiar with the basic concepts for treating CCFs in PRAs, as outlined in the main report.

E.2 PRELIMINARIES

We begin with a simple example. Consider a common cause component group consisting of three components. Let A, B, and C represent basic events of three similar components. The failure model for each component is given by

$$\begin{aligned} A_T &= A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC} \\ B_T &= B_I \cup C_{AB} \cup C_{BC} \cup C_{ABC} \\ C_T &= C_I \cup C_{AC} \cup C_{BC} \cup C_{ABC} \end{aligned} \tag{E.1}$$

where the subscript T denotes total failure from all causes, I denotes failure from independent causes, and C_{XY} denotes common cause failure of components X and Y. All events are mutually exclusive (e.g., $A_I \cap C_{AB} = \phi$). The failure probability of A_T, B_T, and C_T is given by the following equation:

$$Q_T = Q_1 + 2Q_2 + Q_3 \tag{E.2}$$

where $Q_1 = P[A_I] = P[B_I] = P[C_I]$, $Q_2 = P[C_{AB}] = P[C_{AC}] = P[C_{BC}]$, and $Q_3 = P[C_{ABC}]$. This is referred to as the **Basic Parameter Model** for CCF analysis.

Figure E-1 contains the reliability block diagram for this configuration. For a 1-out-of-3 success criterion (i.e., all components must fail), the minimal cutsets are the following: $[A_I, B_I, C_I]$, $[A_I, C_{BC}]$, $[B_I, C_{AC}]$, $[C_I, C_{AB}]$, and $[C_{ABC}]$. The failure probability for the undesired event $S = A_T \cap B_T \cap C_T$, which is denoted by Q_S, is given, in terms of the basic parameter model:

$$Q_S = Q_1^3 + 3Q_1Q_2 + Q_3 \tag{E.3}$$

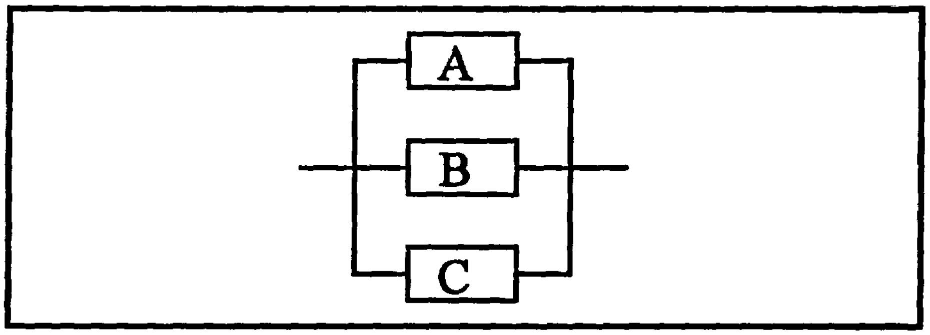


Figure E-1. Reliability block diagram for a three-component group.

The MGL representation and the alpha factor representation are reparameterizations of the Basic Parameter Model. References E-1, E-2, E-3 and the present document contain details of each and their relationships. The alpha factor formulation is best for considering the statistical implications and the data collection aspects. The MGL representation is a conditional formulation of the model. For the three-component system considered above and assuming a staggered testing scheme, $\alpha_1 = 1 - \beta$, $\alpha_2 = \beta\,(1 - \gamma)$, and $\alpha_3 = \beta\,\gamma$. Equations can also be obtained relating the two representations for nonstaggered testing, although they are more complicated (see Appendix A). With this background, we are now ready to demonstrate how to treat common cause failures in an event assessment or in a conditional analysis.

E.3 TREATMENT OF CCF IN EVENT ANALYSIS

In an event assessment we need to calculate the probability of failure given the event or conditions that exist. For CCF analysis we have two cases. The first case is when a component is failed. The second case is when a component is out of service, unavailable, but is not failed. We will discuss each of these cases.

E.3.1 Component is Failed

For this case, we assume that component C is failed. Then, the conditional failure probability of S given C_T is given by

$$P[S\,|\,C_T] = \frac{P[A_T \cap B_T \cap C_T]}{P[C_T]} = \frac{Q_S}{Q_T} \qquad \text{(E.4)}$$

This expression can be obtained from the minimal cutsets. C can fail because any one of the events C_I, C_{AC}, C_{BC}, or C_{ABC} occurs. We will develop the conditional probabilities for each cutset. For $[A_I, B_I, C_I]$ we have

$$P[A_I \cap B_I \cap C_I \,|\, C_T] = \frac{P[A_I \cap B_I \cap C_I]}{P[C_T]} = Q_1^2\,\frac{Q_1}{Q_T} \qquad \text{(E.5)}$$

For $[A_I, C_{BC}]$,

$$P[A_I \cap C_{BC} \,|\, C_T] = \frac{P[A_I \cap C_{BC}]}{P[C_T]} = Q_1\,\frac{Q_2}{Q_T} \qquad \text{(E.6)}$$

For $[B_I, C_{AC}]$,

$$P[B_I \cap C_{AC} | C_T] = \frac{P[B_I \cap C_{AC}]}{P[C_T]} = Q_1 \frac{Q_2}{Q_T} \tag{E.7}$$

For $[C_I, C_{AB}]$,

$$P[C_I \cap C_{AB} | C_T] = \frac{P[C_I \cap C_{AB}]}{P[C_T]} = Q_2 \frac{Q_1}{Q_T} \tag{E.8}$$

For $[C_{ABC}]$,

$$P[C_{ABC} | C_T] = \frac{P[C_{ABC}]}{P[C_T]} = \frac{Q_3}{Q_T} \tag{E.9}$$

Adding together the results of equations (E.5) through (E.9) we get

$$Q_1^2 \frac{Q_1}{Q_T} + 2Q_1 \frac{Q_2}{Q_T} + Q_2 \frac{Q_1}{Q_T} + \frac{Q_3}{Q_T} \tag{E.10}$$

which equals Equation E.4. For most practical considerations, $Q_t \approx Q_T$. Equation E.10 reduces to the following in terms of the alpha factor model and assuming staggered testing:

$$Q_1^2\alpha_1 + 2Q_1\alpha_2 + Q_2\alpha_1 + \alpha_3 \approx Q_1^2 + 2Q_1\alpha_2 + Q_2 + \alpha_3 \approx Q_1^2 + \alpha_3 \tag{E.11}$$

In most PRAs, this three component system is modeled using a single common cause basic event and three basic events that represent the independent failures of A, B, and C, respectively. We can quantify this event, failure of C, by setting the probability of C to TRUE and changing the failure probability of the common cause basic event to the value of α_3.

E.3.2 Component Out for Preventive Maintenance

In this case, we will assume that component C is unavailable due to preventive maintenance and that it is not in a failed state. The potential exists for common cause failures to occur. That is, C_{AC}, C_{BC}, and C_{ABC} have not occurred, but they could occur. Since C is unavailable, the cutsets for this case are $[A_I, B_I]$, $[A_I, C_{BC}]$, $[B_I, C_{AC}]$, $[C_{AB}]$, and $[C_{ABC}]$. Quantification of these yields

$$P[A_T \cap B_T | C_M] = Q_1^2 + 2Q_1Q_2 + Q_2 + Q_3 \approx Q_1^2 + Q_2 + Q_3 \tag{E.12}$$

where C_M denotes that component C is unavailable due to preventive maintenance.

In the simplified plant-specific models, this three-component system is modeled using a single common cause basic event and three basic events that represent the independent failures of A, B, and C, respectively. We can quantify this event, component C out for maintenance, by setting the probability of C to TRUE and changing the failure probability of the common cause basic event to the value of $Q_2 + Q_3$.

E.3.3 Treatment When the CCF Cause Is Known

When the cause for the CCF event is known, the CCF quantification can be tailored for that specific cause. For example, Surry has experienced steam binding in the auxiliary feedwater pumps. This specific common cause was modeled separately in their Individual Plant Examination. The CCF parameter estimates for a single cause such as this will, in general, be much less than the estimate for all CCF causes.

E.3.4 Other Cases

The above development was for a specific system size and success criterion. Other configurations and success criteria exist for a system of a given size. For example, Table E-1 contains the results for a system of size three. Table E-2 contains the minimal cutsets for this example. Each case should be worked out from the basic building blocks of the PRA analysis.

Table E-1. Some configurations for three components.

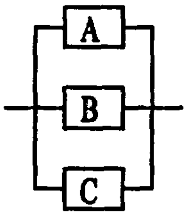
RELIABILITY BLOCK DIAGRAM	NO.	SUCCESS CRITERION	QUANTIFICATION
	1	Three units in standby; one of three (1 of 3) must operate on demand.	$Q_1^3 + 3Q_1Q_2 + Q_3$
	2	Three units in standby; two of three (2 of 3) must operate on demand.	$3Q_1^2 + 3Q_2 + Q_3$
	3	Three units in standby; three of three (3 of 3) must operate on demand.	$3Q_1 + 3Q_2 + Q_3$

Table E-2. Cutsets for configurations for three components.

NO.	NUMBER OF CUTSETS	MINIMAL CUTSETS
1	5	[A_I, B_I, C_I], [A_I, C_{BC}], [B_I, C_{AC}], [C_I, C_{AB}], [C_{ABC}]
2	7	[A_I, B_I], [A_I, C_I], [B_I, C_I], [C_{AB}], [C_{AC}], [C_{BC}], [C_{ABC}]
3	7	[A_I], [B_I], [C_I], [C_{AB}], [C_{AC}], [C_{BC}], [C_{ABC}]

E.4 More Complicated Events

An event can involve failure or the unavailability of more than one component belonging to the common cause component group. To treat this case, we apply the concepts illustrated in Sections E.3.2 and E.3.3 to the event. We will illustrate this with another example.

Let us consider the case where component C is out for preventive maintenance and is not failed. A demand occurs at the plant requiring A and B to start. A starts, but B fails. The conditional probability for the case prior to the demand is given by Equation E.12. The cutsets are given in Table E-3 along with the quantification. The final result, assuming staggered testing is given by

$$Q_1\alpha_1 + Q_1\alpha_2 + Q_2\alpha_1 + \alpha_2 + \alpha_3$$

Table E-3. Quantification for example involving two components.

CUTSET	PROBABILITY	CONDITIONAL PROBABILITY
$[A_I, B_I]$	Q_1^2	$Q_1\alpha_1$
$[A_I, C_{BC}]$	Q_1Q_2	$Q_1\alpha_2$
$[B_I, C_{AB}]$	Q_1Q_2	$Q_2\alpha_1$
$[C_{AB}]$	Q_2	α_2
$[C_{ABC}]$	Q_3	α_3

E.5 CONCLUSIONS

Common cause failure probabilities can be treated properly in event assessments by systematically following the steps illustrated in this appendix. We have illustrated the treatment of failed components and components unavailable due to preventive maintenance. The treatment of these two cases differs. It is generally easier to perform the quantification working with the cutsets associated with the common cause failure group.

E.6 REFERENCES

E-1. U.S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failure in Safety and Reliability Studies: Procedural Framework and Examples*, Volume 1, NUREG/CR-4780, EPRI NP-5613, January 1988.

E-2. U.S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failure in Safety and Reliability Studies: Analytical Background and Techniques*, Volume 2, NUREG/CR-4780, EPRI NP-5613, January 1989.

E-3. U.S. Nuclear Regulatory Commission, *Procedure for Analysis of Common Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801, SAND91-7087, April 1993.

E-4. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 1--Overview*, NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

E-5. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System, Volume 2-- Event Definition and Classification*, NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

E-6. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 3-- Data Collection and Event Coding*, NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

E-7. U. S. Nuclear Regulatory Commission, *Common Cause Failure Data Collection and Analysis System Volume 4--CCF Software Reference Manual*, NUREG/CR-6268, June 1998, INEEL/EXT-97-00696.

E-8. U.S. Nuclear Regulatory Commission, *Common Cause Failure Parameter Estimations*, NUREG/CR-5497, June 1998, INEEL/EXT-97-01328.

NRC FORM 335
(2-89)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See Instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-5485
INEEL/EXT-97-01327

2. TITLE AND SUBTITLE
Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment

3. DATE REPORT PUBLISHED

MONTH	YEAR
November	1998

4. FIN OR GRANT NUMBER
E8247

5. AUTHOR(S)
A. Mosleh, University of Maryland, D. M. Rasmuson, USNRC, F. M. Marshall

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZAITON - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Idaho National Engineering and Environmental Laboratory
Lockheed Martin Idaho Technologies Co.
P.O. Box 1625
Idaho Falls, ID 83415-3129

Subcontractor:
Department of Materials and
Nuclear Engineering
University of Maryland
College Park, MD 20742-2115

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above"; If contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Safety Programs Division
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This report provides a set of guidelines to help probabilistic risk assessment (PRA) analysts in modeling common cause failure (CCF) events in commercial nuclear power plants. The aim is to enable the analyst to identify important common cause vulnerabilities, incorporate their impact into system reliability models, perform data analysis, and quantify system unavailability in the presence of CCFs. Much of the material in this report has been presented in previous reports issued by United States Nuclear Regulatory Commission (NRC). The present document brings together the key aspects of these procedural guidelines supplemented by additional insights gained from their application, and enhanced by the capabilities of the CCF software and its data analysis capabilities, recently developed by the NRC.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Common cause failure

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This page)
Unclassified
(This report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300